Proyecto de Ley N°...8324/2023-CR

CONGRESO de la REPÚBLICA

CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
04 JUL. 2024
RECIBIDO
Firma: Hora: 10:17 AM

LEY QUE PROTEGE LA IDENTIDAD Y ESTABLECE LINEAMIENTOS DE CIBERSEGURIDAD EN EL PERÚ

Los Congresistas de la República que suscriben, miembros del Grupo Parlamentario **PODEMOS PERÚ** a iniciativa del Congresista de la República **CARLOS JAVIER ZEBALLOS MADARIAGA**, ejerciendo la facultad legislativa que le confiere el Art. 107 de la Constitución Política del Perú, y en cumplimiento de lo establecido en los Artículos 67,74, 75 y 76 del Reglamento del Congreso de la República, propone para su aprobación el siguiente Proyecto de Ley.

PROYECTO DE LEY

"LEY QUE PROTEGE LA IDENTIDAD Y ESTABLECE LINEAMIENTOS DE CIBERSEGURIDAD FINANCIERA EN EL PERÚ "

ARTÍCULO 1.- OBJETO DE LA LEY

Establecer el marco legal para la protección de la identidad con huellas dactilares en el territorio nacional y establecer lineamientos de ciberseguridad en el sistema financiero nacional con la finalidad de brindar protección legal a los usuarios digitales para evitar acciones delictivas en perjuicio de los ciudadanos.

ARTÍCULO 2.- AMBITO DE APLICACIÓN

La presente ley se aplicará a todos los peruanos en el territorio nacional y en el extranjero, con registro en el Registro Nacional de Estado Civil (RENIEC).

ARTICULO 3.- Modificatoria a la Ley Nº 26497 Ley Orgánica del Registro Nacional de Identificación y Estado Civil.

Modifíquese el primer párrafo del artículo 32.- de la Ley N° 26497 Ley Orgánica del Registro Nacional de Identificación y Estado Civil, quedando redactado de la siguiente manera:

El Documento Nacional de Identidad (DNI) deberá contener, como mínimo la fotografía del titular de frente y con la cabeza descubierta, además de los siguientes datos...

ARTICULO 4.- PROTECCIÓN DE LA IDENTIDAD DACTILAR

a). - Las huellas dactilares son registros reservados de cada persona, quedan en la base de datos del RENIEC, las cuales solo podrán ser utilizadas mediante software biométrico certificado por OSIPTEL sin visualización, y por autorización expresa judicial para fines de investigaciones policiales, judiciales ó para fines de defensa nacional en salvaguarda de la nación, debidamente sustentadas, ello no prohíbe el recojo de muestras en escenas del crimen por parte de las autoridades competentes.

b). - Para efectos de convenios que celebra el RENIEC con empresas privadas respecto al otorgamiento de acceso a la base de datos de identidad, solo otorgará acceso con los datos según lo previsto en el artículo 3 de la presente ley, las empresas deberán otorgar una carta garantía de responsabilidad civil que permita una reparación civil y/o resarcimiento a las personas y el Estado, que resulten agraviadas por el mal uso de la base de datos, cuyos responsables de acceso deberán firmar declaración jurada de responsabilidad civil, administrativa y civil de uso correcto la cual deberá ser remitida al RENIEC para su custodia.

c). - En el caso de las entidades estatales los responsables de los accesos a la base de datos del RENIEC serán designados mediante resolución de la máxima autoridad ó quien haga las veces y deberán firmar la declaración jurada de responsabilidad administrativa, civil y penal.

d). - En las entidades estatales se prohíbe la retención del documento nacional de identidad, fotocopiado y fotografiado del mismo sin autorización del titular, en el caso de la lectura del código de barras las entidades que tengan acceso a ello sólo podrán solicitar el DNI para dicho fin, para efectos de atención al usuario el no portar el DNI físico no es causal de impedimento para la atención o ingreso, para ello las entidades estatales deben implementar mecanismos

alternativos de identificación de manera que se garantice la atención al usuario.

ARTICULO 5.- LINEAMIENTOS EN CIBERSEGURIDAD

1.- El acceso a servicios digitales por parte de los ciudadanos peruanos donde se verifique la identidad mediante huellas dactilares, las empresas o personas naturales deberán implementar sistemas de software y hardware verificados por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

2.- Las entidades financieras autorizadas por la Superintendencia de Banca y Seguros (SBS) implementarán las medidas de ciberseguridad para los diversos servicios que brindan adicionales a las huellas dactilares, que eviten la suplantación de identidades, clonación de tarjetas y otras maneras delictivas.

ARTICULO 6.- IMPLEMENTACIÓN

La implementación y lineamientos de tecnologías emergentes (inteligencia artificial, biométrica avanzada, reconocimiento facial y otros) para efectos de ciberseguridad financiera y de identidad será establecida mediante el reglamento de la presente ley, a cargo de la Secretaría de Gobierno y Transformación Digital de la PCM en coordinación con la Superintendencia de Banca y Seguros.

