PARLAMENTO ANDINO

RECOMENDACIÓN No. 427

"PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD DURANTE LA CRISIS SANITARIA POR EL BROTE DE COVID-19"

La Plenaria del Parlamento Andino en el marco del periodo ordinario de sesiones del mes de junio, en cumplimiento de sus atribuciones estipuladas en el Acuerdo de Cartagena y en su Reglamento General, y a los 26 días del mes de junio de 2020.

CONSIDERANDO

Que, el Parlamento Andino es el órgano comunitario, deliberante, de control político y participación ciudadana del proceso andino de integración, y tiene como una de sus atribuciones estipulada en el literal E, del Artículo 43 del Acuerdo de Cartagena: "Participar en la generación normativa del proceso mediante sugerencias a los órganos del Sistema de proyectos de normas sobre temas de interés común, para su incorporación en el ordenamiento jurídico de la Comunidad Andina ";

Que, la Comisión Tercera de "Seguridad Regional, Desarrollo Sustentable, Seguridad y Soberanía Alimentaria" se encuentra desarrollando y debatiendo con expertos internacionales sobre una propuesta de Marco Normativo para el Fortalecimiento de la Ciberseguridad e Informática en la Región Andina, que incluirá políticas públicas exitosas y buenas prácticas para apoyar la gestión de los Estados y desarrollar competencias en la población en esta importante temática;

Que, como consecuencia de la actual crisis sanitaria debido al brote mundial de COVID-19, se ha evidenciado un aumento en la realización de actividades cotidianas a través de medios digitales y virtuales, como el teletrabajo, las compras en internet, la realización de pagos de servicios públicos, entre otras;

Que la transformación y aceleración de la digitalización de nuestras sociedades representa oportunidades, y posibilidades actuales de que los cibercriminales pueden aprovechar para interceptar los dispositivos de internet de las cosas interconectados en los hogares, empresas, instituciones públicas, y organismos internacionales y de esta manera invadir la privacidad. Dichos ataques conllevan al robo de credenciales de autenticación de sistemas bancarios, y portales de medios de pagos online, donde la víctima entrega el acceso a su red al ciberdelincuente.

Que, durante la crisis sanitaria y el tiempo de aislamiento social, se ha evidenciado un aumento de delitos informáticos, relacionados con ataques de ingeniería social, basados en fuentes abiertas como la inteligencia de las redes sociales (SOCMINT) y, Inteligencia de fuentes abiertas (OSINT) para obtener información de las personas naturales, compañías, sus proveedores y clientes. El envío de estos ataques de Phishing, de códigos maliciosos y malware tienen como fin la suplantación de identidad. También han nacido nuevos ataques de última generación con inteligencia artificial y ataques Business Email Compromise, los cuales son una de las principales amenazas, los cuales analizan los componentes fundamentales en la actividad diaria de una empresa. Estos ataques tienen como fin engañar a empleados, suplantando la identidad de ejecutivos con el fin de que realicen acciones no autorizadas que conllevan a defraudar a las empresas e institucionales, los cuales consiguen suplantar a sus clientes y proveedores mediante el robo de identidad basado en ingeniería social.

Que, la UNICEF investigó que 1 de cada 3 jóvenes han sufrido algún tipo de acoso cibernético y 1 de cada 5 jóvenes dejaron sus estudios por sufrir acoso en línea. El acoso es una de las problemáticas que más está afectando a niños, niñas y adolescentes, ya sea en línea o físicamente sus consecuencias son altamente negativas. Las víctimas de acoso son más propensas a abandonar sus estudios, consumir alcohol y sustancias psicoactivas[1].

Que, los resultados de Fortinet Threat Intelligence Insider Latin America para finales de 2019 mostraron un incremento de los movimientos de malware, exploits y botnet en la red de América Latina y el Caribe.[2] “En el último trimestre del año, la región sufrió más de 9 mil millones de intentos de ataques, con un total de 85 mil millones en 2019”, (Threat Intelligence Insider Latin America, 2019) siendo esto aproximadamente 12 ataques de malware cada segundo.[3] Dentro de estos se destaca el crecimiento del 9,5% en el phishing financiero.[4]

---

[1] UNICEF (10/02/2020) UNICEF busca empoderar a jóvenes para evitar el acoso y prevenir los riegos en línea. Obtenido de: https://www.unicef.org/colombia/comunicados-prensa/unicef-busca-empoderar-a-jovenes-para-evitar-el-acoso-y-prevenir-los-riesgos-en-linea

