Proyectos de investigación vigentes

Título de proyecto	**Gestión Dinámica de Políticas de Seguridad para controladores SDN en una Red Híbrida Universitaria a través de un Agente Autónomo basado en IA**
Código UTN	SFSITC1158
Director/a	**CALLONI, Juan Carlos**
Dirección de correo	jccalloni@gmail.com
Codirector/a	**YUAN, Rebeca**
Dirección de correo	rebecayuan@gmail.com
Desde	01/04/2026
Hasta	31/03/2029
Resumen técnico del PID	En la última década, el crecimiento del tráfico y la demanda de calidad han superado la capacidad de las arquitecturas de red convencionales, las cuales resultan rígidas y difíciles de adaptar. Frente a este escenario, surge el modelo SDN (Software Defined Networking), que introduce flexibilidad y dinamismo a las redes [1]. Las SDN permiten programar el comportamiento de la red a través de un controlador central, separando el plano de control del hardware físico. Esto habilita una gestión eficiente de los flujos de datos según políticas definidas en capas superiores [2]. El controlador SDN funciona como el cerebro de la red: proporciona una visión global, monitorea el tráfico y coordina dispositivos como switches y routers para manejar dinámicamente el tráfico según las necesidades [3]. Gracias a estas capacidades, las SDN se consideran una arquitectura flexible, eficiente y rentable, ideal para entornos con alta demanda de ancho de banda y aplicaciones cambiantes [4]. Sin embargo, su centralización y capacidad de control también introducen nuevas amenazas de seguridad, especialmente en entornos híbridos, donde la red tradicional coexiste con componentes SDN [5]. En una red híbrida, tecnologías SDN como OpenFlow pueden coexistir con infraestructuras heredadas, permitiendo una adopción progresiva. El controlador SDN puede gestionar selectivamente el tráfico, incluyendo aspectos de seguridad, mientras que el resto de la red continúa operando de manera convencional [6]. A medida que más sistemas se conectan a los controladores SDN, se vuelve imprescindible fortalecer la protección de datos y dispositivos, detectar anomalías y corregir vulnerabilidades para mejorar la seguridad global de la arquitectura SDN [7].

	No obstante, el carácter centralizado del controlador lo convierte en un punto crítico de falla. Por ejemplo, un ataque de denegación de servicio distribuido (DDoS) dirigido a él puede saturarlo, comprometiendo la disponibilidad de toda la red [8][9]. En este contexto, se propone el diseño de un agente inteligente autónomo que, mediante técnicas de aprendizaje supervisado al principio y luego por refuerzo, sea capaz de orquestar de manera dinámica las políticas de seguridad del firewall en una red híbrida SDN universitaria. La elección de una red universitaria no es arbitraria; esta nos brinda un entorno rico y diverso con casi todos los casos de prueba posibles, incluyendo redes LAN, VLAN, Wi-Fi, DMZ, entre otras. Esto permite que el agente se adapte eficazmente a las complejas condiciones de tráfico y a las diversas amenazas detectadas en un entorno real y heterogéneo. Además se propone utilizar un server de IA que tiene la Facultad Regional en conjunto CON El Polo Científico y Tecnológico para realizar las primeras simulaciones.