DISPOSICIÓN COMPLEMENTARIA FINAL

Única. – Reglamentación

El Poder Ejecutivo en un plazo de 120 días reglamentará la presente ley.

FIRMA DIGITAL
Firmado digitalmente por: LUNA GALVEZ Jose Leon FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 03/07/2024 15:01:38-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEBALLOS MADARIAGA Carlos Javier FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 03/07/2024 12:01:05-0500

FIRMA DIGITAL
Firmado digitalmente por: JUAREZ CALLE Heidy Lisbeth FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 03/07/2024 15:30:24-0500

CARLOS JAVIER ZEBALLOS MADARIAGA
Congresista de la República

Firmado digitalmente por: LUNA GALVEZ Jose Leon FAU 20161749126 hard
Motivo: Soy el autor del documento
Fecha: 03/07/2024 15:01:58-0500

FIRMA DIGITAL
Firmado digitalmente por: PAREDES CASTRO Francis Jhasmina FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 03/07/2024 15:10:24-0500

FIRMA DIGITAL
Firmado digitalmente por: BURGOS OLIVEROS Juan Bartolome FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 03/07/2024 15:50:21-0500

FIRMA DIGITAL
Firmado digitalmente por: ALCARRAZ AGUERO Yorel Kira FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/07/2024 09:40:17-0500

CONGRESO DE LA REPÚBLICA

Lima, **04** de **JULIO** de **2024**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglam8ento del Congreso de la República: pase la Proposición **N° 8324/2023-CR** para su estudio y dictamen, a la (s) Comisión (es) de:

1. **CONSTITUCIÓN Y REGLAMENTO; Y**
2. **ECONOMÍA, BANCA, FINANZAS E INTELIGENCIA FINANCIERA.**

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

I. EXPOSICIÓN DE MOTIVOS

Generalmente, al hablar de identidad personal nos referimos a algo semejante a la autoimagen. Es el conjunto de características que definen a un individuo y le permiten reconocerse a sí mismo como un ente distinto y diferenciado de los demás.

No es exactamente un sinónimo de personalidad, ni de carácter, ni de rasgos personales, pero sí es un concepto que pareciera englobar todos estos aspectos, formando así la "esencia" de un individuo.

Sin embargo, desde ciertas perspectivas, como la filosófica, definir este concepto se torna bastante más complicado. ¿Cuál es su naturaleza? ¿Cómo la distinguimos de otros rasgos psicológicos, emocionales o intelectuales del ser humano? ¿Cómo es que puede ser la misma persona y a la vez cambiar en el tiempo? ¿En dónde termina la identidad y comienza el contexto?

Existen numerosos enfoques que buscan definir la identidad personal. Algunos de ellos son:

- El psicologista. Que asigna un rol importante a la memoria y a los procesos mentales dentro de la identidad;
- El fisiológico-somático. Que busca las respuestas en el propio cuerpo del ser humano;
- El narrativo. Que plantea la identidad personal como un relato-de-uno-mismo que constantemente se está contando (y por ende modificando).

Por último, en ámbitos más prácticos, como el de la administración, se suele hablar de identidad personal como el conjunto de datos e información personal con los que podemos tener acceso a algún tipo de cuenta, aplicación o perfil de servicios. Es decir, se piensa la identidad personal a partir de la información que la representa. A esto se le conoce también como "huella digital".

El concepto de identidad personal, comprendido desde distintos puntos de vista, suele tener una serie de características estables, como son:

- Constancia. La identidad es un conjunto de rasgos constantes, es decir, que pueden apreciarse de la misma manera a lo largo del tiempo, si bien es posible al mismo tiempo apreciar sus cambios a largo plazo.
- Coherencia. Cuando decimos que la identidad personal es coherente, queremos decir que podemos predecir algunos de sus rasgos, o sea, algunas de sus reacciones ante determinadas condiciones o estímulos.
- Adaptabilidad. Si bien la identidad personal es constante en un momento determinado, también es cambiante a lo largo del tiempo, a medida que la experiencia y la vida van suprimiendo ciertas conductas e implantando otras.
- Carácter socio-cultural. Esto quiere decir que la identidad se da en contraposición a los demás, ya que está definida en base a las semejanzas o diferencias respecto de quienes comparten con nosotros una comunidad y una cultura.

Durante años, la seguridad de la autorización mediante huellas dactilares ha estado sujeta a un debate encarnizado. En el 2013, poco después del lanzamiento del iPhone 5S con TouchID, los investigadores demostraron que se podía *hackear* esta tecnología al fotografiar una huella dactilar en una superficie de vidrio y usarla para obtener un molde que engañara al sistema. Pero la tecnología no deja de evolucionar y las mejoras han sido alentadoras.

El año pasado, por ejemplo, los fabricantes comenzaron a equipar sus *smartphones* con escáneres de huellas dactilares ultrasónicos que se escondían bajo la pantalla, lo que eliminaba la necesidad de paneles adicionales y los hacía más seguros, al menos en teoría.

Nuestros colegas en Cisco Talos decidieron comprobar la facilidad con la que se podía engañar a los diversos tipos de escáneres de huellas dactilares en los dispositivos modernos; o si la tecnología al menos era segura.

