HORIZONTES DE LA CIBERSEGURIDAD

ESTRATEGIAS, RIESGOS E INNOVACIÓN (SIMPOSIO)

26 DE JUNIO DE 2025
AUDITORIO JORGE CAVODEASSI FALGARI. OEI.
CIUDAD AUTÓNOMA DE BUENOS AIRES

COORDINADORES
HÉCTOR VILLALBA | DIEGO BOLATTI

UGD EDITORIAL

COLECCIÓN magistrales

HORIZONTES DE LA CIBERSEGURIDAD

HORIZONTES DE LA CIBERSEGURIDAD

ESTRATEGIAS, RIESGOS E INNOVACIÓN (SIMPOSIO)

26 DE JUNIO DE 2025. AUDITORIO JORGE CAVODEASSI FALGARI. OEI. CIUDAD AUTÓNOMA DE BUENOS AIRES

COORDINADORES
HÉCTOR VILLALBA | **DIEGO BOLATTI**

Universidad Gastón Dachary
Horizontes de la ciberseguridad : estrategias, riesgos e innovación ; Compilación de Héctor Villalba ; Diego Bolatti. - 1a ed. - Posadas : Universidad Gastón Dachary, 2026.
Libro digital, PDF - (Magistrales)
Archivo Digital: descarga
ISBN 978-631-91368-4-5
1. Ciberdelitos. 2. Seguridad Informática. I. Villalba, Héctor, comp. II. Bolatti, Diego, comp.
CDD 365.641

Editorial UGD
Universidad Gastón Dachary
Salta 1912, Posadas, Misiones, Argentina
editorial@ugd.edu.ar

Diseño. arte y maquetación: Loquepodemos Estudio Editorial
Coordinación editorial: Marina Hlebovich
Edición y asesoramiento editorial: Horacio Moreno

Publicación electrónica - distribución gratuita

Acceso web: https://ugd.edu.ar/es/

AEUP RED DE EDITORIALES DE UNIVERSIDADES PRIVADAS

Índice

Presentación de la colección

La Colección “Magistrales” y el Compromiso con el Conocimiento Estratégico

Estimada comunidad universitaria, especialistas y lectores:

Presentamos formalmente la colección *Magistrales*, un nuevo espacio editorial de la Universidad Gastón Dachary que refleja ideas, debates y análisis que se desarrollan en nuestras aulas y encuentros.

Magistrales nace para dar continuidad a los eventos académicos de la UGD: difundirlos, resguardar sus aportes y convertir sus contenidos y reflexiones en material de consulta. Con esta serie buscamos trascender el evento puntual y poner esas

ideas a disposición de una audiencia más amplia, como insumo para nuevas actividades académicas y como aporte al debate cultural y profesional.

La colección se nutre de producciones académicas generadas en clases abiertas, ciclos de debate, paneles, conferencias y simposios, entre otros formatos, impulsados por nuestras unidades académicas.

La primera publicación de esta colección está dedicada a un tema crucial del mundo contemporáneo: la ciberseguridad. Reúne las principales exposiciones y debates del simposio "Horizontes de la Ciberseguridad. Estrategias, Riesgos e Innovación", realizado el 26 de junio de 2025 en el Auditorio Jorge Cavodeassi Falgari de la Organización de Estados Iberoamericanos (OEI), en la Ciudad Autónoma de Buenos Aires, en el marco del Programa de Posgrados en Seguridad que impulsa la Universidad Gastón Dachary, con la colaboración de instituciones nacionales e internacionales y el sostenido vínculo con el Centro Universitario de la Guardia Civil Española. En conjunto, ofrece una mirada plural e integral sobre desafíos, riesgos y estrategias, con valor tanto académico como profesional.

Agradezco a todos los participantes del simposio, a los curadores de la colección por hacer posible este trabajo colectivo y a las instituciones que colaboraron en esta iniciativa: el Instituto Universitario de Seguridad de la Provincia de Misiones, la

Organización de Estados Iberoamericanos, el Centro Universitario de la Guardia Civil Española, el Instituto Universitario de Seguridad de la Ciudad de Buenos Aires, la Dirección Nacional de Formación y Desarrollo Profesional del Ministerio de Seguridad y el Gobierno de la provincia de Misiones.

Invitamos a la lectura de este material, convencidos de su valor formativo y estratégico para profesionales de las Fuerzas de Seguridad y del Poder Judicial, académicos y responsables de políticas públicas.

Ing. Luis Lichowski
Rector de la Universidad Gastón Dachary

Prólogo

La Universidad Gastón Dachary ha asumido, desde su origen, el compromiso de producir y difundir conocimiento que dialogue con las necesidades reales de nuestra sociedad. El área de la ciberseguridad, atravesada por profundas transformaciones tecnológicas y por nuevos desafíos para la gobernanza pública y privada, exige hoy precisamente ese tipo de reflexión rigurosa, colaborativa y orientada al futuro. En este marco, el simposio “Horizontes de la Ciberseguridad. Estrategias, Riesgos e Innovación” constituye un paso significativo en la construcción de un espacio académico capaz de integrar miradas, experiencias y saberes diversos.

Este volumen, que sistematiza brevemente lo trabajado en aquella jornada, expresa la vocación de nuestra universidad por trascender el evento puntual y proyectar sus resultados hacia la comunidad profesional, educativa, de investigación e institucional. Así como el Rector subraya en la presentación de esta colección la importancia de ampliar la circulación de ideas y fortalecer la vinculación entre actores estratégicos, el presente libro recoge ese espíritu y lo traslada al campo de la seguridad digital.

El encuadre teórico que sostiene estas páginas parte de una premisa compartida por todas las instituciones participantes: "la ciberseguridad es una responsabilidad común". Su complejidad supera la capacidad individual de cualquier organización, por lo que requiere diagnósticos integrados, cooperación efectiva, intercambio de buenas prácticas y la construcción de capacidades colectivas. Las amenazas digitales actuales –dinámicas, transnacionales, apoyadas en inteligencia artificial y orientadas a vulnerar tanto sistemas públicos como privados– nos obligan a repensar nuestras estructuras y a fortalecer la cultura de prevención, respuesta e innovación.

El trabajo en red, uno de los ejes que recorre este libro, no fue una consigna abstracta: fue la práctica concreta que dio forma al Simposio. Su organización reunió a universidades, centros de formación, organismos nacionales, fuerzas de segu-

ridad, referentes judiciales y especialistas internacionales. Cada panel reflejó la preocupación compartida por anticipar escenarios, mejorar la profesionalización, comprender la evolución del delito, fortalecer la soberanía tecnológica y promover la resiliencia de nuestras instituciones y empresas. Esta convergencia, cuidadosamente articulada por los equipos participantes, da cuenta de un consenso fundamental: sólo mediante la cooperación podremos enfrentar los desafíos del entorno digital contemporáneo.

Las exposiciones aquí reunidas ofrecen un panorama integral de los retos actuales y, al mismo tiempo, iluminan caminos posibles para el desarrollo futuro. Desde la innovación en la formación universitaria hasta la investigación del ciberdelito, desde la protección del Estado hasta la estrategia empresarial y la gestión del riesgo, cada contribución ayuda a trazar un mapa conceptual y operativo para quienes se desempeñan en el ámbito de la seguridad.

Con esta publicación, deseamos fortalecer la misión de la colección *Magistrales*: brindar a la comunidad un material que no solo documente un encuentro académico, sino que aporte, fomente el debate informado y potencie el desarrollo profesional. La ciberseguridad representa hoy un desafío decisivo para el funcionamiento del Estado, la justicia, la actividad empresarial y la vida cotidiana de los ciudadanos. Por ello, esperamos

que este libro sirva como referencia para nuevas iniciativas, investigaciones y políticas de formación y gestión.

