PUNTO de EQUILIBRIO

CENTRO DE INVESTIGACIÓN | UNIVERSIDAD DEL PACÍFICO

TECNOLOGÍA

Vulnerabilidad en el sector público y la urgencia de pensar en ciberseguridad, por Freddy Linares

Autor

Comunicaciones CIUP

comunicacionesciup@up.edu.pe

28 marzo, 2022

A mitad del siglo XX, la tercera revolución industrial dio luz a elementos trascendentales como los microprocesadores y el internet (Pinheiro et. al, 2019). La masificación de este último y el acelerado desarrollo de tecnologías ha llegado a transformar los conceptos de infraestructura tradicional para el sector privado y público. El gran valor de los recursos digitales (como la información, sistemas y programas) para la gestión exige modernizar la infraestructura interna para facilitar la gestión pública. Países como EE.UU.[1] o Inglaterra[2], que buscan liderar en servicios públicos digitales, invierten en sistemas de diseño enfocados en propiciar una eficiente experiencia del ciudadano. En Perú, iniciativas como la “Ley de Gobierno Digital” (Decreto Legislativo N° 1412, 2018) afronta esta realidad priorizando servicios digitales para impulsar la gestión dentro de instituciones públicas. Sin embargo, aliarse con las nuevas tecnologías involucra también nuevos retos.

Los medios digitales incluyen potenciales vulnerabilidades, que al no ser minimizadas, facilitan que algunos agentes alteren, copien o secuestren datos o recursos digitales desde distintas y versátiles modalidades. Entre 2016 a 2020, los cibercrímenes causaron pérdidas de $13.3 mil millones (INTERNET CRIME COMPLAINT CENTER, 2020) y “los peligros online” representan la segunda mayor preocupación de las empresas 2021 (PwC, 2021). Estas vulnerabilidades no son ajenas a los espacios y medios digitales manejados por el sector público. Ante todas estas amenazas, la ciberseguridad es una necesidad que se alinea con los intereses de una nación para garantizar el bienestar de su población. Según von Solms & von Solms (2018) la ciberseguridad abarca estrategias y prácticas que resguardan la información y recursos digitales de los usuarios de internet, desde ciudadanos a distintas organizaciones. Según el informe de Estrategia Nacional de Seguridad y Confianza Digital (ENSC) para el periodo 2021-2026, la ciberseguridad es la “capacidad tecnológica de preservar el adecuado funcionamiento de las redes,

activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital" (Gob.pe, 2021).

El conflicto actual entre Rusia y Ucrania demuestra como la ciberseguridad es un elemento más que relevante para garantizar la estabilidad y eficiencia interna de un país. El miércoles 23 de febrero varias páginas de instituciones públicas y bancarias ucranianas sufrieron ciberataques conocidos como de "denegación de servicio", o DoS por sus siglas en inglés (BBC, 2022). Comprometer la infraestructura digital clave de sectores como el financiero o el administrativo en un país desencadenan una serie de daños hacia la población. Sistemas paralizados, incomunicados o inhabilitados tienen consecuencias multisectoriales en el corto, mediano y hasta el largo plazo. En Perú, perder la capacidad de coordinación digital entre entidades públicas causaría daños fatales, especialmente considerando el actual contexto sanitario y económico.

Es por ello, que se torna válido preguntarse: ¿qué tan vulnerable es el Perú? Según el Reporte sobre entidades públicas que implementaron su equipo de respuesta ante incidentes de seguridad digital[3], solo 117 de 2363 informaron tenerlo implementado. En la la lista de entidades pendientes figura la Autoridad Nacional de Datos Personales, el Congreso de la República, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica, la Contraloría General de la República, el Despacho Presidencial, la Fuerza Aérea del Perú, entre otros. Si bien, en términos de arquitectura de ciberseguridad no existe una arquitectura del todo perfecta pues estas poseen fortalezas y debilidades que deben estudiarse a profundidad para sofisticarse (Cano, 2015), una arquitectura desactualizada o descuidada dejará muy vulnerable a un país ante los cibercrímenes.

Durante 2021 en Latinoamérica, los intentos de ciberataques aumentaron en 600% en comparación de 2020 y Perú presentó aproximadamente 11,5 millones de intentos, siendo solo superado por Brasil con 88,5 millones y México con 156 millones de intentos (Fortinet, 2022). Según el informe de ENSC, respecto a otros países de la región como Chile, Argentina, Colombia o Brasil que cuentan con una estrategia de seguridad digital, Perú aún se encuentra en una fase de desarrollo del suyo con un nivel de madurez formativo (Gob.pe, 2021) manteniendo aún vulnerables su ciberespacio y recursos. El historial de ciberataques al sector público peruano parece confirmar este escenario. En el 2011 las páginas web del Ministerio de Economía y Finanzas, Congreso de la República, Policía Nacional del Perú, Oficina Nacional de Gobierno Electrónico e Informática y la de Servicios al Ciudadano y Empresas fueron atacadas por varias horas por la sección peruana del grupo internacional de hackers conocido como Anonymous (Gob.pe, 2011).

