SMARTPHONES: PUERTA DE ACCESO A LOS DATOS CORPORATIVOS

RESUMEN

El ingreso de los dispositivos móviles y posteriormente, de los teléfonos inteligentes al mercado, produjo un cambio radical en el comportamiento de la sociedad. Si bien es cierto, este avance tecnológico ha permitido a millones de personas estar conectadas con otras, independiente de la distancia, la irrupción de estos dispositivos en la vida cotidiana, tanto de las personas como también en la funcionalidad y operatividad de las organizaciones, ha incrementado no solo problemas de comportamiento de las personas, algo que es ya objeto de análisis de la psicología (Nomophobia[1]), sino que también ha abierto insospechadas brechas para la privacidad de los individuos y para la seguridad de la información de las corporaciones y/u organizaciones. En este artículo, se analizarán algunas de las amenazas a las que están expuestas las personas y las organizaciones que cuentan con *smartphones* sin aplicar sobre éstos medidas de protección y el efecto que puede producir la pérdida de datos.

CHRISTIAN MAHN VILICICH
Capitán de Fragata
Magister en Ciencias de la Ingeniería Informática,
Universidad Técnica Federico Santa María.
(cmahn@armada.cl).

Tecnología, smartphone, hacker, ciberespacio, malware

La comunicación es una de las bases para la relación entre los distintos seres vivos, es por esto que el ser humano, desde sus inicios, ha buscado formas y medios para comunicarse con otros individuos. Debido a la limitación que imponen tanto el volumen de la voz y la audición, el hombre ha ideado en el tiempo distintas alternativas de comunicación que le permitan traspasar información a distancia. En un principio, ideó soluciones rudimentarias, tales como señales luminosas con fuego o señales de humo, pero luego, apoyado con el entendimiento de los efectos de la física y de la electrónica, ha logrado interacciones muchísimo más avanzadas, desde la comunicación telegráfica, hasta llegar a las más modernas formas de comunicación vía dispositivos electrónicos, utilizando como medio de enlace, entre otros, radiofrecuencias o fibra óptica

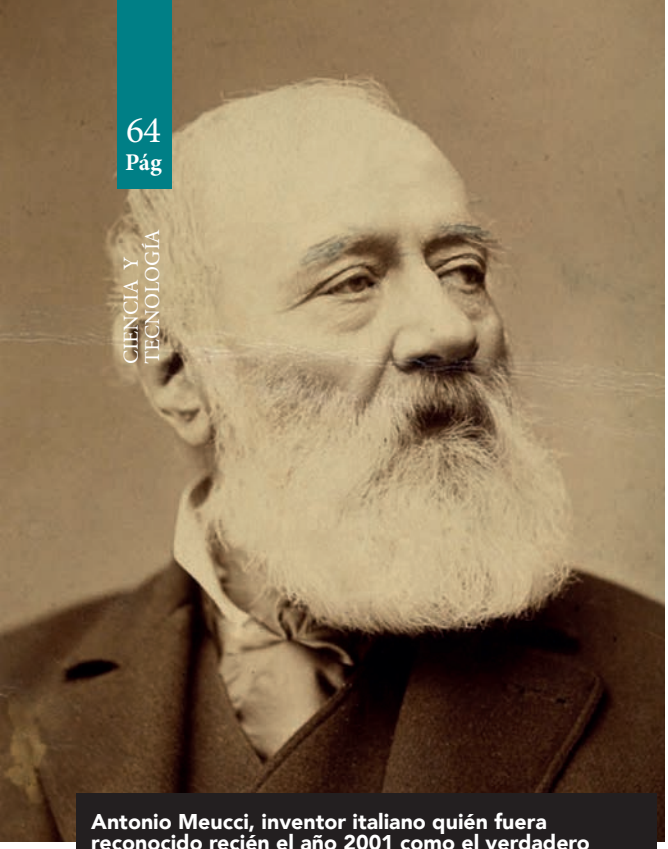
Con la creación de la red militar ARPANET el año 1969, red que posteriormente se convirtió en lo que hoy conocemos como INTERNET, nació un nuevo ambiente por el cual se interconectan y conviven miles de millones de dispositivos, el Ciberespacio. Por este sistema de sistemas, interaccionan millones de personas a lo largo del orbe y circulan millones de *terabytes* de datos, facilitando el acceso y traspaso de información, sin importar el lugar o la distancia, contribuyendo con esto no sólo al acceso del conocimiento, sino que también al avance tecnológico de países en vías de desarrollo. Es tal la importancia que tiene este medio, que tanto las personas como las organizaciones han debido adaptar no sólo los medios físicos con los que antiguamente funcionaban, sino que también han debido modificar su forma de interactuar con personas y con máquinas, es decir, su cultura. A este cambio cultural que involucra un proceso de digitalización, se le denomina actualmente como la transformación digital.[2]

