AMCHAM CHILE

MISIÓN PÚBLICO - PRIVADA

TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN

CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

AUSPICIADOR

UNITED AIRLINES

MISIÓN PÚBLICO - PRIVADA

TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN

CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

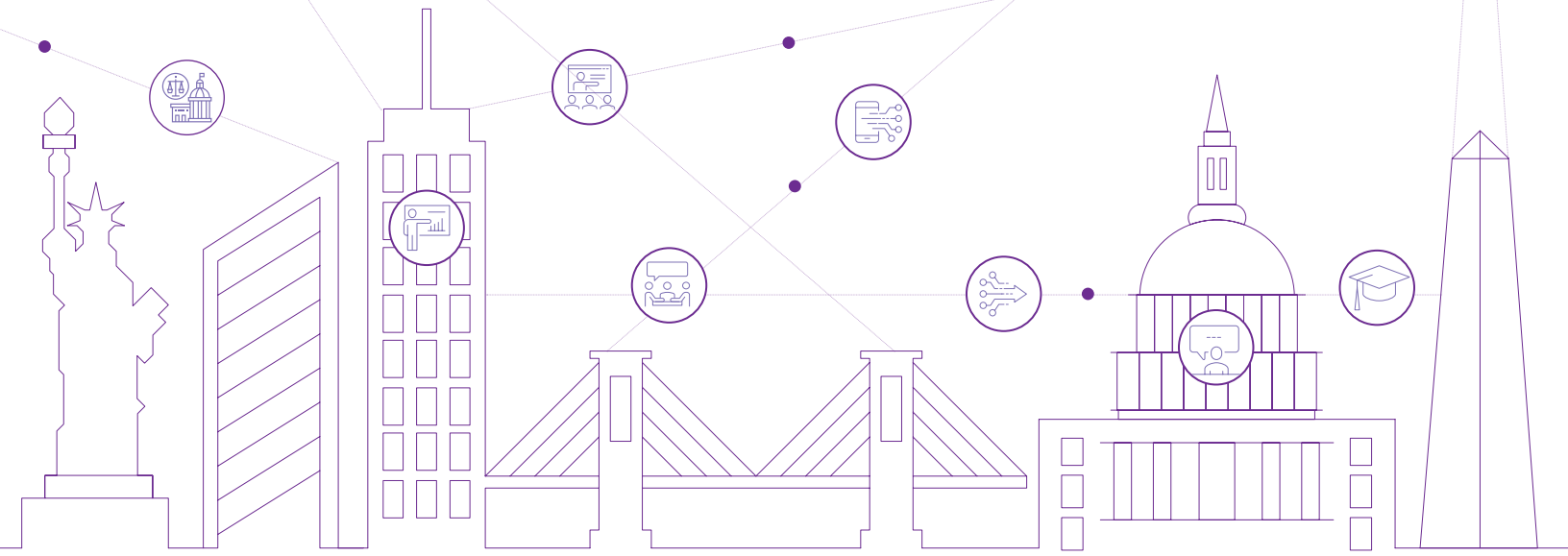
WASHINGTON D.C.
NUEVA YORK

AMCHAM CHILE

La Cámara Chilena Norteamericana de Comercio, AmCham Chile, AmCham Chile, se ha propuesto como uno de sus ejes de trabajo para 2019 la ciberseguridad. Este ámbito hoy es un factor clave para la competitividad de los países, la protección de datos y los nuevos desafíos digitales en el mundo de los negocios.

Desde 2018, AmCham forma parte de la Alianza Chilena de Ciberseguirdad, asociación que integra a reconocidos organismos estatales, privados y de la academia que tienen por objetivo la promoción del desarrollo y fortalecimiento de la ciberseguridad, además de la generación de redes de colaboración y alianzas con otras entidades en torno a esta materia. Parte central de la agenda de este consejo es la organización de la **Misión Público-Privada Tendencias del Mercado y Desafíos Regulatorios en Ciberseguridad** que se desarrollará entre el **6 al 10 de mayo de 2019** en **Washington D.C.** y **Nueva York**.

