Daniel Andrés Birchner 15/10/2025

URUGUAY EN LA MIRA DIGITAL: VULNERABILIDADES CIBERNÉTICAS Y ESCENARIOS ESTRATÉGICOS HACIA 2030

Su atractivo para la instalación de centros de datos extranjeros, así como de interconectividad interna, sólo se compara con su nivel de riesgo a ciberataques. ¿Por qué el ciberespacio de Uruguay representa un riesgo especialmente grave para sí mismo, y a la vez, para la región? ¿Qué hace especial en este sentido al país oriental? La mejora de estas condiciones toma mucho tiempo. Exploremos entonces, distintos escenarios futuros, dadas las condiciones actuales, de la seguridad cibernética en Uruguay.

Se trata de uno de los países más interconectados a Internet de la región. En 2007 lanzó una iniciativa modelo de educación digital, llamada Plan Ceibal. Gracias a su estabilidad fiscal y política aloja grandes centros de datos como Zonamerica y Aguada Park. Así, Uruguay nos ofrece un panorama digital potencialmente rico, confiable, prometedor…. y al mismo tiempo, alarmante. Porque así también, el país oriental sufre el flagelo creciente de los ataques cibernéticos: entre sus causas, incluyendo las razones de siempre propias de la región (falta de inversión, capacitación y perspectiva preventiva), Uruguay es un objetivo especialmente atractivo.

Cifras de digitalización y ataques / vulnerabilidades legales

De acuerdo al Centro Nacional de Respuesta a incidentes de Seguridad Informática de Uruguay (CERTuy), en 2024 se detectaron 14.264 ciberataques, un incremento de 65 % con respecto al año pasado[1]. Este aumento, si bien forma parte de un fenómeno a nivel mundial, también obedece a **ciertas características específicas de Uruguay**: el gobierno no exige formalmente protocolos de ciberseguridad a empresas no estratégicas, dando paso a que de acuerdo al Informe de Ciberseguridad de 2025[2], 152.220 organizaciones asentadas en el país jamás realizaron una evaluación de ciberseguridad en sus sistemas. A esto se suma el dato de que un 85 % de las empresas uruguayas no tienen políticas

[1] Datos: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadisticas-incidentes-seguridad-informacion-2024
[2] Datos: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf

formales de ciberseguridad, y un 60 % de ellas no posee programas regulares de capacitación en ciberseguridad para sus empleados[3]. Este último factor es fundamental, ya que la mayoría de los ataques (fundamentalmente, *ransomware*) se producen mediante técnicas de ingeniería social (siendo el *phishing* el más común), técnicas que específicamente trabajan con la mente del empleado mediante técnicas de manipulación y suplantación de identidad. Es decir, no se trata (en este caso) de implementos técnicos más seguros ni de software de seguridad prohibitivamente caro: la ausencia de una capacitación al personal podría ser consecuencia directa de una falta de cultura de la prevención y la seguridad, en uno de los países más digitalizados de la región, con mayor presencia de empresas internacionales (dadas su facilidades fiscales) y finalmente, una fuerte concentración de centros de datos (lo cual, como exploraremos más adelante, constituye una fuerte vulnerabilidad).

De acuerdo sitio Brecha.uy[4], la gestión en ciberseguridad del país continua fragmentada, en ausencia de un marco regulatorio común y dejando las políticas de ciberseguridad al criterio propio de las instituciones. Es más: el decreto 92/14, que exige a los entes estatales a usar el dominio .uy en sus sitios web y a alojar sus servidores físicos dentro del territorio nacional. Pues bien, al día hoy siguen recibiéndose instrucciones y noticias oficiales de dominios ‘’@gmail.com’’ provenientes de servidores alojados en el extranjero. Este desfasaje (entre ley y su cumplimiento) se debe, probablemente, a la lentitud con la que se adaptan y actualizan los servicios, sujetos a la incapacidad técnica inmediata. Incluso, algunos servicios estatales tienen sus servicios radicados en Europa o Estados Unidos, y no se prioriza la migración de servidores en este caso. Existe un marco legal, pero sin fondos para concretarlo.

Adicionalmente a las condiciones estructurales nacionales como aquellas propias de la región, la ciberseguridad en Uruguay reviste un potencial riesgo no sólo a nivel interno, sino también regional. Los objetivos de este análisis serán: caracterizar los aspectos que hacen de Uruguay un blanco especialmente atractivo en términos de ciberataques, y en base a ello, elaborar tres escenarios prospectivos.