La llegada de la era digital, periodo en que casi todo está conectado, ha supuesto un enorme desafío a gobiernos, organizaciones y a las personas en general, puesto que al existir una enorme cantidad de datos, información y conocimiento circulando libre y abiertamente por la red, se ha suscitado el interés de muchos inescrupulosos altamente capacitados en el área informática, más conocidos como *hackers*, quienes han buscado sacar provecho de esta situación, cometiendo delitos tales como fraudes, espionaje, sabotaje y robo de información, hurtando datos de personas y/u organizaciones, suplantando identidades, filtrando información sensible, en síntesis, produciendo daños que se cuentan en miles de millones de dólares sólo en Latinoamérica.[3]

Por otra parte, el ciberespacio es ahora reconocido y aceptado como el quinto vector o escenario de la guerra moderna (los otros cuatro son aire, mar, tierra y espacio), por lo que diversos estados cuentan con verdaderos ejércitos entrenados para atacar objetivos de valor de acuerdo con sus intereses o bien, con el propósito de defenderse de posibles ataques de otros países.[4]

La irrupción masiva del teléfono móvil a principios de la década de 1990 produjo un cambio radical en la forma de comunicación entre las personas, al otorgar movilidad al teléfono, dispositivo inventado por Antonio Meucci a mediados del siglo XIX.[5] Sin embargo, no fue hasta la aparición de los teléfonos inteligentes (*smartphones*) que estos dispositivos lograron tener un rol fundamental en la transformación digital como también en el ciberespacio.

1. PSYCHOLOGY TODAY. Nomophobia: A rising trend in students. [Consultado el 25 de octubre de 2018]. Disponible en https://www.psychologytoday.com/us/blog/artificial-maturity/201409/nomophobia-rising-trend-in-students
2. POWER DATA. Transformación digital. Qué es y su importancia en relación con los datos. [Consultado 25 de octubre de 2018]. Disponible en https://www.powerdata.es/transformacion-digital
3. INVERSOR, Latam. Ciberseguridad, América Latina en la mira de los ataques. [Consultado 22 de octubre de 2018]. Disponible en http://inversorlatam.com/ciberseguridad-america-latina-en-la-mira-de-los-ataques/.
4. BARRÍA HUIDOBRO, Cristian. Ciberespacio: protección a la infraestructura crítica de la información. Revista Escenarios Actuales, Centro de estudios e investigaciones militares del Ejército de Chile. N°2, Agosto 2016, pp 17-26.
5. CONGRESS.GOV. Resolución 269 House of Representatives, U.S. Government Printing Office. 17 de octubre de 2001. [Consultado el 22 de octubre de 2018]. Disponible en https://www.congress.gov/bill/107th-congress/house-resolution/269/text



Antonio Meucci, inventor italiano quién fuera reconocido recién el año 2001 como el verdadero inventor del teléfono.

En este artículo se analizará la fuerte presencia que tienen los teléfonos inteligentes en la sociedad y cómo, en caso de no aplicar un control integral sobre estos dispositivos, las gobiernos, organizaciones y personas se ven totalmente expuestas al robo de información de datos personales o a ciberataques, tanto por parte de los anteriormente mencionados hackers o bien, por parte de ciber ejércitos. Por otro lado, se analizarán también, los efectos que puede tener la filtración o fuga de datos a través de los teléfonos inteligentes, tales como: comprometer la vida personal, la continuidad operacional de las organizaciones o incluso, la seguridad del país (en el caso de funcionarios de las fuerzas armadas o de gobierno).

El teléfono inteligente (*smartphone*)

Hace solo unas cuantas décadas era impensado contar con un computador personal en el hogar o un teléfono que fuera transportable, debido a las limitaciones tecnológicas que no solo implicaban que estos elementos fueran de enorme tamaño o de gran peso para el caso de los computadores o bien, que estuvieran limitados a la conexión por cable y a la posición física, en el caso de los teléfonos. En la actualidad, gracias a los avances en la composición de los circuitos integrados y de otros elementos de nano tecnología, contamos con dispositivos de gran capacidad que son a la vez de reducido tamaño y bastante ligeros.

El desarrollo de circuitos integrados (chip o microchip) por parte del ingeniero estadounidense Jack S. Kilby[6] a fines de la década de los '50 del siglo XX, significó un enorme avance para la tecnología, particularmente porque permitió reducir el tamaño de los diferentes equipos electrónicos, otorgándoles a estos la capacidad de ser portátiles, algo que sería esencial en el tiempo para dar movilidad a los usuarios.