[2] Threat Intelligence Insider Latin America. (2019). Informe Ejecutivo Fortinet Threat Intelligence Insider Latin America. Threat Intelligence Insider Latin America. Obtenido de https://www.fortinetthreatinsiderlat.com/es/Q4-2019/landing

[3] Luzardo, A. M. (13 de septiembre de 2016). Usuarios de internet sufren 12 ataques de malware por segundo. Obtenido de Enter.Co: https://www.enter.co/especiales/claro-negocios/usuarios-de-internet-sufren-12-ataques-de-malware-por-segundo/

[4] Kanpersky Lab. (18 de febrero de 2020). El phishing financiero creció un 9,5% en el último trimestre de 2019. Obtenido de Kanpersky Lab: https://latam.kaspersky.com/about/press-releases/2020_el-phishing-financiero-crecio-un-95-en-el-ultimo-trimestre-de-2019

Que, en el reciente informe de Kaspersky, se estima que tres de cada cuatro (73%) empleados que se encuentra realizando teletrabajo aún no han recibido ninguna formación en temas relacionados a la ciberseguridad,[5] y que, "uno de cada cuatro (27%) empleados dice haber recibido correos electrónicos de phishing relacionados con COVID-19,"[6] (Kaspersky Lab, 2020) los cuales aumentaron en 74% de febrero a marzo en Latinoamérica.[7]

Que, de acuerdo con la información proporcionada en el último informe de Kaspersky sobre ciberseguridad en la región de América Latina y el Caribe, casi el 50% de los usuarios de internet de estos países fueron víctimas de al menos un intento de ataque en el último año.[8] Por su parte, Perú y Bolivia ocupan el segundo lugar en la lista de países más afectados producto de ataques de malware con 42%, "seguidos de Chile con 40%, México con 39.9% y Colombia con 39.3%."[9] (Luzardo, 2016) Además, con respecto a los correos engañosos, la región se ha visto muy afectada. En este caso, Brasil encabeza el primer lugar con 12.3% de los usuarios afectados por esto, luego se encuentran Argentina (7.5%), Ecuador (5,7%), Bolivia (5,2%) y Venezuela (5,2%).[10]

Que, 2 de cada 5 latinoamericanos no es consciente que sus dispositivos conectados a internet pueden ser hackeados a través del router[11] y "que alrededor de un 23%, en tanto, no entiende o no sabe cómo funciona el Internet de las Cosas (IoT)."[12] (Kaspersky Lab, 2020) Quienes más desconocen sobre el tema son los peruanos

---

[5] Kaspersky Lab. (11 de mayo de 2020). El 73% de los empleados no ha recibido orientación sobre ciberseguridad para el Home office. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_homeworkers-wait-for-protection-73-of-employees

[6] Kaspersky Lab. (11 de mayo de 2020). El 73% de los empleados no ha recibido orientación sobre ciberseguridad para el Home office. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_homeworkers-wait-for-protection-73-of-employees

[7] Kaspersky Lab, (07 de abril de 2020). Ciberataques a dispositivos móviles en América Latina crecieron más del 70% en marzo, según Kaspersky. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_ciberataques-a-dispositivos-m-viles-en-am-rica-latina-crecieron-m-s-del-70-en-marzo-seg-n-kaspersky

[8] Kaspersky Lab. (28 de agosto de 2019). Kaspersky registra 45 ataques por segundo en América Latina. Obtenido de Kaspersky Daily: https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

[9] Luzardo, A. M. (13 de septiembre de 2016). Usuarios de internet sufren 12 ataques de malware por segundo. Obtenido de Enter.Co: https://www.enter.co/especiales/claro-negocios/usuarios-de-internet-sufren-12-ataques-de-malware-por-segundo/

[10] BSA. (2018). Gestión de software: imperativo de seguridad, oportunidad de negocio. Obtenido de ENCUESTA GLOBAL DE SOFTWARE BSA 2018: https://gss.bsa.org/

[11] Kaspersky Lab. (20 de abril de 2020). 2 de cada 5 latinoamericanos ignora que sus dispositivos conectados pueden ser hackeados a través del router. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_2-de-cada-5-latinoamericanos-ignora-que-sus-dispositivos

[12] Kaspersky Lab. (20 de abril de 2020). 2 de cada 5 latinoamericanos ignora que sus dispositivos conectados pueden ser hackeados a través del router. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_2-de-cada-5-latinoamericanos-ignora-que-sus-dispositivos