Invitamos a los lectores a recorrer estas páginas con la convicción de que el conocimiento compartido es la base de la cooperación y que la cooperación es, en definitiva, la condición necesaria para construir un futuro digital más seguro, más justo y resiliente.

Ing. Diego Bolatti, Lic. Héctor Villalba

Capítulo 1.
El Simposio

El Seminario “Horizontes de la Ciberseguridad: Estrategias, Riesgos e Innovación”, también identificado como Simposio, se llevó a cabo el jueves 26 de junio de 2025, en la Ciudad Autónoma de Buenos Aires. El evento tuvo lugar en el Auditorio Jorge Cavodeassi Falgari, de la Organización de los Estados Iberoamericanos (OEI), ubicado en Paraguay 1583.

La organización estuvo a cargo del Instituto Universitario de Seguridad Pública de Misiones (IUSPM) y la Universidad Gastón Dachary (UGD), con la participación y apoyo institucional del Centro Universitario de la Guardia Civil de España (CUGC), Ministerio de Gobierno de la provincia de Misiones, la Organización de Estados Iberoamericanos (OEI), la Dirección Nacional

de Formación y Desarrollo Profesional del Ministerio de Seguridad de la Nación y el Instituto Universitario de Seguridad de la Ciudad de Buenos Aires.

El Seminario no fue solo un encuentro de especialistas, sino una declaración de compromiso institucional frente a los desafíos del mundo digital.

Desde el acto de apertura, las autoridades presentes –incluyendo el Rector de la UGD, Ing. Luis E. Lichowski; el Ministro de Gobierno de Misiones, Dr. Marcelo Pérez; el Coordinador del Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad (ICTS), Dr. Rodolfo Barrere; el Vicerrector del Instituto Universitario de Seguridad de la Ciudad de Buenos Aires (IUSE), Dr. Gabriel Unrein; y el Director Nacional de Formación y Desarrollo Profesional del Ministerio de Seguridad Nacional, Sr. José Luis Parisí– establecieron el marco educativo y estratégico. Se enfatizó que las irrupciones tecnológicas obligan a las instituciones a repensarse. El mensaje central fue la necesidad de que las universidades y los organismos de seguridad fortalezcan la cooperación interinstitucional y el trabajo en red, para generar las capacidades que permitan anticiparse a las necesidades futuras que enfrenta la sociedad. Esta visión se sustenta en la firme convicción de que la formación de calidad es esencial para generar las competencias necesarias y garantizar la actualización permanente de las fuerzas de seguridad, permitiéndoles

estar a la altura de las circunstancias frente a la evolución constante del ciberdelito y los desafíos que este presenta (o que se presentan).

Este espíritu de innovación y profesionalización fue un eje constante a lo largo de la jornada. Se destacó la importancia de adaptar los modelos de formación en seguridad, inspirados en experiencias internacionales como el Centro Universitario de la Guardia Civil de España (CUGC), y la necesidad de cooperación interinstitucional para fortalecer las capacidades del país.

Tanto en la apertura como en las reflexiones finales, se subrayó que la ciberseguridad es una responsabilidad compartida. El Seminario concluyó con un Conversatorio de Cierre titulado "Articulando para proteger. Desafíos compartidos". Este diálogo final permitió identificar desafíos comunes y reiterar la necesidad de promover sinergias entre los sectores público y privado.

La estructura del Seminario se organizó en tres paneles temáticos diseñados para ofrecer una visión integral de los desafíos del ciberespacio, seguidos por un conversatorio de cierre.

El Panel I, denominado "Innovación y profesionalización nuevas dimensiones en la formación y actualización en seguridad", se centró en las tendencias emergentes y experiencias innovadoras en la formación profesional en seguridad, incluyendo la presentación de un programa de posgrado. La mesa fue moderada por Carlos Pérez Rasetti y contó con la participación

del Dr. Paulo Falcón, Coordinador del Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad de la Organización de Estados Iberoamericanos (OEI); el coronel Dr. Fernando Moure Colón, ex Director del Centro Universitario de la Guardia Civil Española y Director del Programa de Posgrados en Seguridad del IUSPM, UGD; y el Mg. Rafael Osudar, Secretario Académico del Instituto Universitario de Seguridad de Misiones.

El Panel II, titulado "Protección digital desde el Estado: seguridad pública y del sector privado", se dedicó a analizar las amenazas actuales y emergentes en la ciberseguridad que impactan la seguridad pública, organismos gubernamentales, sistemas judiciales e infraestructuras críticas. La discusión fue moderada por Martín Nessi, Secretario Académico del Instituto Universitario de Seguridad de la Ciudad de Buenos Aires. Los panelistas fueron la Dra. Daniela Dupuy, Fiscal Penal especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires; el Dr. Miguel Kessler, Fiscal especializado en ciberfraude, también de Ciudad Autónoma de Buenos Aires; y el Mg. Julián Reale, Asesor Legal de la Dirección de Ciberdelito y Asuntos Cibernéticos del Ministerio de Seguridad de la Nación.

El Panel III, "Seguridad corporativa: innovación, riesgos y resiliencia en la ciberseguridad empresarial", exploró cómo las empresas y organizaciones privadas enfrentan el creciente riesgo de ciberataques, abordando la innovación, la gestión de ries-

gos y la ciberresiliencia. Este panel fue moderado por Héctor Villalba, docente e investigador en la Universidad Gastón Dachary y Especialista en Ciberseguridad. Los expositores fueron el Dr. Juan Antonio Gómez Bule, presidente de Walhalla Data Center Services de Valencia, España, y el Lic. Pablo Pi, Líder del área de Seguridad Informática en Emova y docente universitario en ciberseguridad y gestión de riesgos.

Finalmente, la jornada concluyó con el Conversatorio de Cierre titulado “Articulando para proteger. Desafíos compartidos”, un diálogo destinado a identificar desafíos comunes y a promover sinergias en el campo de la ciberseguridad.

El encuentro reafirmó la importancia de la colaboración y el intercambio de buenas prácticas para construir resiliencia cibernética a nivel institucional, corporativo y social, como única vía frente a amenazas globales cada vez más complejas. Como resultado, el Seminario no solo generó una síntesis de conclusiones generales, sino que también sirvió como plataforma para la presentación de próximas líneas de trabajo y cooperación interinstitucional.

Capítulo 2. Panel I: Innovación y profesionalización

Nuevas dimensiones en la formación y actualización en seguridad

Introducción

La acelerada transformación del entorno digital, impulsada por la inteligencia artificial, la automatización y la hiperconectividad, ha redefinido profundamente las competencias requeridas en el campo de la ciberseguridad. En este escenario, las amenazas ya no son estáticas ni previsibles: evolucionan de forma continua, se adaptan a los mecanismos de defensa y explotan tanto vulnerabilidades tecnológicas como debilidades humanas y organizacionales.

Este contexto obliga a repensar los modelos tradicionales de formación. La profesionalización en seguridad ya no puede

limitarse a la adquisición de conocimientos técnicos aislados, sino que debe orientarse a la construcción de capacidades integrales que permitan comprender el riesgo en su totalidad. Esto incluye el análisis de amenazas emergentes, la interpretación de marcos de buenas prácticas de alcance internacional, la gestión de incidentes y la toma de decisiones en escenarios de incertidumbre.

