Revista de la Facultad de Derecho de México
Tomo LXIX, Número 274, Mayo-Agosto 2019
http://dx.doi.org/ 10.22201/fder.24488933e.2019.274-1.69957

La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica

Of the critical infraestructure of the digital age context in Costa Rica

Jonathan Masís Solís*

Resumen: La era digital trae a nuestras vidas las tecnologías de la información. Esto genera exponenciales progresos para el bienestar humano, pero, a su vez, acarrea consigo riesgos y vulnerabilidades en distintas esferas de la vida (pública y privada). En la presente investigación ofrezco una noción de infraestructuras críticas. Abordo la necesaria relevancia jurídica de este tema, a partir de un estudio de doctrina, parte de la normativa regional, entre la cual se destaca, en su haber, la argentina y la experiencia panameña. Enriquece esta investigación un trabajo de campo en el que entrevisté a 12 profesionales en las áreas de computación y electrónica, del cual obtuve resultados de orden práctico acorde con los temas y se originaron valiosas conclusiones. Considero que este tema es el reto que, en la actualidad, juristas, profesionales de la informática y sociedad en general enfrentamos como parte de la gobernanza digital.

* El autor realizó estudios de Derecho y Administración de Negocios en la Universidad de Costa Rica. Actualmente se desempeña como servidor público en el Instituto Costarricense del Deporte y la Recreación. Ejerció como juez suplente interino de la Corte Suprema de Justicia de Costa Rica en materias civil y penal, docente de Derechos Reales y Derecho Privado, ha impartido lecciones de Derecho Comercial y Derecho Tributario para la Escuela de Administración de Negocios en la Universidad Fidélitas. Agradezco a las siguientes personas los aportes, sugerencias y lectura de este documento: Rebeca Parra, Gerardo Arroyo, Pablo Iglesias, Gilberto Loaiza y Alexander Rodríguez. A quienes donaron su tiempo y contestaron las entrevistas que citadas en esta investigación. Dedico esta publicación a mi padre Julio y mi madre Virginia, *in memoriam*. Contacto: <jomaso13@gmail.com>. Fecha de recepción: 13/02/2019. Fecha de aprobación: 11/06/2019.

Palabras clave: seguridad informática; delincuencia informática; infraestructura crítica; derecho informático; gobernanza digital.

Abstract: The digital era brings with it the omnipresence of the technologies of information in our lives. This generates exponential progress for human well-being. However, at the same time, carries risks and vulnerabilities for people, private companies and states, whose goods and services are offered, today, mainly by electronic mechanisms. In this context, in the present investigation I offer a notion of critical infrastructure. Taking on board the necessary legal relevance of these subjects, from a study of the doctrine, review of the regional regulation, amongst which in Argentina and the Panamanian experience. Fortifying this investigation is a field study, an undertaking in which I interviewed 12 professionals in the areas of computing and electronic, obtaining results in practica order in accordance with the subjects, giving rise to valuable conclusions for present and future investigations. I trust that this work will stimulate the investigation and discussion in our country. This subject, I consider is the challenge that, in reality, jurists, IT professionals and society in general face as part of the digital government.

Keywords: It security; internet crime; critical infrastructure; It rights; digital governance.

I. Introducción

Imagine que un día, al salir con su vehículo de su casa, ingresa a una ciudad. Para su sorpresa, los semáforos están apagados; en consecuencia, los peatones cruzan por cualquier parte y los demás vehículos no saben cuándo ni a dónde virar. Además, el lugar al cual usted se dirige ese día probablemente se encuentra cerrado, porque, producto del apagón, está sin electricidad y no brinda sus servicios. Por añadidura, su vehículo requiere combustible, pero su único medio de pago, la tarjeta de crédito, no es recibida, pues ha fallado la comunicación con el ente emisor del servicio. Entonces, el panorama se le complica: ya está atascado en una presa de vehículos que no encuentran ni el norte ni el sur, la mayor parte de las personas en esa ciudad está en una condición similar a la suya y la solución no está en sus manos.

Un caso como el anterior se enmarca en el tema de las infraestructuras críticas,[1] estructuras que forman parte de nuestras vidas

[1] Un tema vital, que debe fortalecerse en colaboración entre informáticos, peritos actuariales y abogados, es la valoración del daño cuando se vulnera una infraestructura crítica. Por ejemplo, la caída por un día de los servidores de una entidad bancaria podría significar una pérdida valorada en mil millones de dólares, entre lo que se encuentran la imposibilidad de realizar transacciones o pagos, pérdidas de tiempo, cobros de intereses y multas contra la cartera de clientes del banco. Al respecto, se ha indicado:

> Ahora bien, ¿se sabe cuánto cuesta exactamente una hora sin servidor? Un estudio de la consultora Techconsult de 2013 impulsado por HP Alemania examinó a 300 empresas medianas del país teutón (de 200 a 4.999 empleados) y, de estas, un 77 % confesó haber sufrido fallos críticos en sus sistemas informáticos en el año previo al estudio. Las empresas más afectadas fueron las de los sectores del comercio, la fabricación y la distribución. La media de caídas del servidor en el período objeto del estudio fue de cuatro apagones por empresa con una duración media de 3,8 horas, en las cuales se incluyen la reparación técnica y la recuperación de los datos.

y que resultan esenciales para su desarrollo: el mantenimiento de servicios públicos y privados que aseguran un nivel de vida óptimo. Tal circunstancia no es parte de una escena de Hollywood: sucedió en julio de 2017 en San José —me sucedió a mí— y, probablemente, afectó a varias personas en Panamá, El Salvador y Honduras. Al respecto, por citar un ejemplo, el medio informativo argentino, informó lo siguiente: "La capital costarricense vivió escenas de caos vial cuando se apagaron los semáforos, mientras que el principal aeropuerto internacional pasó a operar con baterías para seguir funcionando, aunque más lento de lo normal, según el ministro de Obras Públicas y Transporte".[2]

Los costes que se generan por cada hora de no funcionamiento varían en función del tamaño de la empresa, teniendo en cuenta, además, que en ellos confluyen tanto los gastos de producción (cuánto tiempo se ve privado un empleado de realizar su tarea) como los gastos llamados de oportunidad (ventas y tomas de contacto en la página web, quizá irrecuperables). Mientras que aquellas empresas con menos de 500 empleados confirmaron haber sufrido daños de alrededor de 20.000 euros por hora, los costes para las empresas con más de mil trabajadores ascendieron a cerca de 40.000. Así, una caída del sistema puede significar para una empresa de tamaño medio un coste de 25.000 euros por hora sin servicio. Si se añaden los costes de la reparación de la avería y de la restauración de los datos, los efectos de un servidor caído resultan en una pérdida anual de 380.000 euros para la mediana empresa alemana. Es razonable extrapolar estas conclusiones al ámbito global de forma que las cifras tendrían un aspecto similar en otros países con una actividad empresarial equiparable." "Servidor caído: riesgos, efectos y prevención",. *Digital Guide*, 2017, p. 8. Consultado en: <https://www.ionos.es/digitalguide/servidores/know-how/servidor-caido-que-hacer/> (20 de junio, 2017)

[2] "Apagón en América latina: se cortó la luz en cinco países al mismo tiempo", *La Nación* (Argentina), párraf. 1. Consultado en: <http://www.lanacion.com.ar/2039002-apagon-corte-luz-energia-america-latina-costa-rica-panama-honduras-salvador-nicagarua>. (2 de julio, 2017)

Antes de abordar el tema, consideremos un aspecto esencial sobre las tecnologías. Es probable que cuando Internet fue creada –y con ella los diversos servicios que hoy nos mantienen profundamente interconectados–, no se previeron los riesgos que traería consigo. Dado que este es un tema que incumbe a la seguridad de los grupos humanos, particularmente a la de los Estados, la recomendación generada a partir de una investigación realizada por la OEA y la empresa Trend, que se analizará en el transcurso de este artículo y que aborda valiosas herramientas para abordar la presente cuestión, es el siguiente: "Es esencial que los gobiernos trabajen muy de cerca con el sector privado, a menudo en Asociaciones Públicas-Privadas (PPPs) para ayudar a enfrentar las amenazas para estas Infraestructuras de Información Críticas (CCIs) y hallar soluciones" (OEA y Micro Trend, 2015, p. 14.).

II. Una ciudad, una casa

Observando la arquitectura de una ciudad o de nuestra vivienda, podemos imaginar cuáles son sus fortalezas y debilidades y cuáles circunstancias podrían amenazarlas. En nuestras casas, las puertas, ventanas y portones generalmente son lo más resguardado: ahí colocamos portones altos y alambres navaja, instalamos alarmas y cámaras de seguridad, las cuales podemos manipular desde nuestras computadoras o teléfonos móviles; incluso, pagamos seguridad privada, que se vale de dispositivos inteligentes para brindarnos la certeza de que lo más íntimo que tenemos, lo más valioso –nuestros bienes y nuestra integridad física–, estará resguardado aun cuando no estemos cerca.