---

[3] Datos: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf

[4] Amestoy, E. (2025) – *La ciberseguridad en Uruguay: amenazas y desafíos*. Diario Brecha. Disponible en: https://brecha.com.uy/la-ciberseguridad-en-uruguay-amenazas-y-desafios/

Contexto digital y geopolítico del país

Digital: Uruguay tiene una de las tasas más altas de penetración de internet de la región: un 90 %[5], en comparación con Argentina (87 %) y Brasil (86,6 %)[6]. Gran parte de sus servicios de gestión gubernamentales son accesibles mediante internet, aplicaciones para teléfono y registro de usuarios, lo cual permite que la mayor parte de las gestiones personales con el gobierno se realizan de forma remota. El Plan Ceibal convirtió al país en pionero en educación digital, mediante el otorgamiento por parte del gobierno de una computadora a cada niño escolar. Además, Uruguay constituye un ecosistema muy atractivo para la instalación de empresas y surgimiento de fintechs: sus facilidades fiscales, así como una infraestructura 4G muy efectiva (incluso, el país avanza rápidamente con las redes 5G).

Geopolítico: Uruguay goza de los resultados de un posicionamiento tradicionalmente neutral e instrumental. Sin embargo, la apertura a la digitalización de sus servicios estatales y comunicaciones han requerido la configuración geopolítica: el país depende en gran medida de servicios en la nube proporcionados por gigantes norteamericanos como Microsoft, Google y Amazon, además de alinearse en términos regulatorios con **Estados Unidos** (Convenio de Budapest sobre ciberdelito y el Programa Interamericano de Seguridad de la OEA).

Adicionalmente, comparte similares relaciones con la **Unión Europea**. En este caso, conviene destacar que la regulación sobre la protección de datos personales (ley 18.331) fue reconocida como ‘’adecuada’’[7] por la GDPR[8] de la mancomunidad europea, mediante lo cual se facilita el intercambio de datos con países europeos. Además, ante los estándares europeos, la nación oriental se revela como un socio estable y confiable para

[5] Datos: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf
[6] Datos: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf
[7] Es decir: que los niveles de protección de datos personales en Uruguay son mayoritariamente aceptados por la Unión Europea, permitiendo la libre circulación (sin salvaguardas adicionales) de información entre las entidades. Mayor info en https://www.insideprivacy.com/international/european-commission-issues-implementing-decision-finding-uruguays-data-protection-laws-provide-adequ/?utm_source=chatgpt.com.
[8] GDRP: General Data Protection Regulation.

empresas europeas del ámbito digital que desean introducirse en el mercado latinoamericano.

Y también existe una interesante relación con **China**. Uruguay forma parte de la iniciativa de la Franja y la Ruta[9], lo que lo transforma en un receptor de inversión estratégica china en los ámbitos de la infraestructura física de las comunicaciones (cables submarinos, estaciones de recepción, antenas 5G, entre otras). En el tema específico del 5G, Montevideo se ha mantenido en una actitud pragmática al no vetar a Huawei como proveedora de esa infraestructura, a pesar de las reticencias de Washington[10]. Por el momento, la instalación de estas antenas está en una fase más bien embrionaria, pero su asentamiento a largo plazo podría generar resquemores de varios países de Europa y Estados Unidos[11], que han vetado a la empresa china basados en el riesgo de espionaje de sus usuarios[12].

Relevancia estratégica

Uruguay está conectado a Argentina y a Brasil a través del cable submarino UNISUR, con estaciones receptoras en Punta del Este (Uruguay), Las Toninas (Argentina) y Florianópolis (Brasil). Funciona como un nodo adicional (respaldo-tránsito) entre ambos, ya que se ubica en justamente en el medio de esta conexión. Por otro lado, ya mencionamos anteriormente la cuestión de los servidores: Zonamerica y Aguada Park alojan los servicios de varias empresas[13] tanto uruguayas, como brasileras, argentinas y de otros países.