La irrupción de la inteligencia artificial introduce, además, una doble dimensión en la formación: por un lado, como herramienta para mejorar la detección, análisis y respuesta ante incidentes; por otro, como nuevo vector de riesgo, capaz de potenciar ataques más sofisticados, automatizados y difíciles de detectar. Este fenómeno exige profesionales capaces de comprender tanto el potencial como las implicancias éticas, operativas y de seguridad de estas tecnologías.

En paralelo, los modelos educativos enfrentan el desafío de adaptarse a nuevas formas de aprendizaje. La aparición de trayectorias modulares, certificaciones intermedias y esquemas flexibles plantea la necesidad de equilibrar innovación pedagógica con calidad formativa, asegurando que las competencias desarrolladas respondan a estándares exigentes y a necesidades reales del entorno profesional.

Este panel propone situar al lector en ese punto de inflexión: un escenario donde la formación en ciberseguridad

se convierte en un proceso continuo, estratégico y adaptativo. Las experiencias y reflexiones que se presentan a continuación permiten comprender cómo las instituciones están abordando este desafío y qué caminos se abren para fortalecer la profesionalización en un campo en constante evolución.

Desarrollo

Moderador: Carlos Pérez Rasetti
Panelistas: Paulo Falcón, Fernando Moure Colón, Rafael Osudar

El primer panel del simposio abordó los desafíos actuales en la formación universitaria en seguridad, enfatizando la necesidad de innovar en los modelos educativos y de fortalecer la profesionalización del sector.

El moderador, Carlos Pérez Rasetti, abrió el encuentro destacando que el propósito de la mesa era “darle el marco institucional y educativo a los temas específicos que se van a tratar en los paneles siguientes”, recordando que el Instituto Universitario de Seguridad de Misiones, perteneciente a la Universidad Gastón Dachary en convenio con la Provincia de Misiones, “forma personal de las fuerzas de seguridad de la provincia y especialistas en seguridad a partir de un programa de posgrado”.

El Dr. Paulo Falcón inició su exposición titulada “Volver al futuro”, invitando a reflexionar sobre la relación entre universidad, tecnología y sociedad del conocimiento. Señaló que “las irrupciones tecnológicas nos obligan a repensarnos” y que la universidad debe tener la capacidad de “traer el futuro al presente y empezar a construirlo”.

Falcón realizó un recorrido histórico desde el inicio de las universidades, con la universidad de Bolonia, hasta los debates actuales sobre microcredenciales, explicando que el diploma es una representación que le dice a la sociedad que hemos formado a la persona egresada de una carrera en determinado campo, y en el caso de los títulos habilitantes, además permiten el ejercicio profesional. Hoy ese concepto aparece en tensión. Enfatizó que la universidad tiene que recuperar la vanguardia y anticiparse a las necesidades futuras que tienen nuestras sociedades.

Sobre la flexibilización de los sistemas educativos, afirmó: “Tenemos que establecer un diálogo entre presente y futuro, entre lo que somos y lo que podemos llegar a ser en términos de propuestas académicas”. Asimismo, defendió el papel del aseguramiento de la calidad como eje de legitimidad institucional: “No cualquier formación contribuye a la generación de competencias necesarias; las instituciones educativas estamos para formar profesionales y ciudadanos”.

Finalmente, exhortó a no ceder terreno a las empresas tecnológicas, que mercantilizan la educación: “No regalemos conceptos a entidades que solo buscan hacer negocios con la educación; apropiémonos de lo que venimos haciendo hace muchos años, como es el caso de la formación en formato de microcredenciales, porque sabemos hacerlo bien”.

El coronel Dr. Fernando Moure Colón, ex director del Instituto Universitario de la Guardia Civil de España, retomó el eje de la cooperación internacional, subrayando que el intercambio de experiencias permite “buscar puntos de conexión y buenas prácticas que luego puedan adaptarse según las circunstancias de cada institución o país”.

Explicó el proceso de transformación educativa que atravesaron las academias policiales europeas a partir del Espacio Europeo de Educación Superior. “En 1999 se pusieron las bases para que los países pudieran desarrollar sus grados universitarios con estándares comunes”. Describió cómo en Finlandia, Alemania y Hungría, las academias policiales se convirtieron en universidades o centros universitarios, integrando a docentes policiales y civiles.

Sobre el caso español, señaló que “nuestra legislación no permitía que la academia de policía fuera directamente universidad, por eso se crearon los centros universitarios de Policía y de Guardia Civil”, instituciones que hoy imparten programas de

grado y posgrado reconocidos. Agregó que este modelo busca "tener los mejores policías, los mejores guardias civiles, capaces de actuar y combatir el crimen organizado, pero también formados en la universidad".

Moure Colón presentó además una experiencia de innovación educativa, la *Liga de ciberseguridad*, una competencia internacional orientada a captar talento joven. "Queremos que los hackers estén de nuestro lado", expresó, invitando a las autoridades locales a replicar la iniciativa en Argentina.

Finalmente, el Dr. Rafael Osudar, Secretario Académico del Instituto Universitario de Seguridad de Misiones, presentó el Programa de Posgrado en Seguridad desarrollado por la institución. Recordó que "desde 2018 venimos trabajando en la formación de la fuerza de seguridad de la provincia" y que el nuevo programa "surge con una estructura modular, flexible y escalable", pensada para certificar microcredenciales, diplomaturas y una Maestría en Seguridad Pública.

El programa contempla cinco diplomaturas –en ciberseguridad, seguridad tecnológica y corporativa, política y planificación en seguridad, seguridad internacional y amenazas a la seguridad–, todas articuladas en formato virtual, con encuentros sincrónicos y tres instancias presenciales optativas en Buenos Aires, Misiones y España.

Osudar destacó que la propuesta “promueve la colaboración internacional y el aprendizaje entre pares”, reforzando la idea de comunidad académica. Concluyó señalando que el posgrado “cumple con los estándares de calidad requeridos por el Ministerio y la CONEAU”, consolidando así la profesionalización de la formación en seguridad en la provincia.

La reflexión sobre la innovación y la profesionalización en ciberseguridad no puede desvincularse de su aplicación en los ámbitos donde estas capacidades se materializan. La formación de profesionales no constituye un fin en sí mismo, sino el punto de partida para fortalecer las estructuras que deben dar respuesta a las amenazas del entorno digital.

En este sentido, el rol del Estado adquiere una relevancia central. Las competencias desarrolladas en el ámbito académico encuentran su expresión en la gestión de la seguridad pública, la investigación del ciberdelito y la protección de infraestructuras críticas. La transición desde la formación hacia la acción institucional permite comprender cómo el conocimiento se traduce en políticas, capacidades operativas y mecanismos de respuesta frente a riesgos cada vez más complejos.

Capítulo 3.
Panel II: Protección digital desde el Estado

Seguridad pública y del sector privado

Introducción

La digitalización de los servicios públicos, la expansión de las infraestructuras críticas interconectadas y la creciente dependencia de los sistemas digitales han convertido a la ciberseguridad en un componente esencial de la seguridad del Estado. En este contexto, las amenazas ya no se limitan a ataques aislados, sino que adoptan formas complejas, coordinadas y muchas veces transnacionales, afectando tanto al sector público como al privado.

El cibercrimen ha evolucionado hacia modelos organizados, altamente especializados y con capacidades tecnológicas

avanzadas. Fraudes digitales a gran escala, ataques de ransomware, explotación de vulnerabilidades en cadenas de suministro y el uso de inteligencia artificial para automatizar ataques o generar engaños sofisticados son solo algunas de las manifestaciones actuales. Estas dinámicas desafían los modelos tradicionales de investigación y requieren respuestas más ágiles, coordinadas y basadas en inteligencia.