Con respecto a la ciudad, dado que es un espacio colectivo, sabemos que su infraestructura vial forma parte esencial de la vida en comunidad. Un adecuado ordenamiento vial dinamiza la economía de una ciudad, genera trabajo y produce riqueza. Entonces, ¿qué pasaría si los semáforos se apagaran o descoordina-

ran en momentos de intenso tráfico, durante varias horas? ¿O si un importante puente colapsara e impidiera, por horas o días, el paso de vehículos, como *containers*, ambulancias o patrullas? El resultado sería de diversa índole: un gasto excesivo de combustible, riesgos para la integridad física, la salud y la seguridad de las personas, y altas pérdidas económicas en mercancías perecederas que se atrasarían en llegar a su destino.

Situémonos en otro escenario: ¿qué sucedería si un aeropuerto, lugar donde las intercomunicaciones son vitales, es interferido por algún grupo con *jammers*[3] de seguridad, que afectan la frecuencia por donde transitan los datos y las señales que guían los aviones y bloquean los nodos de comunicación? Esto generaría problemas de comunicación con los aviones; y, por consiguiente, pérdidas económicas por atraso de vuelos, cancelación de reuniones comerciales o políticas, etc. Similar circunstancia podría suceder en un muelle, pues se afectaría la salida de cruceros o barcos que transportan alimentos perecederos y hasta turistas.

Finalmente, desplacémonos al sector de abastecimiento, suministro y distribución de fuentes de energía[4] (gasolineras, servicios de electricidad o telecomunicaciones) o al sector de servicios de salud: ¿Qué sería de una entidad financiera, o de un hospital,

[3] El Cambridge Dictionary en línea (2019) define jammer de la siguiente manera: "a device that stops a signal from reaching someone or something: radar/cell phone jammers/ a handheld jammer that can stop satellite signals". En español: ("un dispositivo que impide que una señal llegue a alguien o algo: interferencias en el radar / teléfonos celulares / una interferencia de mano que puede detener las señales de los satélites").

[4] El informe de OEA y TrendMicro (2015) al respecto indica: "De acuerdo con la firma de seguridad CrowdStrike, un grupo de hackers rusos denominado "Oso Energético" provocó estragos importantes en empresas del sector energético de los Estados Unidos. El grupo utilizó un malware [sic] altamente efectivo y recientemente creado que se conoce como "Havex" para penetrar en el sistema de control industrial (ICS)/sistemas SCADA de sus compañías objetivo". (p. 9)

si durante algún tiempo pierde totalmente su abastecimiento de energía eléctrica, ahora que casi la totalidad de documentos y transacciones dependen del uso de tecnología electrónica? En los hospitales, el historial clínico de cada paciente se ordena en bases de datos y se utiliza tecnología de electromedicina de punta.

III. Infraestructuras críticas

A) Generalidades

Esos elementos de ingeniería, electrónica, computación y seguridad, de los cuales nos servimos en la vida diaria y que contienen información importante o desempeñan funciones de orden, transporte y comunicación, constituyen lo que se conoce como estructuras críticas en un determinado país.

Como parte de esta investigación, realicé un cuestionario con la finalidad de indagar el conocimiento que tienen sobre la materia profesionales en el área de la informática y las tecnologías. Para ello, envié el cuestionario a 20 personas y obtuve 12 respuestas. La información sobre esta población, se presenta en la tabla 1.

Realicé la selección de las personas y el instrumento, para tener datos previos de un tema novedoso por explorar, del cual se encuentra ya alguna bibliografía. Por tanto, destaco que hacen falta más datos estadísticos.

http://dx.doi.org/ 10.22201/fder.24488933e.2019.274-1.69957

Tabla 1. *Descripción de los sujetos informantes*

Profesión	Grado académico	Puesto
1Ingeniería en computación	2 Bachillerato	1 Programador de bases de datos
1Ingeniería en electrónica	2 Maestría	2 Gerencia de proyectos
	8 Licenciatura	1 Personal bancario
		1 Docencia
		2 Consultorías
		1 Consultoría y análisis de información
		1 Administrador de TI
		2 Informática
		1 *Automation Engineer*

En este sentido, veamos las respuestas al cuestionario, donde se plantearon estas definiciones:

> Informante 3: Entiendo por infraestructura critica aquella que es necesaria para el desarrollo y sostenibilidad de una nación. Sin infraestructura se impacta el bienestar de sus habitantes en diferentes niveles, dependiendo del tipo de infraestructura afectada.
> Informante 5: Se refiere a todas las redes, servicios, instalaciones, equipos y sistemas de TI que son de carácter público y que si dejan

de funcionar o lo hacen de forma inadecuada podrían afectar la seguridad ciudadana.[5]

Informante 7: Básicamente, estamos ante cualquier infraestructura necesaria para el buen devenir de una sociedad específica. Una depuradora de agua, el sistema de control de los semáforos, una central térmica…[6]

Se observa en estos textos que el informante 5 restringe la noción de infraestructura crítica a bienes públicos; no obstante, la realidad es que, si se afecta un bien privado, las consecuencias de igual forma impactarán a la población que requiera el servicio y, eventualmente, la seguridad de los gobiernos. Asimismo, ciertos fenómenos naturales –inundaciones, huracanes, terremotos– o comportamientos de iniciativa humana que alteren, dañen o interfieran alguna de esas infraestructuras críticas, generarían un efecto "en cascada" de dimensiones exponenciales, impredecibles en sus alcances directos o colaterales, altamente onerosos y volumétricos. El factor de más riesgo hoy es que tal infraestructura tiene un alto nivel de dependencia de Internet y de la conectividad, por lo que el grado de vulnerabilidad aumenta considerablemente.

En parte, los riesgos que hoy enfrentamos se deben a que "El Internet se concibió intencionalmente para ser una red resistente, y fundamentalmente lo sigue siendo. Nunca fue diseñado para ser esa infraestructura de información crítica vital en la que hoy se ha convertido, especialmente para las pequeñas empresas, cuya dependencia del correo electrónico, de los sitios web, del acceso a otros recursos en línea se incrementa cada día".[7]

---

[5] Masís, J., Cuestionarios de entrevistas. Realizados mediante correo electrónico. Entrevistador Jonathan Masís Solís. Entrevistados anónimo, agosto, 2017, p. 3.

[6] Masís, J., *op. cit.,* p. 10.

[7] OEA y Trend Micro Incorporated, "Reporte de seguridad Cibernética e Infraestructura Crítica de las Américas", Washington D.C., 2015, p. 14. Consultado en: <https://www.sites.oas.org/cyber/Documents/2015%20-%20

Las razones por las cuales el acceso a Internet puede fallar pueden ir desde un exacerbado tráfico de datos o la avería de cables de fibra óptica[8] hasta las consecuencias de una emergencia natural. Agreguemos a esto la posibilidad de ser blanco de ataques de ciberdelincuentes. De esta manera, en este punto, podemos decir que una infraestructura crítica está constituida por

> aquellas instalaciones, sistemas, y redes, así como servicios y equipos físicos y de tecnología de la información cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, la gobernabilidad democrática, o el eficaz funcionamiento del gobierno de un Estado.[9]

En el cuestionario, se consultó mediante una lista ofrecida a los sujetos informantes sobre cuáles herramientas tecnológicas son importantes para el resguardo de infraestructuras críticas y se enlistaron las siguientes:

1. Herramientas de gestión y administración para la operación y el mantenimiento de la infraestructura, preferiblemente con acceso público.
2. Herramientas que aseguren el suministro eléctrico.
3. Herramientas para asegurar el espectro radioeléctrico.

OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf>

[8] La conducción de fibra eléctrica, sea por el océano Atlántico o sea por el Pacífico, es una medida que ha permitido una gran estabilidad en la transmisión de datos.

[9] Cfr. OEA, *Declaración de Panamá* sobre la protección de la infraestructura crítica en el hemisferio frente al terrorismo, 2007. Consultado en: <http://www.oas.org/es/sms/cicte/documents/declaraciones/doc_dec_1_07_final_spa.pdf>.

