44˚ Sesión Cerrada de la Asamblea Global de Privacidad

Octubre de 2022

Proyecto de Resolución sobre la Creación de Capacidades de Cooperación Internacional para Mejorar la Regulación de la Ciberseguridad y sobre la Comprensión de los Daños Causados por los Ciberincidentes (v1.9 final)

Esta Resolución es presentada por:

PATROCINADORES:

- Oficina del Comisionado de Información, Reino Unido

COPATROCINADORES:

- Oficina del Comisionado de Información de Australia, Australia
- Comisaría de Protección de Datos Personales, Canadá
- Superintendencia de Industria y Comercio (SIC) de Colombia
- Inspección de Protección de Datos de Estonia, Estonia
- Supervisor Europeo de Protección de Datos, Unión Europea
- Comisión Nacional de Informática y Libertades (CNIL), Francia
- Comisionado de Protección de Datos de Ghana (GDPC), Ghana
- Autoridad Reguladora de Gibraltar (GRA), Gibraltar
- Oficina del Comisionado de Privacidad de Datos Personales, Hong Kong, China
- Autoridad Israelí de Protección de la Privacidad (PPA), Israel
- Oficina del Comisionado de Información de Jersey (JOIC), Jersey
- Comisión Nacional de Privacidad, Filipinas
- Comisión de Protección de la Información Personal, República de Corea
- Agencia Catalana de Protección de Datos, Cataluña, España
- Comisionado Federal de Protección de Datos e Información (FDPIC), Suiza
- Autoridad Turca de Protección de Datos Personales (KVKK), Turquía

- Unidad de Regulación y Control de Datos Personales, Uruguay.

Los 44° Asamblea Global de Privacidad 2022:

DESTACA QUE la economía y la sociedad globales aportan una serie de beneficios, como el comercio mundial, la difusión global de la tecnología y la innovación, la comunicación, la colaboración y el intercambio de conocimientos y recursos para abordar los problemas mundiales, y el intercambio intercultural, y que estos beneficios sólo pueden aprovecharse adecuadamente si los datos personales están debidamente protegidos;

SE PREOCUPA por el hecho de *que* la creciente digitalización de la economía y la sociedad mundiales conlleva, además de ventajas, riesgos crecientes e importantes para los datos personales de los individuos en posesión de las organizaciones públicas y privadas;

NOTA que el riesgo puede incluir amenazas accidentales, pero también deliberadas, tales como los intentos de vigilancia y acceso a los datos procedentes de fuentes como los agentes estatales y las grupos delictivos ajenos al Estado en muchas jurisdicciones, que a menudo tienen operaciones transfronterizas;

RECONOCE que la confidencialidad, la integridad y la disponibilidad, los tres elementos clave de la seguridad de la información, están en riesgo como resultado de estas amenazas; si cualquiera de los tres elementos se ve comprometido, puede haber graves consecuencias para los responsables del tratamiento de datos, y daños significativos para las personas cuyos datos personales se ven afectados;

DESTACA que un principio común a las leyes de privacidad y protección de datos en todo el mundo es que los datos personales deben estar protegidos por garantías de seguridad adecuadas contra riesgos como la pérdida o el acceso no autorizado, la destrucción, el uso, la rectificación, la divulgación o la oposición;

REITERA la importancia de conservar la confianza de los ciudadanos en las redes y los sistemas informáticos a través de los cuales se procesan los datos personales, y la importante función que desempeñan las garantías sólidas a la protección de los datos y la privacidad frente a las ciberamenazas;

NOTA que la resistencia cibernética de los sistemas de procesamiento de datos está bajo un asedio grave y que los medios de comunicación y los analistas de seguridad han informado de un aumento de los ciberataques en todo el mundo, los cuales pueden incluir ataques a la cadena de suministro, accesos no autorizados, *ransomware*, suplantación de identidad o phishing;

SE PREOCUPA porque, según los reportes, los incidentes de ciberseguridad tienen ahora importantes consecuencias económicas para la sociedad y que son la principal amenaza para el éxito financiero de las organizaciones[1] y las posibles barreras comerciales que esto puede causar; y que estas

[1] La ciberseguridad es la principal amenaza que preocupa a los CEO, según una encuesta mundial realizada por PriceWaterHouse Coopers en enero de 2022 (25th Annual Global CEO Survey - PwC). Lo que más preocupa a los CEOs es la posibilidad de que un ciberataque o una crisis macroeconómica socaven la consecución de los objetivos financieros de su empresa.

