# JORGE ALEJANDRO KAMLOFSKY

**Docente e investigador de la Facultad de Tecnología Informática de la Universidad Abierta Interamericana (UAI). Director del proyecto Ciberdefensa de Infraestructuras Industriales.**

**@jorgekamlofsky**

**https://ar.linkedin.com/in/jorgekamlofsky**

Licenciado en Matemática (UAI), Especialista en Criptografía y Seguridad Teleinformática (EST), finalizando una Maestría en TI (UAI) e iniciando un Doctorado en Ingeniería (UNLZ).

Docente adjunto de Matemática Discreta y Física II en la carrera de Ingeniería en Sistemas, dependiente de la Facultad de Tecnología Informática de la UAI.

Investigador Director del proyecto: Ciberdefensa de Infraestructuras Industriales, proyectos de Investigación del CAETI (centro de estudios dependiente de UAI). En el proyecto se investiga acerca de soluciones para la defensa de redes industriales (PLC-Scada).

Algunos artículos en congresos científicos:

Kamlofsky J. *Selective Attacks to Mifare Classic Cards*. CIBSI, 2013.

Kamlofsky J., Veiga D., Abdel Masih S., Hecht P., Colombo H. *Ciberdefensa de Infraestructuras Industriales*. WICC, 2015.

Kamlofsky J., Colombo H, Sliafertas M, Pedernera J. *Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Criticas*. CONAIISI, 2015 (trabajo aceptado, a publicarse).

El trabajo final de la Especialización en Criptografía trató acerca del quiebre de la seguridad de los chips Mifare Classic, presentes dentro de cientos de millones de tarjetas, que se usan mayormente en el pago de transporte público. Se muestra que con una PC y un lector económico pueden modificarse los saldos de las tarjetas. Basado en esto, se presentó un enfoque sencillo para realizar ataques selectivos a las infraestructuras que contienen Mifare Classic (ver CIBSI, 2013).

Actualmente se desempeña como Director del proyecto "Ciberdefensa de Infraestructuras Industriales", radicado en el CAETI. Se pretende desarrollar niveles de seguridad para las redes SCADA, desde el nivel más bajo, incluyendo desarrollos de criptografía basada en estructuras de anillos no conmutativos.

**¿Por qué participar en el CIBSI / TIBETS?**

Hay muy pocos congresos de esta especialidad en la región. Me parece necesario y conveniente participar en el mismo para mostrar nuestros trabajos en desarrollo en criptografía. Además, asistiendo al congreso se puede acceder a las investigaciones presentadas y a sus autores. Algunos de los trabajos que aquí se presentan, muy probablemente pasarán a formar parte del Marco Teórico de mis futuros trabajos.

**En su opinión, ¿cuál es la relevancia de su investigación en este Congreso?**

Nuestro trabajo se enmarca dentro de lo que se conoce como "Criptografía pos-cuántica": aquella que surge como opción luego de la implementación del algoritmo de Shor mediante computadores cuánticos. En especial, usa algoritmia basada en álgebra no conmutativa. En particular, en un sistema de intercambio de claves se usaron números hipercomplejos llamados "cuaterniones". La solución presentó menores tiempos de ejecución frente a otra solución similar que usaba matrices. Los resultados aquí presentados son novedosos e interesantes para esta línea de desarrollo criptográfico.

**¿Cuál piensa que será el devenir de la Seguridad de la Información?**

La tecnología informática forma parte de casi toda nuestra vida cotidiana. A pesar de ello, en el interior y en las cúpulas de muchas empresas y entes estatales, a la Seguridad Informática no se le da la importancia que merece. Mientras, en la red se encuentra en desarrollo la ciberguerra mundial (WWC) donde hackers estatales, paraestatales, delincuentes, activistas y terroristas atacan objetivos de toda clase, destruyendo o dejando fuera de servicio infraestructura, robando información secreta (secretos comerciales, información privada, etc), a través de vulnerabilidades en los sistemas informáticos que surgen a diario, y que no se atienden con prontitud. Los ataques son cada vez más cercanos, y sus efectos, más notorios, dejando en evidencia la falta de activos de defensa. Pienso entonces, que en los próximos años, necesariamente, la Seguridad Informática incrementará su nivel de participación presupuestaria en toda la economía, en todos los niveles.

**¿Cuál es el mayor riesgo que tiene una sociedad como la Iberoamericana en materia de ciberseguridad?**

En hora buena, la ciberseguridad pasó a ser un tema de gobierno. La reacción de muchos estados iberoamericanos fue acertada: han creado oficinas y asignado recursos económicos a tal fin. Sin embargo, aparece en nuestras naciones el riesgo de que los cupos de personal se llenen por conveniencias políticas, sin tener en cuenta la capacidad técnica disponible en la sociedad. Mientras tanto, los avances tecnológicos en esta materia avanzan aceleradamente aumentando más aún la brecha ciberbélica.

**¿Cómo ve a Latinoamérica en materia de seguridad de la información frente al resto del mundo?**

La intensidad de la WWC se acentúa en los lugares de mayor participación económica mundial, de la cual están prácticamente excluidas Latinoamérica y África. Esto nos da una oportunidad: una temporal "seguridad por ocultamiento". Aprovecharla puede permitir prepararnos para cuando el incremento de la WWC nos golpee, de modo de minimizar sus efectos.

## ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

A Diffie-Hellman Compact Model Over Non- Commutative Rings Using Quaternions. *Short Paper*

*Miércoles, 11 Noviembre*
*Bloque Criptografía.*

**Universidad Abierta Interamericana - ARGENTINA**
http://www.uai.edu.ar/
*Grupo Centro de Altos Estudios en Tecnología Informática (CAETI)*
http://caeti.uai.edu.ar/index.asp
*Proyecto Ciberdefensa de Infraestructuras Industriales*
http://caeti.uai.edu.ar/04/03/14/981.asp

El CAETI es una unidad académica de la UAI en búsqueda de soluciones tecnológicas e informáticas a partir de las teorías e instrumentos avanzados que proveen las ciencias, la técnica, el pensamiento organizador y la capacidad de innovación.
El proyecto "Ciberdefensa de Infraestructuras Industriales" se inició en 2014. Se investiga acerca de soluciones en diferentes niveles para la defensa de redes industriales (PLC-Scada).