La teoría detrás de la autorización mediante huellas dactilares

Para empezar, os dejamos con un breve recordatorio sobre cómo funcionan los escáneres de huellas dactilares. La idea principal es muy sencilla: colocas tu dedo en el escáner de un *smartphone*, portátil o un candado inteligente y el sensor extraerá una imagen de tu huella dactilar. Cada tipo de escáner reconoce las huellas dactilares a su modo. El equipo de Cisco Talos se centró en los tres tipos más comunes:

- **Los escáneres capacitivos** son los más comunes. Crean una imagen por medio de una pequeña carga eléctrica generada por los condensadores en miniatura integrados que pueden almacenar electricidad. Cuando el dedo toca el escáner, descarga estos condensadores. Cuanto más extenso sea el contacto (crestas papilares), mayor será la descarga; el espacio entre la piel y el sensor (valles papilares) provocan una menor descarga. El escáner analiza la diferencia y determina el patrón.

- **Los escáneres ópticos** básicamente realizan una fotografía de la huella dactilar. El dispositivo emite una luz hacia el dedo a través de un prisma; las crestas y los valles reflejan esta luz de modo distinto; el sensor lee la información y la convierte en una imagen.
- **Los escáneres ultrasónicos** usan una señal de ultrasonido en lugar de una luz y registran el eco emitido por las crestas y los valles (al igual que el reflejo de luz, las crestas y valles presentan diferentes ecos). Este tipo de escáner no necesita entrar en contacto con el dedo, así que puede situarse debajo de la pantalla. Además, "oye" no sólo la parte del dedo más cercana a la superficie, sino también los bordes más alejados del sensor, de modo que la imagen está más próxima a lo tridimensional, lo que ayuda al escáner a detectar las falsificaciones que usan copias planas de impresiones.

Al leer tu huella dactilar, el escáner o el sistema operativo la compara con la que está almacenada en el dispositivo. Y, como no existe ningún método de lectura de huellas dactilares que sea perfecto, cada fabricante permite cierto margen de error.

Cuanto más amplio es el margen de error, más fácil resulta falsificar una huella dactilar. Si los ajustes son más estrictos y el margen de error es menor, es

complicado engañar al escáner, pero a cambio es más probable que el dispositivo no reconozca a su propietario legítimo.

Cómo falsificaron las huellas dactilares

Para hacer una copia física de una huella dactilar, evidentemente necesitas conseguir una. El equipo de investigación halló tres maneras diferentes.

Cómo robar una huella dactilar. Método 1: elabora un molde

Es posible hacer un molde de la huella dactilar deseada cuando, por ejemplo, la víctima está inconsciente o indispuesta. Cualquier material suave que fije es adecuado; por ejemplo, la plastilina.

Un atacante podría entonces utilizar el molde para falsificar la yema de los dedos. La dificultad es evidente: el atacante necesita que la víctima esté en un lugar adecuado y que se encuentre accesible físicamente.

Cómo robar una huella dactilar. Método 2: apoderarse de una imagen del escáner

Otra forma de hacerse con una huella dactilar es mediante un escáner. Este método es más complicado en el aspecto técnico, pero la buena noticia para los ladrones de poca monta es que no todas las empresas que manejan datos biométricos los almacenan de forma fiable. Por tanto, no resulta imposible encontrar las huellas dactilares escaneadas de alguien o adquirirlas por un bajo precio en la *darknet*.

A continuación, la imagen bidimensional se tiene que convertir en un modelo 3D e imprimirse en una impresora 3D. En primer lugar, el programa con el que los investigadores crearon el dibujo no les permitió determinar su tamaño. En segundo lugar, el fotopolímero usado en una impresora 3D económica tuvo que calentarse después de imprimir, lo que alteró las dimensiones del modelo.

En tercer lugar, cuando los investigadores consiguieron crear un modelo adecuado, resultó que el polímero con el que estaba hecho era demasiado duro, por lo que no pudieron burlar ningún escáner. Para resolverlo, en lugar del modelo de un dedo, los investigadores decidieron imprimir un molde que posteriormente usaron para hacer una prótesis dactilar a partir de un material más elástico.

Cómo robar una huella dactilar. Método 3: haz una fotografía a una huella dactilar en una superficie de vidrio

Otra opción, y mucho más simple, es obtener una fotografía de la huella dactilar deseada marcada en una superficie de vidrio. Eso es exactamente lo que sucedió con el iPhone 5S. La imagen se procesa para lograr el nivel requerido de claridad y después, al igual que antes, se manda a una impresora 3D.

Según lo que señalan los investigadores, estos experimentos con la impresora 3D resultaron largos y tediosos. Tuvieron que calibrar la impresora y encontrar el molde del tamaño correcto mediante un método de prueba y error; además, la impresión efectiva de cada modelo (50 en total) con los ajustes requeridos tardaba un total de una hora. Por tanto, falsificar una huella dactilar para desbloquear un *smartphone* robado no es algo que se puede hacer rápidamente; tampoco es un método muy rápido copiar la huella dactilar de una víctima mientras duerme.