El contar con la capacidad de reducir el tamaño de los equipos permitió posteriormente, a los célebres Steve Woszniak y Steve Jobs, desarrollar el primercomputador personal que fuera distribuido en forma masiva, naciendo de esa forma el Apple II.[7] El ingreso de este aparato computacional al mercado fue trascendental para la transformación digital, ya que en un mundo donde los usuarios eran, generalmente, ingenieros o matemáticos con altos conocimientos en el área, con el tiempo pasarían a ser personas comunes y corrientes con poca experiencia computacional. Esto último fue lo que llevó a la sociedad en general, a digitalizarse.

6. THOUGHCO. Jack Kilby, father of the Microchip. [Consultado el 23 de octubre de 2018]. Disponible en https://www.thoughtco.com/jack-kilby-father-of-the-microchip-1992042
7. HIPERTEXTUAL. Apple II, la historia de los dos Steve. [Consultado el 23 de octubre de 2018]. Disponible en https://hipertextual.com/2016/04/apple-ii-la-historia-los-dos-steve.

Computador Apple II, primer computador personal de venta masiva, desarrollado por Steve Jobs y Steve Woszniak el año 1977

Con la sociedad digitalizada, la industria comenzó a buscar nuevos productos que combinaran las capacidades del computador personal con la movilidad, siempre con la visión de irrumpir en el mercado con dispositivos modernos que cambiaran la vida de las personas, fue así como nació el *Notebook* y posteriormente, el *Tablet*.

Mientras los circuitos integrados permitían a la tecnología computacional avanzar a pasos agigantados, también permitieron en paralelo la transformación de otro elemento tecnológico, el teléfono.

Pocos podrían dudar que el teléfono es uno de los mayores y mejores inventos creados por el hombre en los últimos siglos, ya que ha sido una herramienta vital para la comunicación de los seres humanos, aunque en sus inicios haya estado limitado a la conexión por cables y a su posición estática. En el año 1973, Martin Cooper y la empresa Motorola dieron vida a un dispositivo que cambiaría literalmente la forma en que nos comunicamos, el teléfono móvil.[8] La irrupción del teléfono móvil cambió el comportamiento del ser humano, a tal nivel, que incluso en la actualidad existe una condición patológica llamada *Nomophobia*, que consiste en la dependencia absoluta del teléfono móvil, que lleva a las personas a sentir una profunda desesperación al estar sin ellos.

El primer teléfono móvil desarrollado por Motorola y los siguientes que salieron al mercado, fueron en un comienzo excesivamente costosos, por lo que no cualquier persona podía acceder a ellos. Con el tiempo y gracias a la reducción del costo, entre otros factores, este aparato se masificó a la población, existiendo en la actualidad más teléfonos móviles que seres humanos.[9]

La existencia de variados dispositivos en el mercado y la facilidad de acceso a éstos, permitió que las personas pudieran contar con varios al mismo tiempo, sin embargo, esto desencadenó la incomodidad de los usuarios al desplazarse cargados de estos aparatos, razón por la cual los desarrolladores de tecnología se abocaron en la misión de intentar integrar las distintas capacidades tecnológicas disponibles en un solo dispositivo.

8. WIKIPEDIA, la enciclopedia libre. Teléfono móvil. [Consultado 23 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Tel%C3%Agfono_m%C3%B3vil
9. OTI, En el mundo hay más teléfonos celulares que humanos. Organización de Telecomunicaciones de Iberoamérica [Consultado 23 de octubre de 2018]. Disponible en https://www.otitelecom.org/telecomunicaciones/mundo-mas-celulares-humanos/

Martin Cooper, creador del primer teléfono móvil marca Motorola el año 1973.

Por una parte, las operadoras de telefonía integraron a sus redes la capacidad de transferencia de datos (EDGE, GSM, 3G, 4G etc.) y a los *tablet* se les agregó la posibilidad (que en varios casos aún mantienen) de funcionar como teléfono. Sin embargo, en la práctica, resultó bastante incómodo el utilizar un *tablet* como teléfono, debido a su tamaño, por lo que se optó por desarrollar equipos telefónicos que integraran capacidades similares a las de los *tablets*, naciendo así el concepto de teléfono inteligente o *smartphone*.[10]

En la actualidad, la gran mayoría de los teléfonos inteligentes tienen capacidades equivalentes e incluso superiores a las de algunos computadores disponibles en el mercado, contando, por ejemplo; con conexión a internet de alta velocidad, permitiendo el acceso a redes sociales, correos electrónicos, páginas web, juegos en línea etc., además, poseen cámaras que permiten obtener fotografías de alta gama. Estas y otras características, han transformado al teléfono inteligente en un elemento altamente funcional y de vital importancia para las actividades laborales y personales.

