2

DERECHOS HUMANOS Y SEGURIDAD DIGITAL: UNA PAREJA PERFECTA

El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital: El caso de la OEA

Maricarmen Sequera, Amalia Toledo & Leandro Ucciferri
Mayo 2018

Esta publicación es el segundo documento de la serie *Análisis de políticas sobre ciberseguridad y derechos humanos en Latinoamérica,* que desarrollan en conjunto las organizaciones TEDIC de Paraguay, la Asociación por los Derechos Civiles (ADC) de Argentina y la Fundación Karisma de Colombia. Ha sido posible gracias al apoyo y financiación de Privacy International y Ford Foundation.

Autores:
Maricarmen Sequera, TEDIC
Leandro Ucciferri, ADC
Amalia Toledo, Fundación Karisma

Colaboración:
Francisco Vera
Lucy Purdon

Diseño editorial:
Diantres

Diagramación:
Leandro Ucciferri

Mayo 2018

TABLA DE CONTENIDOS

Introducción

Desde hace más de 7 años, la Organización de Estados Americanos se ha ido posicionando como uno de los organismos clave en las agendas de seguridad digital desarrolladas por diversos países en América Latina, así como también en la generación de tendencias a nivel regional.

En este tiempo, la OEA ha publicado una serie de declaraciones, guías y recomendaciones, ha trabajado con diversos países en la región para incentivar, promover y profundizar el rol de los CSIRT, ha influenciado en la adopción de políticas públicas y prestado asistencia técnica para la elaboración de planes o estrategias nacionales de seguridad digital.

A lo largo de esta segunda entrega en la serie "Derechos humanos y seguridad digital: Una pareja perfecta", realizamos un recorrido adentrándonos en el mundo de la OEA y todos sus organismos vinculados a la seguridad digital, con el fin de facilitar a la sociedad civil una guía para la navegación de este organismo, efectuar un diagnóstico que nos permita situar al lector en la actualidad de la temática a nivel regional y descubrir la agenda de seguridad digital que sostiene la OEA en el continente.

Finalmente, concluimos este informe con una serie de breves recomendaciones dirigidas a los organismos de la OEA. Con ello, esperamos que este órgano reconozca el papel que puede jugar como catalizador en el desarrollo de procesos más inclusivos y abiertos.

Incursión de la OEA y sus organismos en seguridad digital

La OEA es el organismo regional que sirve como foro gubernamental político, jurídico y social de las Américas. Reúne a 35 Estados americanos con el fin de "lograr un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia"[1]. Los principios que guían a la organización en esta labor son la democracia, los derechos humanos, la seguridad y el desarrollo.[2]

Desde su creación en 1948 hasta principios del 2000, la OEA operó bajo el concepto tradicional de seguridad: el Estado como centro y sujeto de la seguridad, y la primacía de las fuerzas armadas en la protección de seguridad nacional.[3]

Sin embargo, al finalizar la Guerra Fría la discusión global empezó a girar en torno a la necesidad de una actualización del concepto, de un cambio de paradigma. Así, se empezó a reconocer la interdependencia de múltiples actores, incluidos los no estatales, y la diversidad de asuntos que afectan la seguridad global y que, además, no eran exclusivamente militares.

En las Américas, este nuevo replanteamiento del concepto se materializó en la adopción, en 2003, de la "Declaración sobre Seguridad de las Américas", que reconoce la necesidad de actualizar el sistema para que responda a la nueva realidad mundial, que dejaba atrás un paradigma como la doctrina de la seguridad nacional. La reconceptualización de la seguridad reconoce que los problemas son de índole multidimensional y los desafíos son de diverso tipo: terrorismo, narcotráfico, crimen organizado, degradación del medio ambiente, pobreza, migraciones, ciberataques, etc.

---

1 Carta de la Organización de los Estados Americanos (1948). Disponible en https://bit.ly/2sijVPM
2 Véase el sitio web de la OEA en https://bit.ly/2LB6oed
3 La OEA es la organización regional más antigua del mundo, cuyo orígenes se remontan a la Primera Conferencia Internacional de los Estados Americanos en 1889. En la Novena Conferencia de 1948, celebrada en Bogotá, Colombia, 22 Estados americanos aprobaron la creación de la organización como hoy la conocemos.

Con esta aproximación, se reconoce que el Estado ya no está en el centro de la seguridad, sino que se traslada a las personas. Por ello, se abordan un rango más amplio de problemas que los puramente militares y en el que convergen diversidad de actores: estatales, no estatales, supranacionales. Además, la Declaración reitera que las "nuevas amenazas" requieren de la cooperación de los organismos especializados de la OEA y de los Estados miembros.

A un año de la adopción del concepto de seguridad multidimensional, durante la 34a sesión ordinaria de la OEA, ve la luz la Resolución 2004 o la "Estrategia Interamericana de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética". Con ella, se aborda una de las múltiples "nuevas amenazas" identificadas –ataques a la seguridad cibernética– en la Declaración de 2003 y sus compromisos para combatirla.

Esta estrategia se apoya especialmente en la experiencia técnica de tres organismos especializados de la OEA: el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y las Reuniones de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). Además, son partes claves en la consecución de los compromisos de la Resolución 2004 a través de varias iniciativas.

En este sentido, es importante entender qué papel juegan estos organismos en el tema de seguridad digital para el Hemisferio, con qué facultades cuentan y qué resultados –si alguno– han obtenido las iniciativas propuestas.

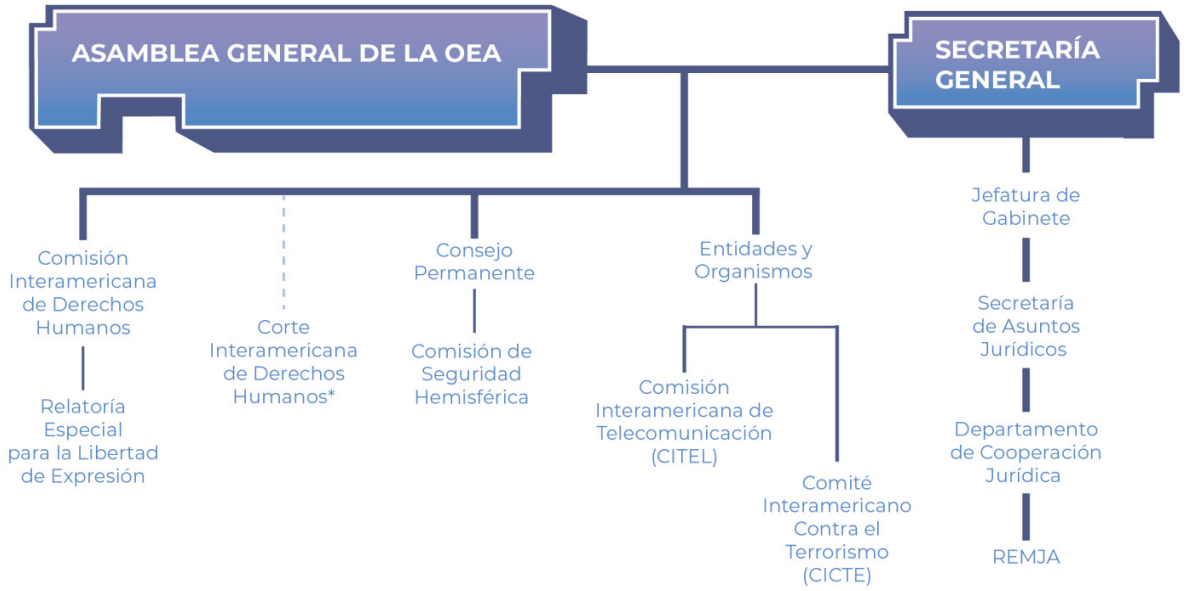

Imagen 1. Diagrama de los organismos y foros de la OEA

CICTE

El CICTE fue creada por la Asamblea General de la OEA en 1999 con el fin de promover el desarrollo y la cooperación entre los Estados miembro para prevenir, combatir y eliminar al terrorismo en cualquiera de sus manifestaciones.[4] Tiene completa autonomía técnica en el ejercicios de sus funciones y depende directamente de la Asamblea General.[5] Debido al carácter intergubernamental del organismo, la primacía es de los Estados miembros. La sociedad civil tiene espacio de participación en reuniones del Comité siempre que sea invitada y reciba la aprobación del gobierno del país donde ocurra la reunión.[6]

Este comité empezó a trabajar los temas de seguridad digital a partir de la Resolución 2004, en la que se le encomendó la creación de una red de alerta sobre seguridad digital para las Américas. El objetivo de la red es ofrecer información actualizada y asesoría a los Estados miembros frente a vulnerabilidades informáticas. En primer lugar, el plan incluía crear una plataforma de colaboración y comunicación entre los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT, del inglés) y ofrecer asistencia técnica para su creación en los países donde no existían; y en segundo lugar, brindar capacitación especializada a miembros de los CSIRT nacionales.

