OEA
Más derechos para más gente

TALLER

CIBERSEGURIDAD Y ELECCIONES:

NUEVOS DESAFÍOS Y BUENAS PRÁCTICAS PARA LA DEMOCRACIA

3 y 4 de abril de 2024

In partnership with Canada

Tabla de contenido

MIÉRCOLES

3 de abril de 2024

Hora	Actividad	Ponentes
09:00 – 09:15	**Bienvenida**	**Palabras de bienvenida al taller:** Francisco Guerrero, Secretario para el Fortalecimiento de la Democracia (SFD) de la OEA. Alison August-Treppel, Secretaria Ejecutiva del Comité Interamericano contra el Terrorismo (CICTE) de la OEA.
09:15 – 10:45	**Ciberseguridad: tendencias y desafíos globales**	Los cada vez más sofisticados ataques cibernéticos se presentan a través de amenazas como el malware, mobile attacks, phishing, ransomware y, en algunos casos, también ataques orquestados y patrocinados por otros estados. Estos ataques han puesto en constante riesgo los datos y activos de instituciones gubernamentales e individuos. En esta sesión se abordarán las tendencias y desafíos globales en torno a la delincuencia cibernética, actores y motivaciones, así como el impacto de la inteligencia artificial en la materia, para conocer mejor el contexto en el que se desarrollan actualmente los procesos electorales. Diego Subero, Oficial de Programa de Seguridad Cibernética de CICTE/OEA Marnix Dekker, Jefe de Sector de Redes y Sistemas de Información, Agencia de la Unión Europea para la Ciberseguridad (ENISA). Katherina Canales Madrid, Ex Directora Operacional del CSIRT del gobierno de Chile.
10:45 – 11:00	Receso	
11:00 – 12:30	**Ciberseguridad en elecciones: amenazas e impacto**	Los ataques cibernéticos pueden interrumpir la prestación de servicios esenciales de un proceso electoral, socavar la integridad de las elecciones y erosionar la confianza pública en el órgano electoral. El uso cada vez más prominente de la tecnología en las elecciones, la expansión de dispositivos conectados a Internet, la utilización de plataformas o aplicaciones móviles, el trabajo remoto y otros cambios sociales, aumentan los riesgos de ser objeto de un ataque. En esta sesión se abordarán las principales amenazas a la infraestructura crítica de un proceso electoral y su posible impacto. Cait Conley, Asesora Senior de la Directora, Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), Departamento de Seguridad Nacional (DHS), Gobierno de Estados Unidos. Tarun Chaudhary, Asesor de Ciberseguridad y Diplomacia de la Fundación Internacional para Sistemas Electorales (IFES). Kat Duffy, Senior Fellow para Política Digital y del Ciberespacio en el Council of Foreign Relations (CFR).
12:30 – 12:40	Cierre primer día	

JUEVES
4 de abril de 2024

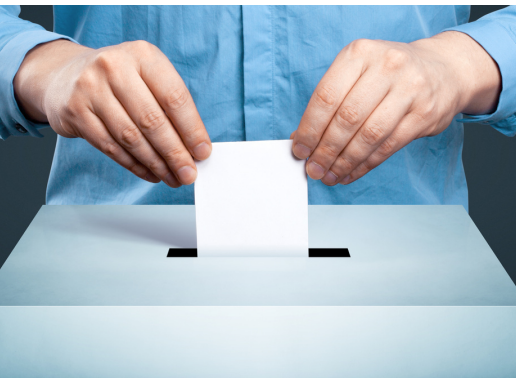
Hora	Actividad	Ponentes
09:00 – 10:00	Sala de Discusión: **Ciberseguridad en los procesos electorales**	El Departamento para la Cooperación y Observación Electoral (DECO) de la OEA brindará una presentación sobre las políticas, principios y prácticas en materia de ciberseguridad electoral que ha observado en la región durante los últimos años. Posteriormente, el grupo de asistentes se dividirá en tres grupos. Durante 45 minutos, y con el apoyo de facilitadores y un panel colaborativo online, cada grupo intercambiará puntos de vista sobre cuáles han sido los principales desafíos y lecciones en materia de ciberseguridad en los procesos electorales que se han llevado a cabo en sus respectivos países. Alex Bravo, Especialista de la Sección de Cooperación Técnica, DECO/OEA.
10:00 – 10:30	**Intercambio de puntos de vista en el plenario**	Los/as participantes en el taller volverán al plenario para compartir lo analizado en las salas de discusión.
10:30 – 10:45	Receso	
10:45– 12:00	**Fortaleciendo las capacidades de los organismos electorales para detectar y responder efectivamente a un ataque cibernético: desafíos, oportunidades y lecciones aprendidas**	La capacitación de funcionarios y electores, la gestión de riesgos de forma continua e integral, la colaboración interinstitucional y el intercambio de experiencias para mejorar el proceso de toma de decisiones, son acciones proactivas que contribuyen a prevenir o mitigar ataques cibernéticos. En esta sesión se abordarán diversas herramientas o acciones para fortalecer las capacidades de los órganos electorales en esta materia. Peter Wolf, Asesor Principal en Elecciones y Digitalización en IDEA Internacional. David Marcos, Honorary Fellow, Departamento de Ingeniería Mecánica, Aeroespacial e Informática, España. Héctor Hernández, Consultor en Tecnología Electoral, Auditoría y Seguridad Informática.