4. Adecuado sistema de monitoreo preventivo que utilice el espectro radioeléctrico, de manera que no se dependa del tendido por postes, que es susceptible a todo tipo de amenazas.
5. Utilización de servicios en la nube.
6. Contratación de *data centers* seguros[10], confiables y robustos.
7. Contar con una red nacional de conectividad. En este caso, se refiere a que todas las instituciones de gobierno estén interconectadas en una sola red de datos, de forma que el Estado tenga una única facturación y se logre disminuir los costos que pagan las instancias por sus propias conexiones de red[11].
8. Fortalecer proyectos, como el Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE)[12], que buscan la integración de datos a nivel institucional, de forma que se pueda centralizar la información relevante para la toma de decisiones de gobierno.
9. Sustituir el sistema actual de las cédulas de identidad, de forma que se utilice un sistema no propietario (que pertenece a una única empresa), para que el Estado pueda ampliar el uso, servicios y facilidades de la codificación de identidad. El problema, en este sentido, es que el código QR[13] que tienen las cédulas de identidad en este momento es hecho por una única empresa y solamente ellos tienen el sistema para poder leer la información de la cédula, lo cual significa que el Estado o cualquier organización (bancos, lectores del bus, servicio

10 En la red existe un amplio y variado mercado de *data centers* que lucen características atractivas para los clientes (v. Amsterdam data center AMS1, s.f.).

11 El denominado "iwan", permitirá que nadie tenga un enlace dedicado, sino que todos utilizaríamos la red pública. Esto conlleva también riesgos importantes, pero libera de costos a instituciones o empresas.

12 Puede consultarse en: <https://www.sinirube.go.cr>

13 Según el sitio web Unitag (2019): "Un código QR es un código de barras bidimensional cuadrada que puede almacenar los datos codificados. La mayoría del tiempo los datos es un enlace a un sitio web (URL)".

al cliente en general, etc.), que quiera realizar lectura de esa información solamente puede contratar a esa empresa, lo que eleva los costos, pues ellos determinan tanto el *hardware* como el *software* que se puede usar.
10. Hospitales móviles.
11. Equipos de rescate.
12. Vías de fácil acceso a muelles y aeropuertos.
13. Aumentar la seguridad informática y física.
14. Dotar los equipos de bases de datos con respaldos y con *firewalls*[14].

Una respuesta con un poco más de análisis fue ofrecida por el informante 7:

A mi modo de entenderlo, *más que falta de recursos tecnológicos, lo que necesitamos es un compromiso social y político que reme en la misma dirección.*

Campañas como la de WannaCry, comentada recientemente, fue un éxito a nivel reputacional, pero no tanto a nivel de impacto económico, y no al menos en España *(el país donde resido)*. Basta mirar todo lo que supuso WannaCry en el sistema sanitario inglés, y el impacto que tuvo en la industria española.

¿La razón? Hubo *una colaboración t*ácita *y real entre fuerzas de seguridad, administraciones y empresas* privadas. Compañías de la talla de Telefónica corrieron raudos y veloces a reconocer que habían sido infectados, y supusieron por tanto uno de los principales frentes para que apenas unas horas más tarde ya empezaran a surgir vacunas para el ransomware.

Una campaña virulenta semejante, ocurrida hace ya una década *(como fue, por ejemplo, Sasser (ES))* estuvo en circulación meses sin que los organismos fueran capaces de coordinarse adecuadamente, y todavía es hoy que si instalamos en un dispositivo Windows XP no actualizado y nos conec-

[14] El *firewall* es una buena herramienta de protección de sistemas informáticos. Sin embargo, un exceso en esta protección podría resultar en un arma de doble filo para las empresas.

tamos a la red a los pocos minutos seguramente estamos ya infectados por este gusano."(la negrita es del original).[15]

De la lista antes indicada, puede concluirse que las herramientas enlistadas por los informantes coinciden con las prioridades de los Estados cuando se trata de resguardar sus infraestructuras críticas (señaladas en el gráfico 1): el respaldo de información en *data centers* confiables, utilización de servicios en la nube[16] para respaldo de datos y protección del espectro radioeléctrico, entre otros.

B) Internet de las cosas

Actualmente, un contexto en que debe analizarse la protección de las infraestructuras críticas es el generado por la tecnología de Internet de las cosas[17] o internet de los objetos (en inglés *Internet of Things*, abreviado *IoT*). Las predicciones[18] nos indican que la tendencia es hacia el fortalecimiento y aumento del uso de esta

---

15 Masís, J., *op. cit.,* p. 11.

16 Uno de los retos en investigación y desarrollo normativo se refiere a derechos de propiedad intelectual de los datos almacenados en la nube, tema que debe ser abordado no solo por las instituciones encargadas de creación normativa, sino también por las empresas que los utilizan, las cuales deben garantizar estos derechos a sus clientes. Véase que gran parte del crecimiento exponencial de acciones de algunas empresas como Microsoft, por ejemplo, tienen como parte de sus atractivos proveer servicios en la nube (v. Fiegerman, 2018).

17 Noción utilizada por Kevin Ashton en 1999 durante una presentación para la Compañía Procter & Gamble. (Rodríguez, Montenegro y Cueva, 2015, p. 53).

18 Martínez, J., Mejía, J., Muñóz, M. y Meredith-García, Y., "La seguridad en Internet de las Cosas: Analizando el tráfico de información en aplicaciones para iOS", *Revista Computación e Informática*, a. 6 núm. 1, Centro de Investigación en Matemáticas CIMAT, A.C., Zacatecas, México, 2017, p. 78.

tecnología: el número de dispositivos conectados ha alcanzado una cifra aproximada de 20 mil millones y se espera que para 2020 llegue a 50 mil millones.

Ahora bien, tener nuestro refrigerador, horno microondas o televisión conectados a Internet, incluso con una cámara digital, nos simplifica la vida, pero podría introducir mecanismos invasivos a la privacidad en nuestra propia casa: es el caso de situaciones vividas por importantes personajes de la vida pública, cuyas cámaras de seguridad habían almacenado contenidos íntimos que luego fueron accedidos por terceros y mostrados al público.

Asimismo, de acuerdo con Martínez, esta tecnología también es relevante en números: "Los productos y servicios asociados a IoT generarán ingresos superiores a los $300 mil millones de dólares para 2020".[19] Y aún mes, el avance tecnológico ha llegado a tal punto que hoy es posible no solo la comunicación entre seres humanos y las cosas, sino también de las cosas entre sí.

C) Las amenazas

El *quid* de la cuestión, luego de definir qué es infraestructura crítica en un país, consiste en enlistar los factores denominados "amenazas" (o "amenazas emergentes"), las cuales actúan como depredadores cibernéticos y que consisten en sujetos o grupos que se benefician de la disponibilidad de información personal y de los estados en redes digitales, situación debida a la dependencia de las telecomunicaciones (como ilustraremos más adelante, con una serie de casos).

No sorprende que todos los miembros encuestados en la investigación antes aludida de la OEA y MicroTrend, citaran las tácticas de *spear-phishing* como el método de ataque más frecuente contra el que tuvieron que defenderse, seguido por la explotación de vulnerabilidades de *software* sin parches. En ese caso, se in-

[19] Martínez, J., *et al*., *op. cit.,* p. 80.

dicaron las siguientes técnicas como las más usadas para atacar infraestructuras críticas:

> *Phishing*: 71% Phising: es el término utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.
> • Para esto se suelen utilizar páginas web construidas como una copia bastante fiel de la original, formularios y en algunas ocasiones métodos de ingeniería social para cometer estos ilícitos.
> • Vulnerabilidades sin parches: 50%. Cualquier programa es susceptible de tener fallos de seguridad. Por este motivo, puede necesitar ser actualizado independientemente del dispositivo en el que se encuentre instalado. Esto incluye los programas y sistemas operativos de ordenadores, tabletas, *smartphones*, consolas de videojuegos e incluso televisiones inteligentes.
> • Es importante mantener el software actualizado, ya que una vez publicado el parche de seguridad, la vulnerabilidad queda descubierta, esto es, que los cibercriminales ya saben dónde atacar, solamente deben ubicar los equipos que no están actualizados e iniciar el ataque.
> • DDos: 42%. son las siglas de Distributed Denial of Service. La traducción es "ataque distribuido denegación de servicio", y traducido de nuevo significa que se ataca al servidor desde muchos dispositivos para no pueda dar abasto con la demanda y deje de funcionar.
> • Los servidores poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

http://dx.doi.org/ 10.22201/fder.24488933e.2019.274-1.69957

• Inyección de SQL: 32. Tanto esta como la anterior se refieren a: "(Inyección SQL/DDoS/XSS) Tipo de explotación de un fallo de seguridad de una aplicación que interactúa con una base de datos, que inyecta una consulta SQL/DDoS/XSS no prevista por el sistema y que puede poner en riesgo su seguridad." Es una vulneración cuyo origen es la falta de protección de una base de datos (lwp. Comunidad de Programadores, 2019).
• *Cross site scripting*: 21%. Abreviado XSS, alude a "Ataques que utilizan los propios scripts de las webs auténticas, que, modificados, pueden hacer que tanto la página como los certificados de seguridad parezcan correctos". Es una técnica de ataque popular en Internet en la que el código malicioso se ejecuta tanto en el lado del servidor como en el del cliente, con el fin de robar datos sensibles o identidades digitales.