4 Véase el sitio web del CICTE en https://www.oas.org/es/sms/cicte/default.asp
5 CICTE. (2005, 17 de febrero). Reglamento del Comité Interamericano contra el Terrorismo. OEA/Ser.L/X.2.5, CICTE/doc.4/05 rev. 1, art. 2(a) y (b). Disponible en https://bit.ly/2G4MeVT
6 Ibid., art. 22.

Con el tiempo, los esfuerzos del CICTE también incluyeron el desarrollo de ejercicios de simulación de incidentes informáticos para evaluar los mecanismos de respuesta e intercambio de información, y la asistencia técnica en la elaboración de estrategias nacionales de seguridad digital.[7]

En 2012 y como respuesta a la "Declaración de Fortalecimiento de la Seguridad Cibernética en las Américas",[8] el CICTE se consolidó como el ente articulador de los múltiples CSIRT en la región y como catalizador de programas de capacitación en materia de seguridad digital. Vale notar también que a partir de esta declaración, el Comité comienza a tomar un rol preponderante de apoyo y acompañamiento a los Estados miembros en los procesos de formulación de estrategias nacionales de seguridad digital. Quizá, el antecedente más importante es el pedido del Gobierno de Colombia en 2014 y 2015 de una Misión Técnica de la OEA para evaluar la situación de la seguridad digital en el país.[9]

Finalmente, al CICTE también se le encomendó la elaboración de proyectos de asistencia técnica para el manejo de riesgos en la infraestructura crítica de los Estados miembros y la identificación de servicios de pago en línea que puedan ser usados por organizaciones terroristas.[10]

Hoy en día, el CICTE, a través de su programa de seguridad cibernética, "emplea un enfoque integral en la construcción de capacidades de seguridad digital entre los Estados miembros".[11] Trabaja tanto aspectos políticos como técnicos de la seguridad digital mediante programas de capacitación, misiones de asistencia técnica, ejercicios de simulación y procesos de sensibilización para promover una cultura de seguridad y confianza digital en el hemisferio.

---

7 CICTE. (2011, 17 de marzo). Informe sobre las actividades de la Secretaría del Comité Interamericano contra el Terrorismo. OEA/Ser.L.X.2.11, CICTE/doc.6/11, p. 13. Disponible en https://bit.ly/2IAXFtA; también véase CICTE. (2013, 8 de marzo). Report on activities of the Secretariat of the Inter-American Committee Against Terrorism. OEA/Ser.L.X.2.13, CICTE/doc.5/13, p. 6. Disponible en https://bit.ly/2rzKxe1

8 Declaración sobre el Fortalecimiento de la seguridad cibernética en las Américas. (2012, 9 de marzo). OEA/Ser.L/X.2.12. Disponible en https://bit.ly/2IytuTZ

9 Loten, J.M. (2015, 23 de marzo). Informe de la Presidente del Comité Interamericano contra el Terrorismo 2014-2015. OEA/Ser.L/X.2.15, CICTE/doc.4/15 Cor.1, pp. 2-3. Disponible en https://bit.ly/2KMsFW1

10 Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes. (2015, 23 de marzo). OEA/Ser.L/X.2.15, párrs. 9 y 10. Disponible en https://bit.ly/2wvckC2

11 Véase el sitio web del programa de Seguridad Cibernética de la OEA en https://bit.ly/1kgBA3n

CITEL

La CITEL es el organismo asesor de la OEA especializado en telecomunicaciones, cuya creación se remonta a 1993.[12] Su enfoque de trabajo es facilitar la colaboración y coordinación con organismos regionales e internacionales de telecomunicaciones, así como entidades que trabajan ese sector; proveer capacitación al sector público y privado en temas de telecomunicaciones; aportar recomendaciones o estudios en aspectos técnicos, jurídicos, económicos y de regulación del sector; determinar las prioridades regionales en telecomunicaciones; entre otros.[13]

Hacen parte de la CITEL los Estados miembros de la OEA, los miembros asociados[14] –agrupados en dos comités permanentes: el de telecomunicaciones/TIC y el de radiodifusión– y los observadores[15]. Cualquier entidad, organización, institución y academia relacionada con la industria de las telecomunicaciones o de las TIC puede adquirir su condición de miembro asociado previa solicitud al respecto y pago de una cuota de membresía.[16] Los miembros asociados pueden participar en todas las actividades de los comités permanente a los que estén adscritos, con voz pero sin voto.[17]

Uno de los objetivos estratégicos de la CITEL es la seguridad digital, tema que fue definido en la Resolución de 2004. En este documento, la Asamblea General de la OEA le asigna a la CITEL la labor de mejorar la seguridad y confidencialidad de la arquitectura de internet.[18] Esto implicaba adaptar cualquier norma o práctica internacional a las realidades nacionales y regionales, sin que afectara la eficacia de toda la red. Para ello, la Resolución 2004 adopta una visión prospectiva con el fin de facilitar la integración de nuevos equipos y tecnologías.

---

12 AG/RES.1224 (XXIII-O/93).
13 Estatutos de la Comisión Interamericana de las Telecomunicaciones (2014, 5 de junio), art. 1. Disponible en https://bit.ly/2jNQq3t
14 Los Miembros Asociados son entidades, organizaciones o instituciones relacionados con las telecomunicaciones o las TIC o la industria. También incluye organizaciones internacionales o regionales relacionadas con el área de trabajo de la CITEL. Ibid., art. 24.
15 Los observadores se dividen en dos grupos: observadores permanente ante la OEA, que pueden participar de las sesiones públicas de la Asamblea de la CITEL, de sus comisiones y, cuando sean invitados, de las reuniones privadas; y aquellos ante la comisión misma, que constituyen los organismos especializados y órganos de la OEA, así como otras organizaciones interamericanas. Ibid., arts. 13 y 14.
16 Reglamento de la Comisión Interamericana de Telecomunicaciones (2014, 5 de junio), art. 85. Disponible en https://bit.ly/2G3xqqk
17 Ibid., art. 86.
18 Estrategia de seguridad cibernética (2004, 8 de junio). AG/RES. 2004 (XXXIV-O/04). Disponible en https://bit.ly/2Ib4H4X

Desde entonces, parte del trabajo de la CITEL se ha concentrado en trabajar la protección de infraestructuras críticas para "compartir estrategias; en mejores prácticas, marcos, experiencias y políticas"[19]; en promover una cultura de la seguridad digital hemisférica[20]; en desarrollar marcos metodológico e identificar mejores prácticas en seguridad digital[21], en fomentar el debate y el intercambio de información sobre políticas/regulaciones de TIC que afecten derechos de las personas, y en trabajar en aspectos técnicos de la seguridad digital de los servicios de telecomunicaciones,[22] etc.