Nuevamente, el 2015 Anonymous atacó páginas de gobiernos municipales y el parque de las leyendas, bloqueando el acceso y mostrando imágenes de protesta como parte de un ataque masivo llamado "#OpIndependencia" (Canal N, 2015). En septiembre de 2015, 12 páginas del Gobierno Regional de Cajamarca fueron

hackeadas de forma similar por Anonymous como muestra de apoyo a la defensora ambiental Máxima Acuña (La República, 2020). En 2018, la organización tecnológica Hiperderecho denunció que un error informático en una página de la ONPE filtró por varios meses datos personales de los ciudadanos volviendo esta información en accesible y descargable (Escalante, 2018; La República, 2018). En mayo de 2020 dos expertos en ciberseguridad denunciaron que 500 hackers robaron cerca de un millón de soles hackeando el sistema de RENIEC dedicado al Bono Universal donde obtuvieron los datos personales de los beneficiarios y los suplantaron (La República, 2020). Por último, en noviembre de 2020, Anonymous se adjudicó la inactivación de la página del Congreso Peruano, la Policía Nacional, el Poder Judicial, y varias otras, como apoyo a las protestas contra el gobierno transitorio de Manuel Merino (France24, 2020; La Vanguardia, 2020). La frecuencia demuestra que no se requiere de un enfrentamiento internacional para vulnerar la ciberseguridad, sino que pueden surgir de agentes individuales o colectivos.

Pese a este historial, no se puede negar que el interés por la ciberseguridad ha estado en agenda. Algunos ejemplos son la firma del Convenio de Budapest para la cooperación internacional en materia de delitos informáticos (2019) (Gob.pe, 2020b), la aprobación de la Ley de Delitos Informáticos (2013), la creación del Comité del Gobierno Digital (2018), la aprobación de la Ley de Ciberdefensa (2019), entre otras (Gob.pe, 2021). Una de las oficinas dedicadas a reforzar la ciberseguridad es el **Equipo de Respuesta ante Incidentes de Seguridad Digital del Perú (también llamado PECERT)** encargado de resolver, anticipar, enfrentar y coordinar la respuesta ante los ciberataques, así como de promover el desarrollo de soluciones y estrategias para la seguridad digital de instituciones privadas y públicas (Gob.pe, 2022). Entre sus actividades, PECERT publica casi diariamente la “Alerta integrada de seguridad digital” que es un informe y análisis técnico sobre ciberataques a entidades públicas y empresas. Este informe es redactado en colaboración de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, el Comando Conjunto de las Fuerzas Armadas, entre otras instituciones (Gob.pe, s.f.). En estos informes se monitorea el ciberespacio y se identifican ciberataques como phishing, denegación de servicios (DoS), malwares, ransomware, exploits, etc (Gob.pe, 2020a).

Finalmente, y pese a que el sector público proyecta aún una fuerte vulnerabilidad ante cibercrímenes que se extiende naturalmente a la población, existen 117 instituciones públicas encaminadas a cambiar ese escenario.

FUENTES:

BBC (26 de febrero, 2022). Rusia invade Ucrania: cómo los ciberataques se convirtieron en otra poderosa arma en el conflicto entre ambos países. [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://www.bbc.com/mundo/noticias-internacional-60508957

Canal N (28 de julio, 2015). Hackearon el sitio web del Gobierno peruano. [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://canaln.pe/actualidad/hackearon-sitio-web-gobierno-peruano-n191446

Cano Carrillo, Jesus. (2015). Arquitecturas distribuidas de gobierno electrónico con ciberseguridad crítica. Tesis doctoral. Escuela Técnica Superior de Ingenieros Industriales. Obtenido de http://e-spacio.uned.es/fez/view/tesisuned:IngInd-Jscano

Decreto Legislativo N° 1.412. Decreto Legislativo que aprueba la "Ley de Gobierno Digital". [fecha de Consulta 6 de Diciembre de 2021]. Disponible en: https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/

El Peruano (13 de setiembre de 2018). Decreto Legislativo N° 1412. Decreto Legislativo que aprueba la Ley de Gobierno Digital. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf

Escalante, Diego (17 de julio, 2020). Hiperderecho (hiperderecho.org). ONPE filtró los datos personales de millones de peruanos durante más de medio año. [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://hiperderecho.org/2018/07/onpe-filtrado-datos-hackaton/

Fortinet (8 de febrero, 2022).FortiGuard Labs presenta reporte de ciberataques en América Latina (fortinet.com). Recuperado de: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

France24 (15 de noviembre, 2020). Anonymous se atribuye el hackeo al Congreso peruano, mientras la crisis en el país se agudiza. [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://www.france24.com/es/am%C3%A9rica-latina/20201115-peru-crisis-anonymous-congreso-manuel-merino

