Comentarios a la Segunda Estrategia Nacional de Ciberseguridad.

La ciberseguridad, como disciplina, es un campo de conocimiento en construcción, ya que los impactos de las tecnologías de la información y la comunicación con cada innovación implica efectos negativos que habrá que evaluar y abordar desde distintas perspectivas, impacto en derechos humanos, disrupciones en los servicios esenciales o hipótesis de conflictos geopolíticos. No obstante, así como hay nuevos riesgos, hay problemas bien conocidos que derivan de los servicios y productos digitales que se originan en deficiencias en sus diseños, desarrollos e implementaciones, como así también en sus infraestructuras tecnológicas y de telecomunicaciones que afectan directamente a las personas usuarias.

En este sentido, es y fue la seguridad de la información y la seguridad informática los campos de conocimientos que brindan las buenas prácticas y los marcos conceptuales para la construcción y provisión de servicios y productos digitales que brinden seguridad a los usuarios y para sus datos. De esta manera y si bien los usuarios deben ser concientizados y formados para los usos responsables igual o más importante es promover la seguridad desde el diseño como principio y durante todo el ciclo de vida. Concepto que podría incluirse entre los objetivos de la Estrategia.

Adicionalmente y como se trata en este punto de diseñar los servicios digitales, vale mencionar que los marcos de capacitación promueven también la privacidad por defecto, como parte de los Marcos de referencia en capacitación en ciberseguridad(1).

En este sentido, la reciente publicación de la Declaración Europea sobre Derechos y Principios Digitales (2) expresa un objetivo concreto en la materia, el cual enuncia como el derecho de toda persona a acceder a tecnologías, productos y servicios diseñados para que las personas estén protegidas, para que sean seguros y para proteger la privacidad.

De esta manera se puede resaltar el tratamiento conjunto que hace la Declaración europea mencionada al tratar la seguridad en conjunto con la privacidad, que puede entenderse, en parte, desde nuestro marco normativo como la protección de los datos personales, ya que en el mundo interconectado y global actual está ansioso por conseguir datos para ajustar preferencias de las poblaciones tanto para vender publicidad como propaganda, con los riesgos que conlleva, a nivel delito como problemática social y política.

Adicionalmente y para evitar uno de los riesgos creciente de “fuga de datos” o incidentes de ciberseguridad en los que datos personales se copian, se extraen para luego venderse, intercambiarse o regalarse es también (como para el resto de los incidentes) necesario mejorar la línea base de las medidas de seguridad de la información, del Sector público como privado y formar al personal operativos y de cargos directivos sobre sus responsabilidades, promover incentivos y controles para establecer ciclos de mejora. Por otro lado, ante el incidente ocurrido, la gestión de este tipo de incidentes debería contribuir a la identificación de las causas, los diagnósticos y la propuesta de mejoras.

Ya en 2016 (3), la OECD recomendó que sean los Equipos de Respuesta Nacionales ante Incidentes, los CERT/CSIRT nacionales los ámbitos de asistencia en los incidentes que afectaran a datos personales, indicando “Un CSIRT bien gestionado es parte esencial de la Protección de datos y la seguridad en una sociedad”, ya que son estos equipos los que deberían tener las capacidades técnicas para realizar los análisis, evaluaciones y asistencias ante incidentes y brindar las recomendaciones para evitar la frecuencia y el impactos de tales incidentes.

En particular, sería deseable que al menos un objetivo promueva la protección de los datos personales, tal como aparece y resulta natural que parte de las acciones de ciberseguridad se orienten en prevenir e investigar delitos que utilicen tecnologías. También a la luz de los incidentes ocurridos en años anteriores y de los cuales no se ha conocido información a nivel de ciberseguridad (vulnerabilidades aprovechadas, procesos deficientes, responsabilidades no asignadas) información que, una vez conocida puede ayudar tanto a saber si se tomaron las medidas razonables de prevención como para dimensionar el alcance y emitir recomendaciones en los casos que, como el incidente ocurrido entre en Ministerio de Saludo y RENAPER afecten a datos de ciudadanos.