(50%), luego los chilenos (46%), brasileños (40%) y colombianos (39%).[13] Sumado a lo anterior, a partir del último estudio realizado por Comparitech (2019) en Ecuador 15,38 % de teléfonos móviles están infectados con malware, en Colombia el 14,23%, en Chile el 11,99% y en Perú el 11,17%.[14]

Que, Bolivia en 2019 ocupó el cuarto lugar en la lista de países atacados por troyanos bancarios móviles teniendo en cuenta la cantidad de usuarios víctimas de este delito. Igualmente, "se estima que una organización boliviana está siendo atacada en promedio 1417 veces por semana en los últimos 6 meses, en comparación con los 528 ataques por organización a nivel mundial. "[15] (Cuenca, 2020) De estos ataques la divulgación de información corresponde al 64%, afectando principalmente a organizaciones y entidades gubernamentales. Además, alrededor del 80% de los archivos que contenían algún tipo de elemento malicioso se trasfirieron por medio correo electrónico, un porcentaje bastante significativo en correlación con el 56% registrado a nivel mundial. [16]

Que, durante 2019 Chile atravesó por más de 1,5 billones de intentos de ataques cibernéticos,[17] lo que significa 4,16 millones de intentos al día, de los que en un gran porcentaje se encuentran "diseñados para entrar en redes bancarias, obtener información financiera y robar dinero."[18] (Salas, 2020) A la par, en el país se registran en promedio de 1.120 a 2.400 ataques diarios de phishing, siendo este el principal método de propagación usado por los ciberdelincuentes con un 91%.[19] En 2020 los delitos informáticos en el país se elevaron en más de un 74% respecto a los últimos

---

[13] Kaspersky Lab. (20 de abril de 2020). 2 de cada 5 latinoamericanos ignora que sus dispositivos conectados pueden ser hackeados a través del router. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2020_2-de-cada-5-latinoamericanos-ignora-que-sus-dispositivos

[14] BISCHOFF, P. (03 de marzo de 2020). ¿Qué países tienen la peor (y mejor) seguridad cibernética? Obtenido de Comparitech: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

[15] Cuenca, C. (23 de abril de 2020). Estado de las amenazas cibernéticas en Bolivia. Obtenido de Observatorio de Delitos Informáticos Bolivia : https://www.odibolivia.org/2020/04/23/estado-de-las-amenazas-ciberneticas-en-bolivia/

[16] Cuenca, C. (23 de abril de 2020). Estado de las amenazas cibernéticas en Bolivia. Obtenido de Observatorio de Delitos Informáticos Bolivia : https://www.odibolivia.org/2020/04/23/estado-de-las-amenazas-ciberneticas-en-bolivia/

[17] Corporateit . (6 de marzo de 2020). Chile sufrió más de 1,5 billones de intentos de ciberataques en el 2019. Obtenido de Corporateit Noticias de Tecnología y negocios: corporateit.cl/index.php/2020/03/06/chile-sufrio-mas-de-15-billones-de-intentos-de-ciberataques-en-el-2019/

[18] Salas, P. (06 de marzo de 2020). Chile sufrió más de 1,5 billones de intentos de ciberataques en el 2019. Obtenido de Corporateit: https://www.corporateit.cl/index.php/2020/03/06/chile-sufrio-mas-de-15-billones-de-intentos-de-ciberataques-en-el-2019/

[19] Agenda País. (06 de enero de 2020). Informe revela las ciberamenazas que afectarán a Chile este 2020. Obtenido de Agenda País: https://www.elmostrador.cl/agenda-pais/2020/01/06/informe-revela-las-ciberamenazas-que-afectaran-a-chile-este-2020/

meses de 2019.[20] Los principales ciberdelitos son del tipo malware, de los cuales el 50% se relacionan con ransomware y afectan principalmente a las empresas y organizaciones.[21]

Que, en Colombia los ataques por malware durante los últimos meses han crecido en un 612%, y que, la cantidad de dinero pagado para rescatar información oscila entre los 32 y los 160 millones de pesos.[22] Por ello, el país se encuentra entre los que son más afectados en la región por ataques de carácter ransomware "con un total de 252 lo que corresponde al 30% después de Brasil y Argentina."[23] (Tecnosfera, 2019) Adicionalmente, de acuerdo con el informe realizado por investigadores del Tanque de Análisis y creatividad de las TIC junto con otras instituciones, el principal interés de los cibercriminales es el lucro, en donde el phishing (42%), la suplantación de identidad (28%),el envío de malware (14%) y los fraudes en medios de pago en línea (16%), son los tipos de ataques con mayor número de ataques reportados.[24]