No obstante, al conectar el teléfono al ciberespacio, se abrió la puerta para que éste estuviese expuesto a acciones maliciosas, siendo especialmente atractivo para los ciber delincuentes, debido a que en general, se aplican muy pocas medidas de seguridad sobre éstos y además contienen una gran cantidad de información relevante.

Actualmente, la gran mayoría de las personas conecta sus teléfonos inteligentes a los computadores, sean estos personales o corporativos, ya sea con el fin de respaldar información (correos, fotos, notas, etc.) o bien, para obtener acceso a internet al utilizar al dispositivo como *router*.[11] Con esta acción, exponen no solo la información almacenada en los mencionados computadores, sino también a toda la organización, en el caso de que el ordenador sea corporativo y esté conectado a una red, la cual puede ser la puerta de acceso utilizada por los *hackers* para obtener información corporativa.

10. WIKIPEDIA, la enciclopedia libre. Teléfono Inteligente. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Tel%C3%Agfono_inteligente
11. WIKIPEDIA, la enciclopedia libre. Router: Dispositivo que proporciona conectividad a nivel de Red. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Router

Malware

Antes de describir qué es el *malware* y la posible acción de éste en los teléfonos inteligentes, es necesario mencionar algunos conceptos básicos de informática que son esenciales para el análisis.

Una computadora está compuesta de dos partes principales: el *hardware*, que es el término genérico utilizado para definir los elementos físicos que la componen (procesador, disco duro, tarjeta de video, placa madre, memoria RAM etc.) y el *software*, que consiste en el conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar ciertas tareas[12] (para este artículo, el *firmware* será considerado como parte del *software*).

Para un teléfono inteligente, es totalmente aplicable lo recientemente descrito, siendo el teléfono físico y sus componentes el *hardware* y el sistema operativo y las distintas aplicaciones el *software*.

El *software* está compuesto por una serie de líneas de texto, llamadas código fuente, que indican los pasos que debe seguir una computadora para ejecutar determinadas acciones.[13] En forma simple, este código es una serie de enunciados escritos en lenguaje humano que la máquina entiende y ejecuta.

En jerga informática, existen dos formas de ver el código; la primera es abierto, lo que significa que cualquier persona puede tener acceso al texto e incluso modificarlo y la segunda es cerrado, en cuyo caso solo el desarrollador del código puede acceder a éste y modificarlo. El código fuente es clave para la ciberseguridad y para los *hacker*, ya que es acá donde generalmente se buscan las vulnerabilidades para poder atacar un sistema informático.[14]

Volviendo al s*oftware*, existen dos tipos de éste: el *software* de sistema (Sistema Operativo, por ejemplo), el cual está orientado particularmente hacia el funcionamiento del computador y en el cual, el usuario en general no tiene mayor injerencia (usuarios avanzados tienen la capacidad de efectuar modificaciones a este tipo de *software*, en especial cuando se trata de *software* de código abierto) y el *software* de splicación, el cual está orientado a la ejecución de tareas por parte de los usuarios (*Office*, *Adobe*, *Paint*, etc.).[15]

12. REAL ACADEMIA ESPAÑOLA. [Consultado el 25 de octubre de 2018] Significado de la palabra "Software". Disponible en http://dle.rae.es/?id=YErlG2H.
13. WIKIPEDIA, la enciclopedia libre. Código Fuente. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/C%C3%B3digo_fuente
14. THE LINUX INFORMATIÓN PROJECT. Source Code Definition. [Consultado el 25 de octubre de 2018]. Disponible en http://www.linfo.org/source_code.html
15. TECNOLOGIA & INFORMATICA ¿Qué es Hardware y Software? [Consultado el 25 de octubre de 2018]. Disponible en https://tecnologia-informatica.com/que-es-hardware-y-software/

El *malware* (Acrónimo de *Malicious Software* en inglés), por definición, es un tipo de *software*, en general de aplicación, desarrollado con el objetivo de atacar a dispositivos informáticos (pueden ser entre otros: computadores, *notebooks*, *tablets*, servidores y teléfonos inteligentes) sin que el propietario lo note.[16] Existen de diversos tipos (virus, troyano, gusano, *spyware*, *ransomware*, etc.), estando en general orientados a espionaje, robo de datos (información), alteración o destrucción de la integridad de los datos (sabotaje) y extorsión o ciber-chantaje.

