Adopción de Criptografía Post-Cuántica y Estándares Avanzados de Seguridad - Propuesta de Modificaciones al Borrador de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay 2024-2030

Introducción: Considerando los últimos avances en criptografía cuántica y las vulnerabilidades actuales en las infraestructuras críticas de Uruguay, propongo una serie de modificaciones para fortalecer la ciberseguridad del país. Estos cambios están enfocados en la adopción de tecnologías post-cuánticas (PQC), la implementación de OWASP Top 10 en los procesos del Estado, y una revisión profunda de las normativas existentes en materia de hackeos y protección de datos personales.

Propuesta de Modificación:

1. **Capacidades Post-Cuánticas: Agregar:** En la sección 5 (Infraestructuras de Información Críticas) y 2.4 (Alineación con marcos normativos), se debe incluir explícitamente la necesidad de implementar criptografía post-cuántica (PQC) en las infraestructuras críticas del país. Específicamente, se debe priorizar la adopción de los tres algoritmos seleccionados por el NIST en agosto 2024: **Crystal Dilithium, Crystal Kyber y Sphincs**. Estos deben ser utilizados en todos los sistemas del Estado que actualmente dependen de RSA o ECC, los cuales son vulnerables a la computación cuántica. Esta medida debe implementarse en un plan de transición detallado que contemple auditorías inmediatas.
2. **Auditorías y OWASP Top 10: Agregar:** En la sección 5.4 (Fortalecer el ecosistema de equipos de monitoreo y respuesta), debe incluirse un mandato para que las auditorías de seguridad cibernética que se realicen en los entes estatales sigan las mejores prácticas del **OWASP Top 10** en lugar de estándares obsoletos como ISO 27001, que ya no están alineados con las amenazas actuales. Las auditorías deben ser obligatorias, periódicas y abiertas a expertos externos. Además, se debe realizar una revisión exhaustiva de los hackeos recientes a instituciones uruguayas, incorporando lecciones aprendidas para evitar vulnerabilidades similares en el futuro.
3. **Protección de Datos Personales: Modificar:** En la sección 7.2.5 (Protección de datos personales), se debe incluir una normativa que prohíba el uso de huellas dactilares como método de identificación para ciudadanos uruguayos, dada la brecha de seguridad de la Dirección Nacional de Identificación Civil (DNIC) en 2020, en la que datos biométricos fueron expuestos y ahora son accesibles públicamente. El Estado debe garantizar la protección de esta información a través de mecanismos de cifrado avanzados y limitar el uso de identificadores biométricos.
4. **Ciberseguridad en la Educación: Agregar:** En la sección 6.2 (Desarrollar y fortalecer las capacidades), se debe incluir un apartado sobre la capacitación en **habilidades de ciberseguridad desde la educación básica**. La formación debe incluir medidas preventivas sobre **phishing, ransomware y otros ciberataques emergentes**. Además, la **televisión nacional** y otros medios masivos deben participar activamente en campañas de concientización, mientras que los grupos de expertos del Estado deben recibir capacitaciones avanzadas para mitigar los ciberataques.

5. **Defensa Cuántica y QKD: Agregar:** En la sección 5.1 (Definir, identificar y clasificar las IIC), es imperativo desarrollar capacidades de **Quantum Key Distribution (QKD)** en los procesos de defensa del país. El despliegue de QKD garantizará que las comunicaciones en infraestructuras críticas sean invulnerables ante ataques cuánticos. Esto debe ir acompañado de una estrategia clara para implementar encriptación post-cuántica (PQC) en todos los sistemas estatales.
6. **Conciencia y Prevención en la Sociedad: Modificar:** En la sección 6.1 (Concientizar a las personas para el uso seguro de la tecnología), fortalecer las campañas educativas, subrayando la urgencia de la **alfabetización en ciberseguridad** desde las primeras etapas educativas. Se debe fomentar una **cultura de ciberseguridad** que no solo se limite a campañas de concientización, sino que involucre a los medios de comunicación, la televisión nacional y los influencers en redes sociales para llegar a las personas con contenidos adecuados a sus realidades.

Estas modificaciones asegurarán que Uruguay no solo aborde las amenazas actuales, sino que se prepare para los desafíos que vienen con la computación cuántica y otras tecnologías emergentes. La implementación de PQC, OWASP Top 10, y el fortalecimiento de la educación y auditorías en ciberseguridad son vitales para mantener la seguridad del país en los próximos años.

Sobre el autor: Nicolás Fiumarelli es ingeniero en computación con una maestría en IoT y gobernanza de internet. Es un destacado experto en criptografía cuántica y ciberseguridad, participando activamente en la Dynamic Coalition on Internet Standards, Security and Safety (DC-IS3C) de las Naciones Unidas, donde lidera iniciativas de seguridad relacionadas con IoT. Miembro del Board de Internet Society Uruguay y colaborador en la organización del IGF Uruguay desde 2019, ha sido ponente en foros globales y regionales, impulsando la adopción de tecnologías avanzadas como la criptografía post-cuántica y la inteligencia artificial. Nicolás también es un defensor de la educación en ciberseguridad, con amplia experiencia en auditorías y desarrollo de políticas para la protección de infraestructuras críticas.