lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias



ISSN 2175-9596

# CIBERSEGURIDAD, INFRAESTRUCTURAS CRÍTICAS DE LA INFORMACIÓN Y USO DE SOFTWARE DE CÓDIGO ABIERTO EN EL ESTADO

*Cibersegurança, infraestruturas críticas da informação e uso de software de código aberto no Estado*

*Cybersecurity, critical information infrastructures and use of open source software in the State*

**Daniela Vásquez Leiva**[a]
**Eduardo Vilches Fuentes**[b]

[(a)] Abogada – Universidad de Chile. E-mail: dvasquez@derecho.uchile.cl.
[(a)] Abogado – Universidad de Chile.

**Resumen**

La Política nacional de Ciberseguridad lanzada en Chile durante el primer semestre de 2017 representa una oportunidad para que el Estado asuma un liderazgo en la protección de las infraestructuras críticas de la información (ICI) que sostienen procesos vitales tanto para la ciudadanía, el Estado, como para los privados. En ese contexto el presente trabajo analiza las ventajas derivadas de promover en estas infraestructuras software de código abierto, considerando al efecto un caso paradigmático de vulnerabilidad sobre una ICI como fue Heartbleed en 2014, la cual atendida su entidad técnica significó la transmisión no cifrada de información sensible y datos personales altamente sensibles.
**Palabras clave:** Ciberseguridad; Infraestructuras críticas de la información; Código abierto; Chile.

***Resumo***

*A Política Nacional de Cibersegurança lançada no Chile durante o primeiro semestre de 2017 representa uma oportunidade para o Estado assumir a liderança na proteção de infra-estruturas críticas de informação (ICI) que sustentam processos vitais para os cidadãos, o Estado e para os particulares. Neste contexto, este trabalho analisa as vantagens derivadas da promoção de*

*software de fonte aberta nessas infraestruturas, considerando um caso paradigmático de vulnerabilidade em um ICI, como foi Heartbleed em 2014, que serviu sua entidade técnica, significou a transmissão de informações não criptografadas de informações pessoais e dados pessoais altamente sensíveis.*
***Palavras-chave:*** *Cibersegurança; Infraestruturas críticas de informação; Código aberto; Chile.*

***Abstract***

*Taking The National Cybersecurity Policy launched in Chile during the first semester of 2017 represents an opportunity for the State to assume leadership in the protection of critical information infrastructures (CII) that sustain vital processes for citizens, the State, and for the private ones. In this context, this work analyzes the advantages derived from promoting open source software in these infrastructures, considering a paradigmatic case of vulnerability on an CII: the Heartbleed case in 2014, which due to its technical entity meant the*
*unencrypted transmission of sensitive information and highly sensitive personal data.*
***Keywords:*** *Cybersecurity; Critical information infrastructure; Open source; Chile.*

## INTRODUCCIÓN

El pasado 27 de abril, la Presidenta Michelle Bachelet lanzó la primera Política Nacional de Ciberseguridad (PNCS o la Política), la cual "contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2022, para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente" (Gobierno de Chile, 2017).

Por su parte, en el marco de los objetivos estratégicos a 2022 la PNCS busca que "el país cuente con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos".

Así, se entiende que un programa o sistema es robusto[1] si reacciona en forma adecuada frente a situaciones a priori imprevistas; mientras que la resilencia, para estos efectos, refiere la capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones; y que constituye un incidente informático[2] aquel evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.

[1] Fuente: http://iie.fing.edu.uy/investigacion/grupos/bicoti/bicoti1/SoftEngineering/softeng01.htm (recuperado el 30 de octubre de 2017).
[2] Fuente: http://www.ciberseguridad.gob.cl/glosario (recuperado el 30 de octubre de 2017).

En dicho marco, el presente informe, busca dar cuenta del estado de la ciberseguridad en Chile, las vías por las cuales se protegen las infraestructuras de la información y las ventajas derivadas de implementar en dichas infraestructuras software de código "abierto", todo ello bajo el análisis de un caso paradigmático sobre vulnerabilidades en una infraestructura crítica de la información (ICI).