Debido a que los ciberataques utilizando *malware* han resultado increíblemente eficientes y lucrativos, combatirlos no solo ha significado un inmenso desafío y esfuerzo por parte de empresas desarrolladoras de *hardware* y *software* para la protección de los sistemas, sino que también ha significado que este problema se haya transformado en una prioridad para resguardar la seguridad de la información personal, organizacional o gubernamental, es por esto que es de vital importancia concientizar a las personas respecto de esta amenaza, considerando que el factor humano es sin lugar a dudas el eslabón más débil.

Acciones maliciosas sobre los teléfonos inteligentes

Con la irrupción del teléfono inteligente en el mercado, nacen personas (informáticos) y empresas desarrolladoras de *software* específicos para éstos, pudiendo ser sistemas operativos o aplicaciones que no son más que *software* de sistema o de aplicación, orientado al usuario y cuyas funciones van desde ser una interfaz hombre máquina atractiva (Sistemas operativos como el IOS de Apple, Android, BlackBerry OS, etc.) hasta una interfaz orientada a entretener (juegos). Actualmente, esta industria es enorme y desarrolla todo tipo de aplicaciones.

Al masificarse el teléfono móvil (o teléfono celular) en la sociedad, nació un tipo de delincuente que, utilizando conocimientos en electrónica y aplicando ingeniería inversa sobre los dispositivos (consiste básicamente en desarmar un dispositivo o elemento y en base al análisis de sus componentes comprender su funcionamiento), puede sacar provecho de las vulnerabilidades de éstos, cometiendo acciones principalmente orientadas a la interceptación de llamadas o bien al fraude

16. SYMANTEC CORPORATION [US]. Malware. Norton. [Consultado el 25 de octubre de 2018]. Disponible en https://us.norton.com/internetsecurity-malware.html

(burlando a las compañías telefónicas y no pagando las llamadas, por ejemplo). A este tipo de acciones se les conoce como *Phreaking* (conjunción de las palabras en inglés *Phone,* teléfono y *Freak,* monstruo).[17] Con el avance de la tecnología y la irrupción del teléfono inteligente, el *phreaking* no sólo ha consistido en vulnerar el *hardware* de los dispositivos, sino que, además, los delincuentes con conocimientos informáticos se han centrado en vulnerar el *software* de éstos.

Uno de los métodos más comunes utilizados en la actualidad por los cibercriminales para vulnerar un dispositivo inteligente, consiste en desarrollar aplicaciones que parezcan atractivas a los usuarios, las cuales son dejadas en forma disponible para ser descargadas desde sitios abiertos, como Google Play por ejemplo, sitio desde donde se bajan aplicaciones para teléfonos inteligentes que utilizan el sistema operativo Android.[18] La persona, al instalar la aplicación, automáticamente infecta el dispositivo, comprometiendo todos los datos almacenados en éstos.

Considerando que, prácticamente todos los teléfonos inteligentes cuentan actualmente con la capacidad de recibir correos electrónicos (personales o corporativos), precisamente es por este medio que los cibercriminales intentan engañar (utilizando ingeniería social[19]) a las personas, enviándoles correos que aparentan ser inofensivos pero que pueden contener enlaces a sitios infectados con malware, procedimiento que es conocido como *phishing*.[20]

Como ya se mencionó, un teléfono infectado no sólo compromete los datos que se encuentran almacenados en el dispositivo, sino que también, en caso de que éste sea conectado a una red que no cuente con sistemas de seguridad que impidan la conexión de estos dispositivos a los computadores (vía USB, por ejemplo), se compromete en general a toda la red, ya que es altamente probable que la persona efectúe respaldos de su teléfono en el ordenador, contagiando con esto al computador receptor de los datos.

Otra acción que puede comprometer seriamente los datos corporativos sensibles, es la filtración de éstos por parte de un funcionario de la propia organización, como le ocurrió a Estados Unidos en el caso Snowden.[21] El *smartphone* puede ser una herramienta sumamente útil para funcionarios que pretenden filtrar información, ya que pueden operar como un dispositivo de almacenamiento de datos, al ser utilizados como router para conexión a internet, permitiendo con esto, el acceso al ciberespacio de dispositivos que debieran estar aislados. Por otro lado, puede ser simplemente utilizado para tomar fotografías o filmar videos de información, acciones o instalaciones, para después filtrarlas.