consecuencias también afectan notablemente a las organizaciones más pequeñas y con menos recursos que procesan datos personales;

PREOCUPADA también porque las organizaciones no siempre ejecutan las acciones necesarias para actualizar las medidas técnicas y organizativas, como la seudonimización o el cifrado, dentro de los sistemas heredados para estar bien equipadas contra los crecientes ciberataques, lo que genera riesgos que tienen que abordar las autoridades de protección de datos y de la privacidad, en colaboración con terceros, y que esos riesgo aumentan si las organizaciones no informan de esos ataques, violaciones de datos y otros incidentes cuando se producen o cuando se descubren;

PREOCUPADA porque un solo ciberataque puede tener graves consecuencias para muchas víctimas en diferentes jurisdicciones; y *DESTACA* la consecuente importancia de evitar la duplicación del trabajo de reglamentación, lo que a su vez demuestra el valor de la cooperación en materia de amenazas comunes, tanto entre las autoridades de los miembros de la GPA, como con los organismos de ciberseguridad cuando sea apropiado y lo permitan las leyes locales;

DESTACA las próximas Recomendaciones de la OCDE sobre la seguridad digital de los productos y servicios, y sobre el tratamiento de las vulnerabilidades, con base en los trabajos existentes realizados por el Comité de Política de Economía Digital de la OCDE en 2021 junto con expertos externos, que promueven la seguridad por diseño y por defecto en los productos y servicios, el uso de la experiencia de los investigadores de seguridad para identificar, informar y revelar las vulnerabilidades de seguridad digital, así como las estrategias de cumplimiento alineadas con los requisitos de la ley de protección de datos;

NOTA que las políticas públicas han comenzado a evolucionar a nivel nacional en el fortalecimiento de la protección de las infraestructuras críticas nacionales, incluida la protección de los servicios públicos y esenciales y la garantía de la notificación precisa de incidentes y violaciones de datos. Al hacerlo, los gobiernos han reconocido la estrecha relación que se requiere entre la legislación/regulación sobre protección de datos y la legislación sobre sistemas de información y seguridad de las redes, para diseñar soluciones eficaces de prevención de incidentes, de respuesta y de aplicación de la ley, en particular cuando se trata de la protección de infraestructuras nacionales críticas;

RECONOCE que las autoridades de protección de datos y privacidad de las distintas jurisdicciones tienen responsabilidades, competencias y poderes muy diferentes en relación con la ciberseguridad; pero *NOTA el* estrecho vínculo de la ciberseguridad con los requisitos de muchas leyes de protección de datos y de la privacidad relativos a la seguridad, la confidencialidad, la integridad y la disponibilidad de los datos personales;

REITERA la misión de la GPA, que incluye la conexión y el apoyo a los esfuerzos a nivel nacional y regional, y en otros foros internacionales, para permitir a las autoridades proteger y promover mejor la privacidad y la protección de datos; y la importancia de la creación de capacidades, la cooperación, el intercambio de información y el conocimiento para promover la misión;

RECUERDA que la primera prioridad estratégica de la GPA es avanzar en la privacidad en una era de digitalización acelerada, así como la relevancia de la ciberseguridad en la consecución de esa prioridad; y *RECUERDA también* que el Plan Estratégico de la GPA 2021-23[2] requiere que la GPA

[2] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

supervise las oportunidades de cooperación, observando los riesgos digitales nuevos y emergentes que se plantean para la privacidad de las personas;

RECUERDA que la GPA ya ha reconocido[3] que la convergencia hacia principios clave y normas elevadas para el acceso de los gobiernos a los datos personales en posesión del sector privado puede contribuir a la seguridad jurídica y a la facilitación de los flujos de datos en la economía digital mundial, y ha destacado la importancia de la ciberseguridad en todos los sistemas y entre ellos;

DESTACA la importancia de la ciberseguridad para la protección de los datos y de la privacidad, y está preocupada por los daños importantes que pueden causar los ciberataques a las personas y, en particular, a las pertenecientes a grupos vulnerables; entre dichos ciberataques están la obtención, el cotejo y la venta de datos personales con fines fraudulentos;

