Comentarios al borrador de la Estrategia Nacional de Ciberseguridad del Uruguay 2024 – 2030

1-Introducción

Como empresa del sector TIC consideramos que la generación de espacios como el que hoy nos convoca son fundamentales para que sea efectiva una norma/lineamiento/estrategia en materia de Ciberseguridad

Estamos comprometidos con el desarrollo del entorno global, bajo una perspectiva de brindar servicios de alta calidad para toda la ciudadanía y a todos los sectores productivos de Uruguay promoviendo la seguridad digital, la innovación, el respeto a la privacidad, la promoción de la libertad de expresión y el derecho a la intimidad

En ese orden de ideas es que ya hemos participado y formado parte de estos espacios inclusivos, presentado durante el proceso, "*mesas de trabajo para definiciones estratégicas*" iniciado el año pasado, distintos comentarios que consideramos fundamentales que la AGESIC y URSEC adopten en toda normativa, lineamiento o precepto regulatorio.

Notamos que muchas de nuestras contribuciones fueron contempladas en el presente "*borrador de la Estrategia Nacional de Ciberseguridad del Uruguay 2024 – 2030"* ; independientemente de ello en la sección "2 Comentarios " haremos foco a los puntos que se les debería dar mayor certidumbre colaborando con nuevos aportes

Reiteramos en este posicionamiento que el tema es complejo y dinámico por lo tanto hay que utilizar recomendaciones de organismos/asociaciones con aval internacional por su experiencia en la materia. Asimismo, tener en consideración las recomendaciones y aportes realizados por los distintos stakeholders (industria y academia) y en base de ellos crear una norma o lineamiento que no restinga la innovación y contribuya a la seguridad y confianza de las personas usuarias de tecnologías digitales

2-Comentarios

La participación de los distintos stakeholders del proceso que inició el Estado uruguayo es un acierto. En el anterior borrador "*primer borrador de la Estrategia Nacional de Ciberseguridad del Uruguay 2024 – 2030",* propusimos se incluya dentro de los principios a la seguridad desde el diseño, pero no fue incorporado en la presente versión.

Si bien se hace mención, dentro del Pilar 2. Marco normativo, Línea 2.1 Consolidar un marco normativo integral en la parte de acciones "*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."* y en el Pilar 7. Ecosistema e industria de la ciberseguridad en dentro de la Línea 7.2 Impulsar una industria de TI segura *"Una industria local dinámica, capaz de ofrecer soluciones de alta calidad, es fundamental para proteger los intereses nacionales y para impulsar la innovación en el sector. Asimismo, es esencial que la industria del software y servicios a nivel nacional adopte las mejores prácticas internacionales en materia de seguridad, teniendo como objetivo que sus productos sean* ***seguros por diseño*** *y contribuyan a elevar el nivel de ciberseguridad del país*. Consideramos no es suficiente este enfoque ya que tiene que ser la seguridad desde el diseño un principio único por la importancia de su alcance. Al especificarlo en la "Línea 7.2 Impulsar una industria de TI segura" lo limita a esa categoría siendo insuficiente.

Justificación para incluir a la seguridad desde el diseño dentro de los principios

Reiteramos, por la importancia que tiene, que sea considerado como un principio de aplicación a todos los involucrados tanto para el ámbito público como privado. Todas las partes vinculadas deben implementar medidas de seguridad en toda la cadena de valor siendo las mismas fiables así la "seguridad por diseño inicial" debe aplicarse desde el inicio, la etapa intermedia y la final de los servicios y dispositivos digitales.

Por ello corresponde diseñar el software y el hardware para que desde el principio sean seguros e implementar actualizaciones de seguridad automatizadas como parte del proceso del ciclo de vida. Es esencial definir y aplicar planes armonizados de certificación de la seguridad cibernética para toda la cadena de valor de los servicios y productos digitales.

La seguridad también se asocia a la responsabilidad que tienen los proveedores de cada eslabón del ecosistema digital. Por lo tanto, cada interviniente debe tener obligaciones y responsabilidades claras y limitadas conforme su función

Al implementar medidas de seguridad desde el diseño se tutela el derecho a la privacidad y la seguridad de la información en el entorno digital ya que todos los agentes de la cadena de valor en la prestación de los servicios deben garantizar la seguridad de sus prestaciones además se deben establecer claramente las responsabilidades de cada agente que participa. Asimismo, el sector público por la sensibilidad de la información que administran debe cumplir con altos parámetros de seguridad de la información obligatorios teniendo responsabilidades claras y con procedimientos de riesgos certeros.

En ese sentido, son una buena incorporación manuales de uso, voluntarios para los privados, por ejemplo, los publicados por el regulador mexicano. El Instituto Federal de

Telecomunicaciones (IFT) divulgó los Códigos de Mejores Prácticas para la Ciberseguridad uno para terminales móviles ("Código ETM") y otro para dispositivos IoT[1] que tienen por finalidad incluir a los principales agentes que participan del ecosistema móvil y digital para propiciar la seguridad desde el diseño e incentivar la innovación tecnológica .