Sistemas para el control y algunas recomendaciones

Con la aparición de cibercriminales dedicados a la vulneración de los *smartphones*, se desarrollaron soluciones que centraron sus esfuerzos en darle un mayor nivel de seguridad a los teléfonos inteligentes, lo cual ha estado enfocado principalmente en el mercado corporativo. Al mismo tiempo, se desarrollaron sistemas de control para los dispositivos en forma remota, permitiendo con esto aplicar políticas de seguridad que les pondrían limitaciones (bloquear cámaras, audífonos, prohibir descargas, forzar contraseñas, etc.) e incluso permitirían borrar el dispositivo remotamente. A dichos sistemas se les conoce actualmente como MDM, por su sigla en inglés *Mobile Device Management*.[22]

17. WIKIPEDIA, la enciclopedia libre. Phreaking. [Consultado el 30 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Phreaking
18. MCAFEE, Mobile threat Report Q1 2018.
19. MITNICK, KEVIN y SIMON, William. El arte del engaño, 2001
20. AVAST Software, Inc. [US] Phishing. [Consultado el 31 de octubre de 2018]. Disponible en https://www.avast.com/es-es/c-phishing
21. 24 HORAS INTERNACIONAL. La completa cronología del mes marcado por el caso Snowden. [Consultado el 31 de octubre de 2018]. Disponible en https://www.24horas.cl/internacional/la-completa-cronologia-del-mes-marcado-por-caso-snowden-731177
22. WIKIPEDIA, la enciclopedia libre. Mobile device management. [Consultado el 9 de noviembre de 2018]. Disponible en https://en.wikipedia.org/wiki/Mobile_device_management

La implementación de medidas de seguridad en los teléfonos inteligentes, tales como el desarrollo de sistemas operativos, cuyo código fuera cerrado y bastante complejo de ser vulnerado por *malware*, produjo una limitación en la posibilidad de instalar en éstos aplicaciones de uso masivo, ya que los desarrolladores de este tipo de programas, al no poder interactuar con el código, difícilmente podían desarrollar aplicaciones compatibles, lo cual produjo finalmente que los usuarios, quienes en general privilegian la comodidad por sobre la seguridad, dejaran de adquirir este tipo de dispositivos. Un buen ejemplo de esto fue lo que ocurrió con *Blackberry*, empresa pionera en el desarrollo de teléfonos inteligentes que privilegiaban la seguridad por sobre cualquier otra consideración.

En la actualidad, existe una inmensa cantidad de sistemas MDM y de aplicaciones que permiten aumentar la seguridad de los dispositivos móviles y de los teléfonos inteligentes, pero en general, no son utilizados por los usuarios por lo descrito anteriormente (limitaciones de usabilidad) o por el costo que conlleva la implementación de estos sistemas. El no contar con medidas de seguridad, implica un inmenso riesgo, tanto para los usuarios como para las organizaciones donde trabajan, particularmente para aquellas que han aplicado el concepto BYOD[23] (*Bring Your Own Device*), que consiste en que los usuarios llevan sus dispositivos móviles personales para realizar tareas corporativas.

Como se explicó anteriormente, un dispositivo infectado o una persona inescrupulosa puede comprometer gravemente a las organizaciones, afectando directamente la integridad, la confidencialidad o directamente, la disponibilidad de los datos, es por esto, que tanto las personas y especialmente las organizaciones, deben tomar conciencia de la necesidad de contar con medios que permitan robustecer las medidas de seguridad sobre los datos que circulan por los distintos dispositivos móviles, en especial en los teléfonos inteligentes, ya que, si nos preguntamos hoy en día, cuántas personas tienen instalado un anti *malware* en su teléfono, seguramente la respuesta será muy pocas, no así en el caso de los computadores.

Debido a que, tal como se mencionó anteriormente, en la cadena de seguridad de la información, el eslabón más débil va a ser siempre la persona, es altamente recomendable que todas las organizaciones inviertan en soluciones de control y auditoría sobre los teléfonos inteligentes, minimizando con esto el riesgo de acciones maliciosas, tanto de personas como de los *hackers*. A la vez, es recomendable obligar, al menos a los funcionarios corporativos que ingresan dispositivos a las instalaciones, a cumplir con ciertas normas de seguridad, tal como implementar contraseñas de acceso a éstos, tener versiones del sistema operativo actualizadas o contar como mínimo, con una aplicación de *antimalware* instalada. En el caso de los teléfonos inteligentes de la organización, estos debieran contar con todo lo anteriormente mencionado, pero, además, se debería aplicar sobre ellos mayores políticas de seguridad, dependiendo del perfil del usuario, tal como bloqueo de cámaras o prohibición de descarga e instalación de aplicaciones sin previa autorización. Por otro lado, también es recomendable prohibir la utilización de los teléfonos inteligentes como *routers* inalámbricos o que dichos dispositivos sean vinculados a través del puerto USB, a los ordenadores conectados a la red corporativa.