Fabricar un molde para falsificar la huella dactilar tan solo es la mitad del camino. La elección del material para el propio modelo resultó ser mucho más difícil, ya que la falsificación estaba destinada a probarse en tres tipos de sensores, cada uno con un método diferente de lectura de huellas dactilares. Por ejemplo, para los sensores ultrasónicos y ópticos, resulta irrelevante si el material puede conducir corriente, pero no para el de tipo capacitivo.

Sin embargo, sin ir más lejos, esta parte del proceso es accesible para todos: el mejor material para hacer impresiones falsas es un pegamento barato para telas.

Qué dispositivos se pudieron desbloquear con las huellas dactilares falsificadas

Los investigadores probaron sus falsificaciones en varios *smartphones*, *tablets* y portátiles de diversos fabricantes, así como en candados inteligentes y dos unidades USB protegidas con un sensor de huellas dactilares: Verbatim Fingerprint Secure y Lexar Jumpdrive Fingerprint F35.

Los resultados fueron desalentadores: se pudieron desbloquer la mayoría de los *smartphones* y *tablets* en un 80 % – 90 % de las veces; en algunos casos,

la tasa de éxito fue del 100 %. Los moldes de la impresora 3D eran los menos efectivos en la escala, pero la diferencia realmente no era mucha; los tres métodos descritos anteriormente en realidad funcionaron bien.

Sin embargo, hubo algunas excepciones. Por ejemplo, el equipo de investigación no pudo burlar por completo el *smartphone* Samsung A70, aunque vale la pena aclarar que el A70 es el más propenso a no reconocer a su verdadero propietario.

Los dispositivos con Windows 10 también resultaron impenetrables, independientemente del fabricante. Los investigadores atribuyen esta notable uniformidad al hecho de que el sistema operativo es el que compara la huella dactilar, así que no depende mucho del fabricante del dispositivo.

Por su parte, las unidades extraíbles protegidas resultaron dignas de ese nombre, pese a que nuestros colegas advirtieron que también pueden ser susceptibles a ataques más sofisticados.

Y, por último, aunque no por ello menos importante, los escáneres de huellas dactilares ultrasónicos fueron los más fáciles de burlar. A pesar de su capacidad para percibir una imagen 3D, leyeron las impresiones falsas como genuinas cuando un dedo real colocaba la falsificación sobre el sensor.

Protección mediante huellas dactilares para los usuarios comunes

De acuerdo con los investigadores, la seguridad de la autorización mediante huellas dactilares deja mucho que desear, e incluso hasta cierto punto su situación se ha deteriorado en comparación con años pasados.

Dicho esto, elaborar un dedo falso es un proceso un tanto costoso, al menos desde el punto de vista del tiempo requerido, lo que significa que el usuario común no tiene nada que temer. Pero es una historia muy diferente si te encuentras en el punto de mira de un grupo de delincuentes o de un servicio de inteligencia bien financiado. De ser así, lo mejor es que protejas todos tus dispositivos con una clásica contraseña que sea segura. Después de todo, desbloquear una contraseña fuerte es más difícil y siempre puedes cambiarla si sospechas que ha podido caído en manos equivocadas.

Los países más vulnerables

El informe de Microsoft identifica a **Ucrania como uno de los países más atacados** por ciberataques en el último año. Esto no es sorprendente, dado el conflicto en curso con Rusia y su posición geopolítica. Los **ataques cibernéticos dirigidos a Ucrania** han variado desde intrusiones destructivas hasta operaciones de espionaje y desinformación. Se ha observado un aumento en los ataques de *phishing* y el uso de vulnerabilidades de día cero en productos de Microsoft para atacar a organizaciones gubernamentales en Ucrania y en sectores clave de países de la OTAN. Además, se han registrado ataques destructivos con *ransomware*, como el caso de Prestige contra Polonia.

Por otro lado, **Israel, Corea del Sur y Taiwán** también figuran en la lista de los países más atacados. Israel, ubicado en una región geopolíticamente sensible, enfrenta amenazas constantes de ciberataques que van desde operaciones de influencia hasta intrusiones en sistemas críticos. Corea del Sur, conocida por su tecnología avanzada, se ha convertido en un objetivo constante para los ciberdelincuentes, y los ataques incluyen operaciones de espionaje y desinformación. Taiwán, en una situación geopolítica delicada, enfrenta ataques dirigidos a su infraestructura crítica y a la defensa, con un enfoque en la recopilación de información sensible.

PROBLEMÁTICA

La Policía Nacional del Perú (PNP) detuvo a tres individuos en el parque Kennedy de Miraflores, a quienes se les acusa de clonar huellas dactilares y acudían a los cajeros para sacar d*uplicados de tarjetas de diversos bancos.* Los detenidos serían miembros de una organización criminal conocida como 'Los Huelleros del Norte', que opera desde 2020.