JUEVES
4 de abril de 2024 de 2024

Hora	Actividad	Ponentes
12:00– 13:00	Estudio de casos: **Buenas prácticas para la promoción de la seguridad en el espacio cibernético: lecciones de las Américas**	En este espacio, los/as participantes podrán profundizar los conocimientos sobre el fortalecimiento de capacidades de los organismos electorales frente a amenazas de ciberseguridad, a través de iniciativas que se han realizado en el pasado y que están actualmente en curso en diferentes países de la región. Las experiencias compartidas abordarán acciones efectuadas en distintos momentos del proceso electoral, con foco en diferentes vulnerabilidades digitales. A continuación, los participantes tendrán la oportunidad de presentar en el plenario sus puntos de vista y dudas sobre los paneles de discusión. Joshua Kilbert, Centro Canadiense de Seguridad Informática.
13:00 – 13:10	**Palabras de clausura del taller**	El Director del Departamento de Cooperación y Observación Electoral de la OEA, Gerardo de Icaza, dará unas palabras de cierre para concluir esta iniciativa. Gerardo de Icaza, Director del Departamento de Cooperación y Observación Electoral (DECO) de la OEA.

Nota conceptual

Ciberseguridad y elecciones: nuevos desafíos y buenas prácticas para la democracia



El Departamento para la Cooperación y Observación Electoral (DECO) de la Organización de los Estados Americanos (OEA) organiza este taller sobre ciberseguridad en elecciones para propiciar un diálogo participativo entre diferentes actores de la región, con el objetivo de conocer las tendencias en materia de ciberdelincuencia a nivel global, intercambiar puntos de vista respecto del impacto de esta materia en las elecciones, profundizar en torno a cómo contrarrestar estas amenazas y fortalecer las capacidades de los organismos electorales, así como abordar oportunidades estratégicas para promover la integridad y la seguridad digital en la democracia.

Durante tres sesiones plenarias de presentaciones de expertos/as, una sala de discusión entre participantes y un panel de estudios de caso, los/as asistentes podrán compartir conocimientos y experiencias, y generar redes de cooperación para futuras iniciativas. Todas las sesiones del taller son convocadas bajo la Regla de Chatham House[1]. Este taller se realiza gracias al apoyo financiero del Gobierno de Canadá.

Con el incremento en el uso de las tecnologías de información y comunicación, gran parte de los procesos asociados a una elección están basados en servicios informáticos. El registro de votantes y candidatos, las herramientas para el control del financiamiento, el procesamiento y transmisión de resultados, así como la propia mecánica del ejercicio del voto, son algunos de los ejemplos en que la tecnología juega o puede jugar un rol esencial. Pero, así como las tecnologías de la información pueden facilitar y fortalecer las diversas etapas del ciclo electoral, su alcance y prevalencia también elevan los riesgos de sufrir ataques cibernéticos.

[1] Esto implica que los/as participantes tienen el derecho de utilizar la información que reciben, pero no se puede revelar ni la identidad ni la afiliación de los oradores ni participantes.

A continuación, se desarrollan en esta nota conceptual algunos de los temas que serán abordados durante las sesiones programáticas. Su objetivo no es resumir las sesiones del evento, sino más bien proveer información introductoria que podría ser de utilidad para que los/as participantes reflexionen con anterioridad al taller sobre comentarios y/o preguntas que podrían realizar a expositores o demás participantes.

SESIÓN 1 *Ciberseguridad: tendencias y desafíos globales*

El contexto actual de constantes evoluciones tecnológicas ha convertido a la ciberseguridad en un componente imprescindible de la era digital. La mayor fluidez de la información y de la conectividad en el ciberespacio ha creado nuevas oportunidades de negocio y beneficios para la sociedad, pero también ha ampliado las posibilidades para el crimen y la manipulación de datos, que dejan de estar limitados a un determinado espacio geográfico o sometidos a una única jurisdicción. Esto, por lo tanto, presenta nuevas demandas para la prevención de amenazas, la adopción de estrategias de respuesta y la promoción de la confianza en los medios digitales.

Se puede definir la ciberseguridad como “la preservación – a través de políticas, tecnología y educación – de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, para mejorar la seguridad de las personas tanto en línea como fuera de línea”[2]. Otras definiciones añaden que esta preservación de la información permite protegerla contra la interrupción, inutilización, destrucción o control malicioso[3].

Informes publicados por empresas de tecnología indican que solamente entre 2021 y 2022 hubo un aumento de 38% en los ataques cibernéticos a nivel mundial[4], lo que tiende a incrementarse con la diaria actualización y sofisticación de estas amenazas y la ampliación del uso de tecnologías como la inteligencia artificial. La ciberseguridad resulta particularmente relevante para los países de América Latina y el Caribe, ya que son blanco constante de los ciberdelincuentes, con uno de los mayores porcentajes de aumento del cibercrimen y con registros que suman 1600 ataques por segundo a empresas de la región[5].