REMJA

Las REMJA son el foro político y técnico del Hemisferio en materia de justicia y cooperación jurídica internacional. Desde 1997 y cada dos años, ministros de Justicia, Procuradores y/o Fiscales Generales de los Estados miembros de la OEA que tienen responsabilidades en cooperación jurídica internacional en materia penal se reúnen para trabajar en la coordinación de políticas públicas, formular recomendaciones e intercambiar información en las áreas de competencia del proceso.[23] Además de los ministerios y autoridades máxima para la cooperación jurídica, participan en las REMJA: los Estados observadores permanente ante la OEA, los organismos de la OEA cuyas competencias estén relacionadas con el trabajo de este foro, los organismos regionales e internacionales, y las organizaciones de la sociedad civil registradas ante la OEA.[24]

Los acuerdos alcanzados en las REMJA son conocidas como recomendaciones, que se adoptan de forma consensuada y cuyo seguimiento se realiza a través de grupos de trabajo, entre ellos, el de Delito Cibernético. Este grupo se ha encargado de trabajar los temas de seguridad digital desde un ámbito penal. Más específicamente, las REMJA tienen la labor de asegurar que las autoridades judiciales y policiales de los Estados miembros de la OEA cuenten con la capacidad y los instrumentos jurídicos necesarios para perseguir y enjuiciar delitos informáticos.[25]

---

19 Consejo Permanente. (2008, 19 de marzo). Informe Anual de la Comisión Interamericana de Telecomunicaciones a la Asamblea General. OEA/Ser.G CP/doc. 4282/08, p. 10. Disponible en https://bit.ly/2G7CyKs
20 Consejo Permanente. (2011, 24 de febrero). Informe Anual de la Comisión Interamericana de Telecomunicaciones al Cuadragésimo primer Período Ordinario de Sesiones de la Asamblea General. OEA/Ser.G CP/doc.4540/1, p. 11. Disponible en https://bit.ly/2jODPgu
21 CITEL. (2011). Informe anual 2011, p. 9. Disponible en https://bit.ly/2rAq7S3
22 CITEL. (2015). Informe anual 2015, pp. 9-10. Disponible en https://bit.ly/2K8RRVC
23 REMJA. (2012, 29 de noviembre). Documento sobre el proceso de las REMJA: Documento de Washington. OEA/Ser.K/XXXIV.7.1. Disponible en https://bit.ly/2wtOTsF
24 Ibid.
25 Estrategia de seguridad cibernética, op. cit. (nota 18). REMJA. (2004, 30 de abril). Conclusiones y recomendaciones de la REMJA V. OEA/Ser.K/XXXIV.5. Disponible en https://bit.ly/2jQ8E4y

En este sentido, las REMJA juegan un importante papel en las Américas para el fortalecimiento de los mecanismos de intercambio de información y cooperación entre Estados, empresas del sector privado y de tecnología, e instancias internacionales en material de delito informático. También ha fomentado la adhesión de los Estados americanos al Convenio del Consejo de Europa sobre la Delincuencia Cibernética (conocida como el Convenio de Budapest).[26] Finalmente, ofrece capacitaciones a los Estados para el desarrollo de legislación y medidas procesales relacionadas con los delitos cibernéticos y pruebas electrónicas.[27]

Lamentablemente, existe poca información disponible al público y mucha falta de transparencia sobre los planes de trabajo, pero de la reunión bianual podemos extraer algunos supuestos, como la retención de datos, que no parecieran estar armonizados con los estándares interamericanos de derechos humanos.

Otros organismos que se han involucrado de alguna u otra forma en las temáticas sobre seguridad digital son la Comisión Interamericana de Derechos Humanos (CIDH), a través de la Relatoría Especial para la Libertad de Expresión (RELE), y la Comisión de Seguridad Hemisférica.

CIDH – RELE

La CIDH y la Corte Interamericana de Derechos Humanos (CorteIDH) conforman las institución del sistema interamericano de protección de los derechos humanos (SIDH).[28] La Comisión tiene como misión la promoción del cumplimiento y defensa de los derechos humanos, además de servir como órgano consultivo de la OEA en la materia. Su trabajo lo realiza a través del sistema de petición individual, en el que recibe y procesa denuncias o peticiones sobre casos individuales en los que se alegan violaciones a los derechos humanos, y el monitoreo de la situación de derechos en los Estados miembros. También presenta notificaciones sobre posibles violaciones ante la CorteIDH. En su labor de monitoreo, cuenta con el apoyo de relatorías especiales que se encargan de hacer seguimiento y análisis a determinados temas, entre ellos, el de la libertad de expresión.

La forma en la que la CIDH se ha involucrado en el campo de la seguridad digital ha sido por medio del monitoreo. De hecho, a la fecha ha publicado dos informes (2013 y 2016) que

26 REMJA. (2008, 30 de abril). Conclusiones y recomendaciones de la REMJA VII. OEA/Ser.K/XXXIV.7.1. Disponible en https://bit.ly/2xr6VMG
27 REMJA. (2010, 26 de febrero). Conclusiones y recomendaciones de la REMJA VIII. OEA/Ser.K/XXXIV.8. Disponible en https://bit.ly/2IUGPqz
28 Véase el sitio web de la CIDH en https://www.oas.org/es/cidh/

han empezado a develar la posición del organismo en relación a este tipo de políticas. El análisis que se hacen en estos informes destacan el impacto de internet en los derechos humanos. Así, en 2013, se resalta cómo internet ha actuado como un potenciador de los derechos humanos, específicamente, la libertad de expresión.[29]

Hasta donde hemos podido ver, la OEA, con el apoyo de diferentes organismos, ha establecido que la información y los sistemas que soportan su uso y tráfico en el ciberespacio requieren de protección. Esta visión soporta el supuesto donde el bien que compete las políticas de seguridad digital es la información. En el marco de la Resolución 2004, esto implica que el Estado debe acompañar sus programas de masificación del uso y acceso a internet con la asesoría apropiada para sensibilizar a la ciudadanía de las amenazas e incidentes que se presentan en el ciberespacio y las herramientas que tiene a disposición el Estado para recibir reportes de estos eventos.

En este sentido, una de las preocupaciones de la CIDH que surge de estas políticas es el bloqueo o limitación de contenidos o al acceso a la información. Si bien la Resolución 2004 no aborda el tema de contenidos, pues su propuesta ha girado entorno a fortalecer la capacidad policial, judicial y fiscal para combatir y prevenir, entre otros, los ataques cibernéticos de alta intensidad,[30] podemos anotar que la CIDH debería jugar un papel más activo dentro de la OEA en materia de seguridad digital. En tanto órgano consultivo y garante de los derechos humanos, la CIDH ofrece estándares y recomendaciones que deberían ser tenidos en cuenta.[31]

---

29 Véase el artículo 13 de la Convención Americana sobre Derechos Humanos (1969), que señala: "[t]oda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

30 Aquellos que tienen como objetivo equipamentos militares o la infraestructura crítica, que traería como respuesta una acción bélica del agredido (Ilongueras. 2013).

31 De acuerdo a la RELE-CIDH, el bloqueo de contenidos se justifica cuando se protege otro derecho u otro interés público legítimo, y está establecido en la ley. Además, destaca que esta medida no puede tener como única solución la respuesta policiva. Para ello, recomienda el procesos de sensibilización y educación. Lanza, E. (2017, 15 de marzo). Estándares para una Internet libre, abierta e incluyente. OEA/Ser.L/V/II. Disponible en https://bit.ly/2xRR6hl

Comisión de Seguridad Hemisférica

La última institución que contribuye al ejercicio de la Resolución 2004 es la Comisión de Seguridad Hemisférica (CSH) del Consejo Permanente de la Asamblea General de la OEA.[32] Esta institución cumple el rol de asesor, mediador y experto en asuntos de seguridad y defensa. De hecho, el impulso final para la adopción de la Resolución 2004 surge del informe de 2003 de la CSH.

