

UNIVERSIDAD DE LA DEFENSA NACIONAL

INSTITUTO DE INTELIGENCIA DE LAS FFAA

“Sarg My D. José Antonio ÁLVAREZ DE CONDARCO”

**ESPECIALIZACIÓN EN GESTIÓN DE INFORMACIÓN
MILITAR TERRESTRE**

TRABAJO FINAL INTEGRADOR

**“Internet of Things (IoT), la nueva amenaza, riesgos en el
tratamiento de la información en los teléfonos inteligentes”**

Autor: Primer Alférez Carlos Leopoldo SEGURA

Director: Coronel D. Esteban Guillermo CARLUCCI

Diciembre 2020

“Las ideas expresadas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión del Instituto de Inteligencia de las Fuerzas Armadas y de la Universidad de la Defensa.”

RESUMEN

En los últimos años, el campo de la tecnología nos fue presentando un fenómeno poco habitual, en donde los equipos o sistemas más avanzados no están en manos de las Instituciones, sino que es propiedad de sus empleados. Esto no resulta difícil de imaginar, ya que hoy en día cualquier persona posee un teléfono inteligente, una computadora personal o una conexión con mayor ancho de banda en su domicilio, lo que conlleva que nuestra permanencia en la organización, nos dé una sensación de volver al pasado.

La tendencia en aumento del consumo de las tecnologías de la información y comunicaciones, se ha ido trasladando a las organizaciones, ya que sus integrantes intentan emplear en el ámbito laboral, aquellas herramientas tecnológicas (equipos, dispositivos y servicios) que utilizan en su entorno personal, y con las que aseguran poder ser más productivos en el ámbito profesional, dando origen a una corriente que identificaremos como BYOD¹.

Este fenómeno, se transformó en la organización, en la puerta de entrada para mejoras en lo que respecta al compromiso y satisfacción de sus empleados, llevando a incrementar su eficiencia y productividad, aunque no todas son ventajas, en razón de que el empleo de estos dispositivos representa un grave riesgo a la seguridad de la información de las organizaciones, convirtiendo su control y gestión, en un verdadero reto para los responsables de brindar su seguridad.

Por ello, el presente trabajo pretende mostrar cómo el empleo de los teléfonos inteligentes en el tratamiento de la información no es una moda pasajera; es una tendencia que llegó para afianzarse, y nosotros, como responsables de brindar la seguridad a la Institución, no podemos permitirnos ignorarla.

Palabras clave: Teléfono inteligente, Tecnología de la Información y Comunicaciones, use su propio dispositivo, Tratamiento de la información, Internet of Things y Medidas de seguridad.

¹ BYOD, en inglés Bring your own device, cuyo significado en nuestro idioma es “trae tu propio dispositivo”, es una política empresarial consistente en que los empleados lleven sus propios dispositivos personales a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores, así como datos y aplicaciones personales.

ÍNDICE

Introducción	5
Capítulo I: Formas de empleo de los teléfonos inteligentes	9
1.1 Concepto general	9
1.2 ¿Qué es un teléfono inteligente?	9
1.3 Nuestro asistente personal	10
1.4. Empleo de los teléfonos inteligentes en el ámbito laboral	12
1.4.1 Servicio de nube.....	13
1.4.2 Aislante	13
1.4.3 Home office	13
1.4.4 Seguridad incluida	14
1.5 Conclusiones parciales del Capítulo I	14
Capítulo II: Identificación de vectores de ataque	16
2.1. Introducción	16
2.1.1 Portabilidad	17
2.1.2 Aplicaciones	17
2.1.3 Software	18
2.1.4 Phishing	18
2.2 Vectores de ataque	18
2.2.1 Virus informático	19
2.2.2 Troyano	19
2.2.3 Gusano	19
2.2.4 Spyware	20
2.2.5 Adware	20
2.2.6 Red de robots	20
2.2.7 Phishing	20
2.2.8 Snooping	21
2.2.9 Rogueware	21
2.2.10 Ransomware	21
2.3 ¿Cómo nos atacan?	22
2.3.1 Fase 1 – Reconocimiento	23
2.3.2 Fase 2 – Escaneo	24

2.3.2 Fase 3 – Acceso	25
2.3.4 Fase 4 – Explotación	25
2.3.5 Fase 5 – Eliminación de rastros	25
2.4 Conclusiones parciales del Capítulo II	26
Capítulo III: Medidas de seguridad a prueba de fallos	27
3.1 Doctrina	27
3.2 Implementación de regulación internacional	28
3.3 Conclusiones parciales del Capítulo III	31
Conclusiones generales	32
Bibliografía	33
Anexo I – Encuesta	34

*“Internet of Things (IoT), la nueva amenaza,
riesgos en el tratamiento de la información
en los teléfonos inteligentes”*

INTRODUCCIÓN

El avance tecnológico que viene sucediendo en la última década, trajo aparejada una transformación en todos los niveles de la sociedad. El desarrollo de estas nuevas tecnologías permitió un aumento exponencial del uso de internet, el cual se introdujo en nuestras vidas de tal manera que, la dependencia que se tiene hacia él, era impensada hace unos años atrás.