Cada huella digital estaba hecha de goma —material que utiliza profesionales de la medicina— fue ubicada en los bolsillos y billeteras de los intervenidos, pero negaron su vinculación con esta modalidad de robo. De esta manera, ya estaban en la mira de sus próximas víctimas para vaciar sus cuentas bancarias.

"En el bolsillo izquierdo del señor se le está encontrando una silicona con un código", señaló la autoridad en el operativo, debido a que cada uno poseía estos materiales.

Las autoridades lograron incautar más de 500 impresiones de huellas digitales, cuatro POS, dinero en efectivo, tarjetas y cuentas bancarias. Asimismo, se conocerá si existen más implicados.

¿Cuál es el problema?

Las leyes de protección de datos personales son positivas, pues representan un límite al uso de la información personal realizada por entidades públicas y privadas. El problema es que estas normas suelen incorporar excepciones, casi siempre pensadas para no obstruir el trabajo que realizan ciertas entidades públicas como las que llevan el registro civil, pero que terminan siendo empleadas también por las fuerzas de seguridad del Estado, que suelen operar de forma poco transparente, y sobre las cuales es muy difícil ejercer control alguno.

En el Perú, algunos de los problemas asociados a esta política pública son:

Afectan el derecho a la privacidad de todas las personas porque el almacenamiento de sus datos personales se realiza sin su autorización y no existen disposiciones para oponerse o fiscalizar que el tratamiento se realiza con estándares de seguridad y necesidad.

¿Existen políticas públicas similares en la región y el mundo?

En la mayoría de países del mundo existen leyes de protección de datos personales, que son más o menos garantistas con el derecho de autodeterminación informativa. En ese sentido, queremos comparar el caso del Perú con el de otros países. Para ello vamos a tomar dos ejemplos:

a) Chile

Chile fue uno de los primeros países en implementar leyes de protección de datos. Su norma principal, la Ley N° 19.628 de 1999, disponía la necesidad de inscribir los bancos de datos personales a ser tratados y exigir autorización de sus titulares. De forma similar que la norma peruana, la ley chilena contempla dos excepciones: Cuando la información se trata con fines de "Seguridad Nacional" o en "Interés de la Nación". Hasta hace muy poco, Chile no contaba con una autoridad encargada de vigilar directamente el cumplimiento de esta norma y analizar los casos en disputa, pero desde 2018 se han encargado estas funciones a su Autoridad de Transparencia.

b) Unión Europea

A partir de 2016, entró en vigencia la política europea para la protección de datos: El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), una norma que obliga a todas las empresas que tratan datos personales en países europeos o de ciudadanos europeos a obtener siempre autorización expresa de sus titulares. Además de los derechos ARCO, incorpora también otros derechos como el "derecho al olvido" (desindexación o eliminación de contenidos caducos o inexactos) y el derecho a la portabilidad de los datos personales. Así mismo, incorpora obligaciones nuevas para las entidades privadas, como que estas deben informar si han sufrido incidentes de seguridad. No obstante, igual que en Perú, persisten las excepciones destinadas a permitir el funcionamiento de entidades de registro y de las fuerzas públicas.

Tendencias de los ciberataques a nivel internacional

El informe de Microsoft revela tendencias alarmantes en la evolución de los ciberataques a nivel internacional, con un enfoque en cuatro países en particular: **Rusia, China, Irán y Corea del Norte**.

Rusia

Rusia ha continuado llevando a cabo **ciberataques destructivos en Ucrania**, pero también ha ampliado sus esfuerzos en **actividades de espionaje**. Esto incluye operaciones de influencia destinadas a socavar a las comunidades anfitrionas contra los refugiados de la guerra, especialmente en Polonia y los estados bálticos. Además, se han registrado constantes **campañas de *phishing* contra Ucrania** y los miembros de la OTAN. Rusia también ha utilizado actores estatales rusos que se hacen pasar por diplomáticos occidentales y funcionarios ucranianos para obtener acceso a cuentas e información sensible.

El informe destaca el uso de **vulnerabilidades de día cero** en productos de Microsoft, como Outlook, para atacar a organizaciones gubernamentales en Ucrania y en sectores críticos de países de la OTAN. Además, se han lanzado ataques destructivos con **ransomware**, como el caso de Prestige contra Polonia.

China

China, por otro lado, ha mantenido su enfoque en el espionaje, pero también ha comenzado a prepararse para posibles ataques destructivos en infraestructuras críticas. Ha dirigido operaciones de influencia contra comunidades de habla china en todo el mundo y ha intensificado los ataques contra objetivos militares de Estados Unidos.

Se ha observado que China comprometió dispositivos Fortinet para obtener un amplio acceso a sistemas militares estadounidenses. «Estas campañas pueden
destinadas a proporcionar a China la capacidad de interrumpir la infraestructura crítica y la comunicación entre Estados Unidos y Asia durante una crisis geopolítica», se señala el informe de Microsoft (p. 61).

Además, China ha intensificado sus ataques de espionaje en países del Mar del Sur, incluyendo a Taiwán y naciones del sudeste asiático. Al mismo tiempo, ha dirigido ataques contra países considerados como socios, como Malasia, Indonesia y Kazajstán.