A partir de entonces, ha asesorado a los Estados miembros a través de diferentes foros y reuniones en temas de seguridad y defensa. Un ejemplo de ello tiene que ver con la identificación y presentación de las amenazas e incidentes más frecuentes a las infraestructuras críticas de los Estados miembros. Asimismo, uno de sus mandatos es trabajar en el aseguramiento de que los Estados desarrollen medidas bilaterales, subregionales y regionales que fomenten la confianza y seguridad, incluídas aquellas que conciernen al concepto de la seguridad multidimensional.

32 Véase el sitio web de la CHS en https://www.oas.org/es/council/CSH/about.asp

Declaraciones 2003 – 2016

Imagen 2. Declaraciones de organismos de la OEA vinculadas a seguridad digital.

A comienzos de diciembre de 2002, en el marco de la reunión de la CSH del Consejo Permanente de la OEA, surge la preocupación por la seguridad de los sistemas de información críticos, determinándose en quel entonces la necesidad de que los Estados miembros "desarrollen una estrategia para hacer frente a las amenazas a la seguridad cibernética".

Ese mismo mes, en los días consecutivos a la reunión de la CSH, el Comité Directivo Permanente de la CITEL celebró su duodécima reunión en Buenos Aires, Argentina. En el informe final de la reunión, se mencionan las inquietudes expresadas por los Estados miembros, en primer lugar, en lo respectivo a problemáticas de conectividad, como la creación de capacidades humanas y el desarrollo de infraestructura para reducir la brecha digital. En segundo lugar, se traen a colación las iniciativas que la OEA se encontraba iniciando para alcanzar políticas comunes "en áreas críticas como la ciberseguridad".[33]

33 Informe final de la XII Reunión del Comité Directivo Permanente de la CITEL, 21 de abril de 2003.

En tal sentido, la resolución del Comité Directivo establece que la "creación de una cultura de ciberseguridad" es parte del mandato de la CITEL. Dicha "cultura de ciberseguridad" debe encontrarse enfocada en la protección de las infraestructuras de telecomunicaciones, para generar conciencia en todos los actores involucrados en el uso de redes y sistemas de información, principalmente sobre los riesgos de seguridad de dichos sistemas y el desarrollo de medidas necesarias para enfrentarlos, pudiendo así responder rápidamente a "ciber-incidentes".

Medio año más tarde, en junio de 2003, la Asamblea General de la OEA toma a consideración los hitos ocurridos hasta entonces en materia de ciberseguridad, resolviendo así encomendarle al CICTE, la CITEL y las REMJA que se aseguren de comenzar a trabajar en el desarrollo de un proyecto de estrategia integral de la OEA sobre seguridad cibernética, el cual incluya en su abordaje los aspectos multidimensionales y multidisciplinarios de la misma.[34] Para ello, se tomaría como punto partida la conferencia propuesta por Argentina durante el tercer período ordinario de sesiones del CICTE.

La "Conferencia de la OEA sobre Seguridad Cibernética" finalmente tendría lugar un mes después, del 28 al 29 de julio de 2003, en la ciudad de Buenos Aires.[35] Allí, los participantes subrayan que toda acción eficaz para el abordaje de esta temática debe llevarse a cabo con cooperación intersectorial y coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

Asimismo, la resolución de 2003 de la Asamblea General encomienda al Consejo Permanente que inicie el desarrollo del proyecto de estrategia de seguridad cibernética para los Estados miembros en coordinación y colaboración con la CITEL, el CICTE, el Grupo de Expertos Gubernamentales sobre Delito Cibernético de las REMJA y cualquier otro órgano de la OEA vinculado a la temática, informando al Consejo Permanente sobre la implementación de la resolución y el trabajo llevado a cabo en el trigésimo cuarto período ordinario de sesiones.

A finales de enero de 2004, el CICTE adopta la Declaración de Montevideo, en la cual refuerzan su compromiso para identificar y combatir las amenazas terroristas emergentes, independientemente de su origen o motivación, incluyendo como parte de las mismas a las amenazas a la seguridad cibernética.[36]

Disponible en: https://bit.ly/2Ji4QYd

34 AG/RES. 1939 "Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética", 10 de junio de 2003. Disponible en: https://bit.ly/2J2l0p4

35 "Conferencia de la Organización de Estados Americanos sobre seguridad cibernética", Ministerio de Relaciones Exteriores y Culto (Cancillería), República Argentina, 28 de julio de 2003. Disponible en archivo (accedido por última vez 08/05/2018): https://bit.ly/2JpFGXs

36 "Declaración de Montevideo", Comité Interamericano Contra el Terrorismo (CICTE), 30 de enero

En el trigésimo cuarto período ordinario de sesiones celebrado por la Asamblea General en Quito, Ecuador, a comienzos de junio de 2004, surge la resolución sobre la adopción de una estrategia interamericana integral de seguridad cibernética.[37] La Asamblea General reconoce la apremiante necesidad de aumentar la seguridad de las redes y sistemas de información, particularmente internet, con el fin de abordar las vulnerabilidades y proteger a las personas usuarias, la seguridad nacional y las infraestructuras esenciales ante las amenazas de ataques en el espacio cibernético perpetrados con fines maliciosos o delictivos. Por otra parte, reconoce que es necesario crear una red interamericana de alerta y vigilancia para comunicar información sobre seguridad cibernética en forma rápida, para así responder a crisis, incidentes y amenazas, así como también desarrollar una internet que sea confiable y fiable para las personas.

De ahí nace la antes mencionada Resolución 2004, que insta a los Estados miembros a la implementación de su estrategia y a establecer o identificar grupos nacionales de "vigilancia y alerta", haciendo referencia a los CSIRT.

En la Resolución 2004, la OEA señala la imposibilidad de que el abordaje a las amenazas a la ciudadanía, economías y servicios esenciales (infraestructuras críticas como la electricidad, el agua y las redes de transporte) sea llevado a cabo por un único gobierno o enfrentado utilizando una única disciplina o práctica. En tal sentido, se subraya la necesidad de desarrollar la estrategia adoptando un enfoque integral, internacional y multidisciplinario.

De esta forma, para lograr un marco eficaz que alcance los objetivos de la estrategia, se mencionan determinadas condiciones que deben darse, incluyendo: proporcionar información a las personas y operadores para que puedan asegurar sus computadoras y redes contra amenazas y vulnerabilidades, para así poder responder ante incidentes y recuperarse de los mismos; fomentar asociaciones públicas y privadas para incrementar la educación y la concientización, trabajando además con el sector privado para proteger las infraestructuras que posee y opera, de las cuales generalmente dependen tanto los países como los particulares a nivel global; identificar y evaluar normas técnicas y mejores prácticas, promoviendo su adopción; y finalmente, promover la adopción de políticas y legislación sobre delito cibernético, reconociendo la necesidad de respetar la privacidad de los derechos individuales de las personas en internet.

---

de 2004. Disponible en: https://bit.ly/2J0RD6I

37 AG/RES. 2004 "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética", Asamblea General de la OEA, 8 de junio de 2004. Disponible en: https://bit.ly/2Ib4H4X

La Resolución 2004 marcó el inicio de los mandatos del CICTE, la CITEL y las REMJA como pilares fundamentales para abordar diversos aspectos de seguridad digital. Así, el CICTE es encomendado con la formación de una "Red Interamericana de Vigilancia y Alerta", para responder ante crisis, incidentes y amenazas a la seguridad informática, integrada por CSIRT nacionales que cada uno de los Estados miembros debe formar o identificar, con personal capacitado, sirviendo, además, como punto de contacto para la divulgación de información entre la Red. Por su parte, se le encomienda a la CITEL la identificación y adopción de normas técnicas para lograr una arquitectura segura de internet.

Finalmente, las REMJA se les encomienda supervisar que los Estados miembros cuenten con los instrumentos jurídicos necesarios para proteger a las personas en internet y las redes informáticas, específicamente en lo que respecta a la persecución del delito cibernético y la promoción de la cooperación internacional en asuntos vinculados al mismo. Las REMJA contribuyen a la implementación de la Resolución 2004 mediante el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, a quien se le encarga la creación de materiales de capacitación, brindar asistencia técnica y desarrollar talleres regionales para asistir en la formulación de políticas gubernamentales y leyes enfocadas en la tipificación de delitos que contemplen el uso indebido de equipos y redes informáticas.