## ANTECEDENTES

En Derecho comparado, la Directiva 2008/114 define las infraestructuras críticas (IC) como: "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones". Por su parte, en el ámbito nacional, actualmente existe sólo un cuerpo normativo que regula un tipo especial de infraestructuras críticas: el reglamento contenido en el DTO 60/2012 de Subtel[3], el cual se aboca exclusivamente al ámbito de las telecomunicaciones (ello como consecuencia del terremoto que afectó a Chile en el año 2010) considerando IC: "aquellas redes y sistemas de telecomunicaciones cuya interrupción, destrucción, corte o fallo generaría un serio impacto en la seguridad de la población afectada".

Bajo ese contexto, la PNCS define la ciberseguridad como: "una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido [éste último] como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren", y, en pos de aquélla, la Política propende a la protección de un tipo particular de infraestructura crítica: las ICI, indicando que éstas corresponden a: "las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado"; y que "mientras se adopta una política específica para IC, serán consideradas ICI las relativas a los siguientes sectores: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras".

[3] Reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones. Disponible en: http://bcn.cl/1z17b (recuperado el 30 de octubre de 2017).

## DESAROLLO

En abril de 2014 se hizo público[4] el caso de la vulnerabilidad, que para efectos técnicos y académicos, se considera vulnerabilidad al "*bug*" o error en una o más líneas de código fuente de un programa, cuando un adversario puede usar dicho "*bug*" para afectar la seguridad de un sistema, crítica[5], denominada "*Heartbleed*"[6], que afectó al *OpenSSL*[7], que es definido en su *URL* oficial[8] como: "un proyecto de código [fuente[9]] abierto[10] que proporciona un conjunto robusto, de calidad comercial y con todas las funciones para los protocolos TLS *(Transport Layer Security)* y *Secure Sockets Layer* (SSL), el cual, también es una biblioteca de criptografía de propósito general […] , que es licenciado

[4] De acuerdo con Mark J. Cox de OpenSSL, Neel Mehta (del equipo de seguridad de Google) reportó un Heartbleed en 2014 y en paralelo la empresa Codenomicon habría registrado el dominio Heartbleed.com, no obstante ambos, Mehta y Codenomicon, habían reportado la vulnerabilidad a *OpenSSL*. Dicho reporte, en términos técnicos se denomina *Responsible Disclosure,* entendiéndose que éste ocurre cuando se descubre una vulnerabilidad – el investigador informa al proveedor del sistema. A veces es conveniente tener una tercera parte que coordine, gestione y facilite la comunicación entre revelador y proveedor. Es conveniente esforzarse en que la información sea sólo accesible al menor número de personas posible y de la máxima confianza. Toda la comunicación debería ser por un canal seguro para evitar una filtración. Si el proveedor es receptivo y coopera adecuadamente en la resolución del problema el investigador espera a que se publique el arreglo para revelar toda la información sobre la misma salvo el exploit. Se suele considerar que el proveedor actúa adecuadamente si rápidamente reproduce y reconoce el problema, da méritos a los descubridores, soluciona el problema de forma probada en un periodo apropiado. Fuente: https://es.wikipedia.org/wiki/Revelación_responsable (recuperado el 30 de octubre de 2017).

[5] Se considera "crítica", ya que, según se aprecia en los riesgos señalados más abajo, esta vulnerabilidad en una específica tecnología de la información puede producir importantes repercusiones en la seguridad, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado.

[6] En español 'hemorragia del corazón', lo cual da inmediata cuenta de la magnitud de la vulnerabilidad y sus efectos.

[7] Sin perjuicio de nuevas vulnerabilidades descubiertas con posterioridad, algunas de ellas críticas, pero que no serán parte del presente informe. Para otros ejemplos véase: https://www.certsi.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-openssl (recuperado el 30 de octubre de 2017).

[8] Acceso: https://www.openssl.org.