GESTIÓN (27 de febrero, 2020). Ciberseguridad: en el 2020 van 15 denuncias contra empresas en el Perú. (gestion.pe). [fecha de consulta: 18 de febrero de 2022] Recuperado: https://gestion.pe/peru/ciberseguridad-en-el-2020-van-15-denuncias-contra-empresas-en-el-peru-noticia/

Gob.pe (25 de febrero de 2022). Presidencia del Consejo de Ministros. Equipo de respuesta ante incidentes de seguridad digital del Perú - Gobierno del Perú (www.gob.pe). [fecha de consulta: 17 de febrero de 2022] Recuperado de: https://www.gob.pe/7739-presidencia-del-consejo-de-ministros-equipo-de-respuesta-ante-incidentes-de-seguridad-digital-del-peru

Gob.pe (26 de junio, 2011). OSIPTEL. Anonymous atacó 6 webs del Gobierno Peruano. [fecha de consulta: 18 de febrero de 2022] Recuperado

de: https://www.gob.pe/institucion/osiptel/noticias/179224-anonymous-ataco-6-webs-del-gobierno-peruano

Gob.pe (30 de junio, 2021). Presidencia del Consejo de Ministros. Estrategia Nacional de Seguridad y Confianza Digital - Gobierno del Perú (www.gob.pe). [fecha de consulta: 17 de febrero de 2022] Recuperado de: https://www.gob.pe/institucion/pcm/informes-publicaciones/1998221-estrategia-nacional-de-seguridad-y-confianza-digital

Gob.pe (6 de abril de 2020a). Presidencia del Consejo de Ministros. Alerta integrada de seguridad digital N° 002-2020-PECERT (www.gob.pe). [fecha de consulta: 17 de febrero de 2022] Recuperado de: https://www.gob.pe/institucion/pcm/informes-publicaciones/473226-alerta-integrada-de-seguridad-digital-n-002-2020-pecert

Gob.pe (15 de septiembre, 2020b). Ministerio Público Fiscalía de la Nación. "Convenio sobre la Ciberdelincuencia" permite a jueces y fiscales realizar requerimientos de cooperación internacional- Gobierno del Perú (www.gob.pe). [fecha de consulta: 17 de febrero de 2022] Recuperado de: https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

Gob.pe (s.f.). Presidencia del Consejo de Ministros. Alerta integrada de seguridad digital del CNSD. - Gobierno del Perú (www.gob.pe). [fecha de consulta: 17 de febrero de 2022] Recuperado de: https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital

INTERNET CRIME COMPLAINT CENTER [IC3](2020). Internet crime report 2020. Recuperado de: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

La República (1 de junio, 2020). Anonymous en Perú: conoce las veces que la agrupación hackeó páginas peruanas. [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://larepublica.pe/sociedad/2020/06/01/ataques-de-anonymous-en-peru-recuerda-las-veces-que-varias-paginas-fueron-hackeadas-atmp/

La República (2 de agosto, 2018). Investigan posible filtración de datos personales en la ONPE (larepublica.pe). [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://larepublica.pe/politica/1291073-investigan-posible-filtracion-datos-personales-onpe/

La República. (29 de mayo, 2020). *Ciberdelincuentes hackearon el sistema del bono universal y robaron casi un millón de soles.* [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://larepublica.pe/sociedad/2020/05/28/bono-universal-ciberdelincuentes-hackean-web-y-roban-cerca-de-un-millon-de-soles-destinado-a-familias-en-pobreza/

La Vanguardia (14 de noviembre, 2020). Anonymous hackea web del Congreso de Perú, causante de grave crisis política [fecha de consulta: 18 de febrero de 2022] Recuperado de: https://www.lavanguardia.com/internacional/20201114/49466261194/anonymous-hackea-web-del-congreso-de-peru-causante-de-grave-crisis-politica.html

Pinheiro, P., Putnik, G., Castro, A., Castro, H., Dal Bosco, R., & Romero, F. (2019). Industry 4.0. and Industrial Revolutions: an Assessment based on Complexity. FME Transactions, 47, 831-840. https://scindeks-clanci.ceon.rs/data/pdf/1451-2092/2019/1451-20921904831P.pdf

PwC (2021). 24th Annual Global CEO Survey - A leadership agenda to take on tomorrow. Recuperado de: https://www.pwc.com/cl/es/publicaciones/pwc-24th-global-ceo-survey.pdf

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where? Information & Computer Security, 26(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

[1] Para más detalles revisar: https://designsystem.digital.gov/

[2] Para más detalles revisar: https://design-system.service.gov.uk/

[3] Ver https://www.gob.pe/institucion/pcm/informes-publicaciones/2605569-reporte-sobre-entidades-que-implementaron-su-equipo-de-respuestas-ante-incidentes-de-seguridad-digital