En marzo de 2012, el CICTE reafirma nuevamente su compromiso renovado de implementar la Estrategia Interamericana de Seguridad Cibernética a través de la declaración sobre "Fortalecimiento de la seguridad cibernética en las Américas".[38] En tal sentido, destaca la labor realizada desde el 2004 para la implementación de la Resolución 2004 mediante la creación de un área de "Protección de la Infraestructura Crítica" y, dentro de ella, el "Programa de Seguridad Cibernética". A su vez, vuelve a instarse a los Estados miembros a continuar sus esfuerzos para el establecimiento o fortalecimiento de los CSIRT; aumentar el intercambio de información y la cooperación para la protección de infraestructuras críticas y prevención de incidentes de seguridad cibernética entre Estados miembros; desarrollar estrategias nacionales de seguridad cibernética integrales que involucren a todos los actores pertinentes en su desarrollo e implementación. Se destaca también la importancia de promover la cooperación del sector público con el sector privado y la academia con el fin de fortalecer la protección a las infraestructuras críticas TIC.

38 Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas", CICTE, 7 de marzo de 2012. Disponible en: https://bit.ly/2IytuTZ

Tres años después, a finales de marzo de 2015, el CICTE aprueba la declaración "Protección de infraestructura crítica ante las amenazas emergentes".[39] La declaración refuerza nuevamente el compromiso de fortalecer la cooperación entre los Estados miembros y la colaboración internacional dada la interdependencia local, regional y global de las infraestructuras críticas nacionales. Por otra parte, en la declaración se destaca el nuevo rol encomendado a la Secretaría Ejecutiva del CICTE, la cual –a pedido de los Estados miembros– trabajaría en el desarrollo de un proyecto de asistencia técnica que le permita al Estado requirente elaborar un listado de sus infraestructuras críticas junto con su clasificación, con el objetivo de que puedan llevar a cabo evaluaciones más efectivas sobre vulnerabilidades, brechas, amenazas, riesgos e interdependencia.

A comienzos de 2016, el CICTE aprueba la declaración "Fortalecimiento de la cooperación y del desarrollo en la seguridad cibernética y la lucha contra el terrorismo en las Américas".[40] Además de reiterar y reforzar los puntos establecidos en las declaraciones precedentes, introduce como novedad el compromiso de los Estados miembros para la generación de medidas de fomento de la confianza, que tengan por objetivo el fortalecimiento de la paz y la seguridad internacionales, a la vez que aumenten la cooperación, transparencia, previsibilidad y estabilidad de los Estados en el uso del ciberespacio, reduciendo de esta forma el riesgo de conflicto.

Asimismo, esta es la primera declaración del CICTE que establece menciones expresas al rol fundamental de la sociedad civil. En este sentido, la declaración reconoce la importancia de involucrar a todos los actores y partes interesadas pertinentes en el desarrollo e implementación de estrategias nacionales de seguridad cibernética integrales, dentro de los cuales incluye "al sector privado, la academia, la comunidad técnica, la sociedad civil y otros actores sociales". También se destaca la importancia de promover la cooperación entre dichos sectores con el fin de fortalecer el resguardo y la protección de las infraestructuras críticas TIC.

---

39 Declaración "Protección de Infraestructura Crítica ante las Amenazas Emergentes", CICTE, 20 de marzo de 2015. Disponible en: https://bit.ly/2wvckC2

40 Declaración "Fortalecimiento de la Cooperación y del Desarrollo en la Seguridad Cibernética y la Lucha contra el Terrorismo en las Américas", CICTE, 26 de febrero de 2016. Disponible en: https://bit.ly/2J4b5LK

OEA Cyber

A partir del año 2014, la Secretaría de CICTE emplea el uso del término OEA Cyber para hacer mención al Programa de Seguridad Digital de la organización y abordar de manera integral los compromisos que asumió en 2004. Entre los principales objetivos de la Secretaría se encuentran:

- Desarrollo de estrategias nacionales de seguridad digital;
- Capacitaciones, talleres y misiones técnicas;
- Ejercicios de seguridad digital;
- Desarrollo de CSIRT nacionales y una red hemisférica de CSIRT;
- Sensibilización, investigación y experiencia.

En el año 2013 y 2015, OEA Cyber, junto a la empresa de seguridad Trend-Micro, lanzó dos publicaciones tituladas "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", que expone datos recopilados de todos los países de las América y que reportan un aumento importante del nivel de ataques a sus sistemas de cómputo.[41]

Durante la celebración de la XLIV Asamblea General de la OEA, realizada en Asunción en el año 2014, se lanzó el informe "Tendencias de seguridad Cibernética en América Latina y el Caribe", en el que la OEA Cyber colaboró con la empresa de software de seguridad Symantec.[42] Esta publicación presenta un panorama de las tendencias y desafíos en seguridad digital en la región. El análisis se realizó con la participación de AMERIPOL, Microsoft, el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), la Corporación para la Asignación de Nombres y Números en Internet (ICANN) y el Grupo de Trabajo Antiphishing (APWG).

41 OEA & Trend-Micro (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Disponible en: https://bit.ly/2sukgyf ; OEA & Trend-Micro. (2015). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. Disponible en: https://bit.ly/1Fn3O0u
42 OEA & Symantec. (2014). Tendencias de seguridad cibernética en América Latina y el Caribe. Disponible en: https://symc.ly/1NgmZQg

Este informe recalca que el aumento de ciberdelitos en América Latina y el Caribe es un problema real que requiere la atención inmediata de los gobiernos. Los delitos más comunes contra individuos son relacionados al *phishing*, seguido de robo de la identidad para cometer fraudes financieros o a través de redes sociales. También destaca el significativo aumento de los delitos contra bancos. En contraste, identifica una disminución del vandalismo a sitios web y del "hacktivismo", que, según se señala, puede ser resultado de las acciones de prevención y control implementadas por los gobiernos.

Otro informe publicado por la OEA, en colaboración con el Banco Interamericano de Desarrollo (BID) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, es "Ciberseguridad e infraestructura crítica en las Américas".[43] En el mismo se abordan las vulnerabilidades de América Latina a los ataques cibernéticos, a través de un mapeo actualizado sobre el estado de la seguridad en la región. También revisa la madurez de las capacidades estatales en materia de seguridad cibernética. Así, analiza el estado de preparación de 32 países basados en 49 indicadores y distribuidos en cinco áreas: política y estrategia, cultura y sociedad, educación, marco legal y tecnología.

Entre los hallazgos podemos destacar que en 16 países la capacidad de respuesta a incidentes no es coordinada y que únicamente 4 países de la región superan el nivel intermedio de madurez en este aspecto. Por otro lado, 6 países de la región cuentan con programas educativos en seguridad digital. Según esta investigación, se contó con la colaboración del Center for Strategic International Studies, la Fundação Getulio Vargas, la organización FIRST, el Consejo de Europa, Potomac Institute y el Foro Económico Mundial.

Otras actividades de la OEA Cyber que valen la pena resaltar son la guía "Ciberseguridad. Kit de herramientas para la campaña de concientización" de 2015.[44] Esta publicación contó con el apoyo financiero de los Gobiernos de Canadá y Estados Unidos, y fue diseñada para proporcionar a gobiernos y/u organizaciones orientación y recursos para el desarrollo de campañas de sensibilización en materia de seguridad digital. Asimismo, resaltamos la guía de "Buenas prácticas para establecer un CSIRT nacional", que analiza el proceso de gestión, creación y puesta en marcha de un CSIRT nacional.[45]

Entre algunos de los requerimientos establecidos en la guía se observa el examen de aptitudes de recursos humanos, tanto en términos de contratación como de formación continua, que son necesarios para establecer el personal de un equipo nacional

43 BID, GCSCC & OEA. (2016). Ciberseguridad en América Latina y el Caribe. ¿Estamos preparados?. Disponible en: https://bit.ly/1S3mri3
44 OEA. (2015). Ciberseguridad. Kit de herramientas para la campaña de concientización. Disponible en: https://bit.ly/1jOxHD2
45 OEA. (2016). Buenas prácticas para establecer un CSIRT nacional. Disponible en: https://bit.ly/1S-M0mTg

de respuesta a incidentes. Asimismo, la guía presenta descripciones detalladas de infraestructura, que incluye hardware, software y procedimientos técnicos, así como mecanismos de respuestas a incidentes de seguridad de la información a una comunidad en particular.