[9] El código fuente de un programa está escrito por un programador en algún lenguaje de programación, pero en este primer estado no es directamente ejecutable por la computadora, sino que debe ser traducido a otro lenguaje o código binario; así será más fácil para la máquina interpretarlo (lenguaje máquina o código objeto que sí pueda ser ejecutado por el hardware de la computadora). Para esta traducción se usan los llamados compiladores, ensambladores, intérpretes y otros sistemas de traducción. Fuente: https://es.wikipedia.org/wiki/C%C3%B3digo_fuente.

[10] Doctrinariamente los tipos de software pueden clasificarse según diversos parámetros, uno de ellos distingue según el acceso al código fuente. Así, existen: (a) software propietario que no da el acceso al código fuente a los usuarios sino que sólo les entrega el código ejecutable, e incluso, prohíbe el acceso y modificación del mismo, ello gracias a los derechos de propiedad intelectual, los cuales se manifiestan en las licencias de uso asociadas; (b) software libre: entrega acceso al código fuente y además obliga, vía licencias de uso e.g. GPL, a que cualquier modificación del software debe licenciarse en términos que se permita, copulativamente, la ejecución del software, el acceso al código, la modificación del mismo y la distribución de éste – ello pues entiende al software desde una concepción ética; y (c) software de código abierto: se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas. Así, su modelo de licencia sólo asegura siempre el acceso al código, más no las otras facultades garantizadas por el software libre. De esta forma, cualquier se puede afirmar que todo software libre es *open source*, pero no todo programa *open source* es software libre. Ahora bien, para el caso específico de marras, la *Open Source Initiative*, define este proyecto como aquél que permite un método de desarrollo de software que aprovecha el poder de la revisión distribuida de los pares y la transparencia del proceso. La promesa de código abierto es una mayor calidad, una mayor fiabilidad, una mayor flexibilidad, un menor coste y un alto a las actividades predatorias de bloqueo por parte de los proveedores. Fuente: https://opensource.org/about (recuperado el 30 de octubre de 2017).

a través de una licencia Apache 2.0"[11]. Una muy buena explicación sobre de qué forma funciona SSL señala que éste es:

> […] un protocolo de seguridad utilizado en Internet. Los navegadores suelen indicar que el sitio que estás visitando está asegurado con SSL/TSL mediante un candado verde en la barra de direcciones […].
> Para una conexión SSL se utilizan dos llaves, una pública y una privada. Los navegadores utilizan la llave pública para encriptar los datos y el servidor utiliza la llave privada para desencriptarlos. De esta forma la conexión resulta fácil, cualquiera puede saber la llave pública del host para poder enviarle datos, pero sólo la llave privada puede desencriptarlos. Todo el mundo podrá codificar mensajes con la misma llave, pero nadie podrá descodificarlos sin la llave privada, que está en el lado del servidor (Lázaro, n.d.)

Sobre en qué consintió "*Heartbleed"*, es útil, para estos efectos, citar extractos de prensa especializada:

> [Si] OpenSSL es vulnerable, lo más razonable es que revoques tu certificado SSL y consigas otro nuevo en el que la clave privada no haya podido ser comprometida. […] Los principales riesgos son:
> a) Que alguien pueda suplantar tu servidor web, ya que teniendo la parte pública (se obtiene conectándote al servidor) y la parte privada (a través del ataque), nada impediría configurar un servidor web con esos datos y ser a todos los efectos 'tu' sitio web. Esto no hace que automáticamente alguien que ponga www.tusite.com sea redirigido al servidor del atacante (aquí interviene el protocolo DNS) pero, si el atacante consigue montar un ataque *man-in-the-middle*, puede redirigir las conexiones a su servidor y suplantar el sitio original. El navegador web no mostrará ningún tipo de alerta cuando negocie la sesión SSL, por tanto, el usuario no sería consciente del engaño. 'Esta práctica podría ser de mucha utilidad para países que coartan la libertad de expresión, por ejemplo, China. Con este ataque podrían haberse hecho con la parte privada del certificado SSL de cualquier sitio web vulnerable y que sea de interés, y de esa forma poder espiar a sus ciudadanos'.
> b) Al tener la clave privada, que es la base para descifrar las comunicaciones entre un cliente y el servidor, el tráfico SSL se podría descifrar sin problema. Por tanto, si alguien estuviese a la escucha de nuestras comunicaciones (realizando *sniffing*), el cifrado de las comunicaciones no le importaría porque sería capaz de descifrarlas y acceder a la información circulante por la red" (Velasco, 2014).