Así proponemos el desarrollo de un marco normativo que considere los roles y responsabilidades de los proveedores de servicios y productos tecnológicos.

Por ello la regulación debe aplicarse de manera consistente a todos los proveedores en forma neutral respecto de los servicios y la tecnología por ejemplo en la Unión Europea fines del año pasado se publicó la Directiva RED[2] que refuerza la ciberseguridad de los dispositivos y productos inalámbricos, establece requisitos que sean seguros desde el diseño, su ámbito de aplicación es a teléfonos móviles, tablets, juguetes, monitores para bebés, relojes inteligentes. La normativa incluye un, tiempo de cumplimiento y adaptación para los fabricantes.

Así también lo recomienda GSMA en su documento " *Seguridad y privacidad en las redes móviles"*[3] afirma que *"La ciberseguridad debe cubrir todo el ciclo de vida de un servicio, desde su diseño, hasta su implementación y operación."*

Dentro del Pilar 2. Marco normativo. Línea 2.2 Certificación y Conformidad

Aclaramos que toda auditoria debe ser justificada y fundada para respetar derechos fundamentales y la seguridad jurídica. Además, aquellas organizaciones que tengan certificaciones de alta calidad por ejemplo normas ISO- para evitar erogaciones de recursos- deberían tener que validar ante la autoridad competente en la materia la certificación y no tener que pasar por procesos engorrosos incensarios. En ese orden de ideas es fundamental contar con una Agencia Independiente con recursos y autonomía que sea el organismo que vele por este procedimiento permitiendo el uso de certificados voluntarios

Dentro del Pilar 7. Ecosistema e industria de la ciberseguridad

Nos parece que favorece a la seguridad del entorno digital que se incluya dentro de las acciones del Pilar 7 *"Crear un ecosistema de incentivos fiscales y financieros para impulsar*

[1] https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-publica-codigos-de-mejores-practicas-para-la-ciberseguridad-en-equipos-moviles-y-en

[2] https://ec.europa.eu/commission/presscorner/detail/es/ip_21_5634

[3] GSMA 2018 " Seguridad y privacidad en las redes móviles" https://www.gsma.com/latinamerica/wp-content/uploads/2018/04/Seguridadyprivacidad.pdf

el desarrollo de la industria nacional de ciberseguridad, y la ciberseguridad en toda la industria de TI (servicios de TI, el desarrollo de software seguro, el cumplimiento de estándares establecidos y la adopción de buenas prácticas en el sector)".

Este tipo de acción - desgravación fiscal- nos permite identificar la importancia que tiene para el Estado la ciberseguridad en ese orden de ideas proponemos incluir el seguimiento de KPIs (Key Performance Indicator) de inversión y talento. Somos consintientes que es un desafío entender cuánto se ha invertido en ciberseguridad y cuántas personas con conocimiento especializados hay. Por eso, preguntar cómo se pueden establecer KPIs de seguimiento tanto presupuestario (% sobre inversión/gasto o total) y sobre personas, es fundamental.

La ciberseguridad es una inversión no un gasto y este precepto tiene que ser el estandarte a seguir para todos los que forman parte del ecosistema digital

Dentro del pilar 8 Política internacional

Reiteramos que se agregue de forma expresa promover activamente la ciberdiplomacia, incentivando a nivel regional y global la discusión respecto a la aplicación de normas, derecho internacional, y medidas de fomento de la confianza en el ciberespacio, y el desarrollo de acuerdos bilaterales que refuercen la cooperación en ciberseguridad, y el respeto de los derechos humanos en el ciberespacio.

Tal como lo establece la ITU ya que recomienda a los Estados[4]:

> *Reconocer la importancia de la ciberseguridad como prioridad de la política exterior; es importante fomentar el desarrollo y la utilización de competencias y aptitudes sobre asuntos cibernéticos (ciber-diplomacia)

3-Conclusión

Como ya nos hemos manifestado en otros espacios propuestos por AGESIC y URSEC, este tipo de medidas son las correctas para lograr un ecosistema participativo siendo fundamental para luego poder obtener lineamientos o preceptos normativos legitimados por los múltiples stakeholders.

[4] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Logar emitir normas claras que incluyan a todos los partícipes en base a principio de neutralidad tecnológica o level-playing-field (aplica a todos de igual manera) y la coordinación en base las obligaciones proporcionadas que cada uno tiene basadas en riesgos es esencial

Como se planteó en la estrategia propuesta la problemática de la Ciberseguridad es un tema global requiriendo de una visión holística

En ese orden de ideas es fundamental reforzar la cooperación internacional para establecer principios comunes y evitar la fragmentación normativa. El diálogo y compromiso internacional para la elaboración de directrices de aplicación global debe ser prioritario

Por eso es positivo, incluido en la propuesta, en el Pilar 3. Ciberdelitos se incluya dentro de las acciones avanzar con la adopción del Convenio de Budapest al igual que lograr una relación fluida entre los múltiples gobiernos para trabajar de forma mancomunada y así lograr un ecosistema digital fiable y seguro