**Propuesta de Agregados y Modificaciones a la Estrategia Nacional de Ciberseguridad de Uruguay**

## 2. Estado actual de la ciberseguridad, desafíos y oportunidades
### 2.2 Contexto nacional

El borrador actual reconoce algunos incidentes cibernéticos en el país, pero es fundamental que se incluyan ejemplos recientes de hackeos para resaltar la vulnerabilidad de las instituciones uruguayas, como el ataque a la Dirección Nacional de Identificación Civil (DNIC) en 2020 y el más reciente a la Intendencia de Paysandú en 2024.

**Propuesta de agregados:**

- Incluir ejemplos concretos de incidentes locales como los ciberataques a **Guyer & Regules**, **SMI**, y **Geocom**, que demuestran cómo las infraestructuras críticas no solo son vulnerables, sino que los efectos a largo plazo aún no han sido adecuadamente gestionados. Estos ataques subrayan la necesidad urgente de políticas de ciberseguridad más robustas, enfocadas en la protección de datos personales y financieros.
- Comparar cómo países como Chile y Argentina han implementado respuestas más rápidas y completas ante ciberataques similares, fortaleciendo la comunicación entre el sector privado y público, lo cual podría ser un modelo a seguir para Uruguay.

**Corrección:**

El borrador actual omite mencionar el riesgo continuo de los **datos biométricos filtrados** (como las huellas dactilares del hackeo de la DNIC), que no pueden ser modificados. Es crucial incluir este riesgo en el contexto nacional para reforzar la necesidad de normativas específicas que protejan este tipo de información. Estos datos, como las huellas dactilares, no pueden cambiarse, y su compromiso perpetuo es un riesgo constante.

**Pilar 1: Gobernanza**
**Línea 1.1 Fortalecer la estructura de gobernanza nacional**

El borrador menciona el fortalecimiento de la gobernanza, pero no aborda cómo coordinar la respuesta ante incidentes cibernéticos como los sufridos en Paysandú o en el sector financiero.

**Propuesta de agregados:**

- Crear un equipo central de coordinación para incidentes cibernéticos a nivel nacional, similar al **N-CERT** en otros países, para gestionar respuestas a hackeos en entidades gubernamentales y privadas en tiempo real. Este equipo debe tener la capacidad de movilizar recursos rápidamente y gestionar crisis de manera proactiva.

**Pilar 2: Marco normativo**
**Línea 2.1 Consolidar un marco normativo integral**

El borrador actual se centra en la consolidación del marco normativo, pero no menciona los casos recientes de hackeos en sectores financieros y legales. La normativa debería incluir obligaciones específicas para los sectores críticos que manejan grandes volúmenes de datos.

**Propuesta de agregados:**

- Incluir una normativa específica para la **protección de datos financieros y legales**, obligando a la implementación de auditorías de seguridad anuales y la aplicación de estándares de cifrado más estrictos, como lo exige **OWASP**, para prevenir vulnerabilidades comunes explotadas en estos ataques.

**Corrección:**

El borrador no menciona marcos internacionales como el de la **ENISA o NIST**. Sería importante agregar un compromiso de alinear la normativa nacional con estas guías internacionales para mejorar la resiliencia cibernética.

**Pilar 3: Ciberdelitos**
**Línea 3.1 Desarrollar las capacidades relativas al combate de los ciberdelitos**

Aunque el borrador aborda el combate a los ciberdelitos, no profundiza en la necesidad de equipos especializados para combatir ransomware y otros ataques, como los sufridos en Paysandú y GEOCOM, entre otros.

**Propuesta de agregados:**

- Crear una **unidad especializada** dentro de las fuerzas del orden para manejar cibercrimen avanzado, con formación continua y colaboración internacional con organismos como **Interpol** y la **OEA**, que han sido claves en otros países de la región para resolver hackeos a gran escala. Siempre respetando los principios de una red abierta, segura y confiable, sin caer en medidas como fragmentación o bloqueos de contenidos.

**Pilar 5: Infraestructuras de Información Críticas (IIC)**
**Línea 5.1 Definir, identificar y clasificar las IIC**

El borrador actual define las IIC, pero no detalla cómo protegerlas de los ataques recientes a entidades gubernamentales y de telecomunicaciones.