Los participantes de esta misión tendrán la oportunidad de conocer la experiencia de Estados Unidos en estos temas y el desarrollo que ha tenido la ciberseguridad, además de establecer redes que contribuyan al intercambio de información con miras a la discusión de este ámbito en el contexto chileno.



MISIÓN PÚBLICO - PRIVADA

TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN

CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

AMCHAM CHILE

OBJETIVOS

Explorar nuevos **sistemas operativos** y **protocolos de acción** en torno a la ciberseguridad que diversos sectores deberán incorporar en forma oportuna a sus operaciones.

Aprender sobre **leyes** y **regulaciones** de seguridad cibernética y analizar las fortalezas, efectividad y cumplimiento.

Aprender sobre las **competencias** y **habilidades** que serán requeridas según las exigencias del mercado laboral del futuro.

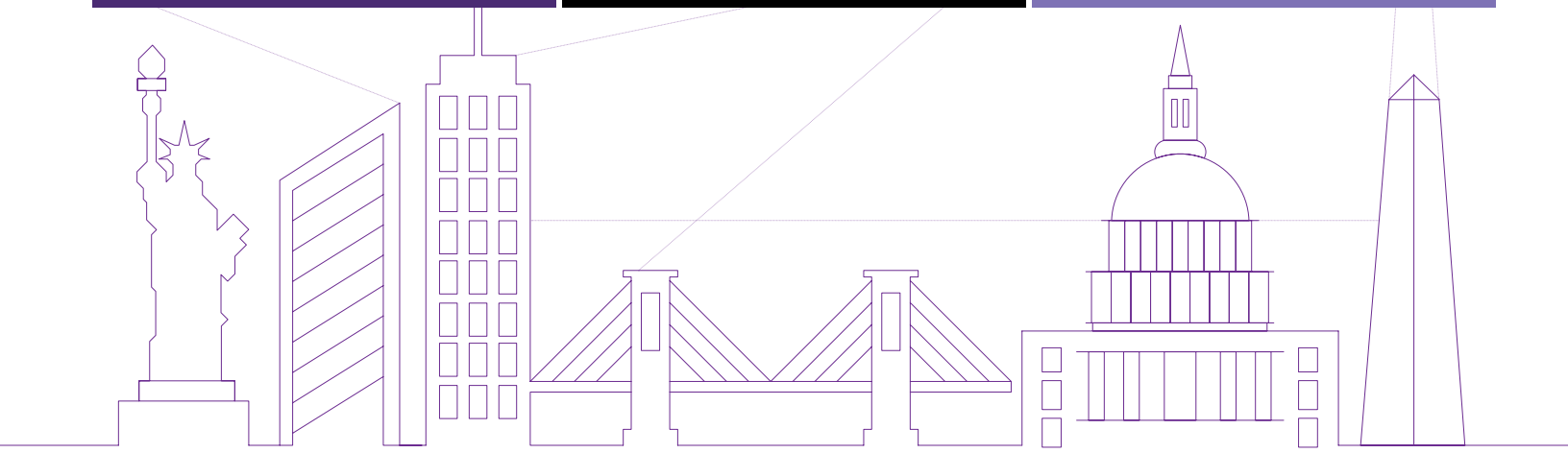
Conocer ejemplos virtuosos de **implementación** y **adaptación** a nueva infraestructura tecnológica y procesos de seguridad.

Analizar **tendencias** y **riesgos** asociados a servicios ***cloud, IoT, botnets, cryptojacking, ransomware, information security, third -party trisks, brand security y physical security.***

Detectar **enseñanzas** y **buenas prácticas** de entidades federales, *think tanks*, centros de investigación y empresas líderes, con el objetivo de asegurar la administración responsable de información sensible dentro el sector público y privado.

Casos prácticos de adopción de sistemas de ciberseguridad en diversos sectores productivos.

Dialogar con **expertos** y **académicos** sobre **fronteras** y **desafíos** que enfrenta el ámbito de la ciberseguridad.