[2] Why Do We Need a New Definition for Cybersecurity? - Freedom Online Coalition

[3] Understanding Cybersecurity Throughout The Electoral Process: A Reference Document An Overview of Cyber Threats and Vulnerabilities in Elections | IFES - The International Foundation for Electoral Systems

[4] Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks

[5] NEW AQ: Hacker's Paradise: Why Latin America Is So Vulnerable (americasquarterly.org)

Por estas razones se hace cada vez más imperativa la divulgación de estrategias que permitan actuar de manera continua para mitigar los riesgos cibernéticos, capacitando a los países de la región para su aplicación en todos los sectores de la sociedad.

El primer paso para la prevención y combate a las amenazas es conocer de qué se tratan y cómo se presentan. Por ello, este panel tiene por objetivo explorar las principales tendencias en materia de ciberdelincuencia y ciberseguridad, que permita ahondar en los desafíos actuales y futuros. Asimismo, será una oportunidad para conocer sobre el impacto que puede tener la inteligencia artificial en la materia.

Algunos de los riegos más comunes para los sistemas informáticos son:

- **Malware:** Programa que se inserta en un sistema, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima, o de causar disrupciones de cualquier otro tipo a la víctima[6]. Ejemplos de malware son: Virus, Gusanos, Troyanos, Ransomware, Keyloggers.

- **Ransomware:** Tipo de malware que en general secuestra y cifra los archivos en un sistema de almacenamiento, para luego pedir un rescate, habitualmente a través de pagos mediante criptomonedas, sin la garantía de que todos los archivos puedan ser descifrados o sean devueltos con las mismas condiciones[7].

- **Phishing:** Phishing es una ciber amenaza que usa técnicas de ingeniería social para engañar a los usuarios a fin de que revelen información de identificación personal. Por ejemplo, los atacantes cibernéticos envían correos electrónicos que inducen a los usuarios a hacer clic e introducir los datos de la tarjeta de crédito en una página web de pagos ficticia. Los ataques de phishing también pueden incitar a la descarga de datos adjuntos malintencionados que instalen malware en los dispositivos[8].

- **DDoS:** Un ataque de denegación de servicio distribuido (DDoS) es un trabajo coordinado para sobrecargar un servidor enviando un gran volumen de solicitudes falsas. Estos eventos impiden que los usuarios normales se conecten o accedan al servidor de destino[9]. Un ejemplo de este tipo de amenazas son ataques cibernéticos dirigidos a los servicios de redes en la nube que intentan interrumpir, deshabilitar o destruir la integridad de la información disponible en un sitio web.

[6] Retos y Estrategias - Las consideraciones de los ataques de ransomware en las Americas_SPAN.pdf (oas.org) Según definición de: https://csrc.nist.gov/glossary/term/malware

[7] Retos y Estrategias - Las consideraciones de los ataques de ransomware en las Americas_SPAN.pdf (oas.org)

[8] ¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS (amazon.com)

[9] Ibid.

SESIÓN 2 *Ciberseguridad en elecciones: amenazas e impacto*

La proliferación de servicios informáticos en las diversas etapas de un proceso electoral, la expansión de dispositivos conectados a Internet, el uso de plataformas o aplicaciones móviles para gestionar diversos procesos e información, el trabajo remoto y otros cambios sociales recientes, han aumentado los riesgos de que una elección pueda ser objeto de un ataque. Las amenazas a las elecciones no son ficticias o potenciales, sino que ya son una realidad en América Latina[10].

Algunas de las formas en que se pueden manifestar ataques cibernéticos en los procesos electorales incluyen:

- Robo o manipulación de información disponible online, incluyendo datos de electores.
- Ataques a los sitios web del órgano electoral, que dificultan el acceso público a información crucial.
- Ataques a la infraestructura crítica como energía eléctrica, infraestructura de telecomunicaciones y sistemas informáticos que pueden interrumpir la prestación de servicios esenciales.
- Intrusiones en los sistemas de transmisión, cómputo, tabulación y publicación de los resultados electorales.
- Suplantación y envenenamiento de DNS, donde un cibercriminal podría redirigir a los votantes a un sitio web falso que se parece al sitio web oficial de las elecciones, para ocasionar robo de identidad del votante o interrupción del proceso de votación a través de la inundación de los servidores DNS con tráfico.
- Uso de herramientas cibernéticas para espionaje con fines políticos.
- Explotación de errores en la gestión de activos informáticos y fallas de seguridad (vulnerabilidades del día cero).
- Explotación de vulnerabilidades asociadas a dispositivos móviles de acceso remoto que acceden a información sensible o privada y que están fuera del control de la entidad electoral.

Cuando los ataques cibernéticos son exitosos pueden socavar la confianza pública en la integridad del proceso y del órgano electoral. La percepción de que las elecciones no son seguras o justas puede impactar significativamente en la estabilidad política y social, y minar la confianza en el sistema democrático.

[10] Ejemplos recientes en la región incluyen el caso de las elecciones de 2018 en Colombia, donde la Registraduría registró ataques cibernéticos días antes de la elección (Detectan ataques cibernéticos a ente electoral de Colombia – DW – 08/03/2018); y de Ecuador 2023, donde la autoridad electoral confirmó que el voto telemático sufrió ataques provenientes de siete países durante la jornada electoral (Voto telemático en el exterior sufrió ataques cibernéticos, confirmó la presidenta del CNE | Política | Noticias | El Universo).