En el caso de instalaciones corporativas sensibles, se recomienda la prohibición total del acceso a ellas por medio de teléfonos inteligentes o dispositivos móviles de cualquier tipo, ya que nunca hay que olvidar la posibilidad de fuga de datos internos (caso Snowden), ni tampoco se deben subestimar las capacidades de los hackers, independiente de las medidas de seguridad aplicadas sobre los dispositivos.

23. SONDA. Bring Your Own Device, hacia una nueva cultura colaborativa dentro de la empresa. [Consultado el 9 de noviembre de 2018]. Disponible en https://www.sonda.com/media/uploads/columnas/Bring-your-own-device.pdf

Otra recomendación esencial, es la de concientizar permanentemente a las personas y funcionarios de la organización, respecto de los riesgos a los que están expuestos si no aplican las medidas de prevención necesarias sobre sus dispositivos o no cumplen con la normativa en seguridad corporativa vigente. Las auditorías internas para verificar el correcto cumplimiento de la normativa dispuesta, debe ser un deber fundamental de los encargados de seguridad y en lo posible, se debe encargar esta tarea a organizaciones externas de tal forma que la auditoría sea objetiva.

Conclusiones

Los avances tecnológicos de las últimas décadas han sido exponenciales, especialmente en las áreas de la computación y de la telefonía, debido al desarrollo de los circuitos integrados, más conocidos como chip o microchip, elementos vitales para el funcionamiento de los dispositivos electrónicos.

Con la llegada de la era digital, se produjo una transformación que significó la digitalización de las personas y organizaciones, lo que provocó a su vez, la apertura de una nueva brecha en cuanto a los riesgos de seguridad que enfrentaban hasta ese entonces; la seguridad de la información en el ciberespacio, por lo que, en relación a este nuevo vector, nacen cibercriminales que intentan sacar provecho de sus conocimientos informáticos con el objetivo, no solo de vulnerar la privacidad de personas, organizaciones o gobiernos, sino que también, con el fin de cometer ilícitos o simplemente provocar perjuicios.

El teléfono inteligente es en la actualidad, prácticamente un minicomputador portátil, por lo que este tipo de dispositivo es altamente sensible a ser objeto de vulneración, más aún considerando que las personas lo utilizan para prácticamente todo tipo de acciones, desde almacenar fotografías personales, realizar transacciones bancarias, hasta utilizar el dispositivo como *router*, permitiendo con esto la conexión a internet abierta incluso desde computadores corporativos, comprometiendo con esto a toda la red y en consecuencia, a toda la información de la organización.

Conscientes de este problema, algunas empresas desarrolladoras de teléfonos inteligentes y de *software* asociados a éstos, crearon equipos mucho más seguros y que contaban al mismo tiempo, con sistemas de control sobre éstos, teniendo en un principio un alto éxito comercial. Con la aparición de aplicaciones de uso masivo que no podían ser instaladas en los sistemas operativos de estos teléfonos, que privilegiaban la seguridad por sobre otras consideraciones, este tipo de dispositivo lentamente desapareció del mercado.

Con la desaparición de los teléfonos inteligentes robustos en seguridad, se volvió a abrir la brecha hacia el acceso de la información por parte de hackers e inescrupulosos que desean aprovecharse de esta situación, en especial para aquellas organizaciones que no cuentan con medidas de seguridad suficientes que permitan, a lo menos, mitigar la posibilidad de ocurrencia de incidentes, por lo mismo, es absolutamente recomendable que las organizaciones inviertan en sistemas de seguridad aplicables a los teléfonos inteligentes y que a su vez, normen y elaboren políticas de seguridad que deban ser cumplidas por los usuarios.

Todo lo anterior será en vano si no se realizan auditorías aleatorias constantes para verificar el correcto cumplimiento de las medidas de seguridad por parte del personal, ya que no debemos olvidar que las personas son el eslabón más débil en la cadena de seguridad de la información, más aun considerando que el aumento de la seguridad en los dispositivos implica una mayor incomodidad para el usuario,

Repetir una acción genera un hábito, un hábito genera cultura, eso es lo necesario para poder combatir a los ciberdelincuentes, inescrupulosos y a los negligentes, una cultura personal y organizacional que haga que los usuarios de tecnología por defecto, tomen las medidas de seguridad que al menos

dificulten la posibilidad de incidentes informáticos, contribuyendo con ello, no sólo al resguardo de la seguridad de la información personal, sino que también, al resguardo de datos corporativos e incluso en algunos casos extremos, la protección de información de seguridad nacional.