En este escenario, el Estado asume un rol central no solo como actor operativo, sino también como articulador de políticas, regulaciones y mecanismos de cooperación. La protección digital implica desarrollar capacidades institucionales para prevenir, detectar, responder y recuperarse frente a incidentes, integrando enfoques técnicos, legales y estratégicos. Asimismo, requiere fortalecer la colaboración con el sector privado, que en muchos casos gestiona activos críticos o infraestructuras esenciales para el funcionamiento de la sociedad.

La existencia de marcos de referencia y buenas prácticas de alcance internacional aporta lineamientos clave para estructurar estas capacidades, promoviendo enfoques basados en gestión de riesgos, resiliencia y mejora continua. Sin embargo, su implementación efectiva depende de la adaptación a los contextos locales, las capacidades institucionales y la madurez de cada organización.

Este panel invita al lector a comprender la complejidad del rol estatal en la protección digital, explorando cómo se abordan las amenazas actuales, qué desafíos persisten y cuáles son las estrategias emergentes para fortalecer la seguridad en un entorno cada vez más dinámico e interdependiente.

Desarrollo

Moderador: Martín Nessi

Panelistas: Daniela Dupuy, Miguel Kessler, Julián Reale

El segundo panel del seminario se centró en los desafíos que enfrenta el Estado en materia de protección digital y ciberseguridad, tanto en la esfera pública como en el ámbito privado. Participaron especialistas del Poder Judicial y del Ministerio de Seguridad, quienes aportaron su experiencia en la investigación de delitos informáticos y la gestión de ciberamenazas.

El moderador, Martín Nessi, Secretario Académico del Instituto Universitario de Seguridad de la Ciudad de Buenos Aires, dio inicio al panel destacando la amplia participación de representantes de todo el país y de quince países latinoamericanos, desde Guatemala hasta Chile. Señaló que el objetivo del encuentro era “analizar las amenazas actuales y emergentes en el ámbito de la ciberseguridad, identificando su impacto en la

seguridad pública, los organismos gubernamentales, los sistemas judiciales y otras instituciones".

La Dra. Daniela Dupuy, Fiscal Penal especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires, abrió la mesa subrayando la evolución del cibercrimen en la última década. Recordó que "hace diez años los casos eran aislados y locales; hoy enfrentamos organizaciones internacionales complejas de cibercrimen". Explicó que las investigaciones actuales requieren cooperación constante entre países, debido a que "los autores están diseminados en diferentes naciones, las víctimas en otras y la evidencia digital alojada en jurisdicciones extranjeras".

Dupuy enfatizó la importancia de la cooperación internacional: "Sería imposible afrontar este flagelo sin coordinación entre fiscales e investigadores de distintos países". También destacó el papel de las fuerzas de seguridad especializadas, a quienes considera "el binomio perfecto para una investigación eficiente".

En su exposición, la fiscal destacó el crecimiento exponencial de los casos vinculados con la explotación sexual infantil. Señaló que "el año pasado, 2024, recibimos en nuestro país 120.000 denuncias o reportes de explotación sexual infantil, y a julio de este año ya superamos esa cifra". Agregó que desde 2016 la tendencia es ascendente y que la ONG National Center for Missing and Exploited Children canaliza los reportes de las principales plataformas tecnológicas hacia las fiscalías argentinas.

Dupuy advirtió que "en un 38 % de los casos los autores son profesionales, docentes, médicos o padres de familia" y que muchos derivan en "*grooming*, abuso sexual y corrupción de menores". Entre las nuevas problemáticas, señaló la aparición de contenidos creados con inteligencia artificial: "Hoy tenemos un gran desafío con la creación de imágenes o videos ficticios de niños en actividades sexuales; lamentablemente, aún no es delito en nuestro país".

También mencionó casos de *sexting* y difusión no consentida de imágenes íntimas, señalando que "en CABA es una simple contravención con multa de 300 pesos, y en muchas provincias ni siquiera está tipificado". Concluyó con una reflexión sobre la urgencia de la prevención. "Hoy hay más peligro en el ciberespacio que en la calle; los chicos son captados en redes sociales o plataformas de juegos sin que padres o docentes lo adviertan".

El Dr. Miguel Kessler, fiscal especializado en ciberfraude de la Ciudad Autónoma de Buenos Aires, continuó con una exposición sobre la creación y funcionamiento de la Fiscalía de Ciberfraudes (FSEC). Agradeció a las autoridades que impulsaron su creación y explicó que "la fenomenología criminológica se especializa y se complejiza", motivo por el cual surgió la necesidad de una fiscalía dedicada al fraude digital.

Detalló los tipos de delitos abordados por su equipo, desde defraudaciones con tarjetas hasta manipulación de sistemas

informáticos, e insistió en la necesidad de una reforma penal. “Podemos tener un fraude de 1.500 millones de pesos con una pena mínima de un mes de prisión”.

Planteó que la especialización permitió pasar “de la persecución caso por caso a una investigación penal inteligente, que busca patrones y sistematiza información”. Explicó que, tras su primer año de funcionamiento, la fiscalía registró “1.291 casos de fraude por transferencias bancarias, 597 por compras con tarjeta de crédito, y múltiples episodios de hackeos de dispositivos y fraudes con criptomonedas, donde el dinero desaparece en minutos dentro de autopistas digitales imposibles de rastrear sin la clave semilla”.

Kessler resaltó la importancia del trabajo colaborativo: “Trabajar solo no alcanza; la colaboración y el intercambio de información son esenciales”. Asimismo, abordó la urgencia de responder ante fraudes digitales, señalando que “un minuto es una eternidad en el mundo digital”, y destacó la necesidad de capacitación continua en ciberseguridad.

Expuso estadísticas de la fiscalía: entre junio de 2024 y junio de 2025 se registraron “casi 9.000 millones de pesos defraudados y más de un millón de dólares”. Añadió que se detectaron “l.791 cuentas vulneradas, de las cuales 430 correspondían a bancos públicos y 1.361 a bancos privados”. Señaló que “sin trabajo colaborativo esto no se puede hacer” y describió los

convenios con el Banco Central y entidades financieras para prevenir fraudes mediante cuentas mulas y transacciones inusuales. Concluyó: “el fraude vino para quedarse; no podemos erradicarlo, pero sí reducirlo si trabajamos juntos”.

El Mg. Julián Reale, Asesor Legal de la Dirección de Ciberdelito y Asuntos Cibernéticos Ministerio de Seguridad Nacional, cerró el panel aportando la perspectiva estatal sobre la protección de infraestructuras críticas. Presentó el Programa de Fortalecimiento en Ciberseguridad e Investigación del Ciberdelito (FORCIC), destacando el rol del “Centro de Sinergias Cibernéticas y el CSIAT-MinSeg”, encargados de gestionar vulnerabilidades y coordinar las cinco fuerzas federales.

Reale explicó que “el *ransomware* sigue siendo una de las principales amenazas a la ciberseguridad del Estado y de los operadores privados” y que las “amenazas persistentes avanzadas (APT) buscan explotar vulnerabilidades desconocidas durante meses”. También mencionó ataques de *phishing* dirigido y fallos en la implementación de políticas de seguridad, advirtiendo que “usuarios desvinculados con permisos activos o credenciales débiles pueden poner en riesgo a todo un organismo”.

Planteó la necesidad de “fortalecer el marco normativo y unificar criterios de gestión de incidentes”, tomando como ejemplo la Directiva NIS2 de la Unión Europea. Recalcó además

que “la ciberseguridad debe ser una política de Estado, sostenida entre lo técnico, lo estratégico y lo jurídico”.