Que, en Ecuador se registran un promedio de 10 a 12 ataques cibernéticos por segundo,[25] de los cuales los cuatro ciberdelitos con mayor cantidad de denuncias corresponden a: "el acceso no consentido a un sistema, el ataque a la integridad de sistemas informáticos, la interceptación ilegal de datos y la revelación ilegal de bases de datos."[26] (Dávila, 2019) Conjuntamente, según un estudio elaborado por la Policía Nacional, Interpol y el Centro de respuesta a Incidentes Informáticos (Ecucert), aproximadamente el 85% de los ciberataques son consecuencia de los errores de los usuarios, quienes no toman precauciones al hacer uso del internet y de aplicaciones. Al mismo tiempo, un 58% de las personas suele olvidar sus teléfonos móviles en sus vehículos o lugares de trabajo, dejando expuesta información sensible y el 60% usa

---

[20] Agenda País. (06 de enero de 2020). Informe revela las ciberamenazas que afectarán a Chile este 2020. Obtenido de Agenda País: https://www.elmostrador.cl/agenda-pais/2020/01/06/informe-revela-las-ciberamenazas-que-afectaran-a-chile-este-2020/

[21] RoiPress. (09 de mayo de 2020). Aumenta el cibercrimen en Chile en el contexto de COVID-19 - Cifras de Marzo. Obtenido de RoiPress: https://www.roipress.com/2020/05/aumenta-el-cibercrimen-en-chile-en-el.html

[22] TicTac. (2019). Tendencias del Cibercrimen en Colombia 2019-2020. Bogotá: TicTac. Obtenido de https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[23] Tecnósfera. (30 de octubre de 2019). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. El Tiempo, págs. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790.

[24] Tanque de Análisis y Creatividad de las TIC. (2019). Tendencias del Cibercrimen en Colombia 2019-2020. Obtenido de Cámara Colombiana de Informática y Telecomunicaciones: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[25] Redacción Justicia. (24 de abril de 2019). 12 ataques por segundo se registran en Ecuador. El Telégrafo, págs. https://www.eltelegrafo.com.ec/noticias/judicial/12/delitosinformaticos-coip-policia-fiscalia.

[26] Dávila, E. (19 de septiembre de 2019). Los cuatro delitos informáticos más recurrentes en Ecuador. Obtenido de Primicias: https://www.primicias.ec/noticias/tecnologia/estos-delitos-informaticos-mas-recurrentes-ecuador/

de manera indiscriminada la misma contraseña en dispositivos personales y laborales.[27]

Que, en el Perú, según Digiware un poco más de 4 mil millones de dólares se pierden al año como producto de ciberataques. Sumado a ello, de acuerdo con la empresa de seguridad Eset, las empresas se ven afectadas frecuentemente por la infección con malware, los casos de phishing y la falta de disponibilidad de servicios críticos. Indistintamente, de acuerdo con datos proporcionados por la policía peruana, semanalmente se realizan entre 30 y 35 denuncias de delitos informáticos. Es decir, un promedio de 120 casos por mes. De estos, un poco más del 50% de los casos corresponden a la modalidad de fraudes electrónicos, un preocupante 20% se relaciona con pornografía infantil, un 10% hace referencia a la suplantación de identidad y el resto tiene que ver con otro tipo de ciberdelitos.[28]

Que, la ciberseguridad debe ser entendida como un aspecto fundamental de la seguridad nacional de los Estados dada la coyuntura actual, ya que ésta puede llegar a tener profundas incidencias en el desarrollo normal de las actividades sociales, económicas e incluso políticas de los países andinos. Por lo tanto, es necesaria la adopción de acciones urgentes para fortalecer la ciberseguridad en nuestros países, de manera conjunta, consciente y coordinada.

Por las consideraciones antes expuestas la Plenaria del Parlamento Andino, en uso de sus atribuciones y conforme a lo prescrito en su Reglamento General,

RECOMIENDA

,

ARTÍCULO PRIMERO. A los órganos e instituciones de los poderes estatales al sector privado, a los organismos internacionales y multilaterales, al sector académico y a la ciudadanía en general de los países miembros del Parlamento Andino, considerar las siguientes ‘buenas prácticas’ para acceder a información relevante en materia del brote de COVID-19:

- Revisar la información exclusivamente de fuentes oficiales, accediendo de manera directa a los sitios webs de estas instituciones o medios de

[27] Sandoval, F. (16 de agosto de 2016). En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. El Telégrafo, págs. https://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario.

