



CLAUSTRO PLENO ORDINARIO 2026

PONENCIA

Sebastián Berríos González

Jefe de Laboratorios e Infraestructura, Esc. de Ingeniería

Buenos días.

Quisiera comenzar saludando cordialmente a las autoridades universitarias, académicos, funcionarios y estudiantes que participan en este Claustro Pleno.

La Pontificia Universidad Católica de Valparaíso ha construido, durante más de noventa años, una trayectoria de excelencia académica, investigación e innovación, consolidándose como una institución de reconocido prestigio a nivel nacional e internacional. Su aporte trasciende la formación de profesionales, contribuyendo al avance científico, tecnológico y social mediante la generación de conocimiento, la transferencia tecnológica y la colaboración con instituciones públicas, privadas y académicas, fortaleciendo así el desarrollo sostenible y la competitividad del país en un contexto global. Sin embargo, hoy enfrentamos un escenario distinto al de hace apenas algunos años: la transformación digital ha modificado profundamente la manera en que enseñamos, investigamos, administramos nuestras instituciones y nos relacionamos con la sociedad. Esta transformación, sin embargo, trae consigo un desafío que muchas veces pasa inadvertido: la seguridad del mundo digital.

Actualmente, las universidades no solo forman profesionales; administran infraestructura crítica, desarrollan investigación de alto impacto, almacenan enormes volúmenes de datos personales y científicos, y participan en proyectos nacionales e internacionales que requieren elevados niveles de confianza digital. En consecuencia, la ciberseguridad ha dejado de ser una responsabilidad exclusiva de las áreas de informática para convertirse en un componente estratégico que garantiza la continuidad operacional, protege el conocimiento generado por la universidad y preserva la confianza de la comunidad universitaria y de la sociedad.



CLAUSTRO PLENO ORDINARIO 2026

“Viviendo en la **verdad** y en el **amor**” (Ef. 4, 15)

Las cifras confirman esta realidad. Según un informe de Microsoft, los ataques dirigidos contra universidades y establecimientos educacionales aumentaron un 63 % entre 2023 y 2025. El ransomware, el robo de credenciales, el phishing y la sustracción de propiedad intelectual afectan con creciente intensidad a instituciones de educación superior en todo el mundo.

Este tampoco es un desafío ajeno a nuestra realidad nacional. Chile avanza decididamente hacia una institucionalidad más sólida en materia de ciberseguridad y protección de datos,

exigiendo mayores capacidades de gestión de riesgos, controles verificables y protocolos claros de respuesta ante incidentes a todas las organizaciones que administran información sensible. Nuestra Universidad resguarda investigación científica, información clínica, bases de datos de estudiantes y múltiples proyectos estratégicos. Por ello, cumplir con estos estándares no debe entenderse únicamente como una exigencia normativa, sino como una responsabilidad institucional con el conocimiento, las personas y la sociedad.

La pregunta, entonces, no es si debemos fortalecer la ciberseguridad, sino cómo construiremos una universidad más resiliente, capaz de proteger su patrimonio digital, garantizar la continuidad de sus funciones esenciales y seguir cumpliendo su misión de formación, investigación y vinculación con el medio frente a un entorno de amenazas cada vez más complejo. En este escenario, la inteligencia artificial emerge como una herramienta fundamental para fortalecer las capacidades de prevención, detección y respuesta frente a los desafíos de la seguridad digital.

Frecuentemente hablamos de la inteligencia artificial como una tecnología orientada a mejorar la productividad o automatizar procesos. Sin embargo, desde la perspectiva de la ciberseguridad, representa mucho más que eso. Permite detectar ataques en tiempo real, identificar comportamientos anómalos antes de que produzcan daños, analizar millones de eventos de seguridad en cuestión de segundos y asistir a los equipos humanos en la respuesta frente a incidentes.

Pero también incorpora nuevos riesgos. Los ciberdelincuentes ya utilizan inteligencia artificial para desarrollar campañas de phishing más sofisticadas,



CLAUSTRO PLENO ORDINARIO 2026

“Viviendo en la **verdad** y en el **amor**” (Ef. 4, 15)

suplantar la identidad de académicos y autoridades mediante voces e imágenes sintéticas, generar contenido falso prácticamente indistinguible del real, automatizar ataques y descubrir vulnerabilidades con una velocidad sin precedentes. Estamos entrando en una nueva etapa en la que la inteligencia artificial potenciará tanto las capacidades de defensa como las de ataque.

Por ello, la verdadera ventaja competitiva no radicará únicamente en disponer de mejores tecnologías, sino en formar profesionales capaces de comprender estos nuevos escenarios y desarrollar soluciones responsables, seguras y éticamente sustentables. La Pontificia Universidad Católica de Valparaíso tiene una oportunidad única para liderar este proceso.

No solo formando especialistas en ciberseguridad, sino promoviendo una auténtica cultura de seguridad digital en todas las disciplinas. Un abogado deberá comprender los desafíos regulatorios de la inteligencia artificial; un ingeniero diseñará infraestructuras resilientes; un profesional de la salud protegerá información clínica altamente sensible; y un investigador tendrá la responsabilidad de resguardar la propiedad intelectual de sus descubrimientos. La ciberseguridad ya no pertenece exclusivamente a la informática: constituye una competencia transversal para toda la universidad.

Estoy convencido de que la PUCV posee el talento humano, la capacidad científica y el compromiso institucional necesarios para consolidarse como un referente nacional e internacional en investigación, formación e innovación en ciberseguridad. Desde la Escuela de Ingeniería Informática renovamos nuestro compromiso de seguir impulsando iniciativas de investigación, transferencia tecnológica, vinculación con el medio y formación especializada que permitan enfrentar los desafíos de la transformación digital desde una perspectiva segura, ética y sostenible. Sin embargo, este desafío no corresponde únicamente a una escuela ni a un grupo de especialistas; es un desafío institucional que requiere el compromiso y la participación de toda la comunidad universitaria.

Proteger nuestro patrimonio digital no es únicamente una tarea tecnológica; es una responsabilidad con la historia de nuestra Universidad, con las personas que



CLAUSTRO PLENO ORDINARIO 2026

“Viviendo en la **verdad** y en el **amor**” (Ef. 4, 15)

integran nuestra comunidad y con las futuras generaciones que confiarán en la Pontificia Universidad Católica de Valparaíso para formarse, investigar e innovar. La resiliencia digital que construyamos hoy será la base sobre la cual preservaremos nuestro conocimiento, fortaleceremos la confianza institucional y continuaremos aportando al desarrollo de Chile y de la comunidad internacional.

Las universidades han sido históricamente las guardianas del conocimiento. En el siglo XXI, debemos ser también las guardianas de la confianza digital. Porque la transformación digital sin ciberseguridad genera vulnerabilidad; la inteligencia artificial sin ciberseguridad incrementa el riesgo; y una universidad que aspira a liderar el futuro debe hacer de la ciberseguridad un pilar estratégico para proteger el conocimiento, impulsar la innovación y servir responsablemente a la sociedad.

Muchas gracias.