Consulta Pública – Estrategia Nacional de Ciberseguridad

La presente respuesta tiene como objetivo proporcionar comentarios y recomendaciones sobre el borrador de la Estrategia Nacional de Ciberseguridad de Uruguay, alineados con las posiciones y políticas de Microsoft en materia de ciberseguridad.

Desde Microsoft celebramos el enfoque integral adoptado en el borrador, que abarca tanto la protección de las infraestructuras críticas como la educación en ciberseguridad.

Pilar 2. Marco normativo

Marco normativo integrado, coherente y adaptable que garantice protección de los datos y privacidad.

Línea 2.1. Consolidar un marco normativo integral

Establecer un conjunto de leyes, normas estándares y regulaciones base sólida y ciberseguridad en el país, con especial énfasis en la protección de los datos personales, sin olvidar cuestiones esenciales como la seguridad de las infraestructuras de información críticas.

Adoptar el marco de ciberseguridad adecuado para los sectores y servicios críticos del país contemplando la cadena de suministro, y generar su respectiva regulación cuando corresponda.

Asegurar el marco normativo nacional vele por la ciberseguridad a nivel supraterritorial en concordancia con los estándares y las obligaciones asumidas por el país a nivel internacional.

Comentario: *Respecto del Marco Normativo recomendamos que todo marco normativo sobre ciberseguridad y los requisitos de ciberseguridad impuestos por el gobierno deben centrarse en los resultados (es decir, no en estándares prescriptivos), ser interoperables y estar armonizados en todos los sectores de infraestructura crítica.*

Para lograr estos resultados, recomendamos la adopción de los estándares internacionales basados en el riesgo lo que permite:

- *Evitar la duplicación o redundancia.*
- *Optimizar la asignación de recursos enfocada en la seguridad y la gestión de riesgos en lugar de simplemente cumplir con las normativas. Como resultado, las organizaciones y los proveedores externos invertirán en innovación en seguridad con más confianza, fomentando el desarrollo de nuevas técnicas y capacidades.*
- *Fomentar la colaboración transfronteriza, lo que mantendrá las relaciones globales de manufactura y subcontratación, promoviendo así el crecimiento económico y el avance rentable de la tecnología.*
- *Utilizar procesos de desarrollo más abiertos, colaborativos e iterativos en el desarrollo de requisitos de gestión de riesgos de ciberseguridad.*

Ejemplos de estándares basados en riesgo pueden ser los del Instituto Nacional de Estándares y Tecnología (NIST) y la Organización Internacional de Normalización (ISO) proporcionan dos de los principales marcos y estándares de gestión de riesgos de ciberseguridad reconocidos internacionalmente.

Pilar 3. Ciberdelitos

Línea 3.1. Desarrollar las capacidades relativas al combate de los ciberdelitos.

Comentario: *Es recomendable también la participación en otros foros internacionales como por ejemplo el Grupo de Expertos Gubernamentales sobre los Avances en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.*

Pilar 5. Infraestructuras críticas

Línea 5.1. Definir, identificar y clasificar las IIC

Acciones

- Identificar las IIC del país y actores involucrados en gestión y administración

Comentario: *Es recomendable el uso de las Buenas Prácticas del GFCE sobre las directrices de protección de IICC para la identificación de infraestructuras de información crítica.*

- Analizar interconexiones y dependencias entre IIC para evaluar el alcance e impacto de un potencial incidente.

Comentario: *Es importante la distinción entre servicios y funciones críticas de los operadores entidades relacionadas con la infraestructura crítica debido a que no todas las funciones o servicios que se proveen serán servicios críticos. Esta distinción es importante para que esos operadores puedan identificar las funciones críticas y priorizar los riesgos.*

Sugerimos que primero se identifiquen de las funciones que deben ser protegidas y preservadas, independientemente de la red, sistema o activo usado para proveer dichos servicios. De esta manera, puede establecerse un sistema nacional de gestión de riesgos que permita a las organizaciones incorporar esa gestión de riesgos a sus procesos corporativos.

Línea 5.2. Proteger la IIC

Acciones

- Incrementar y fortalecer las capacidades de monitoreo y detección de incidentes en las IIC, esto implica desarrollar capacidades para identificar y responder de manera efectiva a incidentes de ciberseguridad, incluyendo la implementación de sistemas de monitoreo y la creación de equipos especializados en ciberseguridad, impulsando un abordaje sectorial bajo la coordinación del CERTuy.

Comentario: *A los efectos del incremento y fortalecimiento de las capacidades de monitoreo, detección y respuesta entendemos importa la integración de tecnologías de inteligencia artificial. De esta manera, se pueden analizar grandes volúmenes de datos en tiempo real, identificando patrones y amenazas que podrían pasar desapercibidos para los analistas humanos.*

Línea 5.4. Fortalecer el ecosistema de monitoreo y respuesta en sectores públicos, privados y academia

Acciones

- Desarrollo de estándares y guías para CIRTs y SOCs
- Trabajar con co-reguladores para establecer obligaciones legales y reglamentarias claras e implementar incentivos y sanciones. Definir responsabilidades de actores y establecer mecanismos para garantizar el cumplimiento de las normas.

Comentario: *Es importante que las obligaciones, especialmente en materia de notificación de incidentes de ciberseguridad sean claras y precisas a los efectos de poder lograr una respuesta rápida y coordinada, minimizando el impacto de los ciberataques.*

<u>Pilar 6. Cultura de ciberseguridad</u>

Línea 6.1. Concientizar a las personas para el uso de la tecnología

Acciones

- Promover el uso de identificaciones digitales fuertes y firmas digitales como herramientas fundamentales para proteger la identidad en línea y realizar

transacciones seguras. Universalizar el acceso de identificaciones seguras fortalecidas por autenticadores biométricos, certificados digitales u otras.

Comentario: *Entendemos que entre las mejores prácticas que sería recomendable incluir como mejores prácticas de higiene digital también deberían incluirse las actualizaciones regulares de los softwares y la utilización de las autenticaciones multifactor.*

Agradecemos nuevamente la oportunidad esperando poder seguir colaborando en el futuro.

Saludos cordiales,

Marina Bericua
Directora de Asuntos Públicos, Corporativos y Gubernamentales
Microsoft Uruguay y Argentina