En 2017, OEA Cyber publica el informe "Impacto de los incidentes de seguridad digital en Colombia", elaborado junto con el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el BID.[46] En él se recoge una visión del nivel de preparación de entidades públicas y empresas privadas colombianas para enfrentar amenazas a su seguridad digital. El estudio permite también conocer los costos económicos que los incidentes cibernéticos representan para los diferentes sectores de la economía del país, presentando sus hallazgos en función de los perfiles de las empresas consultadas. Este reporte proporciona recomendaciones claves para fortalecer la capacidad del sector público y las empresas privadas para prevenirlos.

A finales del 2017, Amazon Web Services firmó un acuerdo con la OEA para avanzar en desarrollar esfuerzos educativos en temas de seguridad digital para los 35 Estados que lo conforman y adaptado a los diferentes idiomas oficiales.[47] Este acuerdo incluyen seminarios web sobre seguridad digital y transformación de las tecnologías de la información, participación en múltiples eventos de seguridad digital organizados por la OEA en los Estados miembros, desarrollo de documentos técnicos (*white papers*) sobre políticas de seguridad digital, y mejores prácticas y colaboración en políticas clave e iniciativas legislativas.

Durante el primer semestre del 2018, se presentaron los siguientes documentos técnicos en el marco de esta alianza: "Un llamado a la acción para proteger a Ciudadanos, Sector Privado y Gobiernos"[48] y "Gestión nacional de riesgo cibernético"[49], con el que invitan a una reflexión sobre las oportunidades que representa la economía digital y los riesgos de la inseguridad cibernética. También se analiza el estado de la seguridad digital en las Américas con el fin de aumentar el nivel de conciencia de los líderes gubernamentales, las empresas y la sociedad en general. De otra parte, se realiza un análisis de 4 marcos estratégicos (gubernamentales, internacionales, académicos y técnicos) para que los gobiernos puedan implementar estrategias que garanticen la seguridad en el ciberespacio a la ciudadanía, las empresas y las administraciones. El informe plantea una metodología

46 BID, MinTIC & OEA. (2017). Impacto de los incidentes de seguridad digital en Colombia 2017. Disponible en: https://bit.ly/2wvny56
47 Amazon Web Service. (2017, 13 de octubre). AWS se asocia con la Organización de Estados Americanos para la seguridad cibernética [blog post]. Disponible en: https://amzn.to/2snqUGt
48 Amazon Web Service & OEA. (2018). Un llamado a la acción para proteger a Ciudadanos, Sector Privado y Gobiernos. Disponible en: https://bit.ly/2JgaI3W
49 OEA. (2018). Gestión nacional de riesgo cibernético. Disponible en: https://bit.ly/2IXoHbC

para la gestión de riesgo a largo plazo, así como unas recomendaciones para la definición e implementación de indicadores de desempeño. La publicación cuenta con los aportes de Melissa Hathaway, autora principal y miembro del Consejo de Regentes en el Potomac Institute for Policy Studies.

Por último, la OEA y Microsoft lanzaron el informe "Protección a infraestructura crítica en Latinoamérica y el Caribe 2018" en un esfuerzos para fortalecer las alianzas público-privadas con el fin de mitigar ataques en infraestructura crítica.[50] La encuesta incluida en el informe recolecta respuestas de cerca de 500 dueños y operadores de infraestructura crítica. En el documento se destaca que 69% de quienes respondieron indicaron que han notado un incremento en el número de ataques a sus sistemas computacionales y/o redes en los últimos 12 meses. Solo un 57% señaló que no cuentan con un presupuesto dedicado para medidas en seguridad digital, aunque haya un interesante incremento en sus presupuestos para la protección de la infraestructura crítica.

En resumen, todas las publicaciones realizadas por la OEA Cyber en alianza con el sector privado y los Gobiernos están centradas en la vulnerabilidad de la infraestructura crítica. También incluyen servicios que son esenciales para el buen funcionamiento de una sociedad, como servicios financieros, energía, comunicaciones y suministro de agua. Por tanto, existe una gran ausencia en situar a la persona en el punto central de esta política pública e incluir una aproximación de derechos humanos. No se contemplan políticas para la defensa de la privacidad y libertad de expresión de las personas, ni sobre las medidas de vigilancia llevadas a cabo por el propio Estado y empresas respecto de su población.

A primera vista, se lanzan propuestas que parecen necesarias e indispensables, pero que se muestran muy generales como la adhesión al Convenio de Budapest. Este documento despierta muchas controversias y se encuentra en discusión a nivel mundial. Por lo tanto, es importante realizar un análisis previo.

También se resalta una narrativa que habla de crisis inminente, algo que se mantiene en todos los informes y publicaciones citadas. Con ello, se genera un lenguaje cargado de sensación de alarma y que a la vez nubla la necesidad objetiva y evidente de fundamentar los peligros que nos ocupan.

Además, se discuten términos no consensuados como "hacktivismo" desde un punto de vista negativo, sin presentar ningún tipo de evidencias. El "hacktivismo" aparece a lo largo y ancho del planeta como forma de protesta, muy a menudo en defensa de los derechos humanos. Es una forma de libertad de expresión que se opone a veces al Gobierno,

50 Microsoft & OEA. (2018). Critical infrastructure protection in Latin America and the Caribbean. Disponible en: http://www.oas.org/cipreport

aunque no siempre. Por ejemplo, en 2015 se realizó una Hackatón Parlamentaria en el Senado de Paraguay, en la que muchos activistas se reunieron para encontrar soluciones ingeniosas a problemas de los sistemas de información del Congreso.[51]

Por otro lado, los procesos de construcción de informes, aunque reciban el apoyo del sector privado, deberían ser más abiertos en su producción y redacción final, a modo de evitar conflictos de intereses y ser percibidos como promotores de la agenda de las empresas. En todos los casos, las empresas que colaboran reciben reconocimiento de marca y validación y eso, de por sí, es un tema que podría ser potencialmente preocupante.

Planes nacionales de seguridad digital y la OEA

La OEA acompaña el desarrollo de estrategias nacionales de seguridad digital en los países de América Latina. En líneas generales, este acompañamiento consiste en que luego de la firma de un acuerdo de trabajo, la OEA elabora un análisis situacional del estado de la seguridad digital en el país. Esto puede implicar visitas *in situ* con funcionarios del Gobierno y otras partes interesadas nacionales relevantes al tema, incluidos representantes de la sociedad civil, la academia y el sector privado.

El proceso de diseño también puede implicar la organización de mesas redondas y moderadas discusiones de grupos de trabajo, la administración de encuestas y la recopilación de otra información necesaria para preparar un marco más detallado para la implementación de la iniciativa. Esta iniciativa contiene, además, una revisión de la experiencia internacional y buenas prácticas internacionales. Todo esto se realiza a través de un trabajo conjunto entre personas expertas, gobiernos y partes interesadas. El resultado final del proceso propende a desarrollar un mejor marco de ciberseguridad y una solución adaptada a sus necesidades.

Los países que han recibido asesoría técnica directa por parte del programa de OEA Cyber a la fecha han sido: Colombia, Paraguay, México, Panamá, Costa Rica, Trinidad y Tobago, Surinam y Jamaica.