Tipos de ataques: Esta vulnerabilidad se divide en dos grandes grupos: el primero se conoce como XSS persistente o directo y el segundo como XSS reflejado o indirecto.

Directo o persistente. Consiste en invadir código HTML mediante la inclusión de etiquetas <script> y <frame> en sitios que lo permiten.

Indirecto o reflejado. Funciona modificando valores que la aplicación web pasa de una página a otra, sin emplear sesiones. Sucede cuando se envía un mensaje o ruta en una URL, una cookie o en la cabecera HTTP (pudiendo extenderse al DOM del navegador).

• *Hacktivistas*: 21%: el hacktivismo es una forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers no ciberdelincuentes, se debe dejar claro que no son la misma cuestión) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales.
• APTs: 18%: , son las siglas de

> Advance Package Tool o en español amenazas persistentes avanzadas: consiste en un programa que administra el sistema de paquetes de Debian (*.deb)". A su vez, Debian, o más exactamente Debian Common Core Alliance (DCCA) es la organización cuyo objetivo es estandarizar las distribuciones Linux basadas en la distribución Debian con una serie de normas a seguir y una certificación, además de promocionar su adopción en el sector empresarial con una serie de productos y servicios. En ningún caso la DCCA va a crear una distribución, si no unas normas para certificar a las distribuciones de los fabricantes. Mas Información en <http://www.dccalliance.org/> "(lwp. Comunidad de Programadores, 2019). Esta modalidad de ataque es explicada a un medio de comunicación nacional por el coordinador del Centro de Respuesta de Incidentes de Seguridad Informática del Ministerio de Ciencia, Tecnología y Telecomunicaciones (Csirt-Micitt), Roberto Lemaitre: son "ataques reiterados que buscan hacerlos en un gran lapso, que buscan vulnerar la seguridad de una entidad específica", además el abogado detalló: "Lo que buscan es que no se detecte y utilizan complejas herramientas que usan varios sectores de ataque, buscando aprovechar alguna debilidad en el sistema en el que se encuentre… buscan estar mucho tiempo dentro de una empresa, organización, con el fin de recuperar información, obtenerla o conseguir otra que les permita realizar una actividad económica relacionada con lo que persiguen.[20]

Hay dos maneras de ver esto: APT como una cosa y APT como una persona. Por un lado, una Amenaza Avanzada Persistente (APT) se refiere a una especie de ciberataque muy preciso. Por otro lado, las APT pueden referirse también a grupos, a me-

[20] Cfr. Villalobos, P., "Costa Rica fue blanco de ataques de espionaje cibernético de Corea del Norte en 2018, según informe" en *Ameliarueda.com*. Consultado en: <https://www.ameliarueda.com/nota/costa-rica-blanco-ataques-espionaje-cibernetico-corea-norte-informe> (06 de abril, 2019).

nudo apoyados o financiados de otras formas, que son responsables del lanzamiento de dichos ataques de precisión.

Las verdaderas APT son contrarias a la intuición. Cuando se hace referencia a la mayoría de los cibercriminales y en otros propagadores de malware, se cree que su objetivo es el de infectar la mayor cantidad de computadoras posibles con sus credenciales de hurto, construcciones de botnet (esto es una red de computadores infectadas que son utilizadas para ataques), u otros softwares maliciosos. Cuanto más amplia sea la red, más oportunidades tendrán de robar dinero, recursos de computación, o cualquier objetivo que tengan. Los actores en las APT están interesados en infectar las máquinas de ciertas personas en particular.

El objetivo final de un ataque del estilo de las APT es el de comprometer una máquina en donde haya algún tipo de información valiosa. Sería un éxito obvio si el atacante lograra cargar un keylogger (esto es un programa que se encarga de capturar lo que el usuario teclea, lo almacena en un archivo y lo envía a su creador) o instalar una "puerta trasera" en la máquina del ejecutivo en jefe o del oficial de información de una compañía prominente, pero debes detener este tipo de atacantes a tiempo. Son listos. Tienen equipos de seguridad y herramientas buscándolos. En otras palabras, podría ser muy difícil hackear con éxito a estos individuos empresariales.

En este contexto, se hace necesario realizar un inventario sobre reportes de incidentes de seguridad en el sector público nacional y encausar sus posibles soluciones de forma organizada y unificada. Además, se hace evidente la importancia de establecer prioridades y planes estratégicos que aborden el tema de la ciberseguridad, de manera que se asegure la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

A la pregunta: ¿Cuáles considera son los métodos más peligrosos mediante los cuales se puede afectar una infraestructura crítica digital? Las respuestas de todos los sujetos entrevistados puede sintetizarse asi:

1. La principal amenaza proviene del acceso no autorizado en

sistemas informáticos (o "hackeo" de información), ya sea para robar datos, encriptarlos u obtener cuentas de acceso a servidores.

2. El uso de consultas masivas a servidores de datos, por medio de robots, lo cual causa la saturación y caída de los sistemas (este aspecto se consideró "muy peligroso").

3. El principal vector de ataque, por facilidad y por eficiencia, *sigue siendo el factor humano*, debido a que es más sencillo en términos técnicos e, incluso, de recursos, intentar sobrepasar la seguridad humana o física que la cibernética: es decir, es más fácil introducir un dispositivo USB infectado en un servidor a través de uno de los operarios de una planta que intentar "bypasear" los controles con que cuenta el servidor. De esto se extrae la importancia que tiene seleccionar, formar y capacitar adecuadamente al personal encargado de sistemas de computación sobre los riesgos que enfrentan, sobre métodos de *phishing* y sobre ingeniería social. Lo anterior, sin descuidar la tecnología adecuada, la objetividad y subjetividad humanas en los ecosistemas digitales.

4. El no contar con restricciones físicas hacia los sitios donde se encuentra el equipo electrónico o informático que gestiona la información (este aspecto también fue considerado como muy peligroso).

IV. Gobernanza e infraestructura crítica

A) Generalidades

Actualmente, los gobiernos están migrando sus servicios públicos hacia la modalidad de gobierno digital (*egoverment*). Por tanto, en la actualidad se manejan, almacenan y comunican gran parte de las informaciones gubernamentales y oficiales por medios digitales, como los correos electrónicos. Por estos canales circulan *bits* (que conforman paquetes de *terabites*) con información sensible sobre

decisiones políticas, estrategias, datos personales de la ciudadanía, etc. En otras palabras, se ha constituido a nivel gubernamental una importante infraestructura crítica, que es esencialmente vasta. Entonces, para establecer una adecuada política de gobernanza digital, que esté prevenida frente a las amenazas que se ciernen sobre las infraestructuras, es necesario comenzar por hacer un mapeo que permita a los tomadores de decisiones conocer cuáles son las infraestructuras críticas en un determinado país.

Dada la importancia de este aspecto, como parte de esta investigación, elaboré un cuestionario, el cual fue aplicado vía correo electrónico a cuatro profesionales de la computación que trabajan en empresas privadas y que tienen un grado académico en materias relacionadas con la seguridad informática. Por medio de dicho instrumento, consulté a los informantes cuáles herramientas deben desarrollarse en la práctica en nuestro país para que se dé una gobernanza digital.

Las respuestas aportan datos valiosos. Uno de los sujetos informantes contestó que desconocía totalmente el tema;[21] otro indicó, en cambio, que esa gobernanza pasaba por mejorar los mecanismos legales que permitieran una justicia pronta y cumplida necesaria para el gobierno digital, y además sugirió que haya "entrenamiento y equipos para el sistema de justicia para prepararse ante desastres", así como "educación y legislación para evitar el vandalismo"[22]

Otra de las respuestas, con la cual coincido plenamente es:

> Debería existir un marco legal para exigir la creación de una institución que regule y supervise la seguridad de infraestructuras críticas. Ahorita son más recomendaciones, pero no hay una exigencia real. Por ejemplo, la mayoría de los datacenters [sic] de instituciones gubernamentales se encuentran dentro de la Gran Área Metropolitana (GAM), por lo que un evento que afecte la

[21] Masís, J., *op. cit.,* p. 15.

[22] Masís, J., *op. cit.,* p. 2.

> GAM deja al descubierto al resto del país. Hoy sin los sistemas de información es imposible administrar un país.[23]

Al respecto, un tercer profesional opinó que nuestro país carece absolutamente de cualquier medida sobre gobernanza digital. Y aconsejó que mediante una ley sea "obligatorio hospedar todo en la nube y nada en centros de datos locales; generar un marco legal es deseable para la gobernanza, pero en este país no va a suceder en el mediano plazo"[24]

En el *argot* de seguridad digital se conocen como "formuladores de políticas públicas" a aquellos órganos del Estado encargados de formular e implementar las decisiones sobre seguridad cibernética en general, los cuales están organizados en Centros para políticas públicas (conocidos como Cecir's), y distribuidos en determinados sectores de servicios electrónicos. Dichos centros tienen como función el intercambio de información sobre seguridad de las infraestructuras críticas, el planteamiento y establecimiento de alianzas público-privadas[25], como se verá adelante.