NOTA que algunas autoridades de protección de datos y privacidad ya han empezado a mapear los daños a la ciberseguridad en relación con otros perjuicios y a identificar los daños sociales y personales generados por los incidentes cibernéticos; sin embargo, saben que es necesario hacer más ejercicio de comparación entre jurisdicciones: los daños, más que los abusos identificados, (por ejemplo, los daños físicos, psicológicos, culturales, políticos, económicos y de reputación tanto a nivel individual como social); los modelos utilizados para evaluar o categorizar estos daños; el análisis de las deficiencias; y cuáles deberían ser las consecuencias normativas;

DESTACA que los daños causados por los incidentes de ciberseguridad son diversos y ameritarían un mayor análisis sobre la mejor manera de proteger a las personas de esos daños;

OBSERVA que los gobiernos de muchas jurisdicciones están colaborando para proteger la seguridad nacional y las infraestructuras nacionales críticas;

DESTACA que los reguladores de la protección de datos y privacidad también deben estar dispuestos a colaborar, según proceda, en las estrategias internacionales y nacionales para proteger los datos de las personas en relación con los incidentes cibernéticos; y también que la GPA está muy bien dispuesta para promover el intercambio eficaz de datos reglamentarios entre sus miembros en torno a las vulnerabilidades y amenazas la ciberseguridad;

Por lo tanto, la 44° Asamblea Global de Privacidad resuelve:

1. **Adoptar medidas para desarrollar una comprensión de las competencias y responsabilidades de las autoridades miembros del PAM en relación con la ciberseguridad;**
2. **Explorar las posibilidades de cooperación internacional, el intercambio de conocimientos e información, incluyendo la experiencia técnica y las mejores prácticas, entre los miembros de la GPA para evitar la duplicación en las investigaciones u otras actividades reguladoras en relación con los problemas de ciberseguridad y los enfoques reguladores en lo que respecta a la protección de datos y la privacidad;**
3. **Solicitar al Grupo de Trabajo de Cooperación para el Cumplimiento de la Normativa Internacional de la GPA que realice un trabajo exploratorio para el otoño de 2023, teniendo en cuenta el trabajo realizado por otros Grupos de Trabajo de la GPA cuando sea pertinente y consultando con el Panel de Referencia de la GPA, según corresponda. La GPA también**

[3] 20211025-GPA-Resolución-Government-Access-Final-Adopted .pdf (globalprivacyassembly.org)

deberá determinar si prosigue el trabajo en el marco de su próximo Plan Estratégico a partir de 2023.

4. **Solicitar al Grupo de Trabajo de Cooperación Internacional para el Cumplimiento de la Normativa que acuerde un plan de trabajo para llevar a cabo los pasos anteriores, centrado en resultados claros y prácticos que deberían incluir la celebración de una sesión cerrada sobre cuestiones de ciberseguridad en 2023.**

Nota explicativa

La creciente prevalencia de los ciberataques en todas las regiones del mundo exige una respuesta normativa sólida y coordinada para proteger los datos personales de las personas. Los actores gubernamentales y los grupos criminales ajenos al Estado suponen amenazas en el ciberespacio cada vez con más facilidad, en parte debido a la rápida aceleración de la interconexión digital de la sociedad desde el advenimiento de la pandemia por COVID-19[4] , pero también debido a las vulnerabilidades de la cadena de suministro en los productos finales. Esta resolución se centra en la mitigación y reparación de los ciberataques. Los miembros de la GPA han llevado a cabo un importante volumen de investigaciones sobre incidentes cibernéticos en los que se ha descubierto un pésimo manejo de las categorías de datos más sensibles, como el cambio de sexo, los datos sanitarios y la identidad física (que podría incluir la raza o el origen étnico, etc.). La falta de concienciación en materia de seguridad en las organizaciones, la falta de responsabilidad en materia de seguridad de la información, la gestión eficaz de los riesgos y las comprobaciones periódicas a lo largo de la cadena de suministro suelen ser temas problemáticos.

Los complejos ecosistemas de proveedores de servicios pueden significar un mayor riesgo de vulnerabilidad, por ejemplo, un ataque a la cadena de suministro en un único punto débil generado por una mala gestión del riesgo de la cadena de suministro puede permitir a los ciberatacantes el acceso persistente a muchos otros servidores a nivel mundial durante un período sostenido. El dinero, los datos personales y la información de los individuos están en riesgo y su acceso a los servicios y conocimientos del sector público y privado se ve afectado de manera importante como resultado de estas ciberamenazas.