SALA DE DISCUSIÓN *Ciberseguridad en los procesos electorales*

Durante esta sesión se abordarán algunas de las vulnerabilidades de ciberseguridad más relevantes identificadas por la OEA en materia electoral. Ello incluye deficiencias en la gestión de seguridad de la información; vulnerabilidades del día cero; errores en configuración y programación; vulnerabilidades asociadas a dispositivos móviles, acceso remoto, aplicaciones móviles (información sensible o privada); y ataques cibernéticos dirigidos a sistemas informáticos que operan en la nube.

Luego de la presentación, los/as asistentes se dividirán en tres grupos y durante 45 minutos intercambiarán puntos de vista sobre cuáles han sido los desafíos y lecciones en materia de ciberseguridad en los procesos electorales que han monitoreado en sus respectivos países. Por favor notar que esta sesión de discusión es convocada bajo la Regla de Chatham House, lo que implica que los/as participantes tienen el derecho de utilizar la información que reciben, pero no se puede revelar ni la identidad ni la afiliación de los oradores ni participantes.

Las sesiones están estructuradas en base a unas preguntas guías que estimularán el intercambio de ideas. Los facilitadores formularán preguntas al grupo, y los/as participantes tendrán unos minutos para postear sus comentarios en una aplicación de fácil uso llamada padlet. Se trata de una aplicación colaborativa en la cual, con el único requisito de un link de acceso, los/las participantes podrán postear, en tiempo real, ideas y comentarios, e incluso, adjuntar documentos pertinentes, links a noticias o iniciativas, etc. De igual manera, los/las participantes podrán realizar intervenciones verbales para compartir experiencias desde sus realidades.

Algunas de las preguntas que guiarán la discusión en esta sesión son:

- ¿Cómo la institución a la que pertenece ha trabajado en materia de ciberseguridad? ¿Hay algún cuidado específico direccionado a los periodos electorales?
- ¿Han observado amenazas cibernéticas recientes en sus países que hayan impactado a los servicios gubernamentales? En caso afirmativo, ¿alguna de ellas direccionada al organismo electoral?
- ¿Cuáles considera usted que son las dificultades más grandes que enfrentan los procesos electorales en materia de ciberseguridad?

SESIÓN 3 *Fortaleciendo las capacidades de los organismos electorales para detectar y responder efectivamente a un ataque cibernético: desafíos, oportunidades y lecciones aprendidas*

Fortalecer la ciberseguridad en las elecciones requiere una actitud proactiva, que permita mitigar los efectos de las amenazas cibernéticas, adoptar medidas robustas para la prevención y prepararse para la contingencia y la respuesta estratégica a incidentes. Si bien la complejidad tecnológica y la rápida evolución de las amenazas son desafíos continuos, existen oportunidades de mejora y buenas prácticas que pueden ser adoptadas para solventar estos retos.

Una de las dificultades que enfrentan muchos organismos electorales se refiere a la ausencia de capacidad o recursos, tanto financieros como de personal, para habilitar o mantener programas de ciberseguridad. Las asociaciones estratégicas con otras instituciones gubernamentales, organizaciones de la sociedad civil o la cooperación técnica con organismos internacionales, se presentan como alternativas para garantizar la implementación de medidas de seguridad digital. La responsabilidad compartida puede incluso ser promovida por los formuladores de políticas cuando no exista de manera espontánea[11].

La adopción de tecnologías seguras, así como su revisión y actualización frente a posibles vulnerabilidades, es un importante paso para la protección de los procesos electorales. La misma debe venir acompañada de la capacitación de los funcionarios electorales para que conozcan las amenazas existentes y las maneras de prevenirlas. La educación digital contribuye a la prevención de errores humanos que pueden incluir: el diseño, configuración y programación de sistemas, la mala elaboración de pruebas y control de calidad, incorrecta gestión de usuarios y sistemas, el mal uso y la exposición de los sistemas a malwares.

De hecho, la capacitación y la divulgación de información a través de talleres y campañas de concientización pública son fundamentales también para la ciudadanía, periodistas, candidatos y demás actores políticos, como forma de fomentar la ciberhigiene y fortalecer la seguridad en todo el proceso electoral.

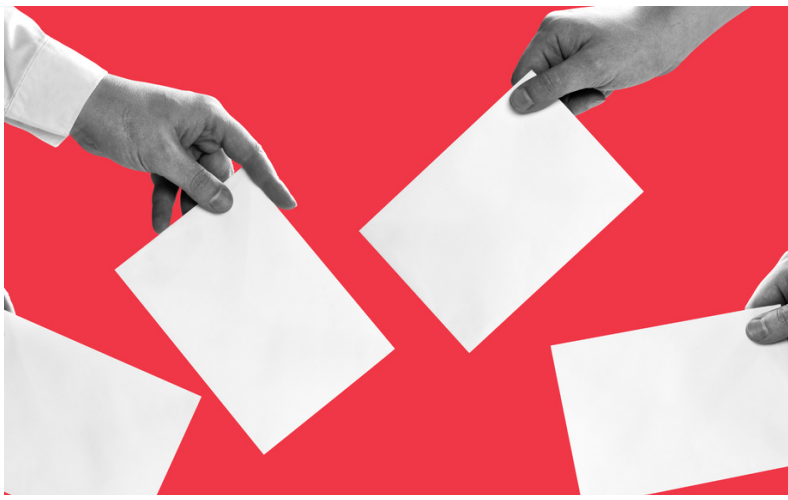
La gestión de la ciberseguridad debe darse de manera continua, y no solo durante las elecciones, buscando realizar una constante evaluación y retroalimentación de las medidas adoptadas para su mejora y consolidación. De la misma forma, adoptar una postura transparente y gestionar las percepciones públicas sobre las amenazas cibernéticas a un proceso electoral es fundamental para promover la confianza en el proceso, siendo casi tan importante como defenderse de las propias amenazas[12].