Irán

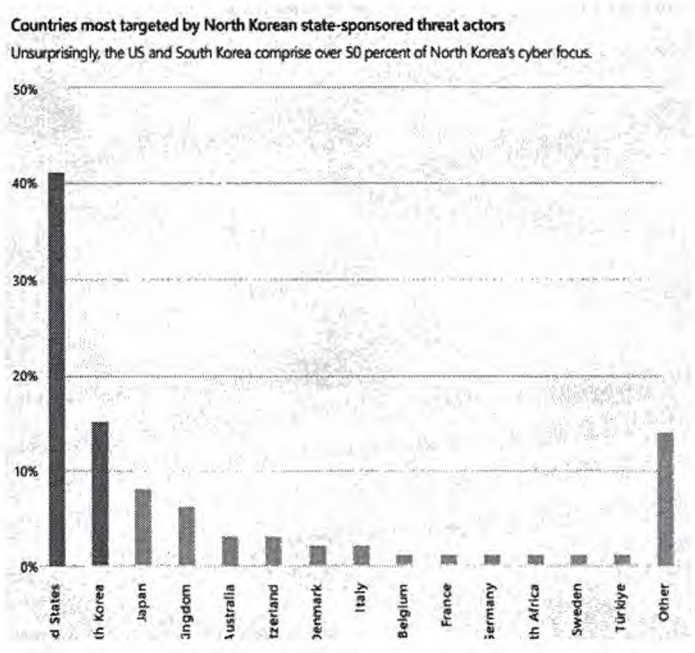
Irán ha mejorado significativamente sus capacidades cibernéticas, moviéndose de intrusiones en sistemas locales a **sistemas basados en la nube**. Han utilizado nuevas herramientas personalizadas para obtener acceso más amplio y duradero a los sistemas de sus rivales geopolíticos.

Además, Irán ha mostrado una mayor inclinación por los **ciberataques destructivos**, como los observados en Albania el año pasado. Han ampliado sus redes de desinformación para contrarrestar protestas recientes y fomentar disturbios en países del Golfo. Por otro lado, han expandido su superficie de ataque de espionaje a países en **América Latina, África y Asia** y han coordinado más **operaciones cibernéticas con Rusia**. Se ha observado también un aumento en la explotación de herramientas de monitoreo y gestión remota para mantener el acceso a entornos comprometidos.

Corea del Norte

Corea del Norte ha continuado robando millones de dólares en **criptomonedas** y ha evolucionado significativamente sus capacidades cibernéticas para llevar a cabo formas de ataques previamente invisibles. En enero de 2023, la Oficina Federal de Investigación (FBI) atribuyó públicamente el robo de 100 millones de dólares en criptomoneda del Horizon Bridge de Harmony a ciberactores norcoreanos.

Se ha observado que utilizaron un ataque de cadena de suministro para habilitar otro compromiso de cadena de suministro, un enfoque sin precedentes en la ciberseguridad. Además, han expandido sus objetivos para incluir organizaciones en el sector marítimo y de construcción naval. Se ha informado que los hackers norcoreanos también han comprometido empresas de defensa en **Brasil, República Checa, Finlandia, Italia, Noruega y Polonia**. Al mismo tiempo, han dirigido ataques contra aliados como **Rusia**, específicamente en la energía nuclear, la industria de defensa y entidades gubernamentales, lo que sugiere una posible recopilación de inteligencia.



Países más afectados por las amenazas de Corea del Norte. Créditos: Microsoft Threat Intelligence events data

El camino hacia la defensa colectiva

A pesar de las preocupantes tendencias en la ciberseguridad global, el Informe de Defensa Digital de Microsoft también señala avances tecnológicos y la formación de alianzas internacionales como parte de la defensa colectiva contra los ciberataques.

En un mundo cada vez más interconectado, la cooperación entre naciones y empresas se vuelve esencial para proteger la seguridad y la privacidad en línea. La defensa colectiva, la cooperación internacional y la mejora de la ciberseguridad se presentan como elementos clave en la protección de nuestras sociedades en línea en este mundo cada vez más digitalizado y conectado.

Mirando hacia el futuro, **Tom Burt**, vicepresidente corporativo de seguridad y confianza del cliente de Microsoft, destaca que «la inteligencia artificial será un componente crítico para el éxito de la defensa», aclarando que «en los próximos años, la innovación en **ciberdefensa impulsada por IA** ayudará a revertir la actual marea creciente de ciberataques».

Fuente: https://cuadernosdeseguridad.com/2023/10/ciberseguridad-en-el-mundo/#:~:text=El%20Informe%20de%20Defensa%20Digital,digital%20cada%20vez%20m%C3%A1s%20complejo.

infobae

PERÚ

Cae banda que clonaba huellas dactilares para vaciar cuentas bancarias: así operaba red

El coronel PNP José Manuel Cruz Chamba, jefe de la División de Investigación de Estafas y Otras Defraudaciones, detalló que comenzó operando en Trujillo

Por Clara Geraldo

22 Jun 2024 01:01 p.m. PE

Cae banda que robaba cuentas con huellas dactilares: delincuentes ...