Otro aspecto que completa la escena de la seguridad en infraestructuras críticas son los denominados *Computer Emergency Response Team* (CERT)[26], que constituyen un equipo de respuesta ante emergencias informáticas. En otras palabras, son centros de

---

[23] Masís, J., *op. cit.,* p. 4.

[24] Masís, J., *op. cit.,* p. 5. Sobre lo acontecido en Puerto Rico con la recuperación de datos en la nube luego de un desastre natural, véase Protección de datos Intech: Claves para la continuidad del negocio, 2018.

[25] Universidades y publicaciones académicas utilizan el sistema "Doi" que garantiza que no se pierda información y referencia de los documentos (v. DOI, 2019).

[26] En México, existe el UNAM-CERT, el cual examina las vulnerabilidades de los sistemas informáticos en el país, provee información sobre riesgos de seguridad informática y proporciona respuestas a entidades en caso de ataques (al respecto de este tema v. Servidor caído: riesgos, efectos y prevención, 2017).

respuesta a incidentes de seguridad en tecnologías de la información.

En cuanto a la pregunta: "¿Cuáles herramientas legales, considera debe crearse o fortalecerse para resguardar las infraestructuras críticas?", es de destacar que de las 12 personas entrevistadas, al menos 4 dijeron no tener ni idea sobre gobernanza digital en el tema de infraestructuras crítica, a pesar de que habían contestado ampliamente las preguntas sobre el tema de infraestructuras críticas. Las respuestas obtenidas, se sintetizan en la siguiente lista:

1. Fortalecer y socializar el ordenamiento jurídico que regula la materia sobre delitos informáticos[27] (informática forense) y protección de datos, para contar con una respuesta pronta y cumplida ante acciones que afecten las infraestructuras críticas. Además de entrenar y equipar al capital humano de los sistemas judiciales para prepararse ante amenazas a sus infraestructuras.

2. Exigir la creación de una institución que regule y supervise la seguridad de infraestructuras críticas.

3. Disponer legalmente el deber de hospedar en la nube toda la información de las personas usuarias de servicios electrónicos vitales.

4. Incluir la ética dentro de la malla curricular de escuelas y colegios, como eje trasversal, en todas las áreas (según el desarrollo del estudiante), así como educación sobre el uso de la Internet (de forma segura) y la protección de datos.

[27] Sobre el tema de delitos informáticos en el ámbito costarricense, recomiendo *Manual sobre delitos informáticos para la ciber-sociedad costarricense*, de Roberto Lemaitre Picado, 2011, *IJSA*.

5. Fortalecer proyectos que se dirijan a ciudades inteligentes, de forma que se disminuya la tramitomanía, el tiempo de respuesta en los servicios públicos y se amplíen la oferta de servicios por medios cibernéticos.

6. A nivel nacional, tener redundancias[28] en los sistemas de telecomunicaciones y energía.

7. Ampliar las responsabilidades del Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT).

8. Garantizar y proteger legalmente los puestos de trabajo de quienes investigan fallos de seguridad y tienen deber de comunicarlos, en las organizaciones, ya sean públicas o privadas.

9. Concientizar al público usuario sobre los riesgos que entraña la utilización de tecnologías: en este sentido, es importante hacerle ver que un descuido en un dispositivo, por insignificante que parezca, puede propagar alguna forma de vulneración que podría tornarse más perjudicial.

Desde esta perspectiva, el informante 7 plantea que "lo peor que podemos hacer es criminalizar a aquellos que dedican tiempo y esfuerzo en encontrar fallas, documentarlas y alertar a los agentes implicados. Ese trabajo debe valorarse *(y no solo hablo del factor económico)*, dotándolo de las garantías legales suficientes para que el trabajo del auditor de seguridad no sea una carrera llena de obstáculos, donde tan pronto te encuentras con una empresa que te agradece el trabajo, como con otra que lo considera un "hackeo" y te suelta a los abogados".[29]

[28] La redundancia consiste en tener dos equipos exactamente iguales funcionando: si uno falla, automáticamente entra el otro a funcionar. Con eso no se pierde el servicio y la persona usuaria no se entera si alguno falló.

[29] Masís, J., *op. cit.,* p. 12.

B) Educación y cooperación

La gobernanza digital es un marco dónde se definen todas aquellas responsabilidades y roles que permiten tomar decisiones con el fin de consolidar la presencia digital (sitio web, servicios automatizados: aplicaciones o sistemas web, documentación digital, redes sociales, etc.) acorde a nuestro interés (independientemente de una entidad pública o privada).

Para emprender una adecuada gobernanza digital, es necesario pasar por la educación en la materia. Es vital, así mismo, compartir información en tiempo real entre los gobiernos sobre las amenazas que enfrentan los sistemas digitales y electrónicos vinculados con infraestructuras críticas.[30]

Una de las principales dificultades que enfrenta el abordaje sobre el tema, tanto en el ámbito gubernamental y como en el de la empresa privada, consiste en que algunas amenazas a las infraestructuras críticas, como el ciberterrorismo, se miran distantes. Esa distorsión sobre el tema entorpece con la toma de decisiones políticas inmediatas, si se le compara con otros asuntos que requieren mayor atención por parte del sector político. Sin embargo, es fundamental hacer esfuerzos para que los países identifiquen los riesgos frente a esta amenaza y adecuen sus ordenamientos jurídicos internos para saber cómo actuar si se presentan.

Considero que la educación y la capacitación sobre seguridad informática, son elementos clave ineludibles, junto con la participación ciudadana, en la elaboración de políticas al respecto. En cuanto a ello, es relevante el informe OEA-TrendMicro que aconseja: "Brindar capacitación: Es fundamental permanecer actualizados en el entorno de seguridad cibernética que está en constan-

[30] Cfr. OEA y Trend Micro Incorporated, "Reporte de seguridad Cibernética e Infraestructura Crítica de las Américas", Washington D.C., 2015. Consultado en: <https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf>

te evolución. Se ha comprobado que brindar capacitación técnica a los funcionarios es un medio bastante exitoso para mejorar la seguridad cibernética a escala nacional y regional".[31]

En este sentido, es concordante con la Declaración de Panamá, que indica: "Se encomienda a la Secretaría del CICTE a que promueva en los Estados Miembros actividades de educación y capacitación para crear una cultura pública de reconocimiento de la infraestructura crítica a fin de sensibilizar la sociedad civil".[32]

El instrumento que elaboré y el cual describo en la introducción de este artículo fue aplicado a una población, constituida mayoritariamente por personal informático, arrojó las siguientes opiniones sobre la necesidad de capacitación sobre infraestructuras críticas:

1. Capacitación y participación en simulacros en caso de desastres.
2. Implementación de un plan de continuidad de negocio.
3. Consideración de cómo prevenir el terrorismo informático.
4. Involucramiento del Colegio de Profesionales en Informática y Computación en el resguardo de la infraestructura física.
5. Socialización sencilla y clara de los avances que se han estado realizando en materia de infraestructuras críticas.

Al respecto, un informante estima que la problemática es el desconocimiento en estos tópicos, porque la gente no tiene interés en formarse; incluso, se percibe un retroceso en el manejo de estos temas; además, criticó el nivel de formación académica en estudiantes universitarios y en grupos profesionales hoy. Otra persona entrevistada apuntó la necesidad de reforzar los aspectos éticos y humanistas de quienes trabajan en tecnología de forma especializada, según su sector de trabajo, más allá de los conocimientos dados por certificaciones de tecnologías,

31 OEA y Trend Micro Incorporated, *op. cit.,* p. 4.

32 *Idem.*

metodologías y reglamentos oportunos. Al respecto, el informante 7 apuntó:

> Realmente no me pagan por saber programar o por saber utilizar x herramienta, sino más bien por tener la cabeza lo suficientemente bien amueblada como para traducir todas esas miles o millones de filas de datos en información que aporte valor al negocio del cliente. Y para ello, la parte técnica solo llega a la hora de entender cómo funcionan las APIs de extracción de datos y qué nos ofrece la herramienta o herramientas usadas. El resto, que es lo verdaderamente importante, viene dado por las aptitudes y los conocimientos, enmarcados más en el mundo de las humanidades que en el de la ingeniería

C) Sobre las alianzas público-privadas

Se dice que más del 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por este.[33] Al respecto, orienta uno de los redactores del Informe de la OEA y Trend Micro, Tom Kellermann: "Esta investigación debe servir como una llamada de alerta para advertir que las infraestructuras críticas se han convertido en un objetivo prioritario para los cibercriminales. Estos grupos han intensificado sus ataques mediante el aprovechamiento de las campañas destructivas contra las infraestructuras del Hemisferio Occidental".[34]

Además, indicó: "(…) ver a los líderes de gobierno y de la industria valorar la gravedad de esta amenaza y que expresen una

---

[33] Cfr. OEA y Trend Micro Incorporated, *op. cit.,* p. 3.