VISITAS
SECTOR PRIVADO

MISIÓN PÚBLICO - PRIVADA
TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN
CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

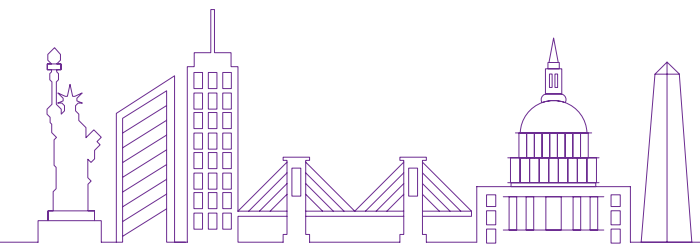
AMCHAM CHILE

LookingGlass ofrece protección unificada contra amenazas y contra los ataques cibernéticos sofisticados para empresas y agencias gubernamentales a nivel global. Su cartera integral de servicios gestionados, plataformas de amenazas, feeds legibles por máquina, y productos automatizados de respuesta a amenazas—todos apoyado por un equipo global de analistas de inteligencia.

Cisco Security Business Group, un líder en soluciones de ciberseguridad inteligente, está transformando la forma en la que las organizaciones medianas a grandes y agencias del gobierno manejan y minimizan los riesgos de seguridad en las redes. Con soluciones desde las redes hasta los usuarios finales, Cisco Security Business Group provee a los clientes con Agile Security el cual es tan dinámico como el mundo real al que protege y atacantes de los cuales defiende. Cisco Security Business Group ha sido constantemente reconocido por sus innovaciones y liderazgo industrial con docenas de patentes, investigación mundial y tecnología premiada. Hoy en día, el nombre de Cisco Security ha crecido y es sinónimo de innovación, seguridad inteligencia y protección ágil de punto a punto.

UnitedHealth Group es la compañía de atención de la salud y bienestar distintivamente diversificada con sede en los Estados Unidos y un líder mundial en ayudar a las personas a llevar vidas más saludables y colaborar para hacer que el sistema de salud funcione mejor para todos. Su compromiso se orienta hacia introducir enfoques, productos y servicios innovadores que puedan mejorar la salud personal y promover poblaciones más saludables en las comunidades locales. Sus prestaciones principales se relacionan a experiencia clínica, tecnología, datos e información de salud de avanzada con el fin de satisfacer las necesidades emergentes de un entorno cambiante de atención de la salud

AT&T es una compañía de medios que reúne contenido de calidad superior, relaciones directas con el consumidor, tecnología de publicidad y redes de alta velocidad para brindar una experiencia de cliente única. A &T Communications ofrece servicios móviles, de banda ancha, video y otros servicios de comunicaciones a consumidores estadounidenses y a más de 3 millones de compañías, desde las empresas más pequeñas hasta casi todas en la lista Fortune 1000, con soluciones inteligentes y altamente seguras.



VISITAS
ACADÉMICAS Y THINK TANK

MISIÓN PÚBLICO - PRIVADA
TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN
CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

AMCHAM CHILE

University of Maryland cuenta con títulos innovadores de seguridad cibernética en línea, conexiones de la industria y un equipo de seguridad galardonado. UMUC es un nombre líder en educación sobre seguridad cibernética. El Centro de Estudios de Seguridad de la UMUC ofrece recursos educativos, creación de redes y oportunidades de capacitación profesional para profesionales que trabajan en la educación cibernética. UMUC ha sido designada como Centro Nacional de Excelencia Académica en Aseguramiento de la Información y Educación en Defensa Cibernética por la Agencia de Seguridad Nacional y el Departamento de Seguridad Nacional y como Centro Nacional de Excelencia Académica Forense Digital por parte del Centro de Defensa Cibernética del Académico Alianza Académica para el Ciber Currículo.