Finalmente, subrayó la importancia del factor humano: “El eslabón más débil de la cadena de la ciberseguridad sigue siendo el ser humano”, e instó a reforzar la capacitación, la conciencia y la adopción del doble factor de autenticación. Cerró su intervención afirmando que “solo trabajando de manera mancomunada y coordinada podremos mejorar la ciberseguridad del país”.

El análisis de la protección digital desde el Estado evidencia que la ciberseguridad trasciende el ámbito gubernamental y se proyecta sobre todo el entramado socioeconómico. La interdependencia entre organismos públicos y organizaciones privadas hace que los riesgos y las amenazas no puedan abordarse de manera aislada.

En este contexto, el sector empresarial se posiciona como un actor clave en la gestión de la ciberseguridad. Las organizaciones no solo son destinatarias de políticas y regulaciones, sino también protagonistas en la implementación de estrategias de protección, gestión del riesgo e innovación tecnológica. Comprender cómo las empresas enfrentan estos desafíos resulta fundamental para completar la visión integral del ecosistema digital.

Capítulo 4.
Panel III: Seguridad corporativa

Innovación, riesgos y resiliencia en la ciberseguridad empresarial

Introducción

En el ámbito empresarial, la ciberseguridad se ha consolidado como un factor determinante para la continuidad operativa, la protección de activos y la sostenibilidad del negocio. Las organizaciones se enfrentan a un entorno en el que las amenazas son persistentes, adaptativas y, en muchos casos, impulsadas por modelos de negocio criminal altamente rentables.

La incorporación de tecnologías emergentes, especialmente aquellas basadas en inteligencia artificial, ha ampliado las capacidades de las empresas, pero también ha incrementado su superficie de exposición. La automatización de procesos,

la digitalización de operaciones y la interconexión con proveedores y socios estratégicos generan nuevas dependencias y, con ellas, nuevos riesgos.

Los ataques actuales no solo buscan interrumpir sistemas, sino también afectar la reputación, comprometer información sensible o generar impactos financieros significativos. El *ransomware*, el fraude digital, los ataques dirigidos y la explotación de vulnerabilidades en terceros son ejemplos de amenazas que obligan a las organizaciones a adoptar una visión integral de la seguridad.

En este contexto, la gestión del riesgo deja de ser una función aislada para integrarse en la gobernanza corporativa. La adopción de marcos de buenas prácticas ampliamente reconocidos a nivel internacional permite estructurar programas de seguridad más robustos, orientados a la prevención, detección y respuesta, así como a la mejora continua.

La resiliencia cibernética emerge como un concepto central, entendido como la capacidad de anticipar incidentes, resistir su impacto y recuperar las operaciones en tiempos aceptables. Este enfoque reconoce que la seguridad absoluta no existe y que la preparación para el fallo es tan importante como la prevención.

El presente panel propone una mirada estratégica sobre la ciberseguridad empresarial, invitando al lector a comprender

cómo las organizaciones están abordando estos desafíos, qué rol juega la innovación en este proceso y cómo se construyen capacidades que permitan sostener el negocio en entornos de alta incertidumbre.

Desarrollo

Moderador: Héctor Villalba

Panelistas: Juan Antonio Gómez Bule, Pablo Pi

El tercer panel del simposio abordó los desafíos de la ciberseguridad desde la perspectiva empresarial, subrayando el papel estratégico de la innovación, la gestión de riesgos y la resiliencia organizacional.

El moderador, Héctor Villalba, destacó la gravedad de los incidentes que afectan a las empresas privadas, advirtiendo que "hay compañías que no logran recuperarse tras un ataque porque sus clientes pierden la confianza o los daños económicos resultan irreparables".

El Dr. Juan Antonio Gómez Bule, presidente de Walhalla Data Center Services (Valencia, España), ofreció una exposición de alto impacto conceptual sobre los vínculos entre ciberseguridad, geopolítica y soberanía tecnológica. Señaló que "vivimos en un entorno de cambio global en el que la ciberseguridad es

un elemento fundamental" y recordó su trayectoria de más de 25 años colaborando con las fuerzas de seguridad españolas.

Sostuvo que la defensa de la información y de los activos estratégicos "es un asunto de seguridad nacional" y comparó a las empresas con los Estados: "Una empresa es un país. Debe desarrollar su propia estrategia de defensa, con liderazgo, formación y capacidad de respuesta".

Planteó que las empresas y los Estados "tienen que ser defendidos con un criterio de estrategia nacional". Subrayó que "es fundamental que los actores trabajen todos conjuntamente", porque "la ciberseguridad es una gran herramienta que permite el trabajo en equipo y la gestión de crisis". Explicó que estas situaciones "implican formación, tecnología, capacidad, liderazgo y decisión", cualidades que, afirmó, "son las que llevan a un país a ser soberano o a una empresa a ser soberana".

Advirtió que "estamos en una batalla global y que el que diga que no estamos en guerra no dice la verdad, porque el conflicto es permanente y la elasticidad del combate es continua y activa". Describió el nuevo escenario internacional: "Ya no asistimos solo a guerras convencionales; vivimos guerras asimétricas, guerras económicas, ambientales, de divisas, de deuda o de sanidad. Cualquier herramienta es buena para generar una ventaja contra el contrincante".

Gómez Bule identificó en el anonimato digital una de las mayores ventajas de los atacantes y vinculó esa amenaza con la criminalidad organizada y económica. Recordó la importancia del principio *know your customer* y la necesidad de "una cultura de seguridad, de defensa y de inteligencia que permita identificar los riesgos a los que nos enfrentamos". Concluyó que "estamos en una guerra fría cibernética permanente. La tecnología afecta a las empresas, a los ciudadanos y a los gobiernos. Todos debemos preguntarnos para qué y hacia dónde queremos dirigir nuestras acciones".

Para Gómez Bule, la soberanía tecnológica equivale a independencia y libertad: "Dependemos tecnológicamente, y la soberanía tecnológica de un país es exactamente igual a libertad". Por eso, defendió la necesidad de fortalecer la autonomía tecnológica de las empresas para proteger los intereses estratégicos nacionales.

Al abordar el impacto económico de la inseguridad digital, subrayó que "el coste de la no ciberseguridad alcanzará los diez billones de dólares este año y podría duplicarse el próximo; es un negocio extraordinariamente rentable para el delito organizado".

Desarrolló luego un eje central sobre la cultura de inteligencia corporativa, planteando que "la ciberseguridad no es solo tecnología: es estrategia, defensa e influencia". Propuso entenderla como una disciplina transversal que involucra lide-

razgo, decisión y cooperación entre actores públicos y privados. “La seguridad se hace entre todos. Todos formamos parte de esta telaraña que genera estabilidad y riqueza en nuestros países”, sostuvo.

En uno de los pasajes más citados de su ponencia, afirmó que “el campo de batalla somos todos nosotros; incluso un directivo puede ser el punto de entrada de un ataque dirigido, planificado y financiado con grandes recursos”. Por eso, insistió en la necesidad de fortalecer las capacidades de análisis y contrainteligencia: “Tenemos que pensar como el contrincante, analizar su conducta y anticipar sus movimientos”.

A partir de allí, introdujo una reflexión sobre el pensamiento complejo y abstracto como base de la gestión moderna del riesgo. Sostuvo que “el pensamiento uniforme en un equipo es peligroso; el pensamiento agregado y abstracto, en cambio, enriquece la mirada y permite anticipar escenarios”. En su visión, la ciberseguridad requiere “ver la película completa, no una sola escena”, y asumir que “el riesgo no desaparece: se transforma”. Defendió la integración de la teoría del caos y la incertidumbre en la planificación corporativa, recordando que “no sabemos cuándo seremos objetivo, pero lo seremos; debemos convivir con la incertidumbre y prepararnos para adaptarnos”.