[11] Cybersecurity in Elections (idea.int)

[12] Ibid.

En resumen, dado que la ciberseguridad electoral es esencial para preservar la integridad de los procesos democráticos y la estabilidad en un entorno cada vez más digital, fortalecer las capacidades de los organismos electorales implica la combinación de concientización, colaboración, adopción de mejores prácticas y aprendizaje continuo.

Este panel tiene por objetivo abordar las principales definiciones, decisiones y herramientas que un organismo electoral requiere adoptar para una estrategia efectiva de ciberseguridad, tomando en cuenta las limitaciones, oportunidades y experiencias en la materia.



ESTUDIO DE CASOS *Buenas prácticas para la promoción de la seguridad en el espacio cibernético: lecciones de las Américas*

En este espacio, los/as participantes podrán profundizar y conocer más sobre el fortalecimiento de las capacidades de los organismos electorales frente a amenazas de ciberseguridad, a través de iniciativas que se han realizado en el pasado y que están actualmente en curso en diferentes países de la región. Las experiencias compartidas abordarán acciones efectuadas en distintos momentos del proceso electoral, con enfoque en diferentes vulnerabilidades digitales. A continuación, los/las participantes tendrán la oportunidad de presentar en el plenario sus puntos de vista y dudas sobre los paneles de discusión del día. Los casos de estudio son:

- **Canadian Centre for Cyber Security**
- **TBC**

Panelistas

FRANCISCO GUERRERO

Secretario para el Fortalecimiento de la Democracia de la OEA

Doctor en Relaciones Internacionales y Maestro en Análisis de Conflictos Internacionales, ambos por la Universidad de Kent en Canterbury, Inglaterra. Es licenciado en Derecho titulado con mención honorífica por la Universidad Nacional Autónoma de México (UNAM). Es experto en asuntos electorales, políticas públicas, asuntos internacionales, democracia y transición política, gobierno y transparencia. Fue Consejero Electoral del Instituto Federal Electoral de México de 2008 a 2013.

En el ámbito académico, fue fundador y coordinador del Doctorado en Gestión Estratégica y Políticas del Desarrollo y de la Maestría en Economía y Gobierno, así como titular de la Cátedra sobre Reformas Estructurales de la Facultad de Economía y Negocios de la Universidad Anáhuac México Norte. Ha sido coordinador académico de diversos cursos, seminarios y diplomados; investigador visitante en diferentes países; y ha impartido clases a nivel doctorado, maestría y licenciatura. En enero de 2008, fue elegido como uno de los cinco beneficiarios mexicanos de la reconocida Beca Eisenhower. Ha sido articulista en varios diarios de circulación nacional en México, revistas y publicaciones especializadas. Es colaborador semanal en el periódico Excélsior con la columna Punto de equilibrio.

ALISON AUGUST TREPPEL

Secretaria Ejecutiva del Comité Interamericano contra el Terrorismo de la OEA

Se ha desempeñado como Secretaria Ejecutiva del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos desde agosto del 2016, donde es responsable de promover la agenda antiterrorista de la OEA en América Latina y el Caribe y de dirigir la asistencia técnica de la OEA en esferas como la ciberseguridad, la gestión fronteriza, la prevención de la financiación del terrorismo y la proliferación de armas de destrucción masiva, entre otros.

Originalmente de los Estados Unidos, la Sra. Treppel tiene casi 30 años de experiencia trabajando en el sistema interamericano, los últimos 15 de los cuales se han centrado en cuestiones de seguridad multidimensionales. Como Jefa de Sección y posteriormente Directora Adjunta del Departamento de Seguridad Pública de la OEA desde 2006 al 2016, apoyó los esfuerzos para prevenir y contrarrestar las amenazas a la seguridad ciudadana, incluyendo el tráfico de armas de fuego, la trata de personas y otras manifestaciones de crimen organizado transnacional. También ha servido de enlace político a numerosos organismos relacionados con la seguridad de la OEA, entre ellos la Comisión de Seguridad Hemisférica.

La Sra. Treppel tiene una licenciatura en Relaciones Internacionales y Español de Dickinson College y completó un programa de educación ejecutiva en seguridad nacional e internacional de la Escuela de Gobierno Kennedy de la Universidad de Harvard.