Los gobiernos y las autoridades regionales o las agrupaciones de cooperación gubernamental han reaccionado con nuevas leyes, políticas e iniciativas de investigación para proteger sus infraestructuras nacionales críticas, a fin de salvaguardar su función en el mantenimiento de sus funciones públicas, y los medios de operación de las empresas, que son fundamentales para la salud de las economías nacionales. La ciberseguridad no supone un único factor para las organizaciones; es necesario considerar factores clave como la seguridad de los datos, la seguridad de los sistemas, la seguridad en línea y la seguridad de los dispositivos para evitar que se produzcan daños.

[4] Por ejemplo, el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) informó en 2021 que se habían triplicado los incidentes de ransomware, y que el gobierno, las empresas y las personas habían sido atacados de forma más agresiva que antes: ISC-Annual-Report-2019-2021.pdf (independent.gov.uk)Y para fuentes comerciales: 2021_NCC_Group_Annual_Threat_Report.pdf Página 19.

Los gobiernos siguen reconociendo la necesidad de alinear la legislación sobre protección de datos y sistemas de información en red y de seguridad, con el fin de proporcionar un esfuerzo de aplicación y prevención más completo.

Los desarrollos en Europa y América son sólo algunas de las recientes adiciones del marco general de ciberseguridad a los libros de normas legales e iniciativas de cooperación que han surgido en los últimos dos años para generar resistencia, prevenir el acceso no autorizado a las redes y permitir planes de recuperación cuando los ataques han tenido éxito. Esto puede incluir soluciones como los equipos de respuesta a incidentes de seguridad informática (CSIRT), o la institución de una autoridad nacional competente para emitir directrices y gestionar incidentes de información o seguridad.

Las leyes regionales, nacionales y locales han exigido a los ayuntamientos y a otras autoridades públicas con capacidad de decisión que aumenten significativamente su capacidad de resistencia, y algunas autoridades de protección de datos y privacidad ya están estudiando la forma de ayudar en estos esfuerzos.

Algunas entidades intergubernamentales como la OCDE han reconocido[5] la necesidad de coordinar e informar mejor a las partes interesadas a lo largo de las cadenas de suministro para abordar eficazmente las amenazas a la vulnerabilidad, comprender mejor la posición de los investigadores de seguridad y desarrollar formas para que la buena gestión de la vulnerabilidad sea reconocida como indicador de cumplimiento de la legislación sobre privacidad como el GDPR. Asimismo a través de varios informes transnacionales de organizaciones regionales[6] como la Agencia de la Unión Europea para la Ciberseguridad (ENISA) o la Organización de Estados Americanos (OEA) se han destacado algunas de estas necesidades.

Las autoridades de protección de datos y privacidad pueden ayudar a orientar sobre el cumplimiento con la ley, así como sobre lo que significan las nuevas leyes para una mejor protección de los datos personales en caso de ciberataque. Existe un reconocimiento incipiente de los vínculos que las autoridades de protección de datos y privacidad deben forjar con sus homólogos nacionales para ofrecer una respuesta coordinada, sólida y basada en el riesgo contra las ciberamenazas. Sin embargo, también hay que contemplar el establecimiento de vínculos con entidades de otras partes del mundo para combatir más eficazmente las amenazas internacionales a los datos personales de los individuos y mantener la estabilidad del ciberespacio.

La Asamblea Global de Privacidad (GPA) ha empezado a estudiar con más detalle las amenazas aisladas a la ciberseguridad en los últimos años, desde que surgió la pandemia del COVID-19, en particular estudiando temas como la reutilización de credenciales robadas, y la forma en que las empresas de videoteleconferencia (VTC) pueden proteger a sus usuarios de las amenazas a las reuniones en línea.

No obstante, la GPA puede actuar de forma más amplia en relación con la promoción y la creación de una mejor comprensión entre sus miembros sobre la gama de daños a la ciberseguridad, tanto

[5] pdf (oecd.org) Grupo de Trabajo sobre Seguridad en la Economía Digital - Informe: Página 76, FOMENTO DEL TRATAMIENTO DE VULNERABILIDADES Gestión, tratamiento y divulgación responsables de las vulnerabilidades, febrero de 2021

[6] Políticas coordinadas de divulgación de vulnerabilidades en la UE - ENISA (europa.eu) ENISA, abril de 2022 y National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf (oas.org) OEA, junio de 2022

individuales como sociales, a partir de investigaciones recientes realizadas por cada uno de los miembros de la GPA.