BIBLIOGRAFÍA

1. MITNICK, Kevin y SIMON, William. El arte del engaño, 2001.
2. AVAST Software, Inc. [US] Phishing. [Consultado el 31 de octubre de 2018]. Disponible en https://www.avast.com/es-es/c-phishing.
3. BARRÍA HUIDOBRO, Cristian. Ciberespacio: protección a la infraestructura crítica de la información. Revista Escenarios Actuales, Centro de estudios e investigaciones militares del Ejército de Chile. N°2, Agosto 2016, pp 17-26.
4. CONGRESS.GOV. Resolución 269 House of Representatives, U.S. Government Printing Office. 17 de octubre de 2001. [Consultado el 22 de octubre de 2018]. Disponible en https://www.congress.gov/bill/107th-congress/house-resolution/269/text
5. HIPERTEXTUAL, Apple II, la historia de los dos Steve. [Consultado el 23 de octubre de 2018]. Disponible en https://hipertextual.com/2016/04/apple-ii-la-historia-los-dos-steve.
6. INVERSOR, Latam. Ciberseguridad, América Latina en la mira de los ataques. [Consultado 22 de octubre de 2018]. Disponible en http://inversorlatam.com/ciberseguridad-america-latina-en-la-mira-de-los-ataques/.
7. MCAFEE, Mobile threat Report Q1 2018
8. MITNICK, KEVIN y SIMON, William. El arte del engaño, 2001
9. OTI, En el mundo hay más teléfonos celulares que humanos. Organización de Telecomunicaciones de Iberoamérica [Consultado 23 de octubre de 2018]. Disponible en https://www.otitelecom.org/telecomunicaciones/mundo-mas-celulares-humanos
10. POWER DATA. Transformación digital. Qué es y su importancia en relación con los datos. [Consultado 25 de octubre de 2018]. Disponible en https://www.powerdata.es/transformacion-digital
11. PSYCHOLOGY TODAY. Nomophobia: A rising trend in students. [Consultado el 25 de octubre de 2018]. Disponible en https://www.psychologytoday.com/us/blog/artificial-maturity/201409/nomophobia-rising-trend-in-students
12. REAL ACADEMIA ESPAÑOLA. [Consultado el 25 de octubre de 2018] Significado de la palabra "Software". Disponible en http://dle.rae.es/?id=YErlG2H
13. SYMANTEC CORPORATION [US]. Malware. Norton. [Consultado el 25 de octubre de 2018]. Disponible en https://us.norton.com/internetsecurity-malware.html
14. SONDA. Bring Your Own Device, hacia una nueva cultura colaborativa dentro de la empresa. [Consultado el 9 de noviembre de 2018]. Disponible en https://www.sonda.com/media/uploads/columnas/Bring-your-own-device.pdf
15. TECNOLOGIA & INFORMATICA ¿Qué es Hardware y Software? [Consultado el 25 de octubre de 2018]. Disponible en https://tecnologia-informatica.com/que-es-hardware-y-software
16. THE LINUX INFORMATIÓN PROJECT. Source Code Definition. [Consultado el 25 de octubre de 2018]. Disponible en http://www.linfo.org/source_code.html
17. THOUGHCO. Jack Kilby, father of the Microchip. [Consultado el 23 de octubre de 2018]. Disponible en https://www.thoughtco.com/jack-kilby-father-of-the-microchip-1992042
18. WIKIPEDIA, la enciclopedia libre. Código Fuente. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/C%C3%B3digo_fuente
19. WIKIPEDIA, la enciclopedia libre. Mobile device management. [Consultado el 9 de noviembre de 2018]. Disponible en https://en.wikipedia.org/wiki/Mobile_device_managementWIKIPEDIA, la enciclopedia libre. Phreaking. [Consultado el 30 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Phreaking
20. WIKIPEDIA, la enciclopedia libre. Router: Dispositivo que proporciona conectividad a nivel de Red. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Router
21. WIKIPEDIA, la enciclopedia libre. Teléfono Inteligente. [Consultado el 25 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Tel%C3%A9fono_inteligente
22. WIKIPEDIA, la enciclopedia libre. Teléfono móvil. [Consultado 23 de octubre de 2018]. Disponible en https://es.wikipedia.org/wiki/Tel%C3%A9fono_m%C3%B3vil
23. 24 HORAS INTERNACIONAL. La completa cronología del mes marcado por el caso Snowden. [Consultado el 31 de octubre de 2018]. Disponible en https://www.24horas.cl/internacional/la-completa-cronologia-del-mes-marcado-por-caso-snowden-731177