Panelistas

KATHERINA CANALES MADRID

Ex Directora Operacional del CSIRT del Gobierno de Chile

Katherina es especialista en ciberseguridad y cuenta con una vasta experiencia en la creación, vinculación e implementación de políticas públicas de ciberseguridad. Reconocida como mujer destacada en ciberseguridad en Chile, y Top Women in Cybersecurity en Latinoamérica. Fue directora operacional del CSIRT del Gobierno de Chile, líder en la implementación de programas de concientización sobre seguridad cibernética, experta en estrategias de ciberseguridad, con especial énfasis en la creación, implementación y maduración de los equipos de respuesta ante incidentes de seguridad informática. Entre sus logros profesionales se encuentran: la creación y legitimación del CSIRT del Gobierno de Chile, coautoría de la ley de delitos informáticos, el proyecto de ley marco de ciberseguridad y la normativa sectorial vinculada al efecto. Es una reconocida columnista y relatora nacional e internacional especializada en la ciberseguridad.

MARNIX DEKKER

Jefe de Sector de Redes y Sistemas de Información de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Marnix trabaja en ENISA, la Agencia de la Unión Europea para la Ciberseguridad, donde es Jefe del Sector de Redes y Sistemas de Información, en el que dirige un equipo de expertos apoyando a las autoridades nacionales de ciberseguridad en la implementación de la Directiva SRI. Se enfocan en aumentar la ciberseguridad y la resiliencia en los sectores críticos de la UE, que abarcan las telecomunicaciones, las infraestructuras de internet, la confianza, la energía, la salud, el transporte, etc. Junto con las autoridades nacionales, trabajan en cuestiones técnicas (por ejemplo, la caja de herramientas 5G de la UE, la seguridad de la cadena de suministro), y también en la aplicación de políticas (por ejemplo, el NIS2, la UE wallet toolbox). Marnix tiene un Doctorado en Seguridad Informática y un Máster en Física Teórica (Física Cuántica). Dejó ENISA durante unos años para trabajar en la oficina del CISO de la Comisión Europea, donde ayudó a crear la función corporativa de seguridad informática, desarrolló la estrategia corporativa de seguridad informática y actuó como enlace entre los equipos operativos de seguridad y la alta dirección de la Comisión. Antes de incorporarse a ENISA, trabajó como auditor informático en KPMG en La Haya, como arquitecto y diseñador de protocolos para los sistemas de identificación electrónica del gobierno holandés y como desarrollador de software en Italia.

Panelistas

DIEGO SUBERO

Oficial de Programa de Seguridad Cibernética del CICTE de la OEA

Ingeniero de sistemas que por más de 16 años se ha desempeñado en el campo de la seguridad de la información, especialmente en temas de gestión de incidentes cibernéticos en la región. Desde hace 10 años es oficial de Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la OEA.

Su objetivo primordial es liderar proyectos orientados al desarrollo de capacidades técnicas en equipos de respuestas a incidentes de seguridad informática (CSIRTs) en Latinoamérica y el Caribe. A su vez, impulsó la creación de la red de CSIRTs gubernamentales de las Américas para fomentar la cooperación regional y facilitar canales operativos para el intercambio de amenazas e incidentes cibernéticos entre los Estados Miembros de la OEA.

CAIT CONLEY

Asesora Senior de la Directora, Agencia de Seguridad de la Infraestructura y Ciberseguridad (CISA) de los Estados Unidos.

Cait Conley es la Asesora Principal de la Directora, un cargo que incluye responsabilidades de apoyo a los esfuerzos de seguridad electoral de CISA. Conley dirige el trabajo de CISA de colaborar con funcionarios electorales estatales y locales para gestionar y reducir el riesgo para la infraestructura electoral de la nación.

Conley aporta a este cargo una gran experiencia y conocimientos en seguridad electoral, ya que anteriormente fue directora ejecutiva del proyecto bipartidista Defending Digital Democracy Project, del Centro Belfer de la Universidad de Harvard. Como directora ejecutiva, dirigió el desarrollo y la implementación de estrategias, herramientas y recomendaciones para que los administradores electorales, los proveedores de infraestructuras electorales, las organizaciones de campaña y los líderes involucrados en los procesos democráticos pudieran defender mejor contra las amenazas cibernéticas.

Conley es una experimentada veterana de combate con un liderazgo demostrado en operaciones globales especiales, operaciones cibernéticas y antiterrorismo. Recientemente, Conley ocupó el cargo de Directora de Antiterrorismo del Consejo de Seguridad Nacional, antes de incorporarse a CISA como Asesora Senior de la Directora.

Coley se graduó de la Academia Militar de los Estados Unidos en West Point y posee un máster en Administración de Empresas por el Instituto Tecnológico de Massachusetts y un máster en Políticas Públicas por la Escuela de Gobierno Kennedy de la Universidad de Harvard.

Panelistas

TARUN CHAUDHARY

Asesor de Ciberseguridad y Diplomacia de la Fundación Internacional para Sistemas Electorales (IFES)

En su función, el Dr. Chaudhary proporciona asesoramiento técnico y programático experto en ciberseguridad a toda la cartera de actividades de IFES y a sus socios en todo el mundo. El Dr. Chaudhary también se concentra en hacer crecer y madurar el liderazgo de pensamiento y la investigación de IFES en el ámbito de la ciberseguridad electoral como parte del Centro de Integridad Cibernética y de la información de IFES.

Antes de llegar al IFES, el Dr. Chaudhary trabajó en el Departamento de Energía de Estados Unidos. También cuenta con 15 años de amplia experiencia en consultoría de la industria de defensa, habiendo prestado servicios de consultoría especializada a una amplia variedad de clientes, incluida la Oficina de Evaluación de Redes del Pentágono, grandes contratistas de defensa y muchos otros clientes nacionales y extranjeros.