Es importante también que en los distintos ámbitos de la formación y concientización en seguridad informática y ciberseguridad se aborden los principios de protección de datos establecidos en la legislación vigente ya que desde el Estado es importante la protección de los servicios, la información que se maneja para llevar adelante las misiones y funciones y la seguridad de los datos personales como custodio y dueño de los riesgos ante incidentes de ciberseguridad.

A fin de que la sociedad civil y los distintos actores involucrados puedan realizar un seguimiento de los distintos objetivos resultaría conveniente, estimar plazos e hitos concretos, junto al presupuesto asignado. Si bien es entendible la compleja coyuntura, tener referencias para un seguimiento ordenado puede ayudar a evaluar el desempeño en el cumplimiento de los objetivos, además de ser una premisa para la transparencia de los actos públicos.

Otro aspecto importante a resaltar es que, como ya fuera mencionado, que al prevenir incidentes y promover servicios, productos e infraestructuras resilientes, la ciberseguridad opera en la prevención de delitos a partir del fortalecimiento y aplicación de principios y buenas prácticas técnicas aplicadas a las tecnologías. No obstante ello, cuando corresponde, la ciberseguridad también contribuye con la investigación o análisis de los delitos. De tal modo, surge entre ambos enfoques la existencia de un espacio común de acción. Sin embargo centrar el objetivo de la ciberseguridad en la segunda de las áreas de trabajo señaladas, resulta un error con severas implicancias que afectan el desarrollo de una estrategia integral en materia de ciberseguridad.

En la actualidad existen déficits no resueltos por los diseños institucionales vigentes definidos a partir de una visión meramente penal. En tal sentido, vale señalar, a modo de ejemplos de esta realidad, la persecución penal por parte de las autoridades de las personas que reportan vulnerabilidades, las violaciones al Derecho al anonimato, los déficits de público conocimiento en materia de salvaguarda de información personal en el marco de los procesos penales.

Esta experiencia previa, en base a la cual resulta dable efectuar diagnósticos sobre viejos errores que posibiliten una provechosa reconducción del accionar institucional, nos posibilitan indicar que la inclusión del “delito” como parte del objeto de la ciberseguridad resulta una medida innecesaria que, muy seguramente, terminara por sesgar los esfuerzos en la materia de un modo contrario a la obtención de los objetivos propuestos.

Resumen de comentarios para evaluar su inclusión en la Estrategia Nacional de ciberseguridad:

- Incluir seguridad de la información desde el diseño y durante todo el ciclo de vida para productos y servicios digitales.
- Promover las medidas de seguridad de la información para proteger datos personales y la privacidad de todas las personas.
- Promover la capacitación conjunta de la seguridad de la información y la protección de datos en los planes de educación de todos los niveles de formación.
- Promover línea base (requisitos mínimos) de seguridad de la información para productos y servicios digitales para el Sector público y privado.
- Incluir hitos/metas concretas con estimación de plazos y presupuestos como anexo o en ANEXOS.
- Fortalecer las capacidades del CERT nacional y promover la formación de CSIRT sectoriales.
- Fomentar la atención de incidentes de seguridad con impacto en datos personales por parte de los CSIRT a fin de tratar la problemática a nivel ciberseguridad identificando vulnerabilidades, amenazas y recomendaciones.
- Eliminar la referencia al delito en la definición de ciberseguridad y orientar el objetivo 3 al fortalecimiento de las capacidades de prevención, detección y respuesta ante incidentes de seguridad informática o ciberseguridad, en la misma línea.

1 European Cybersecurity Skills Framework https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

2 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)&from=EN

3 Capítulo 14.: Gestión de Riesgos de Seguridad Digital, Políticas de banda ancha para América Latina y el Caribe: Un Manual para la Economía Digital, 7 nov 2016, https://read.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean_9789264251823-en#page12

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2023-17579657-APN-DGDYD#JGM

CIUDAD DE BUENOS AIRES
Miércoles 15 de Febrero de 2023

Referencia: Documentación respaldatoria

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.02.15 17:27:10 -03:00

Tomas Francisco POMAR - 27323183851
en representación de
OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO
O.D.I.A. - 30716467828

Digitally signed by Gestion Documental Electronica
Date: 2023.02.15 17:27:10 -03:00