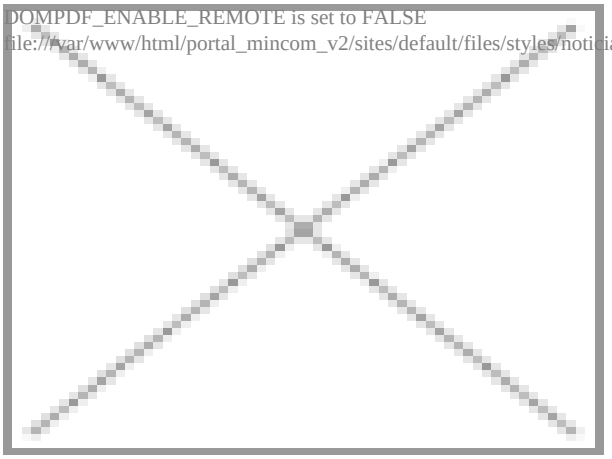
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/sigestic-1-580x435_1.jpg



Fuente:
Tomando de Cubadebate

La sesión pre-taller como antesala a Sigestic 2025, se está desarrollando durante los días 20 y 21 de mayo. Bajo el tema central “Tecnologías de hoy para un futuro sostenible”, este espacio reúne a especialistas en informática y comunicaciones para abordar los desafíos actuales y las oportunidades de innovación en el sector.

El evento contará con un segmento de carácter científico, en el que participarán líderes de opinión y expertos de Cuba, Colombia, Chile, México, Argentina, Canadá, España y Rusia. Entre los temas a debatir se incluyen la inteligencia artificial y la ciencia de datos, el desarrollo de software seguro en la era digital, las infraestructuras críticas, la gestión de procesos y la innovación.

Uno de los proyectos expuestos, titulado “¿Metodologías o sentido común? Equilibrio perfecto en proyectos de TI”, de Alejandro Ruiz Douglas, abordó la importancia de encontrar un balance adecuado entre el uso riguroso de metodologías formales y la aplicación del sentido común en la gestión de proyectos de tecnologías de la información.

El contenido se enfocó en destacar las causas más comunes del fracaso de los proyectos, como la falta de objetivos claros, deficiencias en la comunicación, escaso compromiso de los interesados, estimaciones poco realistas de tiempo y presupuesto, recursos inadecuados, cambios inesperados en el alcance del proyecto y riesgos no previstos. Estos elementos reflejan las complejidades prácticas que se enfrentan en el ciclo de vida de un proyecto.

La presentación también subrayó una serie de buenas prácticas que son esenciales para el éxito de los proyectos. Entre ellas se encuentra la elaboración del Acta de Constitución del Proyecto, donde se definen elementos clave como los objetivos, limitaciones, calendario, presupuesto, interesados y el enfoque a seguir.

Asimismo, se enfatizó la necesidad de un chequeo periódico de las actividades planificadas, acompañado de un Plan de Gestión de Riesgos. “Este monitoreo continuo debe centrarse en verificar si se están cumpliendo los objetivos, si el proyecto se mantiene dentro del alcance y presupuesto previstos, y en qué estado se encuentra la comunicación con los interesados y el control de cambio”, afirmó el expositor.

Otra presentación realizada fue “Seguridad Inteligente: IA como Motor de Cambio en la Videovigilancia”, de Ernesto A. Riccardi Quintana, que abordó el papel transformador de la inteligencia artificial en los sistemas modernos de videovigilancia.

Enfatizó en cómo esta tecnología está revolucionando el enfoque tradicional de la seguridad, al pasar de sistemas pasivos de registro a soluciones proactivas que previenen y analizan incidentes en tiempo real.

A su vez, planteó una evolución histórica de la videovigilancia, dividida en tres etapas: la era análoga, caracterizada por grabaciones básicas y revisión manual; la era digital, que mejoró la calidad de imagen y el almacenamiento pero mantenía dependencia de supervisión humana; y la era inteligente, donde la IA permite que los sistemas actúen como “cerebros”, analizando patrones y anticipando situaciones.

La inteligencia artificial en este contexto se explica a través de tres componentes principales: visión computacional, machine learning y análisis predictivo. Estos elementos permiten que los sistemas identifiquen objetos y situaciones específicas, aprendan de datos históricos y anticipen comportamientos para emitir alertas antes de que ocurran incidentes.

Entre las funcionalidades principales de la IA en seguridad se incluyen la detección de movimientos anómalos, el reconocimiento de objetos como armas o paquetes abandonados, las alertas automatizadas al personal de seguridad, y el análisis de comportamiento que permite evaluar acciones sospechosas antes de que se materialicen como amenazas.

Riccardi Quintana mencionó, además, diversas aplicaciones gratuitas de IA aplicadas a la videovigilancia, entre ellas: detección de rostros, detección de personas, vehículos, ocupación, cambios de escena, detección de no uso de mascarillas, y aprendizaje en sitio, lo que demuestra el alcance actual de estas tecnologías.

“Entre los resultados reales del uso de la videovigilancia con IA, es notable una reducción del 42% en robos en comercios minoristas, un 65% de incremento en la detección de comportamientos sospechosos en bancos y un ahorro del 30% en personal de vigilancia en instalaciones grandes, lo cual evidencia su efectividad”, confirmó Riccardi.

Por otra parte, destacó también el proyecto “Protección y seguridad: La importancia de Puesta a Tierra”, realizado por Ernesto Jesús Pérez del Sol, quien abordó de manera técnica y detallada la función crítica que desempeña el sistema de puesta a tierra en la seguridad eléctrica de las instalaciones.

Se realizaron también otras presentaciones como: HPC: El cerebro colectivo que resuelve lo imposible, de Fernando de la Nuez; Pentesting como seguridad proactiva en entornos de Directorio Activo, elaborada por Reiluis Valentín Soueysch; Orquestando el caos: DevOps y el sueño de la automatización total de José O. Morales Rodríguez; Dominando la fibra óptica: aprende a fusionar y diseñar redes de alta velocidad, de Alexis Pita Labrada y ¿Estamos perdiendo la guerra por privacidad? Desafíos globales en protección de datos, expuesta por Kevin Cogle.

Asimismo, “Ransomware bajo la lupa: estrategias clave para proteger entornos industriales”, de Abel Tamayo León, y “De la crisis al ‘felices para siempre’: una historia de planes y respuestas”, de María Carla Silveira. Ambas apuntaron hacia el fortalecimiento de la resiliencia cibernética en sectores sensibles, abordando tácticas preventivas y de respuesta ante incidentes.

Estas temáticas completan una agenda diversa que combina innovación, ciberseguridad, automatización e inteligencia estratégica.

En esta primera jornada se ha puesto de manifiesto el valor de los espacios colaborativos donde confluyen el conocimiento técnico, la experiencia práctica y la visión estratégica. Los participantes han tenido la oportunidad de compartir ideas, herramientas y enfoques que abordan desde la automatización de procesos hasta los desafíos más complejos de la ciberseguridad, sin dejar de lado el papel creciente de la inteligencia artificial en la toma de decisiones y la protección de entornos críticos.

Esta antesala confirma que Sigestic 2025 será un espacio clave para seguir construyendo soluciones reales a los retos que plantea el futuro digital.