[34] OEA, *OEA y Trend Micro presentan Informe sobre "Seguridad Cibernética e Infraestructura Cr*ítica *en las Américas*. Consultado en: <http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15> (07 abril, 2015).

fuerte voluntad de abordar el desafío a través de una mayor inversión y de la colaboración público-privada".[35]

Entre otras conclusiones, dicho informe destaca su crítica a que todavía exista una falta de cooperación proactiva entre los gobiernos y las organizaciones privadas, a pesar de que todos los Estados Miembros acordaron en una reciente declaración del CICTE, denominada *La protección de las infraestructuras críticas de amenazas emergentes*, que la colaboración público-privada es un esfuerzo importante por emprender. En igual sentido, la declaración de Panamá indica: "10. La necesidad de alentar a los Estados Miembros a estrechar vínculos con el sector privado y la sociedad civil, cuando corresponda, en sus respectivos países, para desarrollar programas de fomento de la capacidad preventiva y de protección contra las amenazas a la infraestructura crítica".[36]

En el cuestionario realizado para la presente investigación, uno de los profesionales en informática, a la pregunta sobre la necesidad de alianzas público privadas, respondió de forma categórica: "Todo gira alrededor de la empresa privada; somos los que tomamos la delantera en esos temas; pues el sector público está atrasado décadas. Basta sacar la lista de instituciones que tengan capacidad de seguir operando si pasa una catástrofe en su datacenter [sic]. Sin embargo, la resistencia a buscar alternativas como soluciones en la nube es mayúscula".[37]

Entre los aportes que se consideran necesarios por parte de las empresas privadas se encuentran:

1. Brindar acceso controlado a su infraestructura.

---

35 *Idem.*

36 *Ibidem,* p. 4.

37 OEA y Trend Micro Incorporated, "Reporte de seguridad Cibernética e Infraestructura Crítica de las Américas", Washington D.C., 2015, p. 5. Consultado en: <https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Proteccion%20de%20la%20Inf%20Critica.pdf>

2. Compartir la información que se considere de carácter público en caso de ser necesario (i.e. grabaciones hacia áreas externas).
3. Dar asesorías y brindar capital para construir alternativas en puntos estratégicos del país.
4. Establecer lazos de cooperación con el sector público, a fin de aportar tecnología y capital humano.
5. Mejorar la oferta económica de los servicios privados que contrate el Estado.
6. Realizar esfuerzos para acreditar carreras con SINAES, en el caso de las universidades privadas.
7. Tener programas de capacitación y actualización sobre el tema de infraestructuras críticas en la propia empresa y también colaborar con las ajenas.
8. Formar conciencia en la gente, pues en el ámbito de la seguridad, lo que afecta a un sector, afecta al resto.
9. Fomentar equipos investigativos en las empresas.

V. Ejemplos en Latinoamérica

A) Introducción

En América Latina, el país más digitalizado es Brasil: es el que ha hecho la mayor inversión en TI de la región y se reporta como el cuarto lugar de los países con el mayor número de público usuario de Internet del mundo, con más de 100 millones de personas conectadas. Esta circunstancia se debe, en parte, a que hay incentivos estatales para ello: la presidencia de la República de Brasil, "aprobó el Marco Civil de Internet en abril de 2014, el cual plantea las reglas, los derechos y las obligaciones del uso de Internet, así como la protección de los datos".[38]

[38] OEA y Trend Micro Incorporated, *op. cit.,* p. 17.

Por otra parte, Panamá es un país con experiencia en el tema: ahí el Canal de Panamá se ha erguido como ejemplo de infraestructura crítica a la vez que ha catapultado a este país económicamente y lo ha obligado a mantener altos estándares de calidad en productos económicos, servicios bancarios, de seguridad y demás. Precisamente, fue en Panamá donde se suscribió la "Declaración de Panamá sobre la Protección de la Infraestructura Crítica en el Hemisferio frente al Terrorismo", durante el sétimo período ordinario de sesiones del Comité Interamericano Contra el Terrorismo (CICTE)[39] de la Organización de los Estados Americanos,[40]

[39] El CICTE es un comité de la OEA. Entre sus propósitos destacan promover la cooperación internacional entre estados para prevenir, combatir y eliminar el terrorismo, de acuerdo con la Carta de la OEA y la Convención Americana contra el Terrorismo. Forman parte de él todos los estados de la OEA y organiza una sesión regular anual, donde se discute y toman decisiones sobre terrorismo y medidas de cooperación bilateral y multilateral a nivel internacional y regional. (v. OEA, 2017).

[40] Revisar OEA, <http://www.oas.org/es/sms/cicte/default.asp>. Relacionados con infraestructura crítica se han producido los siguientes instrumentos de derecho internacional: resoluciones de la Asamblea General de la OEA, AG/RES. 1939 (XXXIII-O/03), y la AG/RES. 2004 (XXXIV-O/04) en materia de seguridad cibernética, que constituyen un avance sobre el tratamiento de medidas para fortalecer la infraestructura crítica de los Estados miembros; *la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*; y los trabajos realizados por el Grupo Relator sobre ciberseguridad e infraestructura critica de la Comisión Interamericana de Telecomunicaciones (CITEL), relativos al desarrollo de redes de comunicación. Además, en 2004 la Asamblea General de la OEA aprobó por unanimidad la *Estrategia Interamericana Integral de Seguridad Cibernética*; seguida de la *Declaración de Fortalecimiento de la Seguridad Cibernética de las Américas* (firmada en 2012). El instrumento más reciente en ese ámbito es la *Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes de 2015*, adoptado por el Comité Interamericano contra el Terrorismo (CICTE).

celebradas del 28 de febrero al 2 de marzo de 2007, en Ciudad de Panamá. La Declaración fue aprobada en la tercera sesión plenaria, celebrada el 1 de marzo de 2007. El criterio axiológico que guía dicha Declaración es la lucha contra el terrorismo como herramienta de protección de los derechos humanos, la paz y seguridad.

B) Normativa de Argentina[41]

Este país ha sido otro pionero en este tema: cuenta en su haber con normativa sobre esta temática desde 1999, la cual fue derogada por una norma posterior, cuando se creó el Programa antes mencionado.[42] En efecto, mediante la Resolución JGM N.º 580/2011 suscrita en Buenos Aires, Argentina, el 27 de julio de 2011, se creó el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC), cuyo propósito es "impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado".[43]

---

41 En este tema, recomiendo el estudio *Delincuencia Informática en Argentina y el Mercosur*, de Marcelo Riquert (2009), particularmente pp. 72-79 y pp. 189-191.

42 Cfr. InfoLEG, Información Legislativa. Resolución 580/2001, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, 2017. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>

43 InfoLEG, Información Legislativa. Resolución 580/2001, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, 2017. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>; <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>.

El programa nacional ICIC atiende la demanda de ciberseguridad en el sector público nacional, los organismos interjurisdiccionales y las organizaciones civiles, así como los entes del sector privado que así lo requieran, con el fin de lograr la colaboración de dichos sectores en pos del desarrollo de estrategias y estructuras adecuadas para un accionar coordinado en la implementación de las tecnologías pertinentes, entre otras acciones. Esta iniciativa surgió de la conciencia que en dicho país se hizo sobre la actual dependencia de las infraestructuras físicas de la infraestructura digital, la cual se ha hecho imprescindible para el funcionamiento de bienes y servicios relacionados con esta tecnología.