Desde el punto de vista corporativo, enfatizó que la ciberseguridad debe integrarse al negocio: “Si la seguridad no va

alineada con el negocio, no sirve". Planteó que el director de seguridad será "el responsable de la gobernanza de la compañía y de su gestión de riesgos", ya que los ataques pueden comprometer tanto los activos digitales como la reputación y la continuidad operativa.

Definió la ciberresiliencia como "la capacidad de una empresa para recuperar su actividad en un tiempo prudente después de un ataque", recordando que "cuando se entra en una crisis, nunca se sale igual". Por ello, propuso aprender haciendo (*learning by doing*) a través de simulaciones reales que preparen a las organizaciones para gestionar incidentes complejos.

Finalmente, subrayó la dimensión ética y colectiva de la seguridad: "Tenemos que conseguir gente leal y demostrar lealtad a nuestras organizaciones. Nadie puede afrontar el problema solo". Cerró con una advertencia estratégica: "La ciberseguridad empresarial no puede desvincularse de la seguridad nacional ni de la protección de los ciudadanos".

El moderador coincidió con esta mirada, destacando la necesidad de "hacer que atacar a una empresa no sea rentable para el adversario y de mantener una capacidad disuasoria creíble".

A continuación, Pablo Pi, especialista argentino en seguridad informática, reforzó la idea de la ciberseguridad como "pilar estratégico de las organizaciones", explicando que antes era

un tema limitado al área de TI o al sector financiero, pero que hoy "todas las organizaciones y todas las personas son responsables de protegerse en el mundo digital".

Pi insistió en que la ciberseguridad debe asumirse como inversión y no como gasto, ya que "invertir en seguridad es proteger la reputación, el negocio y la confianza de los clientes". Destacó la importancia de alinear los proyectos de seguridad con los objetivos corporativos, señalando que "la organización no tiene como objetivo hacer ciberseguridad, sino ganar dinero; por eso, los proyectos de seguridad deben apoyar la rentabilidad y la continuidad del negocio".

En relación con las amenazas, explicó que "el *ransomware* sigue siendo el principal riesgo", y que las nuevas variantes combinan el cifrado con la exfiltración de datos y ataques de denegación de servicio (RDoS). Subrayó que "los delincuentes han encontrado en esto un modo estable y lucrativo de obtener dinero".

También se refirió a la evolución del *phishing*, que "ya no es un correo con errores ortográficos; hoy son ataques personalizados, reforzados con inteligencia artificial y *deep fakes* que imitan voces y rostros para engañar incluso a directivos".

Presentó casos reales como el de Mercado Libre, que logró contener un ataque mediante detección temprana y comunicación transparente; el de Maersk, que perdió millones de dóla-

res tras NotPetya pero se recuperó por su planificación de respaldo distribuido; y el de Target, que sufrió durante tres años el robo de tarjetas de crédito a través de su cadena de suministro. "La detección temprana es clave: cuanto antes sepamos que algo ocurre, antes podremos reaccionar", subrayó.

Pi propuso un enfoque integral basado en personas, procesos y tecnología, afirmando que "el eslabón más débil sigue siendo el ser humano; podemos tener los mejores sistemas, pero todo se pierde con un solo clic". Por ello, destacó la necesidad de fomentar una cultura de seguridad sostenida por la capacitación permanente y el compromiso del liderazgo.

Explicó que "un usuario entrenado detecta e informa un incidente más rápido que uno que no lo está", y recomendó "trasladar las buenas prácticas laborales al ámbito personal: usar contraseñas robustas, activar el doble factor de autenticación y evitar repetir claves en distintos servicios".

Por último, propuso medidas técnicas y organizativas para fortalecer la resiliencia: "segmentar las redes, realizar copias de seguridad cifradas, probar periódicamente su restauración y adoptar soluciones basadas en inteligencia artificial para acelerar la detección de anomalías".

Cerró destacando el valor de la comunicación y la formación: "No basta con saber qué es un *malware*, hay que saber explicar sus consecuencias a quienes toman decisiones. La co-

municación efectiva con la dirección es tan importante como la tecnología".

Las perspectivas abordadas en los paneles anteriores —formación, gestión estatal y estrategia empresarial— ponen de manifiesto la complejidad del escenario actual de la ciberseguridad. Cada dimensión aporta elementos esenciales, pero ninguna resulta suficiente por sí sola para dar respuesta a los desafíos del entorno digital.

Esta interdependencia plantea la necesidad de avanzar hacia modelos de articulación que integren capacidades, conocimientos y recursos. La convergencia entre actores se vuelve indispensable para construir respuestas efectivas, sostenibles y adaptativas frente a amenazas en constante evolución.

Capítulo 5. Conversatorio de Cierre

Articulando para proteger. Desafíos compartidos

Introducción

El entorno digital contemporáneo se caracteriza por una creciente interdependencia entre sistemas, organizaciones y sectores. En este contexto, la ciberseguridad deja de ser un problema individual para convertirse en un desafío colectivo que requiere articulación, cooperación y una visión compartida del riesgo.

Las amenazas actuales –cada vez más sofisticadas, automatizadas y potenciadas por tecnologías como la inteligencia artificial– no distinguen fronteras ni jurisdicciones. Afectan simultáneamente a gobiernos, empresas y ciudadanos, ponien-

do en evidencia la necesidad de respuestas coordinadas y de marcos de actuación comunes que permitan abordar la complejidad del problema.

La experiencia internacional demuestra que la adopción de principios, estándares y buenas prácticas compartidas contribuye a generar lenguajes comunes, facilitar la cooperación y mejorar la capacidad de respuesta ante incidentes. Sin embargo, su efectividad depende de la capacidad de los actores para trabajar de manera conjunta, compartir información relevante y construir confianza.

Este espacio de cierre invita al lector a integrar las perspectivas presentadas en los paneles anteriores, reconociendo que la formación, la gestión pública y la estrategia empresarial son dimensiones interdependientes de un mismo fenómeno. La protección del entorno digital exige no solo capacidades técnicas, sino también liderazgo, gobernanza y una cultura de seguridad extendida.

Más allá de los desafíos, la ciberseguridad representa también una oportunidad: la posibilidad de fortalecer capacidades institucionales, impulsar la innovación y construir sociedades más resilientes. Este conversatorio refleja esa visión, destacando que la única respuesta viable frente a un entorno de amenazas en constante evolución es la construcción

de ecosistemas colaborativos basados en el conocimiento, la confianza y la acción coordinada.

Desarrollo

Moderador: Héctor Villalba
Participantes: Juan Antonio Gómez Bule, Pablo Pi, Coronel Fernando Moure Colón.
Cierre Institucional: José Luis Parisí (Ministerio de Seguridad de la Nación)

El simposio culminó con un espacio de diálogo abierto, diseñado para identificar desafíos comunes y promover sinergias entre los sectores público, privado y académico. El Rector de la UGD, Ing. Luis Lichowski, introdujo este segmento destacando que el objetivo no era solo intercambiar opiniones, sino "captar necesidades" y establecer un "punto de partida" para futuras líneas de trabajo conjunto.

El intercambio se estructuró a partir de inquietudes planteadas por los asistentes y ejes temáticos transversales:

Gestión de dispositivos y seguridad corporativa

Se abordó la problemática del *Bring Your Own Device* (BYOD). El Lic. Pablo Pi explicó que, si bien la incorporación de

dispositivos personales en el ámbito laboral representa un riesgo, existen soluciones de software (MDM) que permiten crear "compartimientos estancos" para aislar la información corporativa, aplicando políticas de cifrado y seguridad sin comprometer la privacidad personal del usuario.