[28] Andina. (2017). Riesgos y desafíos en el día del internet. Agencia Peruana de Noticias, pág. http://portal.andina.com.pe/edpespeciales/2017/ciberseguridad/index.html.

comunicación, evitando siempre ingresar a través de enlaces proporcionados por mensajes de texto, redes sociales o correos electrónicos.

- Verificar la dirección de correo electrónico del remitente de un mensaje antes de abrirlo, es indispensable contrastar esta información con la recibida en casos anteriores o la información publicada en el sitio web de la institución, ya que los ciberdelincuentes son capaces de crear enlaces y direcciones similares a las cuentas legítimas.
- Evitar entregar datos personales a solicitudes o sitios web a los que se haya accedido a través de enlaces en redes sociales, mensajes de texto, aplicaciones de mensajería, o correos electrónicos, especialmente si se desconoce al remitente, es preferible ingresar este tipo de información en los sitios oficiales de las organizaciones e instituciones;
- Analizar exhaustivamente los contenidos de los mensajes o correos electrónicos, evitando ingresar a enlaces o descargar contenidos si se encuentran errores gramaticales, fallas de ortografía, saludos genéricos (“Respetado ciudadano”, “Estimado Sr/Sra.”) o si le solicita realizar acciones como ingresar a enlaces con urgencia y de manera injustificada.

ARTÏCULO SEGUNDO. A las organizaciones e instituciones estatales, las pequeñas, medianas y grandes empresas, los organismos e instituciones multilaterales e internacionales, las organizaciones no gubernamentales, y las organizaciones sociales, implementar los siguientes consejos para garantizar la ciberseguridad e informática en los procesos de teletrabajo y trabajo a distancia:

- Establecer los accesos remotos a la red de la organización solo cuando sea estrictamente necesario y mediante canales seguros como redes virtuales privadas (VPN-Virtual Private Network).
- Implementar un doble factor de autenticación para el acceso a cuentas de correo electrónico, a la red de la organización o a cualquier tipo de información que tenga un carácter confidencial y de seguridad para institución. La doble autenticación es una medida extra de seguridad que, generalmente, implica un código generado de manera aleatoria, que será enviado a través de un mensaje de texto o correo electrónico, y posteriormente solicitado por el sistema para cualquier tipo de ingreso a la red, al sitio web o a una cuenta institucional.
- Hacer uso de servicios remotos exclusivamente a través de protocolos seguros (HTTPS), estos accesos deben restringirse únicamente a zonas aisladas de la red institucional y a servicios permitidos que no contienen información confidencial de la organización.

- Verificar la existencia de controles en los equipos personales que accederán de manera remota a la red de la organización, es indispensable validar la implementación de antivirus, firewalls, actualizaciones y configuraciones de seguridad.
- Garantizar que los equipos personales posean la opción de cifrado de disco y revisar los controles para prevenir la fuga de información confidencial de la organización.
- Definir claramente los canales y protocolos de comunicación para reportar cualquier riesgo, amenaza o situación sospechosa en el funcionamiento de la red institucional, las cuentas de correo electrónico, los equipos y servidores de acceso remoto.
- Realizar respaldos continuos y permanentes de la información crítica y confidencial de la organización.

ARTÍCULO TERCERO. A los órganos e instituciones de los poderes del Estado, las instituciones del sector académico, el sector privado, los organismos multilaterales e internacionales y las organizaciones de la sociedad civil, implementar soluciones de criptografía (como Blockchain y firma digital) para la protección y seguridad de la información y la documentación institucional. La criptografía permite, a través del uso de matemática aplicada, reducir la utilización de papel en los trámites de las instituciones, generando procesos más seguros y ágiles.

ARTÍCULO CUARTO. A las instituciones estatales de los países miembros del Parlamento Andino definir líneas de financiamiento nacional y local, así como oportunidades de obtención de financiamiento a nivel multilateral, para el desarrollo de proyectos creativos y de innovación en materia de ciberseguridad para afrontar el brote de COVID-19 y realizar seguimiento al cumplimiento de los Objetivos de Desarrollo Sostenible y la Agenda 2030 de las Naciones Unidas.

Dada y suscrita a los veintiséis (26) días del mes de junio de 2020.

Notifíquese y publíquese

PARLAMENTO ANDINO
PRESIDENCIA

P.A. VÍCTOR ROLANDO SOUSA
Presidente

PARLAMENTO ANDINO
SECRETARIA GENERAL

DR. EDUARDO CHILIQUINGA MAZÓN
Secretario General