A continuación se describen las experiencias de Colombia, Paraguay y México, que recibieron acompañamiento técnico por parte de la OEA Cyber. Además, son los únicos tres países que cuentan con procesos sistematizados para la creación de sus estrategias, que incluyen descripción de las mesas de trabajo, audiencias, comentarios y seguimientos

51 Tedic. (2015, 24 de noviembre). Primer hackatón parlamentaria en Paraguay [video]. Disponible en: https://bit.ly/2L6SrmW

en la implementación por diferentes actores . En cambio, los demás países que recibieron apoyo técnico de la OEA Cyber solo cuentan con resúmenes de prensa de firmas de compromisos de apoyo técnico, visitas oficiales de la OEA Cyber al país y lanzamientos de las estrategias nacionales, por lo tanto, no podrán ser valorados en este informe.

Colombia

La primera acción del Gobierno de Colombia en seguridad digital se remonta a 2005. En aquel año varias entidades estatales trabajaron en la creación de un equipo nacional de respuesta a emergencias cibernéticas –llamado posteriormente colCERT–, cuyo objetivo era proteger las infraestructuras críticas del país de incidentes digitales. Dos años más tarde, encontramos por primera vez la colaboración directa del CICTE con el Gobierno colombiano. Esto se dio a través de una capacitación y una mesa de diálogo, que concluyó con la asignación del liderazgo nacional del Ministerio de Defensa en la elaboración de una política de seguridad digital y de mecanismos nacionales de respuestas de incidentes digitales.[52]

A partir de esta designación, en 2011, se aprueba la primera política nacional de seguridad digital, conocida como "Lineamientos de Política para ciberseguridad y ciberdefensa". La política estaba orientada a enfrentar amenazas digitales contra la seguridad de la información, la infraestructura crítica, la seguridad y defensa nacional.[53] El enfoque adoptado puso en el centro al Estado y asumió que la entidad con mejores capacidades técnicas para coordinar su implementación era el Ministerio de Defensa.

Al acercarse el final de vigencia de la política de 2011[54] y con varios escándalos de interceptación ilegal de comunicaciones ocurriendo,[55] el presidente Juan Manuel Santos, en febrero de 2014, solicitó a la OEA una Misión de Asistencia Técnica para evaluar el estado de la seguridad digital del país.[56] De esta forma, una comisión internacional conformada por consultores, fiscales, directores de agencias de seguridad cibernética,

52 Departamento Nacional de Planeación. (2011, 14 de julio). Lineamientos de Política para Ciberseguridad y Ciberdefensa. CONPES No. 3701, p. 13. Disponible en: https://bit.ly/2J1ArtW
53 Ibíd., p. 5.
54 Para conocer más sobre algunos de los logros y desaciertos de la política de 2011, véase Sáenz, M.P. (2016, 5 de abril). Sobre ciberseguridad en Colombia: mucho ruido y pocas nueces [blog post]. Disponible en: https://bit.ly/2lDSRVV
55 Chuzadas: así fue la historia (2014, 8 de febrero). Revista Semana. Disponible en: https://bit.ly/2Jiz6SU. Caso Andrés Sepúlveda (s.f.). Wikipedia. Disponible en: https://bit.ly/2L5aaLC. Ocando, C. & Reyes, G. (2014, 22 de febrero). Masivo hackeo al correo electrónico del presidente Santos (2014, 22 de febrero). Univisión. Disponible en: https://bit.ly/2LFWYy3
56 OEA. (2014, 4 de abril). Misión de Asistencia Técnica en Seguridad Cibernética: conclusiones y recomendaciones. Disponible en: https://bit.ly/2GZURS4

asesores jurídicos y académicos de Canadá, España, Estados Unidos, Estonia, Corea del Sur, Israel, Reino Unido, República Dominicana y Uruguay, prestaría asistencia a una Comisión Nacional, encargada de formular una nueva política nacional en seguridad digital, a través de un diagnóstico y la elaboración de recomendaciones.

Esta misión de asistencia técnica elaboró un conjunto de recomendaciones que se enfocaron en 4 áreas: desarrollo de capacidades institucionales de respuesta; fortalecimiento del marco legal; generación de capacidades; e impulso a la cooperación internacional.[57] Si bien la comisión de expertos no contó con la participación de la sociedad civil, podemos destacar que en estas recomendaciones se hace hincapié en la necesidad de involucrar a este sector en las conversaciones y en cualquier plan de seguridad digital que surgiera como resultado de este proceso.

Cabe destacar que en estas recomendaciones también se puede apreciar la influencia del trabajo de las REMJA en cuanto a la adhesión y/o armonización de la legislación penal, sobre todo en los temas procesales, con el Convenio de Budapest. Finalmente, puede desprenderse de las recomendaciones un reconocimiento a la necesidad de adoptar un enfoque que separe cuestiones de ciberdefensa y ciberseguridad. Esto, sin lugar a duda, muestra una evolución en la aproximación de la OEA a su trabajo con los Estados miembros, en el que se aprecia mayor apertura en el concepto de seguridad digital y los actores que deben estar involucrados.

La política de seguridad digital vigente en el país fue finalmente adoptada en 2016 después de un largo camino en el que, en diferente capacidad y formas, intervinieron la OEA, otros organismos internacionales como la OCDE y diferentes sectores de la sociedad.[58] Hoy, esa política acoge un enfoque de desarrollo económico y social, aunque con una prominencia del primero.[59]

Paraguay

Desde noviembre del 2014, el Gobierno paraguayo mostró interés en desarrollar una estrategia nacional de seguridad digital. La OEA, a través de su asistencia técnica, ha apoyado la elaboración de un borrador de plan que, en la actualidad, lidera el Equipo

57 Ibíd.
58 Departamento Nacional de Planeación. (2016, 11 de abril). Política Nacional de Seguridad Digital. CONPES No. 3854. Disponible en: https://bit.ly/1SchHow
59 Para un análisis más profundo de la Política Nacional de Seguridad Digital de 2016, véase Castañeda, J.D. (2016, 3 de junio). ¿Qué es el Conpes de seguridad digital y por qué está mal? [blog post]. Disponible en: https://bit.ly/2L7GNZb

de Respuesta de Incidentes de Seguridad Informática de Paraguay (CERT), entidad dependiente de la SENATICS.

Durante el 2015, se desarrolló un encuentro y se realizaron varias reuniones de consulta pública a grupos interesados de la sociedad civil, empresas y Gobierno para la construcción del borrador.[60] Esta actividad se inicia a partir de una visita organizada de la OEA con expertos del Instituto de Ciberseguridad de España (INCIBE) y la comunidad de Dominios de Alto Nivel de la región (Colombia.CO), que trabajaron en conjunto con los actores claves de diferentes sectores y el Gobierno paraguayo para definir prioridades del país, además de generar la propuesta escrita del plan.[61]

Actualmente, el "Plan Nacional de Ciberseguridad" fue firmado por Decreto presidencial a comienzo del 2017.[62] El Plan tiene una duración de 3 años a partir de su vigencia y se divide en las 6 secciones: diagnóstico sobre la ciberseguridad, principios Orientadores, ejes y objetivos del Plan, sistema nacional de ciberseguridad, monitoreo y evaluación, y revisión del plan.

Algunos puntos a rescatar de esta experiencia fue la implementación de un modelo híbrido de múltiples partes interesadas en el Plan de Ciberseguridad de Paraguay. En el mismo, se plantea la creación del Sistema Nacional de Ciberseguridad, que está conformado exclusivamente por una comisión de instituciones del Estado. Sin embargo, se permitirá a la participación de la sociedad civil, sector privado, academia y gremios profesionales en grupos de trabajo ad hoc a establecerse a partir de solicitudes oficiales al sistema. Este modelo es híbrido porque no contempla el modelo de múltiples partes interesadas por defecto y tampoco se aplica en todo el proceso. Es un punto intermedio y procesal hacia la configuración plena en todas las etapas del plan.