El Dr. Chaudhary es Doctor en Asuntos Internacionales, Ciencia y Tecnología por el Instituto de Tecnología de Georgia, en Atlanta, donde también obtuvo un máster y una licenciatura. Su investigación se centra en cómo los profesionales de la ciberseguridad se organizan y colaboran para reconocer y remediar problemas a gran escala fundamentales para que el Internet siga funcionando. El Dr. Chaudhary ha recibido varias becas y premios, entre ellos la beca por servicio de la Fundación Nacional de Ciencia Ciber Corps, la NNSA beca de postgrado y otros. Ha publicado trabajos en el Periódico de Oxford de Ciberseguridad y es coautor de numerosos informes para el Departamento de Defensa de Estados Unidos. También posee la certificación Global de Seguridad de la Información (GIAC) como Profesional Global de la Seguridad de la Información (GISP).

ALEX BRAVO

Especialista del Departamento para la Cooperación Electoral de la OEA

Especialista del DECO desde agosto de 2009. Es responsable de la gestión de proyectos en las áreas de cooperación técnica, observación de tecnología electoral, auditoría integral de registro electoral y generación del software para la gestión de cooperación técnica electoral. Ingeniero en el área de Informática, Alex cursó sus estudios de grado en la Universidad de Maryland. Tiene una Maestría en Seguridad Informática de la Universidad de George Washington.

Panelistas

KAT DUFFY

Senior Fellow para Política Digital y del Ciberespacio en el Council of Foreing Relation (CFR)

Duffy cuenta con más de dos décadas de experiencia trabajando en la intersección de tecnologías emergentes, principios democráticos, responsabilidad corporativa y derechos humanos. En 2023, dirigió el Task Force for a Trustworthy Future Web en el Laboratorio de Investigación Forense Digital del Atlantic Council, donde trabajó como becaria principal y publicó el exhaustivo informe del Task Force, Scaling Trust on the Web. A través de su trabajo anterior en el Departamento de Estado de los Estados Unidos y en la sociedad civil, Duffy ha supervisado la implementación de más de 100 millones de dólares en asistencia externa y ayuda filantrópica en más de 60 países, con un enfoque particular en el apoyo a los defensores de derechos humanos y periodistas, y en iniciativas de la sociedad civil para mejorar la seguridad digital, los derechos digitales y la gobernanza de plataformas. Su trabajo incluyó algunas de las primeras asociaciones público-privadas entre actores de alto riesgo de la sociedad civil en mercados emergentes y empresas privadas de ciberseguridad.

Duffy comenzó su carrera internacional en Colombia, donde trabajó como funcionaria profesional junior del Alto Comisionado de las Naciones Unidas para los Refugiados. Durante cinco años formó parte de la junta de Global Network Initiative, una plataforma que ayuda a las empresas tecnológicas a respetar la libertad de expresión y los derechos a la privacidad cuando se enfrentan a presiones gubernamentales para que entreguen datos de usuarios, retiren contenidos o restrinjan las comunicaciones. También ha sido asesora experta de la iniciativa del Foro Económico Mundial Colaborando con la Sociedad Civil en la Cuarta Revolución Industrial y ha dado conferencias en las universidades de Yale, Stanford y Georgetown sobre política tecnológica e innovación.

Duffy es licenciada por la Universidad de Yale y doctora en Derecho por la Universidad de Michigan. Además de Estados Unidos, ha vivido y trabajado en Colombia, Cuba, Sudáfrica y Túnez, y es una orgullosa "trailing spouse" dentro del servicio exterior estadounidense.

PETER WOLF

Asesor Principal en Elecciones y Digitalización en IDEA Internacional

Peter Wolf es el Asesor Principal en Elecciones y Digitalización y trabaja en el Programa global de Procesos Electorales en la oficina central de IDEA Internacional en Estocolmo, Suecia. Su trabajo se centra en la aplicación y el impacto de las tecnologías digitales en las elecciones, los nuevos retos y la implementación fiable de las TIC en los procesos electorales. Es autor de numerosas publicaciones, sobre biometría, ciberseguridad, certificación, voto electrónico, datos abiertos, tecnología de código abierto, acuerdos especiales de votación y gestión electoral.

La experiencia previa de Wolf incluye un período en el Departamento de Elecciones de la Misión de la OSCE en Bosnia y Herzegovina. Ha participado en misiones internacionales de observación electoral en todos los continentes como experto en registro de votantes y voto electrónico y ha trabajado como consultor y experto en tecnología en proyectos de asistencia electoral desde finales de los años noventa.