Evolución y mutación de las amenazas

Uno de los puntos centrales fue la naturaleza cambiante de los ataques. Ante la consulta sobre la adaptación a riesgos mutantes, los especialistas coincidieron en que los ataques son cada vez más "polimórficos" y diseñados para distraer a la defensa. Juan Antonio Gómez Bule señaló que el objetivo final del atacante es a menudo "despistar" mediante señuelos, mientras que la tecnología actual hiperacelera estas herramientas. Se concluyó que la defensa debe evolucionar hacia el uso de Inteligencia Artificial para detectar patrones anómalos y responder a la misma velocidad que los atacantes.

La postura defensiva y el marco legal

Se debatió sobre la capacidad de respuesta de las organizaciones ante un ataque. El coronel Moure Colón y Gómez Bule aclararon que, en el contexto actual, la postura es fundamentalmente defensiva ("ciberresiliencia") debido a las limitaciones le-

gales y geopolíticas. El "contraataque" por parte de una empresa o institución podría escalar conflictos o vulnerar derechos, por lo que el uso legítimo de la fuerza permanece en manos del Estado. Sin embargo, se reconoció la existencia de una "zona gris" normativa donde la tecnología avanza más rápido que la legislación.

Impacto social y transversalidad

El diálogo se abrió a reflexiones sobre el impacto de la ciberseguridad en la vida cotidiana y la infraestructura crítica. Se analizó cómo la dependencia digital ha convertido a la conectividad en un recurso tan vital como el oxígeno, y cómo la falta de preparación ante incidentes (como apagones o caídas de servicios) revela la fragilidad de las sociedades modernas. Se hizo hincapié en la necesidad de "resiliencia emocional" y educación digital para enfrentar la sensación de vulnerabilidad que genera la pérdida de activos digitales, tanto para una empresa como para un ciudadano común.

Palabras Finales y Proyección a Futuro

El cierre formal del evento estuvo a cargo del Sr. José Luis Parisí, Director Nacional de Formación y Desarrollo Profesional del Ministerio de Seguridad de la Nación. En su alocución, Parisí

revalidó el compromiso de la cartera nacional con la cooperación internacional y el trabajo federal.

Destacó que la diversidad de actores presentes en el simposio –instituciones educativas internacionales, fuerzas federales, policías provinciales, universidades, organismos internacionales como la OEI y el sector privado– es la clave para enfrentar una problemática que "no respeta fronteras ni jurisdicciones".

Como conclusión general, se estableció que la "ciberseguridad es una oportunidad educativa y profesional de futuro". Las autoridades coincidieron en que la única vía para proteger los intereses de los ciudadanos y los sistemas de vida nacionales es la "producción de conocimiento pertinente" y "la gestación de redes de cooperación" que integren la agilidad del sector privado, la capacidad regulatoria del Estado y la excelencia académica de las universidades.

El evento finalizó con la reafirmación de que "Horizontes de la Ciberseguridad" no fue un evento aislado, sino el inicio de una agenda de trabajo mancomunada para la construcción de soberanía y seguridad en el entorno digital.

A lo largo de este recorrido, se ha puesto en evidencia que la ciberseguridad no es únicamente un problema tecnológico, sino un fenómeno complejo que involucra dimensiones educativas, institucionales, económicas y sociales. La construcción

de entornos digitales seguros requiere una visión integrada, capaz de articular formación, regulación, estrategia y cultura organizacional.

Este enfoque sistémico no solo permite comprender mejor los desafíos actuales, sino también identificar oportunidades para fortalecer capacidades y promover la cooperación entre actores. En un contexto donde la incertidumbre es una constante, la articulación se consolida como el principal mecanismo para construir resiliencia.

Sobre los expositores, moderadores y coordinadores

CARLOS PÉREZ RASETTI

Profesor en Humanidades, especialidad Letras por la Universidad Nacional del Sur. Es profesor titular e investigador de la Universidad Nacional de la Patagonia Austral, de la que fue el primer rector y donde dirige la Especialización en Gobierno y Gestión de la Universidad (Interinstitucional, con la Universidad Nacional del Centro de la Provincia de Buenos Aires) dirigida a los nodocentes de las universidades públicas nacionales. Es director de la Maestría en Gestión y Evaluación de la Educación Superior en la Universidad Gastón Dachary y director de la Especialización en Docencia Universitaria de la Universidad Nacional de José C. Paz. Integró el directorio de la CONEAU,

fue Secretario Ejecutivo de los Consejos Regionales de Planificación de la Educación Superior (Ministerio de Educación), Subsecretario de Formación en el Ministerio de Defensa, y de Planeamiento y Formación en el Ministerio de Seguridad, respectivamente. Fue Coordinador de la Red Iberoamericana de Indicadores de Educación Superior (Red IndicES) desde su fundación en 2016 hasta 2019, actualmente integra el Grupo de Expertos de la Red. Dirigió el Programa de Mejoramiento de la Formación en Seguridad para la OEI (2017-2019). Asesora a varias universidades en temas de gestión, organización institucional y calidad. Es autor de numerosas publicaciones sobre Educación Superior, y dictó cursos de posgrado y conferencias en diversas universidades de Argentina y América Latina.

PAULO FALCÓN

Es abogado, especialista en Ciencias Políticas con Proyección en Argentina y América Latina, Especialista en Docencia Universitaria, Magíster en Gestión de la Educación Superior y Magíster en Diplomacia y Política Exterior, así como Doctor en Humanidades. Actualmente se desempeña como Rector de la Universidad CAECE en Buenos Aires, Argentina. Es docente regular, investigador categorizado en el sistema universitario argentino y profesor invitado en diversas universidades del extranjero. Cuenta con una destacada trayectoria pública y académica,

habiendo ejercido diferentes cargos de gestión en universidades nacionales y ocupado el puesto de Director Nacional de Gestión Universitaria del Ministerio de Educación de la Nación. En el ámbito de la cooperación internacional, integra el Consejo Directivo de la Asociación de Universidades de América Latina y el Caribe para la Integración (AUALCPI), es consultor especial del Grupo de Cooperación Internacional de las Universidades Brasileñas (GCUB) y miembro del Consejo de la International Student Participation Network (ISPN). Su labor con la UNESCO destaca por haberse desempeñado como miembro del Consejo de Gobierno del IESALC y como coordinador de eje en la Conferencia Regional de Educación Superior (CRES+5). Asimismo, conduce y participa activamente en procesos de creación, evaluación y acreditación de universidades en América Latina y Estados Unidos, y se encuentra nominado para integrar el Consejo de Dirección de la United Nations University (ONU). Además de su amplia labor institucional, es autor de libros y publicaciones, y participa como habitual columnista en medios de comunicación abordando temáticas de educación y universidad.

FERNANDO MOURE COLÓN

Coronel de la Guardia Civil de España (en reserva con destino), Doctor y Máster Universitario en Seguridad por la Universidad Nacional de Educación a Distancia (UNED), y gradua-

do en Derecho por la Universidad Antonio de Nebrija. Además de abogado, es ingeniero en seguridad. Posee una vasta trayectoria de liderazgo, habiendo sido Director del Centro Universitario de la Guardia Civil (CUGC) entre 2018 y 2020 (y subdirector desde su fundación en 2012), así como Director de la Academia de Guardias de la Guardia Civil. Ha sido observador policial y de derechos humanos de la ONU, y es autor de libros sobre seguridad global.