Esta inserción desmedida de internet en nuestra vida diaria, le permitió a la sociedad abrir nuevas puertas en un mundo cada vez más globalizado, constituyéndose en la base en que se organizan desde un simple individuo (para comunicarse, buscar información o entretenerse), a empresas públicas u organismos gubernamentales (para la recopilación de información, organización de bancos de datos, entre otras actividades).

Debido a esto, y al desarrollo de la Tecnología de la Información y Comunicaciones²(TICs), existen diferentes dispositivos con capacidad de mantener una conexión a internet además del ordenador, desde los teléfonos, relojes y televisores inteligentes, las tablets, interruptores de luz y cámaras de seguridad, hasta heladeras o secarropas, derivando en “el internet de las cosas”³, el cual, nos lleva a una conectividad tan profunda y ampliada, como nunca se imaginó.

Dentro de la multiplicidad de dispositivos señalados precedentemente, me resulta pertinente detenernos en los teléfonos inteligentes, los cuales fueron desarrollando aplicaciones que le permitieron cumplir funciones similares a las computadoras, sumado a su capacidad de conectividad y a la gran variedad de aplicaciones que puede personalizar para satisfacer las necesidades y requisitos de sus usuarios. Así lograron ser indispensables para el desenvolvimiento diario de las personas, siendo que tiene un poco más de cinco mil millones de usuarios, posicionándose en los últimos años, como el dispositivo con mayor penetración en los hogares, superando ampliamente a los ordenadores.

² Tecnología de la Información y la comunicación (TIC), hace referencia al conjunto de tecnologías que enfatizan el papel de las comunicaciones unificadas, la integración de las telecomunicaciones y las computadoras, para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas.

³ Internet de las cosas (Internet of things – IOT), hace referencia a una interconexión digital de objetos cotidianos con internet, es decir, potencia objetos que antiguamente se conectaban mediante circuito cerrado, como comunicadores, cámaras, sensores, y demás, y les permite comunicarse globalmente mediante el uso de la red de redes.

Estos equipos, que han sido adquiridos con fines personales, para comunicarse por llamadas, mensajes o redes sociales, entretenerse, escuchar música, sacar fotos o el sinfín de actividades que puede cumplir hoy un teléfono inteligente, también son usados para ver el correo del trabajo, enviar archivos, almacenar información, o simplemente guardar las contraseñas de los bancos de datos.

Por ello, aunque hablar de hacker o de la vulnerabilidad de la información en el ciberespacio sea un tema desarrollado en cientos de investigaciones y que pueda carecer de toda pretensión de originalidad, la referida convergencia entre las telecomunicaciones, la digitalización y el desarrollo de internet, nos sigue dando que hablar, generando un proceso de sinergia y retroalimentación de estas tecnologías, que ampliarán mucho más de lo que estamos imaginando las capacidades del ciberespacio.

Este avance de la tecnología e internet, nos demostró por medio de incontables casos, que todos los dispositivos son susceptibles de ser hackeados, y que no basta con un antivirus, la huella dactilar, el patrón o la contraseña de inicio del equipo, entendiendo que tener protegida la información almacenada en estos dispositivos, ya sea privada o de la Institución, representa una tarea cada vez más compleja.

Entendiendo que la seguridad de la información, independientemente a la clasificación de seguridad asignada, resulta un tema crucial para nuestra Institución, que la llevó a adoptar un conjunto de medidas preventivas y reactivas, que le permitan resguardar y proteger la información que se encuentra almacenada en los diferentes ordenadores que integran su sistema y, teniendo en cuenta que a través de este dispositivo, se cumplen actividades tanto del ámbito personal como del laboral, debido a que la mayoría de los empleados con la necesidad actual de trabajar de forma remota, acceden cada día a datos de la Institución desde sus dispositivos móviles, la lógica nos lleva a preguntarnos ¿no deberían tener igual o mayor seguridad que los ordenadores?