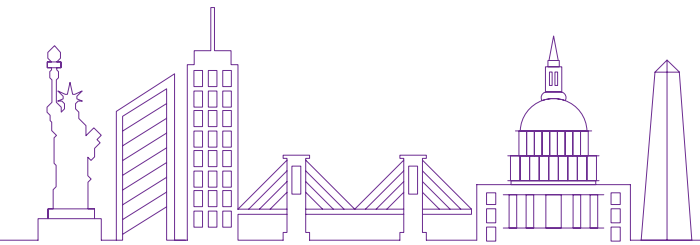
UNIVERSITY OF MARYLAND
University College

Public Knowledge es una think tank que promueve la libertad de expresión, una Internet abierta y el acceso a herramientas de comunicación asequibles y trabajos creativos. Trabajamos para dar forma a la política en nombre del interés público. Public Knowledge trabaja en la intersección de derechos de autor, telecomunicaciones e internet. Ley, en un momento en que estos campos están convergiendo. La experiencia de PK en las tres áreas lo pone en una posición ideal para abogar por políticas que sirvan al interés público.

Public Knowledge

El **Centro de Ciberseguridad** se dedica a desarrollar la capacidad para mantener los datos seguros y privados durante toda su vida, un enfoque central del Instituto de Ciencia de Datos de la Universidad de Columbia. El Centro reunirá y desarrollará la investigación de los departamentos de Ciencias de la Computación e Ingeniería Eléctrica, y el trabajo de la Escuela de Negocios de Columbia, entre otros. A modo de ejemplo, el año pasado se lanzaron nuevas empresas como CellRox, basadas en tecnología relacionada con la seguridad digital.

COLUMBIA UNIVERSITY
Data Science Institute



VISITAS
SECTOR PÚBLICO

MISIÓN PÚBLICO - PRIVADA
TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN
CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

AMCHAM CHILE

El **Instituto Nacional de Estándares y Tecnología (NIST)** fue fundado en 1901 y ahora es parte del Departamento de Comercio de los Estados Unidos. NIST implementa la ciberseguridad y la privacidad prácticas a través de la divulgación y la aplicación efectiva de los estándares y las mejores prácticas necesarias para que los EE. UU. adopten las capacidades de ciberseguridad.

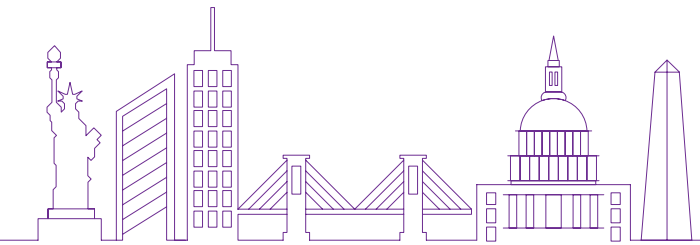
El ciberespacio es fundamental para la forma en que funciona todo EE. UU. En el **Departamento de Defensa**, permite a los militares obtener ventajas informativas, atacar objetivos de forma remota y trabajar desde cualquier lugar del mundo. Su estrategia cibernética nacional está basada en cuatro pilares:

- Proteger la sociedad civil, la patria y al estilo de vida estadounidense salvaguardando redes, sistemas, funciones y datos.
- Promover la prosperidad de los Estados Unidos fomentando una economía digital segura y próspera y fomentando una fuerte innovación nacional
- Preservar la paz y la seguridad mediante el fortalecimiento de la capacidad de los EE. UU
- Promover la influencia estadounidense para extender los principios clave de una Internet abierta, interoperable, confiable y segura.

En asociación con otros países, el Departamento de Estado lidera esfuerzos del gobierno de los Estados Unidos para promover una infraestructura de información y comunicaciones abierta, interoperable, segura y confiable que respalde el comercio internacional, fortalezca la seguridad internacional y fomente la libre expresión y la innovación.
La Oficina del Coordinador para Asuntos Cibernéticos del Departamento de Estado se responsabiliza por:

- Coordinar el compromiso diplomático global del Departamento en temas cibernéticos.
- Servir como enlace del Departamento con la Casa Blanca y los departamentos y agencias federales en estos temas
- Asesorar al secretario y a los secretarios adjuntos sobre temas y compromisos cibernéticos
- Actuar como enlace con entidades del sector público y privado en temas cibernéticos.
- Coordinar el trabajo de las oficinas regionales y funcionales dentro del Departamento involucrado en estas áreas.