Panelistas

DAVID YEREGUI MARCOS

Honorary Fellow, Departamento de Ingeniería Mecánica, Aeroespacial e Informática, España

El profesor David Yeregui Marcos del Blanco es ingeniero en informática con intensificación en robótica y control industrial, así como doctor con mención cum laude en ingeniería de producción y computación por la Universidad de León. Adicionalmente, posee un MBA in International Business Management del ICEX-CECO junto con la UIMP. David es coautor de más de 25 artículos de investigación en revistas de alto impacto sobre ciberseguridad, machine learning y biotecnología. El profesor Marcos del Blanco empezó su Carrera profesional como Trading Officer para el área de industria e inversiones de la Oficina Económica y Comercial de la Embajada de España en Japón entre 2006-2008. Posteriormente, estableció el departamento de ciencia y tecnología del Instituto Cervantes de Tokio, siendo su primer director. En 2008, co-fundó la compañía biotecnológica Genhelix, dedicada a la investigación, desarrollo y fabricación de anticuerpos monoclonales y otras terapias biológicas contra el cáncer y enfermedades autoinmunes. Actualmente, la empresa es parte del grupo alemán Fresenius Kabi, emplea a más de 400 personas y está valorada en más de 1.000 millones de USD.

Desde 2018, el Dr. Yeregui Marcos es Partner de Quantum Group y DPI Group en Tokio y Singapur respectivamente, habiendo co-liderado la financiación, diseño, construcción y OPV de un REIT para un total de más de 400 MW y 1.000 millones de USD de activos solares generados en Japón, España e Italia. De 2018 a 2020, fue lead consultant para la Organización de Estados Americanos en su proyecto “Cybersecurity applied to Electoral Processes in Latin American and the Caribbean Region”. En paralelo, David es Entrepreneur in Residence en IE University, siendo profesor de la misma institución desde 2018 así como Honorary Fellow del departamento de ingeniería mecánica, aeroespacial e informática de su alma mater, la Universidad de León.

HÉCTOR TEODORO HERNÁNDEZ

Especialista en Tecnología Electoral, Auditoría y Seguridad Informática

Es perito y auditor informático, especialista en voto electrónico y tecnología electoral. Es experto universitario en hacking ético, seguridad de la información y seguridad de dispositivos móviles y master en pruebas profesionales. Posee una Diplomatura Universitaria en Implementación y Auditoría de Sistemas de Gestión de Seguridad de la Información bajo ISO/IEC 27001 de la Universidad Tecnológica Nacional en Argentina, es Diplomado en Planificación de Recursos Empresariales de la Universidad Nacional de Córdoba y es Diplomado en Forensia Informática. Tiene título nacional de Analista Programador de Sistemas Informáticos y una Maestría en Seguridad, Auditoría y Peritaje Informático ESAPI.

Además cuenta con certificaciones internacionales en seguridad y buenas prácticas informáticas como: Lead Auditor ISO 27001, PCI DSS Implanter certificate e ITIL Best Practices Certificate EXIN Holanda. También posee las certificaciones oficiales en ciberseguridad: Certified Cyber Security Management Professional, Certified Information Security Management Professional, Blockchain Professional Certified.

Moderación y clausura

GERARDO DE ICAZA

Director del Departamento para la Cooperación y Observación Electoral de la OEA

Es el Director del Departamento para la Cooperación y Observación Electoral desde el 1 de marzo de 2014. En su cargo como Director ha dirigido más de 100 Misiones de Observación Electoral en 27 países. Entre febrero y julio de 2018, se desempeñó como Secretario interino para el Fortalecimiento de la Democracia. Anteriormente, en el Instituto Nacional Electoral (INE) de México, fue Subdirector de Normatividad en la Coordinación del Voto de los Mexicanos Residentes en el Extranjero y Coordinador del Comité Técnico de Especialistas para el Voto de los Mexicanos Residentes en el Extranjero. Fue además Secretario de Estudio y Cuenta, y Jefe de la Unidad de Asuntos Internacionales en el Tribunal Electoral del Poder Judicial de la Federación de México. Es Licenciado en Derecho y cuenta con una Maestría en Relaciones Internacionales y Comunicación. Ha sido docente universitario y es un reconocido conferencista internacional. Su más reciente publicación "Derecho Internacional de la Democracia" coordinada con Luis Almagro, es una de sus numerosas publicaciones académicas sobre democracia y sistemas electorales.

CRISTÓBAL FERNÁNDEZ

Jefe de la Sección de Cooperación Técnica, DECO/OEA

Abogado de profesión, cursó sus estudios superiores en la Facultad de Derecho de la Universidad de Chile y tiene un LL.M. en Derecho Internacional por la American University. Ha participado en más de 25 Misiones de Observación Electoral, siendo Subjefe de Misión en varias MOEs en Colombia, El Salvador, Guatemala, Honduras, Nicaragua y República Dominicana. Como Jefe de la Sección de Cooperación Técnica del Departamento para la Cooperación y Observación Electoral (DECO) de la Organización de los Estados Americanos, coordina los proyectos de cooperación electoral que la OEA implementa en sus Estados Miembros. Ha liderado proyectos, brindado apoyo técnico y participado en actividades de cooperación en diversos países de América Latina y el Caribe, en temas como registro electoral, organización electoral, justicia electoral, tecnología electoral, participación política de mujeres, combate a la desinformación y reformas electorales. Es co-autor de la metodología para observar la participación electoral de Pueblos Indígenas y Afrodescendientes, así como de la "Guía para organizar elecciones en tiempos de pandemia".

TALLER

CIBERSEGURIDAD Y ELECCIONES:

NUEVOS DESAFÍOS Y BUENAS PRÁCTICAS PARA LA DEMOCRACIA

OEA Más derechos para más gente

In partnership with Canada