En dicho contexto, en que diversos estudios[12] dan cuenta de que la vulnerabilidad en *OpenSSL* era

[11] Este tipo de licencia entrega a cada colaborador una licencia perpetua, mundial, no exclusiva, sin cargo, libre de regalías e irrevocable para reproducir, preparar obras derivadas, exhibir públicamente, públicamente realizar, sublicenciar y distribuir el trabajo y las obras derivadas en forma de código fuente o código objeto. Fuente: https://www.apache.org/licenses/LICENSE-2.0 (recuperado el 30 de octubre de 2017).

[12] Por ejemplo, el informe "The Matter of Heartbleed" de Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman y Michael Bailey. Acceso: https://jhalderm.com/pub/papers/heartbleed-imc14.pdf (recuperado el 30 de octubre de 2017).

conocida con meses de antelación previo a su puesta en conocimiento público, cabe preguntarse: ¿cuál sería la razón de promover el uso de código abierto respecto de sistemas relativos a infraestructuras críticas de la información? Ello, pues, una primera aproximación indicaría que dado que el analizar el código habría permitido conocer el "*bug*" y explotar éste, sería mucho más eficiente restringir el acceso al código fuente, mediante sistemas de licencias propietarias.

La respuesta es simple, la gran característica del código "abierto" es que permite a los desarrolladores y usuarios conocer y analizar libremente las líneas de códigos y los algoritmos de los programas, con lo que se produce el efecto de comunidad, por el cual, gracias a esa transparencia una gran cantidad de sujetos, bajo distintos incentivos nobles u oscuros[13], revisa el código aumentando, en consecuencia, la probabilidad de reporte de errores hacia el desarrollador o bien disminuyendo el tiempo, y con ello el impacto de la explotación de un vulnerabilidad *"Zero Day"*[14].

Piénsese, por ejemplo, que si en el caso de *OpenSSL* el código fuente hubiese sido propietario, probablemente aún estaríamos todos los usuarios de internet (personas comunes, compañías, activistas, Estados, etc.) confiando nuestros hábitos y patrimonio en un certificado digital cuya seguridad no sería tal. Lo anterior, pues no existen incentivos nobles para revisar este tipo de código, ya que es técnicamente complejo (e.g. requiere técnicas de ingeniería reversa) y jurídicamente arriesgado.

El último punto referido, riegos legales, es particularmente relevante para quienes se atreven a reportar vulnerabilidades, pué se exponen a persecución judicial debido a la vulneración de *copyright,* por ejemplo en Chile la ley n. 17.336, sobre propiedad intelectual, garantiza los derechos de los titulares de derechos de autor al proteger en el numeral 16 de su artículo 3°: "los programas computacionales, cualquiera sea el modo o forma de expresión, como programa fuente o programa objeto, e incluso la documentación preparatoria, su descripción técnica y manuales de uso" y sólo exceptúa determinadas y especificas acciones consignadas en el artículo 71Ñ, respecto de programas computacionales y específicamente sobre "*copias obtenidas legalmente"* que no sería el caso. Asimismo, en Chile algunas acciones de auditoría de código podrían caer en el tipo penal consagrado en el artículo 2º de la

[13] Entre los incentivos nobles pueden señalarse aquellos académicos, espirituales, o monetarios – e.g. recompensas como el Google vulnerability Reward Prgram. Entre los menos nobles puede citarse la venta de vulnerabilidades a brokers y entre los más oscuros pueden citarse la investigación de vulnerabilidades para fines de vigilancia y opresión.
[14] Zero Day es una nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque. Fuente: https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day (recuperado el 30 de octubre de 2017).