El Plan Estratégico de Implementación 2021-2023 de la GPA ha encomendado claramente a[7] sus miembros que identifiquen y consideren los temas de interés relacionados con la vigilancia de los ciudadanos y consumidores en la economía digital, y que el Grupo de Trabajo de Cumplimiento Internacional y el Grupo de Trabajo de Economía Digital dirijan esta labor, con el apoyo de otros.

La GPA también ha pedido a[8] su Grupo de Trabajo Internacional para la Aplicación de la Ley que siga vigilando las oportunidades de cooperación para la aplicación de la ley, señalando los nuevos emergentes riesgos digitales emergentes a la privacidad de las personas. Los retos expuestos en esta resolución entrarían en el mandato actual de este Plan Estratégico.

El Grupo de Trabajo Internacional para el Cumplimiento de la Normativa debería considerar y acordar las actividades que se detallan a continuación para que su plan de trabajo de 2023 se traduzca en resultados claros y prácticos:

- En los últimos años, el Grupo de Trabajo Internacional para el Cumplimiento de la Ley ha desarrollado la capacidad para llevar a cabo sesiones cerradas sobre el cumplimiento de la ley y, en la actualidad, este Grupo de Trabajo está mejor organizado para llevar a cabo un trabajo exploratorio en 2023 sobre las amenazas y los daños de la vigilancia a las personas y la sociedad.

- El Grupo de Trabajo no funcionaría de manera aislada, sino que tendría en cuenta la labor pertinente llevada a cabo por otros Grupos de Trabajo de la GPA, como la del Grupo de Trabajo sobre el Ciudadano y el Consumidor Digitales, que actualmente examina otros ámbitos de intersección entre las normativas, y consultaría con el panel de referencia de las partes interesadas, según proceda.

- La GPA debería realizar los primeros esfuerzos para explorar las oportunidades de cooperación en este campo. Puede ser útil que las autoridades de protección de datos y privacidad intercambien información para combatir más eficazmente la ciberactividad delictiva en relación con los datos personales de los individuos. Esto puede incluir el explorar cómo se pueden tomar medidas comunes para resolver los problemas a los que se enfrentan simultáneamente todas las jurisdicciones. Esto ayudará a evitar la duplicación de esfuerzos en las investigaciones de los miembros de la GPA.

- La GPA también podría, según el caso, participar en el intercambio de información y explorar la cooperación con las organizaciones regionales e internacionales que se ocupan de la ciberseguridad.

- La Asamblea sigue estando dispuesta a actuar con base en la exitosa colaboración anterior en asuntos aislados relacionados con los incidentes cibernéticos que se han descrito

[7] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org) Ver especialmente la página 16.
[8] Ibid, página 21.

anteriormente. En este caso, la GPA podría compartir experiencias o comparar modelos existentes para prevenir, mitigar o evitar los daños generados por las ciberamenazas, contribuyendo así a la creación de capacidades en materia de ciberseguridad a nivel nacional. a GPA también puede ayudar a aprovechar los conocimientos técnicos de las autoridades con más fuerza en beneficio de los miembros con menos recursos disponibles para esta actividad

Este trabajo de cooperación internacional de la GPA puede ayudar a proteger a las personas en múltiples jurisdicciones de los daños económicos y psicológicos. También puede servir de apoyo a los esfuerzos nacionales para asesorar a las organizaciones en caso de ataques de ransomware, por ejemplo, cuando las organizaciones se quedan sin acceso a sus propios datos hasta que se paga una suma de dinero, u otras consecuencias económicas graves de los ataques a la cadena de suministro.

La GPA deberá determinar en la Sesión cerrada de 2023 si se continúa trabajando en la ciberseguridad y en las amenazas y daños relacionados con la vigilancia. Deberá basarse en el trabajo exploratorio realizado en 2022 en virtud de la presente Resolución. Cualquier trabajo posterior se llevaría a cabo en el marco del próximo Plan Estratégico de la GPA que se adoptará en 2023.

FIN