RAFAEL HORACIO OSUDAR

Abogado, escribano, Especialista en Derecho Procesal y Magíster en Alta Dirección de Seguridad, actualmente Maestrando en Gestión y Evaluación de la Educación Superior. Se desempeña como Secretario Académico del Instituto Universitario de Seguridad de la provincia de Misiones, profesor en la Universidad Gastón Dachary y Secretario del Juzgado de Paz de Itaembé Guazú. Su área de especialización e investigación abarca el Derecho, la Seguridad y la Cooperación Judicial. Cuenta con amplia experiencia en gestión universitaria y participa activamente en asociaciones académicas, siendo Director Ejecutivo de la Revista Jurídica del Nordeste Argentino (ISSN 2545-6423, IJ Editores) y Coordinador Académico de la Maestría en Seguridad de la Universidad Gastón Dachary.

ALAN MARTÍN NESSI

Abogado egresado de la Universidad de Buenos Aires (1993), con un posgrado en Derecho Penal por la Universidad de Palermo (1999). Es Secretario Académico del Instituto Universitario de Seguridad de la Ciudad Autónoma de Buenos Aires, Secretario de Fiscalía de Cámara del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires y coordinador de la Fiscalía Especializada en Ciberfraudes. Es funcionario judicial en materia criminal desde 1990 a la fecha. Cuenta con una amplia trayectoria desempeñando roles claves como Director del Cuerpo de Investigaciones Judiciales - Policía Judicial del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires (2009–2014), Coordinador del Observatorio Metropolitano de Seguridad Pública del Instituto Superior de Seguridad Pública (2009-2017) y Secretario Académico del Instituto Superior de Seguridad Pública (2020-2024). Asimismo, fue Presidente de la Asociación Civil Unidos por la Justicia (2010-2019), Asesor de la Subsecretaría de Justicia y Política Criminal del Ministerio de Justicia y Derechos Humanos de la Nación (2018-2019) y Asesor del Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires (2014-2018). Además, actúa como consultor experto del BID y del Banco Mundial en distintos programas para la mejora del sistema de Justicia y Seguridad, y es profesor

universitario en la Universidad Católica Argentina, el Instituto Superior de Seguridad Pública y la American Bar Association.

DANIELA DUPUY

Se desempeña como Fiscal Penal especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires. Es además la directora del Observatorio de Ciberdelitos (OSEDIC) de la Universidad Austral. Cuenta con más de diez años de experiencia dedicada al cibercrimen, habiéndose convertido en el año 2013 en la fiscal de la primera Fiscalía especializada en la materia tanto en Argentina como en Latinoamérica.

MIGUEL KESSLER

Es fiscal especializado en ciberfraude en la Ciudad Autónoma de Buenos Aires y titular de la FSEC (Fiscalía Especializada en Ciberfraudes). Combina su trabajo judicial con el ámbito académico, ya que ejerce como docente en el Instituto Universitario de Seguridad y en la Universidad Católica Argentina.

JULIÁN REALE

Es abogado y ejerce como Asesor Legal y Coordinador de la Dirección de Ciberdelitos y Asuntos Cibernéticos del Ministerio de Seguridad de la Nación de Argentina. Es Magíster en Derecho de la Ciberseguridad y Entorno Digital por la Universidad de León (España) y cuenta con una certificación como delegado de

Protección de Datos Personales otorgada por la Agencia Española. Además, se desempeña como Director de la Diplomatura en Análisis Forense Digital y formador de Fuerzas y Cuerpos de Seguridad para el Instituto de Ciberseguridad de España.

PABLO PI

Es Licenciado en Informática y especialista en ciberseguridad argentino, que acumula más de veinticinco años de experiencia en tecnologías de la información. Actualmente trabaja en la seguridad de la información de EMOVA (la red de subterráneos de Buenos Aires) y se desempeña como Coordinador de Seguridad Informática en el sector privado, combinando estos roles con la docencia universitaria. Un aspecto para destacar en su nuevo perfil es que posee prestigiosas certificaciones internacionales como CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control) y CISSP (Certified Information Systems Security Professional), y es miembro activo de asociaciones reconocidas como ISACA (Information Systems Audit and Control Association) y (ISC)² International Information System Security.

JUAN ANTONIO GÓMEZ BULE

Es un destacado emprendedor español que se desempeña como Presidente de Walhalla Data Center Services en Valencia y como Head of Intelligence de Opinion Makers. Es

presidente de dos compañías y promotor de la seguridad que ha fundado empresas tanto de telecomunicaciones como de ciberseguridad. Aporta más de veinticinco años de experiencia en el sector colaborando, en conjunto con fuerzas y cuerpos de seguridad del Estado, como la Guardia Civil.

SOBRE LOS COORDINADORES

DIEGO ÁNGELO BOLATTI

Es Ingeniero en Sistemas de Información, Magíster en Administración de Negocios y doctorando en Ciencias Informáticas por la Universidad Nacional de La Plata (UNLP). Se desempeña como docente investigador en la Universidad Tecnológica Nacional (UTN), Facultad Regional Resistencia y es **miembro del Comité de Seguridad de la Información de la UTN**, participando en la definición y revisión de políticas institucionales de ciberseguridad.

Su área de especialización se centra en **ciberseguridad, seguridad de la información, gobernanza de TIC, Internet de las Cosas (IoT)** y **redes de próxima generación**, con especial énfasis en el desarrollo de marcos de referencia, controles y arquitecturas de seguridad para entornos empresariales y académicos. Dirige y participa en **proyectos de investigación y**

desarrollo financiados por la Universidad Tecnológica Nacional, orientados a la ciberseguridad en redes IoT, detección de anomalías y gestión de riesgos tecnológicos.

Cuenta con una amplia trayectoria como **revisor académico** en congresos y conferencias nacionales e internacionales, y ha participado como autor y coautor en publicaciones científicas, reportes técnicos y contribuciones a estándares internacionales. Se destaca su colaboración con la **Unión Internacional de Telecomunicaciones (ITU-T)**, en el desarrollo de reportes técnicos y propuestas de estándares, y con el **Center for Internet Security (CIS)** como colaborador en documentos y plantillas de políticas alineadas a los CIS Controls.

En el ámbito profesional, se desempeña como **asesor técnico en ciberseguridad** para organizaciones públicas y privadas, incluyendo entidades financieras y organismos gubernamentales. Su trayectoria integra investigación aplicada, docencia universitaria y práctica profesional, con foco en la protección de activos de información, la gestión de riesgos y la resiliencia digital.

HÉCTOR VILLALBA

Es Licenciado en Sistemas de Información por la Universidad Gastón Dachary y Máster en Ciberseguridad por la European Business School (CEUPE)

En el ámbito académico se desempeña como Profesor Universitario Titular en la Universidad Gastón Dachary, donde además es Coordinador de la Diplomatura en Gestión de la Ciberseguridad y Protección Digital y ejerce como profesor en el Instituto Universitario de Seguridad de la provincia de Misiones

Como especialista en ciberseguridad y gestión de infraestructuras críticas, actualmente trabaja en KIU System Solutions.

Cuenta con una sólida trayectoria profesional asumiendo roles de liderazgo en seguridad, configuración, operaciones y digitalización en entornos corporativos de alta exigencia, tales como TS Group, Banco Macro, Atos y Siemens Itron

Adicionalmente, posee certificaciones internacionales clave, destacándose como Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2022 certificado por TÜV Rheinland, orientando su práctica profesional a la protección integral de los sistemas, la gestión de controles de acceso y el cumplimiento de estándares internacionales.