Ley n. 19.223 que indica "el que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio"; o bien en el tipo del artículo 4° de la misma Ley "el que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio".

## CONCLUSIÓN

La experiencia ha demostrado que la seguridad total no existe, que el software cien por ciento seguro es sólo una estrategia de venta, por tanto, en caso de sistemas relacionados a infraestructuras críticas de información debería promoverse, como política de Estado, la mayor apertura posible mediante licencias de software libre o bien *open source*, ello para garantizar a la comunidad técnica que el análisis y *disclosure* responsable de vulnerabilidades no les traerá aparejada sanciones relativas a *copyright* o delitos informáticos[15].

Así, el modelo propuesto, evidenciado en el caso de *OpenSSL*, permite disminuir el impacto de vulnerabilidades asociadas a infraestructuras críticas de la información, ya que, como indica la máxima informática: "existen dos tipos de sistemas, los que sabemos que han sido comprometidos y aquellos que aún no nos enteramos de que han sido comprometidos"; más aún si se considera que, como indica Gustavo Crespi (2017, paginación indisponible): "Las compras públicas representan alrededor del 12% del PIB en países de la OECD, cifra que en América Latina y el Caribe llega al 20%. Por ello, la demanda del Estado y su poder de compra, puede ayudar a crear un mercado lo suficientemente importante para contrarrestar la incertidumbre, estimulando la inversión privada en investigación y desarrollo (I+D) e innovación, y convirtiéndose en ese primer comprador de productos y servicios innovadores que hagan más eficiente la provisión de bienes públicos".

[15] De allí, por ejemplo, que debido a las implicancias que *Heartbleed* producía, gigantes tecnológicos vinculados al mundo del software propietario hayan decidido invertir en mejoras al modelo de *open source* que soporta infraestructuras de la información críticas – e.g.: "Gigantes como IBM, Intel, Microsoft, Facebook y Google se han comprometido a invertir millones en mejoras para open source. El proyecto denominado Core Infrastructure Initiative estará administrado por Linux Foundation y buscará financiar proyectos de código abierto para ayudar a mejorar sus niveles de seguridad". Fuente: https://www.welivesecurity.com/la-es/2014/04/24/microsoft-facebook-google-invertiran-open-source-luego-heartbleed (recuperado el 30 de octubre de 2017).

## REFERÊNCIAS

Crespi, G. (2017, noviembre 07). Aprovechando la demanda del estado: ¿Cómo Implementar un programa de compra pública de innovación? *Puntos sobre la i.* Recuperado el 30 de octubre de https://blogs.iadb.org/puntossobrelai/2017/11/07/demanda-del-estado-programa-compra-publica-innovacion.

Decreto n. 60, de 12 de mayo de 2012 (2012). Reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones. Diario Oficial de la República de Chile. Santiago: Ministerio de Transportes y Telecomunicaciones.

Gobierno de Chile (2017). Política Nacional de Ciberseguridad. Recuperado el 30 de octubre de 2017 de http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

Lázaro, D. (n.d.). *SSL y OpenSSL en PHP: Disponer de una conexión segura SSL en una aplicación web es importante aunque no se trate de un sitio web e-commerce.* Recuperado el 30 de octubre de 2017 de https://diego.com.es/ssl-y-openssl-en-php.

Ley n. 17.336, de 03 de noviembre de 2017 (2017). Propiedad intelectual. Diario Oficial de la República de Chile. Santiago: Ministerio de Educación Pública.

Ley n. 19.223, de 07 de junio de 1993 (1993). Tipifica figuras penales relativas a la informática. Diario Oficial de la República de Chile. Santiago: Ministerio de Justicia.

Unión Europea (2008). Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Diario Oficial de la Unión Europea, L345/75. Recuperado el 30 de octubre de 2017 de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008L0114.