PUBLICIDAD

Así operaba la organización criminal:

La División de Investigación de Estafas y Otras Defraudaciones de la Dirincri informó que esta banda criminal empleaba avanzadas tecnologías de clonación y mecanismos sofisticados para copiar las huellas digitales de sus víctimas y usar tarjetas clonadas con ellas. El objetivo era vaciar completamente las cuentas bancarias de los afectados.

El coronel PNP José Manuel Cruz Chamba, jefe de la División de Investigación de Estafas y Otras Defraudaciones, detalló que todo comienza cuando identifican a su víctima al recoger un voucher que las personas obtienen al realizar cualquier transferencia.

Funcionarios darían información

En el marco de esta investigación, se presume que los involucrados podrían tener acceso a información sensible desde algún punto dentro del sistema de almacenamiento de datos. La PNP señala que los datos son los que se encuentran en el Registro Nacional de Identificación y Estado Civil (Reniec), por lo cual se investiga si existe un mal funcionario dentro de la institución.

La magnitud de las transferencias identificadas en la operación refuerza la teoría de un posible fraude a gran escala. Esta sospecha surge luego de una reciente intervención donde se encontraron 50 comprobantes de retiro con montos que superan los S/ 150 mil solo en un día.

"Vienen operando desde el 2020 aproximadamente. Estamos estimando un aproximado de más de S/5 millones.", agregó en referencia de los últimos 4 años.

La Policía Nacional del Perú (PNP) ha señalado que esta banda organizada comenzó su operación en la ciudad de Trujillo, y con el tiempo, ha extendido su influencia y actividades a otras regiones del país. Las autoridades están llevando a cabo investigaciones para desarticular la organización y frenar sus actividades delictivas, la cual estaría integrada por siete personas.

Recomendaciones y prevención

Pablo García, gerente de Ciberseguridad en TIVIT, brindó algunas recomendaciones para prevenir esta modalidad.

- Limpieza regular de dispositivos: García recomienda limpiar frecuentemente las superficies de teléfonos, tabletas y computadoras para evitar la clonación de huellas digitales. Sugiere usar paños de microfibra y soluciones adecuadas.

- Autenticación multifactorial: aconseja activar la autenticación multifactor (MFA) en cuentas bancarias y servicios sensibles para añadir una capa extra de seguridad.

- Contraseñas robustas: destaca la importancia de usar contraseñas complejas y únicas para cada cuenta, cambiándolas regularmente y evitando datos personales identificables como nombres o fechas de nacimiento.

Q | ÚLTIMAS NOTICIAS POLÍTICA VIDEOS PERÚ LIMA ECONOMÍA INVESTIGACIÓN

Perú21

Lo Último AFP | Copa América Eurocopa #Sostenibilidad21 #Biodiversidad #DileNOalGotaa

Alertan sobre clonación de huellas dactilares

Banda 'robó' identidad de ciudadanos con buen historial crediticio y compró celulares de alta gama.

Suplantar la identidad de un ciudadano con un buen historial crediticio se convirtió en el negocio perfecto para una banda de delincuentes. Estos, aunque antes habría parecido imposible, clonaban las huellas dactilares de distintas personas para 'robarles' su identidad y, así, adquirir celulares de alta gama.
Esta organización criminal clonó las huellas dactilares de al menos 35 ciudadanos y **suplantó a 27** de estos para adquirir modernos equipos valorizados en más de **S/100 mil**. Los lectores biométricos de distintas empresas de telefonía no detectaron ningún problema al momento de verificar las identidades.

El coronel Edgardo Oré, jefe de la División de Investigación Criminal de Lima Sur de la Dirincri, señaló a Perú21 que "en su momento se creía que el sistema biométrico era una de las mejores garantías de seguridad de identidad para

evitar suplantaciones en compras, transacciones bancarias, trámites notariales, pero cada día se comprueba que es más vulnerable".
¿Cómo lo hacían? Los hampones, que tenían acceso a bases de datos de clientes bancarios, seleccionaban a ciudadanos con un buen historial crediticio, es decir, que no figuraran en Infocorp.
Luego de elegir a la víctima, obtenían su ficha original del Reniec, en la que aparecía su huella dactilar. Esta era escaneada en una impresora 3D (que capta las crestas papilares) y dicha imagen la plasmaban en una lámina de silicona del tamaño del dedo índice.

ROBO DE IDENTIDAD

Paralelamente, en Azángaro, obtenían el DNI falso de la víctima, al que colocaban la fotografía del delincuente que iba a hacer la suplantación. Así, este último se colocaba la huella dactilar clonada y se presentaba en la tienda de telefonía.

En los 27 casos antes mencionados, los maleantes adquirieron celulares de precios mayores a los S/2,800, sin efectuar ni un solo pago, pues supuestamente se trataba de excelentes clientes que podían renovar sus equipos. De esta manera, cualquier ciudadano podía resultar con una deuda que nunca buscó.