**Propuesta de agregados:**

- Ampliar la definición de IIC para incluir a servicios críticos **financieros y de salud**, como **CASMU** y **RedPagos**, que han sido objetivos de ciberataques recientes. Estos sectores deben ser prioridad en la clasificación y protección de las IIC para evitar la explotación de sus sistemas. Además, tal como se recomienda en el anexo, es importante que Uruguay regule los algoritmos de cifrado utilizados por entes estatales, privados, y sobretodo financieros y de salud, asegurando el uso de algoritmos resistentes a computadoras cuánticas tal como lo establece el NIST en sus estándares de Agosto 2024 (Es hora de actualizar el borrador a estos últimos

avances en computación cuántica y en estándares internacionales que nos protejan de las amenazas cuánticas, a la vez que por qué no en conjunto con la Facultad de Ingeniería e Instituto pasteur sobre el desarrollo de infraestructura de protección usando Quantum key distribution aprovechando el despliegue de fibra óptica del país para establecer comunicaciones cifradas usando comunicaciones cuánticas para el intercambio de claves QKD. En Europa ya están muy avanzados en estos despliegues.

**Corrección:**

El borrador no especifica un plan de ciberdefensa específico para las **instituciones financieras y de salud**. Incluir un plan de respuesta a incidentes dirigido a estos sectores es crucial para proteger los datos financieros e historias clínicas de ciudadanos uruguayos. Además se deberían sumar esuferzos por mejorar la infraestructura actual de datos en Uruguay e interoperabilidad, que aún le falta algún empujón (por favor no usar información dactilar, esto debe ser prohibido, leer la sección sobre el hackeo a más de 86.000 pasaportes electrónicos públicos en internet)

**Pilar 6: Cultura de ciberseguridad**
**Línea 6.1 Concientizar a las personas para el uso seguro de la tecnología**

El borrador menciona la concientización, pero no detalla cómo las personas pueden protegerse contra los tipos de phishing y ransomware que han afectado a instituciones uruguayas recientemente. Pero también a otro tipo de ataques de ingeniería social haciendo uso de IA y deepfakes tanto de imagenes como de audio.

**Propuesta de agregados:**

- Desarrollar campañas nacionales de concientización que utilicen **ejemplos reales de ataques recientes** a nivel local, como el hackeo a la Mutualista SMI, para que los ciudadanos y empleados puedan identificar mejor las amenazas y proteger sus datos.

**Pilar 8: Política internacional**
**Línea 8.2 Incrementar la presencia y participación de Uruguay en espacios regionales e internacionales**

El borrador menciona la presencia internacional, pero no aprovecha el potencial de cooperación internacional para aprender de los ataques sufridos en otros países.

**Propuesta de agregados:**

- Fortalecer la colaboración con organismos internacionales de ciberseguridad, como la **OEA** y el **Foro de Gobernanza de Internet (IGF)**, para acceder a las mejores prácticas sobre cómo otros países de la región han mejorado sus defensas cibernéticas tras ataques similares a los de Uruguay. Entre otros se destaca el trabajo de las Coaliciones Dinámicas, en particular la de security and Safety (DC-IS3C) así como una interrelación más profunda con la comunidad técnica como ser LACNIC y Internet Society Uruguay, aprendiendo sobre su experiencia en

seguridad de enrutamiento (RPKI) y extensión de seguridad para nombres de dominio (DNSSEC) y el desarrollo de estándares de seguridad en el IETF y la IEEE.

**Actualización sobre Criptografía Cuántica:**

El borrador debe actualizarse para incluir el impacto de la computación cuántica en la seguridad. Mencionar desarrollos recientes, como el cifrado **post-cuántico** con algoritmos como **Crystal Dilithium** y tecnologías como **Quantum Key Distribution (QKD)**, es clave para estar preparados ante futuros ataques cuánticos. Con el desarrollo de computadoras cuánticas de más de **500 qubits**, los algoritmos de **Shor** y **Grover** ya están demostrando cómo reducen la complejidad de 2^n2 a n^3, afectando la seguridad de RSA, ECC y AES, ampliamento usado en sistemas estatales y privados en Uruguay y el resto del sur global. Esta realidad subraya la urgencia de adoptar nuevas tecnologías para proteger la infraestructura crítica, en un plan multisectorial que incluye mesas con todos los sectores, incluyendo la comunidad técnica y la sociedad civil.