[9] Uruguay firmó un Memorando de Entendimiento con China en 2018 para integrarse a la BRI, siendo el primer país del MERCOSUR en hacerlo.
[10] Council on Foreign Relations. *China in Latin America: Febreaury 2025*. Disponible en: https://www.cfr.org/article/china-latin-america-february-2025?utm_source=chatgpt.com
[11] La reacción de Washington ante el avance de Huawei en Uruguay ha sido de cautela, pero en línea con su política regional de contención del avance tecnológico chino.
[12] Kapko, M. (2024) – *Feds raise alarm on China-liked infiltration of telecom networks*. Cybersecuirty Dive. Disponible en: https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576/?utm_source=chatgpt.com
[13] Algunos ejemplos: Assist Card, Despegar, Sabre, Tata, CITI, Mercado Libre, Globant, entre muchas otras.

Análisis de vulnerabilidades:

- **Infraestructura crítica digital desprotegida**: el cable UNISUR es factible de ser saboteado o cortado. Un corte dejaría *gravemente, pero no totalmente*[14] aislado al país oriental, pero no afectaría directamente a Brasil y Argentina ya que estos dos países tienen conexiones (en forma de cables terrestres) alternativas, aunque si empobrecería la calidad y seguridad de las conexiones al funcionar como un respaldo.
- **Capacidad estatal limitada**: El país carece de un documento doctrinario que reúna los conceptos y perspectivas de ciberseguridad, ciberdefensa y Ciberinteligencia en una misma estrategia, aunque existen esfuerzos fragmentados[15]. Uno de los efectos más notables que esta limitación, se manifiesta en que la seguridad física y lógica de los centros de datos mencionados depende de protocolos privados, con limitada supervisión estatal. Asimismo, la formación en personal es reciente: la gran mayoría de las capacitaciones universitarias y especializaciones en ciberseguridad y ciberinteligencia no son de grado universitario, consistiendo más bien en cursos terciarios y maestrías pero sin llegar a grados.
- **Dependencia tecnológica de proveedores extranjeros**: Las instituciones públicas usan software de tecnologías foráneas, así como la infraestructura *cloud* es también provista por potencias extranjeras.
- **Potencial riesgo del país para ser usado como plataforma de actividades encubiertas**: A diferencia de países vecinos como Chile o Brasil, Uruguay no cuenta con un comando conjunto en ciberdefensa. Las FF.AA. muestran interés en el sector, pero sin un presupuesto ni marco legal que habilite su concretización.

Escenarios Prospectivos:

Teniendo en cuenta el contexto general, las oportunidades y desafíos del ciberespacio uruguayo, se plantean los siguientes escenarios:

[14] Si bien UNISUR es el cable principal y de mayor tráfico, no es el único: TANNAT (Maldonado-Santos) además de líneas terrestres menores.
[15] CERTuy para respuesta técnica, AGESIC para regulación administrativa, y el Ministerio de Defensa que trabaja en resiliencia.

- **POSITIVO**: Autonomía digital.

En este escenario, y gracias a la diversificación de su conectividad (mayor distribución de nodos, respaldo terrestre local de datos y a lo mejor, más cables submarinos) la aplicación material del decreto 92/014 y la construcción de un marco legal militar en ciberdefensa, el país consolida su estrategia nacional de ciberseguridad y ciberdefensa de forma coherente y funcional. Tales acciones posicionarían a Uruguay como un referente regional en términos de seguridad y soberanía digital, aumentando su poder de influencia en cuanto a capacitación, experiencia y garantías de seguridad para inversiones privados.

- **AMBIGUO**: Zona gris.

En este escenario, que probablemente sería una prolongación sin cambios de la situación actual, Uruguay mantiene su marco normativo, pero no lograr cerrar la brecha entre norma y práctica. El Estado sigue dependiendo de proveedores extranjeros en términos de software y hardware, así como de personal calificado. El país conserva su imagen de estabilidad y neutralidad, al precio de gran parte de su soberanía digital. El riesgo principal de este escenario es la naturalización del estado actual, quedando subordinado a estándares, software y hardware extranjeros (que a su vez condiciona sus alianzas geopolíticas). Lo que conjuntamente a la velocidad con la que evolucionan las técnicas de guerra cibernética, a la larga no haría más que incrementar las vulnerabilidades del país.

- **NEGATIVO**: Crisis de soberanía informacional.