La banda delincuencial fue descubierta luego de la captura de **Nancy Huayta Salazar de Suárez (29),** el 6 de marzo en el centro comercial Mall del Sur en San Juan de Miraflores. La Policía la detuvo cuando iba a suplantar a una ciudadana.
Luego cayeron su enamorado **Víctor Páucar Elías (26)** –presunto cabecilla– , **Manuel Zela Huarcaya (26)**, **Jonathan Tunjar Rodríguez (26)** y **Junior Quiroz Rosales (41)**. El último es un ex trabajador de una empresa de telefonía que tenía información clasificada.

SABÍAQUE

-La Policía incautó a esta banda un aparato biométrico, 8 DNI falsos y 17 láminas de silicona con huellas dactilares.
-Cabe recordar que la primera vez que se puso al descubierto esta modalidad fue en 2015, durante los exámenes de admisión a universidades. En esa ocasión, clonaron huellas dactilares para suplantar a los postulantes.

Alertan sobre clonación de huellas dactilares

Banda 'robó' identidad de ciudadanos con buen historial crediticio y compró celulares de alta gama.

Fuente: https://peru21.pe/lima/alertan-clonacion-huellas-dactilares-466129-noticia/?foto=2

DIVERSOS MEDIOS DE COMUNICACIÓN INFORMARON SOBRE LA CLONACIÓN DE HUELLAS DACTILARES ENTRE ELLOS EL DOMINICAL (AL ESTAR EXPUESTAS EN L DNI DE LOS CIUDADANOS).

DOMINGO AL DIA DE AMERICA TELEVISIÓN QUE RATIFICA EL MODUS OPERANDI DE DIVERSAS BANDAS DELICTIVAS

Delincuentes elaboraban huellas digitales con silicona para clonar tarjetas. Los sujetos habrían sustraído más de 200 mil soles con este

modus operandi. La banda conocida como "Los Cibernéticos de las Tarjetas de Crédito" fueron capturados por la Policía.

Encuentra el informe del programa AQUÍ ► https://bit.ly/3GlnqrD

Mira el programa completo de **#DomingoAlDía** en **América TV**► https://bit.ly/dadfbtvgo

GRAFICAS:

#DomingoalDía Elaboraban huellas digitales con silicona para clonar tar...

#DomingoalDía Elaboraban huellas digitales con silicona para clonar tar...

#DomingoalDía Elaboraban huellas digitales con silicona para clonar tar...

#DomingoalDía Elaboraban huellas digitales con silicona para clonar tar...

#DomingoalDía Elaboraban huellas digitales con silicona para clonar tar...

ojo

POLICÍA ALERTA

EN LO QUE VA DEL AÑO, SE HAN DETENIDO A 251 ESTAFADORES

CLONACIÓN DE TARJETAS Y SUPLANTACIÓN DE IDENTIDAD SON MODALIDADES MÁS USADAS PARA ROBAR DINERO

AUMENTAN ESTAFAS

EL FRAUDE INFORMÁTICO, EL VAUCHER FALSO Y LA VENTA DE AUTOS POR INTERNET SON OTRAS FORMAS DE ENGAÑO

LIMA, CALLAO, UCAYALI, CUSCO Y LAMBAYEQUE SON LAS REGIONES CON MAYOR INCIDENCIA DE ESTE DELITO

SOLO UN MILAGRO SALVARÁ A PERÚ

"CHARITO" DEJA "AL FONDO HAY SITIO"

RESPIRAMOS AGUA

15 JUEGOS

Diario: Ojo del miércoles 26 de junio del 2024

CLONAN TARJETAS Y ENGAÑAN CON VAUCHERS Y MALETAS

Alertan por aumento de estafas

AL GRANO

PRESENTAN "SUITE ECOLÓGICA PERÚ-ESTILO NATURAL"

RENATO TAPIA ANUNCIA FINAL DE SU MATRIMONIO

CAPACITARÁN A BOMBEROS EN

Diario: Ojo del miércoles 26 de junio del 2024

II.- ANTECEDENTES LEGALES Y CONCORDANTES

- Constitución Política del Perú: en su artículo 2, numeral 6, articulo 10 y 24.
- Ley 29733, Ley de Protección de Datos Personales.

ANALISIS COSTO BENEFICIO

El presente proyecto de ley es una norma positiva en beneficio para toda la Sociedad, la misma que impactará en la economía del ciudadano que en la actualidad se encuentra amenazada por las organizaciones criminales

A modo de resumen, el presente proyecto de ley, responde de manera urgente a las grandes demandas de la ciudadanía que clama seguridad y ciberseguridad, mas aun que en este mundo globalizado donde existe avances progresivos de la ciencia y tecnología.

EFECTO DE LA VIGENCIA DE LA NORMA QUE SE PROPONE SOBRE LA LEGISLACION NACIONAL

La presente iniciativa está conforme a la Constitución Política del país, concordante con las normas que en su articulado establece los principios como el de igualdad de oportunidades y de no discriminación, reconociendo y garantizando además el derecho fundamental de todos los peruanos a la seguridad ciudadana y ciberseguridad.