El artículo 6 del Programa establece una regla importante para garantizar la libertad de los particulares en el uso de redes telemáticas, pues dispone expresamente: "no interceptará ni intervendrá en conexiones o redes de acceso privado de acuerdo a lo estatuido por la Ley Nº 25.326 de Protección de los Datos Personales y su Decreto Reglamentario Nº 1558 del 29 de noviembre de 2001".[44]

VI. Informe de la OEA y Trend Micro

Un insumo valioso al respecto de esta temática es el informe elaborado por la Organización de Estados Americanos (OEA) y la empresa privada Trend Micro Forwaard-looking Threat Research, titulado *Informe sobre seguridad cibernética e infraestructura crítica en las Américas*. En él se presenta una serie de análisis y recomendaciones sobre las infraestructuras críticas, además de una encuesta sin precedente, donde fueron consultados más de 20 Estados miembros de la OEA. Los sujetos participantes en la encuesta pertenecen a agencias de gobierno, así como a diferen-

[44] Cfr. InfoLEG, Información Legislativa. Resolución 580/2001, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, 2017. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>.

tes industrias: comunicaciones, banca y finanzas, manufactura, energía y seguridad, entre otras. Una conclusión vital de dicho informe, es que el hecho de que no exista una asociación pública-privada que regule legalmente las infraestructuras críticas es una serie debilidad que se debe superar.[45]

Algunos datos relevantes de este informe son: el 53% de las personas entrevistadas afirmó haber observado un incremento en los incidentes de los sistemas de cómputo durante el año 2014; el 76% respondió que dichos incidentes se están volviendo cada vez más sofisticados; el 43% dijo haber detectado algún ataque contra una infraestructura crítica de su organización. Finalmente, preocupa a los grupos investigadores el hecho de que un 31% de los sujetos consultados confesó no saber si han sido atacados en sus sistemas de infraestructuras críticas.

VII. En guerra fría digital

Hoy podría resultar más peligrosa la activación de un código malicioso dentro de una computadora que el disparar un misil contra una población determinada. Desde hace décadas, ha comenzado una guerra virtual, solo que el campo de batalla dejó de ser la tierra, el mar, el aire o el espacio, y ahora es el denominado quinto dominio: el ciberespacio.

Actualmente estamos en una guerra fría digital. El *modus operandi* es diverso, pues, aunque generalmente se utiliza el acceso remoto y no autorizado a servidores de información, también se hace por medio de espías infiltrados en organizaciones que manejan información sensible y la secuestran, alteran o codifican.[46]

---

[45] OEA, *OEA y Trend Micro presentan Informe sobre "Seguridad Cibernética e Infraestructura Cr*itica *en las Américas*, p. 7. Consultado en: <http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15> (07 abril, 2015).

[46] Cfr. Nieves, J., "La primera ciberguerra mundial ha estallado ya", *ABC.es*. Consultado en: <http://www.abc.es/tecnologia/redes/20150615/abci-

En cuanto a los objetivos de la ciberdelincuencia, estos pueden ser gubernamentales o particulares. Por ejemplo, imaginemos que un día, al encender la computadora se despliega un mensaje, junto con un cronómetro, que indica: "Ooops, tus archivos importantes están encriptados", y a continuación se exige pagar 300 dólares mediante *bitcoins* (una clase de moneda digital), para desencriptar dichos archivos y recuperarlos".[47] Eso sucedió el 13 de mayo de 2017, cuando atacó el llamado *ransomware*.

El problema de esta guerra es que "(…) en cada ataque, los objetivos suelen ser muy específicos. No existen códigos éticos, ni regulación internacional. Cada uno hace la guerra por su cuenta y el que más recursos tiene más ventajas consigue".[48]

A continuación, enlisto algunos ejemplos de esta batalla cibernética que se está librando:

Caso 1: El día 4 de junio de 2015, el Gobierno de los Estados Unidos hizo público que datos de 4 millones del personal de la Administración Federal habían sido robados tras un ciberataque contra la OPM (Oficina de Administración del Personal del Gobierno). En esa oportunidad, se sospechó de *hackers* de China, pero no había evidencia de si trabajaron por cuenta propia o por encargo del gobierno.

Caso 2: En 2009, se dio la denominada Operación Aurora, un ataque chino contra servidores de Google que terminó con la salida del gigante informático de la nación asiática.

Caso 3: En 2007 y 2008, atacantes de China se colaron en la red de satélites de los Estados Unidos para interceptar sus comunicaciones.

---

ciberguerra-ciberataque-china-201506131801.html> (08 de julio de 2015)

47 Cfr. Oliveira, J. y Jiménez, R., "El ataque de 'ransomeware' se extiende a escala global", *El País*. Consultado en: <https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html> (15 de mayo de 2017).

48 I*dem*.

Caso 4: En 2011, un programa de TV en China transmitió la forma como una universidad norteamericana era "hackeada", mediante un software desarrollado para ciberataques.
Caso 5: En diciembre de 2014, *hackers*, aparentemente de Corea del Norte; accedieron a los equipos de Sony, y lograron llegar a más de cien *terabytes* de información privada, luego de lo cual, difundieron películas y datos confidenciales de la compañía.
Caso 6: En 2013 se dio el robo contra 110 millones de clientes de la empresa Target, lo cual significó que esta, tras un fallo judicial, tuviera que indemnizar hasta por 10 000 dólares a cada consumidor;[49] En dicho fallo, se le ordenó también que mejorara su seguridad de datos y proporcionara educación en seguridad a su personal. Destaca en este caso el gran número de sujetos afectados y que la información sustraída, sumamente confidencial, incluía: nombre, dirección, números de teléfono, correos electrónicos y, en algunos casos, datos de las tarjetas de crédito y débito.
Caso 7: El 13 de mayo de 2017, España, Portugal, Reino Unido y Rusia fueron afectados por un virus denominado *ransomware*, ataque que se expandió a cerca de 74 países en el mundo y a más de 45 mil usuarios de computadoras.[50] El funcionamiento de este virus consistió en instalarse en un equipo, cuando se instala un exploit y accesa un shadow brokers, bloqueando el acceso a archivos importantes (extensiones .doc, .dot, .tiff, .java, .psd, .docs, .xls, .pps, .txt o .mpeg); inmediatamente después, se solicita un rescate en moneda virtual, a cambio de los archivos. La afectación fue crítica en Londres, donde los servicios de salud fueron perjudicados:

---

[49] Cfr. Riley, C. y Pagliery, J., "Víctimas del ataque cibernético a Target podrían recibir hasta 10 000 dólares. *CNN en Español"*. Consultado en: <http://cnnespanol.cnn.com/2015/03/19/victimas-del-ataque-cibernetico-a-target-podrian-recibir-hasta-10-000-dolares/#0> (19 de marzo, 2015).

[50] Cfr. Oliveira, J. y Jiménez, R., "El ataque de 'ransomeware' se extiende a escala global", *El País*. Consultado en: <https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html>_(15 de mayo de 2017).

se afectaron citas, tratamientos y expedientes médicos. Y como el pago de *bitcoins* hace imposible rastrear el depósito de las transacciones a favor de los terroristas, estos no podían ser localizados.

VIII. Conclusiones

La noción de "infraestructura crítica" engloba aquellos elementos materiales y humanos que permiten la vida en comunidad al funcionar como sustrato de las comunicaciones entre personas, el tráfico comercial, mercantil y bursátil, el abastecimiento de energías eléctricas y provenientes del petróleo; además, ordenan las ciudades, almacenan información en bases de datos, y más. En la actualidad, un eje fundamental de las infraestructuras críticas es la Internet y la conectividad que implica. Actualmente, la tecnología denominada Internet de las Cosas (*IoT*) ha llevado a su máxima expresión de dependencia el avance de la conectividad a Internet en la vida diaria. Televisores, electrodomésticos y cámaras de seguridad se encuentran interconectados, nos facilitan y aseguran la vida, incluso la integridad física, pero agregan elementos de vulnerabilidad, pues nos hace propensos a accesos no autorizados. Esta situación vuelve imperativo incrementar las medidas de seguridad en torno al mundo de Internet.

En nuestra región latinoamericana, Panamá es un ejemplo por seguir en el cuido y vigilancia de infraestructuras críticas: allí se suscribió la Declaración de Panamá sobre la protección de la infraestructura crítica en el hemisferio frente al terrorismo, en la cual se concientiza sobre la necesidad de cooperación internacional, estatal y de iniciativa privada para el abordaje de la cuestión. Por otro lado, en Argentina, se creó el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC), el cual constituyendo un paradigma en la identificación y protección de las infraestructuras estratégicas y críticas del sector público nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado.

Ahora bien, desafortunadamente, puede decirse que en la actualidad nos encontramos en medio de una guerra fría cibernética. Los países y grupos criminales organizados preparan y desarrollan técnicas para amenazar y atacar a otros, y afectar sus infraestructuras críticas. Ejemplos existen de diversas índoles en casi todas las latitudes del planeta. De hecho, según el informe de OEA-Trends, las principales amenazas hacia infraestructuras críticas no provienen de accidentes o desastres naturales, sino de *hackers* que utilizan el *phising* para obtener datos de forma no autorizada.

El cuestionario elaborado para esta investigación arrojó la necesidad de que se aborde el tema de gobernanza digital en nuestro país en relación con la seguridad frente a las amenazas que se ciernen sobre las infraestructuras críticas. Actualmente se discute poco, pero es necesario un abordaje interdisciplinario por parte de las autoridades gubernamentales en conjunto con la empresa privada.