Uruguay enfrenta una progresiva pérdida de su autonomía tecnología y jurídica. La falta de inversión sostenida y la casi nula innovación en informática dejan al país expuesto a ataques cibernéticos. Varias empresas y países que alguna vez confiaron en la robustez de seguridad del país abandonan el país, relegando seriamente su reputación y relevancia geopolítica regional. El mismo Estado enfrenta filtraciones masivas de datos de sus ciudadanos y un deterioro progresivo de la infraestructura física de su ciberespacio, causado por la falta de inversión, falta de personal capacitado y mantenimiento de las infraestructuras. Progresivamente, estas condiciones conducen a la consideración de Uruguay como una suerte de protectorado digital, sin software ni hardware soberano, con

marcos legales obsoletos y sin financiación y en dependencia de otras potencias regionales más desarrolladas en ciberseguridad.

Recomendaciones estratégicas hacia 2030 y conclusión

La ciberseguridad como política nacional precisa no sólo de marcos normativos, sino de un financiamiento suficiente, sistemas de control/auditoría, inversión en educación y quizás sobre todo, visión estratégica. A nivel mundial, la ciberseguridad ya no es un tema secundario, sino cada vez más decisivo en tanto día a día aumenta la digitalización de tecnologías de gestión, burocracia y tráfico de información. Así como aumenta la digitalización, también lo hacen los peligros y vulnerabilidades que este avance trae aparejado. En el caso específico de Uruguay, y teniendo en cuenta las falencias expuestas, hacemos las siguientes propuestas estratégicas:

1.- **Elaborar una Estrategia nacional de Ciberseguridad y Ciberdefensa**. Englobar en una sola propuesta todas las mejoras y perspectivas necesarias para centralizar el esfuerzo tanto en el ámbito civil como en el militar. Integrar a los diferentes esfuerzos (AGESIC, CERTuy) y estamentos (Defensa, Cancillería en una doctrina unificada. La meta de esta unificación de esfuerzos se coronaría como la definición de la ciberdefensa como una política de Estado, con presupuesto asignado y capacidad concreta de respuesta.

2.- **Fortalecer la infraestructura crítica y proveedores**. Diversificando rutas de interconectividad internacional (cables submarinos, enlaces terrestres redundantes), garantizar que los servidores que guarden y procesen datos sensibles del Estado estén físicamente localizados dentro de Uruguay (cumplimiento del Decreto 92/014) e incentivando la localización servicios de cloud dentro del país.

3.- **Desarrollar capital humano especializado**. Crear carreras de nivel universitario en Ciberseguridad y Ciberdefensa que no sólo sirvan para formar profesionales para el país, sino para transformar a Uruguay en un referente regional en estas temáticas, definiendo estándares superiores de calidad educativa y profesional. Asimismo, incentivar la retención de talentos locales mediante convenios con el Estado y programas de investigación aplicada.

4.- **Actualizar el marco legal y fortalecer la capacidad de auditoría y sanciones**. Un marco legal anquilosado y sin medidas de control no sirve. La actualización constante en base a los nuevos desarrollos en software (deepfakes, IA maliciosa) y hardware (posesión civil de dispositivos de hacking) debe constituir una prioridad, así como la definición de mecanismos punitorios para garantizar la naturaleza obligatoria y no opcional de estas leyes. Adicionalmente, el establecimiento de una Autoridad Nacional de Protección Digital, entidad que concentraría la fiscalización transversal y coordinación judicial de casos de cibercriminal.

Posiblemente, la aplicación de estas recomendaciones redundaría en la definición de Uruguay como un referente regional y acaso internacional en términos de confianza digital. El país ya goza de confianza en varios ámbitos (institucional, financiero) por lo que enriquecer su posición desde la ciberseguridad y ciberdefensa contribuiría notablemente a su reputación internacional. Este resultado se vería potenciado por la adhesión del país a grupos internacionales como el OTAN *Cooperative Cyber Defense Centre of Excellence* y *Global Forum on Cyber Expertise*, para lograr visibilidad y respaldo estratégico.

Conclusiones:

Uruguay se encuentra ante una oportunidad singular: su ubicación estratégica en el Cono Sur, así como su tamaño pueden ser ventajas si se adopta una estrategia coordinada que priorice la soberanía tecnológica, la capacitación humana y el cumplimiento efectivo de su marco normativo. En caso contrario, sin la aplicación de esas medidas, el país corre riesgo de transformarse en una amenaza indirecta para el resto de la región, un espacio digital dependiente y vulnerable en el Cono Sur.