La División de Ciberseguridad de la Agencia de Seguridad de la Ciberseguridad y la Infraestructura (CISA) lidera los esfuerzos para proteger el dominio federal ".gov" de las redes gubernamentales civiles y para colaborar con el sector privado, el dominio ".com", para aumentar la seguridad de las redes críticas. Esto ocurre a través de cuatro funciones primarias.
El **Centro Nacional de Integración de Ciberseguridad y Comunicaciones** (**NCCIC**, por sus siglas en inglés) de CISA es el centro de defensa cibernética, de incidentes y el centro de integración operacional emblemáticos de EE.UU. Desde 2009, el NCCIC ha servido como un centro nacional para información de ciberespacio y comunicaciones, experiencia técnica e integración operativa, y al operar nuestro centro de atención de incidentes, análisis y respuesta a incidentes 24/7.
Como Agencia de Sector Específico para los sectores de Tecnologías de la Información y las Comunicaciones (TI), CISA coordina informes a nivel nacional que son consistentes con el Marco de Respuesta Nacional (NRF).



MISIÓN PÚBLICO - PRIVADA

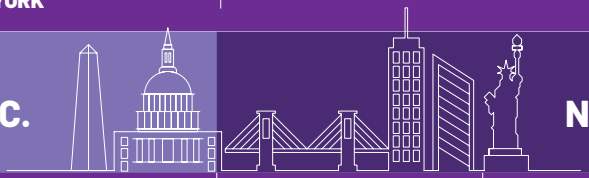
TENDENCIAS DEL MERCADO Y DESAFÍOS REGULATORIOS EN

CIBERSEGURIDAD

6 AL 10 DE MAYO DE 2019

WASHINGTON D.C.
NUEVA YORK

AMCHAM CHILE



WASHINGTON D.C. — NEW YORK

	DOMINGO **5 DE MAYO**	LUNES **6 DE MAYO**	MARTES **7 DE MAYO**	MIÉRCOLES **8 DE MAYO**	JUEVES **9 DE MAYO**	VIERNES **10 DE MAYO**
MAÑANA	Llegada a Washington D.C.	**University of Maryland University College (UMUC)** » Conocer desde la academia tendencias y desafíos en ciberseguridad » Proyectos de investigación **Cisco** » Why Cybersecurity Investment Will Drive Businesses Digitalization » Hacker Operation and New "Business" Models » Hunting for Adversaries in you IT/Compliance Environment	**Looking Glass Cybersolutions** » Third Party Risks » Brand Security » Physical Security **U.S Department of Defense** » Conocer sobre procesos y beneficios de automatización y data analytics a gran escala para identificar ciberataques y sobre la coordinación en el intercambio de información entre el sector público y privado	**Public Knowledge** » Diálogo en think tank sobre la gestación de policy en ciberseguridad **U.S Department of Homeland Security** » Cómo se ve afectada la infraestructura crítica del país ante amenazas de ciberseguridad	**Institución Financiera TBC** » Conocer la experiencia desde la banca en cuanto a los procesos de adaptación e implementación de nuevas regulaciones y sistemas de seguridad **AT&T** » Conocer la experiencia desde las telecomunicaciones de los procesos de implementación frente a nuevas regulaciones y sistemas de seguridad	**Columbia Cybersecurity Center** » Conocer desde la academia tendencias y desafíos en ciberseguridad » Proyectos de investigación **Reunión de cierre y next steps**
TARDE		**NIST** (National Institute of Standards and Technology) » Conocer buenas prácticas y estándares operativos desde el gobierno federal de EE.UU.	**United Health Group** » Desafíos regulatorios y tratamiento de data sensible en el ámbito de la salud	**U.S Department of State** » Conocer sobre el proceso de mapeo de vulnerabilidades y amenazas	**Cisco** » Mesa redonda con empresas sobre los desafíos a enfrentar en Ciberseguridad	Salida a Santiago
NOCHE				Salida a Nueva York	Comida de despedida	

*** Esta agenda puede sufrir modificaciones**

Valores: US$6.000 SOCIOS / US$8.000 NO SOCIOS