Por otro lado, según observaciones de la organización TEDIC, el proceso de elaboración no fue suficientemente claro, recomendando que la metodología de construcción del plan fuera revisada. Si bien el documento cita que se desarrollaron consultas y mesas de trabajo, los temas y ejes centrales no fueron definidos de forma conjunta, no hubo consenso para las acciones prioritarias, deseables o urgentes, ni comunicación entre los grupos de participantes. Por ejemplo, el grupo de trabajo del Estado solo tuvo reuniones con las personas expertas de la OEA y la SENATICS. Esto mismo ocurrió en las mesas

60 SENATICS. (2015). Listado de los participantes para el desarrollo del borrador del Plan Nacional de Ciberseguridad de Paraguay. Disponible en: https://bit.ly/2ssSke3
61 OEA. (2015, 6 de mayo). La OEA apoya a Paraguay en el Desarrollo de su Plan Nacional de Ciberseguridad. Disponible en: https://bit.ly/2xmzoTG
62 Plan Nacional de Ciberseguridad: retos, roles y compromisos. Decreto 7052/2017. Disponible en: https://bit.ly/2IVutyI

de la sociedad civil y academia. Es necesario que las partes interesadas puedan dialogar entre sí, que haya consultas abiertas y con metodología que implementen el modelo *multistakeholder* para la construcción del mejor plan posible para Paraguay.[63]

México

Durante el 2017, la OEA acompañó la elaboración de la "Estrategia Nacional de Seguridad Cibernética" en México. El apoyo consistió en organizar una serie de mesas redondas con diferentes actores nacionales y la sociedad civil. La primera tuvo lugar en abril, donde surgieron una serie de recomendaciones recopiladas por un grupo de expertos internacionales convocados por la OEA, que fueron hechas públicas durante la Asamblea General de la organización.[64]

Consecutivamente, se realizó una mesa de discusión en el mes de julio. En ese marco el Gobierno mexicano presentó el documento de trabajo "Hacia una Estrategia Nacional de Ciberseguridad",[65] y con el apoyo de la OEA se volvió a recopilar comentarios de los actores nacionales para entregarlos oficialmente al Gobierno federal. A finales del mismo año, se realiza el lanzamiento oficial de la versión final del plan consolidado de la "Estrategia Nacional de Ciberseguridad de México".[66]

Cabe resaltar que se realizaron eventos y consultas a la sociedad civil, en una primera instancia con unos pocos grupos, y luego se amplió a pedido de la sociedad civil para incluir más organizaciones de cara a la segunda ronda de consulta pública. Sin embargo, la sociedad civil no estuvo satisfecha con el proceso de diseño y construcción de la estrategia nacional por parte del Gobierno. Por una parte, porque las recomendaciones vertidas en las mesas de trabajo no fueron vinculantes, por tanto no hubo mucho impacto en las recomendaciones por parte de este sector; y por la otra, se considera marginal a la participación de la sociedad civil en este proceso.[67] En tal sentido, muchos participantes de este sector manifestaron su rechazo al documento publicado por el Gobierno y se sintieron que fueron utilizados para avalar el proceso.[68]

63 Tedic. (2016). Comentarios a borrador del plan de ciberseguridad. Disponible en: https://bit.ly/2k-z15PV
64 OEA & Presidencia de la República de México. (2017). Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad. Disponible en: https://bit.ly/2JfcPoU
65 Véase el Documento de Trabajo Hacia una Estrategia Nacional de Ciberseguridad en la plataforma de consulta del Gobierno de México en: https://bit.ly/2siN8t0
66 OEA & Presidencia de la República de México. (2017, 2 de agosto). Hacia una Estrategia Nacional de Ciberseguridad. Consolidación de las Consultas a Actores Nacionales. Disponible en: https://bit.ly/2LF6ilO
67 Laurant, C. (2017, 22 de septiembre). Sociedad civil al margen del diseño de la Estrategia Nacional de Ciberseguridad [blog post]. Disponible en: https://bit.ly/2kwu0nI
68 Sánchez Onofre, J. (2017, 16 de agosto). No tiene legitimidad esta Estrategia de Ciberseguridad. El economista. Disponible en: https://bit.ly/2IVQcXh

Recomendaciones

OEA

Considerar cabalmente que la sociedad civil mantiene intereses y roles diversos, motivo por el cual su participación no se debe encontrar enfocada exclusiva y necesariamente en la provisión de servicios –por ejemplo, educativos– o para representar grupos de personas usuarias, sino para representar posiciones que deben considerarse en cuanto a la calidad de las mismas. En definitiva, la participación de la sociedad civil en sí se encuentra directamente relacionada con la gobernanza de la seguridad digital en la región, esto es: la creación de espacios de participación y deliberación que consideren a todos los actores relevantes, los cuales sirvan de base para generar vínculos y relaciones constructivas en torno al desarrollo de la temática.[69]

Trabajar en el fortalecimiento de los vínculos y la coordinación entre el CICTE, la CITEL y las REMJA con la CIDH a los fines de consolidar la colaboración mutua en sus planes de trabajo y acción con miras a brindar un mensaje armonizado en las temáticas abordadas.

Apertura de espacios de formación y capacitación dirigidos la sociedad civil. Tomando como referencia experiencias como el "Cybersecurity Summer BootCamp", organizado por el Instituto Nacional de Ciberseguridad (INCIBE) de España en colaboración con la OEA,[70] remarcamos la necesidad de generar instancias y espacios de aprendizaje y preparación que incluyan también a organizaciones de la sociedad civil o que se encuentren directamente dirigidos a las mismas, con el fin de elevar el nivel de conocimiento, entendimiento y destreza en las diversas aristas que hacen a la seguridad digital, no solamente en el plano legal, sino fundamentalmente en el apartado técnico.

69 Valenzuela, D. y Vera Hott, F. (2017, febrero). Hacia una Internet libre de censura, Capítulo 2, "Ciberseguridad y derechos humanos en América Latina", CELE, página 63. Disponible en: https://bit.ly/2n7zcPm

70 Instituto Nacional de Ciberseguridad (INCIBE), Cybersecurity Summer BootCamp: https://bit.ly/2H8EqD8

CITEL

- Establecer una categoría de membresía específica para la sociedad civil, dejando de equipararla con el sector privado y distinguiéndola de la academia, al mismo tiempo brindando una subvención con el fin de fomentar la participación en sus espacios, reuniones y debates.

- Mejorar la delimitación de su rol hacia aspectos específicos de seguridad digital, como, por ejemplo, la resiliencia en telecomunicaciones e infraestructuras críticas, en lugar de sostener un abordaje generalizado de las temáticas en sus reuniones.

- Trabajar en el fomento de una mayor coordinación e interacción con la CIDH y sus relatores especiales, de cara a todos sus diversos niveles de trabajo.

- Profundizar su integración con el proceso y espacios de la gobernanza de internet.

Programa de Seguridad Cibernética

- Mejorar la transparencia sobre la gestión de la información, los procesos llevados a cabo y los resultados obtenidos. De esta forma se avanza en la consolidación de la confianza sobre la institución, teniendo como uno de los resultados más importantes el evitar conflictos de intereses y ser percibidos como promotores de la agenda de un sector en especial.

- Trabajar en la apertura, mejoramiento, transparencia y sistematización de los procesos de elaboración de planes nacionales de seguridad digital que son desarrollados como parte del asesoramiento o asistencia técnica brindado por OEA Cyber. Una adecuada documentación sirve para analizar las buenas prácticas para el trabajo con otros países, así como también la renovación de estrategia en países que recibieron el apoyo técnico.

- Monitorear y acompañar la implementación de estrategias en la región, por todas las partes involucradas. En tal sentido, el asesoramiento técnico de la OEA Cyber debe incluir oficialmente una delegación, con los criterios de múltiples partes interesadas, para el apoyo en la elaboración de la estrategia nacional en los países.

por los Derechos Civiles

PRIVACY INTERNATIONAL

TEDIC
TECNOLOGÍA & COMUNIDAD

Fundación Karisma