Los sujetos informantes para este estudio dejaron claro la preocupación existente sobre la seguridad de la *data centers* o centros donde se almacena información de respaldo de las empresas y personas particulares. En este sentido, el almacenamiento de datos en la nube es una de las mejores herramientas disponible. Sin embargo, de acuerdo con el grupo de informantes, no existe optimismo sobre el actual enfoque de gobernanza digital: uno de ellos incluso expresó que no existe gobernanza digital en Costa Rica.

En este sentido, considero que existen retos pendientes e impostergables: se necesitan más recursos para la formación ética en tecnologías, se requiere más involucramiento de las empresas privadas de la mano con el sector público para compartir experiencias y capacitaciones; y se necesita socializar las herramientas jurídicas para la prevención y sanción de vulneraciones a infraestructuras críticas. Sugiero contar con un organismo especializado en seguridad e inteligencia que regule las infraestructuras críticas con que cuenta Costa Rica.

A este respecto, coincido también con las palabras de uno de los informantes:

> […] *lo peor que podemos hacer es criminalizar a aquellos que dedican tiempo y esfuerzo en encontrar fallas, documentarlas y alertar a los agentes implicados.* Ese trabajo debe valorarse *(y no solo hablo del factor económico)*, dotándolo de las garantías legales suficientes para que el trabajo del auditor de seguridad no sea una carrera llena de obstáculos, donde tan pronto te encuentras con una empresa que te agradece el trabajo, como con otra que lo considera un "hackeo" y te suelta a los abogados.[51]

Asimismo, considero que, ante este tema, no podemos permanecer indiferentes:

> [la criminalidad cibernética] afecta a la sociedad en su conjunto, no sólo amenazando la privacidad de los individuos, sino también comprometiendo potencialmente a la infraestructura crítica de un país y su capacidad de brindar servicios imprescindibles a sus ciudadanos. Esto destaca la necesidad de actuar en cuatro niveles distintos: Internacional, nacional, sector privado e individual, pues los individuos también tienen la misma responsabilidad y deben estar conscientes de sus propias vulnerabilidades y de su participación en la higiene cibernética. (OEA y TrendMicro, 2015, p. 3 La finalidad última de este trabajo es, en materia de seguridad informática, intentar descender de ese "cielo" de conceptos en el cual pretenden habitar quienes leen el Derecho en clave solo positiva, pues sus anclas deben clavarse también en aguas metajurídicas, nutrirse de otros saberes, y en este caso, un campo necesario para el jurista es el ámbito sociológico de las ciencias

[51] Masís, J., *op. cit.,* p. 12.

de la computación, advertencias provenientes de la filosofía del Derecho.[52]

IX. Referencias

Amsterdam data center AMS1, *Datacenter.com. The Foundation of Digital Economy,* (s.f.), Consultado en: <https://datacenter.com/datacenter/locations/data-center-amsterdam-ams1/?gclid=EAIaIQobChMIoZP-sqGN4QIVhozICh0X-zQkQEAAYASAAEgIn1vD_BwE>.

"Apagón en América latina: se cortó la luz en cinco países al mismo tiempo", *La Nación* (Argentina). Consultado en: <http://www.lanacion.com.ar/2039002-apagon-corte-luz-energia-america-latina-costa-rica-panama-honduras-salvador-nicagarua>. (2 de julio, 2017)

Fiegerman, S. Microsoft y Apple luchan por ser la compañía más valiosa del mundo. *CNN en Español*. Consultado en: <https://cnnespanol.cnn.com/2018/11/29/microsoft-apple-compania-mas-valiosa-mundo/> (29 de noviembre, 2018).

Haba, P., *Axiología jurídica fundamental: bases de valoración en el discurso jurídico. Materiales para discernir en forma analítico-realista la claves retóricas de esos discursos*, San José, Editorial Universidad de Costa Rica, 2014.

Heisenberg, W., "La responsabilidad del investigador" en Ramírez, R. y Alfaro, M. (comp.), *Ética, ciencia y tecnología*, 4ª ed., Cartago, Editorial Tecnológica de Costa Rica, 1999, pp. 48-59.

[52] HABA, P., Axiología jurídica fundamental: bases de valoración en el discurso jurídico. Materiales para discernir en forma analítico-realista la claves retóricas de esos discursos, San José, Editorial Universidad de Costa Rica, 2014, p. 227.

InfoLEG, Información Legislativa. Resolución 580/2001, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. Objetivos, 2017. Disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>

Ciberataque en EE.UU. afectó datos de 4 millones de empleados federales. (04 junio de 2015). *La Nacion-AFP.* Consultado en: <http://www.nacion.com/mundo/EE-UU-ciberneticos-empleados-federales_0_1491650942.html>.

Lemaitre Picado, R., *Manual sobre delitos informáticos para la ciber-sociedad costarricense de IJSA*, 2011.

Ley N°8279 y sus reformas, Ley del Sistema Nacional para la Calidad. *La Gaceta*, San José, Costa Rica. 2 de mayo de 2002.

lwp. Comunidad de Programadores, Diccionario informático, 2019. Consultado en: <https://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=ddos>

Martínez, J., Mejía, J., Muñóz, M. y Meredith-García, Y., "La seguridad en Internet de las Cosas: Analizando el tráfico de información en aplicaciones para iOS", *Revista Computación e Informática*, a. 6 núm. 1, Centro de Investigación en Matemáticas CIMAT, A.C., Zacatecas, México.

Espectro Radioeléctrico, Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC, 2017. Consultado en: <http://www.mintic.gov.co/portal/604/w3-article-2350.html>

Masís, J. Cuestionarios de entrevistas. Realizados mediante correo electrónico. Entrevistador Jonathan Masís Solís. Entrevistados anónimo, agosto, 2017.

Nieves, J., "La primera ciberguerra mundial ha estallado ya", *ABC.es.* Consultado en: <http://www.abc.es/tecnologia/redes/20150615/abci-ciberguerra-ciberataque-china-201506131801.html> (08 de julio de 2015)

OEA y Trend Micro Incorporated, "Reporte de seguridad Cibernética e Infraestructura Crítica de las Américas", Washington D.C., 2015. Consultado en: <https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf>.

OEA, *OEA y Trend Micro presentan Informe sobre "Seguridad Cibernética e Infraestructura Cr*ítica *en las Américas*. Consultado en: <http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15> (07 abril, 2015).

OEA, *Declaración de Panam*á sobre la protección de la infraestructura crítica en el hemisferio frente al terrorismo, 2007. Consultado en: <http://www.oas.org/es/sms/cicte/documents/declaraciones/doc_dec_1_07_final_spa.pdf>.

Oliveira, J. y Jiménez, R., "El ataque de 'ransomeware' se extiende a escala global", *El País*. Consultado en: <https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html> (15 de mayo de 2017).

OEA, "OEA Más derechos para más gente", 2017. Consultado en: <http://www.oas.org/es/sms/cicte/default.asp>.

"Protección de datos Intech: Claves para la continuidad de negocio", *Blog de Intech: Integration Technologies*. Consultado en: <https://www.intechsp.com/es/proteccion-de-datos-intech-la-continuidad-de-negocio/> (6 junio 2018)

Riley, C. y Pagliery, J., "Víctimas del ataque cibernético a Target podrían recibir hasta 10 000 dólares. *CNN en Español*". Consultado en: <http://cnnespanol.cnn.com/2015/03/19/victimas-del-ataque-cibernetico-a-target-podrian-recibir-hasta-10-000-dolares/#0> (19 de marzo, 2015).

Riquert, Marcelo, *Delincuencia Informática en Argentina y el Mercosur*, Buenos Aires, Ediar, 2009.

Rodríguez, Montenegro y Cuevas, "Introducción al Internet de las Cosas. Redes de Ingenieria", Universidad Distrital Francisco José de Caldas, vol. 6, julio 2019, pp. 53-59.

Sineribe, "Sistema Nacional de Información y Registro Único de Beneficiarios del Estado", Costa Rica, 2019. Recuperado de: <https://www.sinirube.go.cr>.

"Servidor caído: riesgos, efectos y prevención",. *Digital Guide*. Consultado en: <https://www.ionos.es/digitalguide/servidores/know-how/servidor-caido-que-hacer/> (20 de junio, 2017)

Unitag, "¿Qué es un Código QR?", 2019. Consultado en: <https://www.unitag.io/es/qrcode/what-is-a-qrcode>

Villalobos, P., "Costa Rica fue blanco de ataques de espionaje cibernético de Corea del Norte en 2018, según informe" en *Ameliarueda.com*. Consultado en: <https://www.ameliarueda.com/nota/costa-rica-blanco-ataques-espionaje-cibernetico-corea-norte-informe> (06 de abril, 2019).