Por ende, el presente trabajo de investigación, analiza 1) cómo las formas de entretenimiento de una persona en la vida privada podrían provocar una vulnerabilidad en el sistema organizacional, 2) entender que la seguridad de los teléfonos inteligentes debe ser una

preocupación importante, y 3) cómo esto, representa un desafío permanente para quienes tienen que brindar la seguridad de la información.

Entonces, considerando la dirección que se intenta tomar, establecí como el objetivo general del trabajo, exponer cómo el tratamiento de la información a través de los teléfonos inteligentes, potencia inevitablemente las vulnerabilidades. Para ello, el ensayo estará estructurado en tres capítulos, que servirán como base para explicar cada uno de los temas necesarios para entender la situación, los cuales se desprenderán de los objetivos específicos señalados a continuación:

- ✚ Determinar cómo se emplea el teléfono inteligente en el tratamiento de la información y su forma de conectarse al sistema de la organización. Esto, nos permitirá evidenciar el verdadero riesgo al que está expuesta nuestra información (Capítulo I).
- ✚ Identificar los diferentes vectores de ciberataque y cómo pueden afectar a estos dispositivos. Tal como fuere mencionado, el teléfono inteligente es más vulnerable de lo que uno cree. En muchas ocasiones, uno tiende a exagerar la amenaza que esto supone, y en otras, uno no llega a percibir el riesgo real que conlleva el uso de estas tecnologías de la información y comunicaciones; por ello, la individualización de estos fallos de seguridad, nos permitirán adoptar las medidas de seguridad pertinentes, para el resguardo de la información institucional (Capítulo II).
- ✚ Establecer la existencia de medidas de seguridad, para el tratamiento de la información en estos equipos. Conocer las medidas de seguridad dispuestas por la Institución y el grado de rigurosidad en el modo en que son implementadas por parte del personal, nos permitirá determinar qué tan expuesta esta nuestra información (Capítulo III).

Para analizar el problema de nuestra investigación, la estrategia para su diseño será desde un enfoque cualitativo, asociado con el método inductivo, describiendo de forma más clara y exhaustiva posible, los conceptos que son necesarios resaltar para entender el tema estudiado. La investigación será de tipo descriptiva, puesto que se pretende examinar la realidad del tema. En este estudio, además se realizará investigación documental de los datos que se obtengan de fuentes secundarias tanto impresas como digitales.

Por último, al comenzar el desarrollo del ensayo, se implementó un cuestionario sobre los dieciocho integrantes del Curso Básico de Inteligencia 2020 del Instituto de Formación de las Fuerzas Armadas, cuyo resultado se someterá a un análisis, sirviendo como premisa detonante del razonamiento inductivo para la confección del presente trabajo.

CAPÍTULO I

FORMAS DE EMPLEO DE LOS TELÉFONOS INTELIGENTES

1.1. Concepto General

Cada año, se produce un aumento en la utilización de estos dispositivos. De hecho, se prevé que, a fines del año 2020, haya alrededor de siete mil millones de usuarios de estos equipos. En nuestro país, conforme el último informe de la Encuesta Permanente de Hogares del Instituto Nacional de Estadísticas y Censos, reveló que nueve de cada diez personas (91%) tiene un teléfono inteligente, entrando en contacto con estos equipos a partir de los cinco años de edad, quedando expuesto, que diariamente una persona controla de 150 a 200 veces el celular, siendo la primera y última actividad en el día.⁴

Por ello, aunque la idea de este capítulo será enumerar las formas en que empleamos estos dispositivos diariamente en nuestro ámbito laboral, me resulta imprescindible definir qué entendemos como “teléfono inteligente” y mencionar brevemente qué los hace tan indispensables para nuestra vida incluyendo su actualización de forma periódica.

1.2 ¿Qué es un teléfono inteligente?

El concepto de teléfono inteligente tiene su origen en el año 1992, momento en que la empresa IBM lanzara a la venta el primer equipo, el cual además de recibir y realizar llamadas, incluía otras funciones como el calendario, hora mundial, libreta de direcciones, libreta de anotaciones, enviaba y recibía fax, entre otras. En la última década, cobro una mayor notoriedad, ya que el avance de la tecnología le ofreció ciertas funciones básicas que los hace más completos, desde la conexión a internet, reproductores multimedia, cámaras digitales y dispositivos de navegación GPS.

⁴ Instituto Nacional de Estadística y Censos - República Argentina. (2020, febrero). Acceso y uso de tecnologías de la información y la comunicación. EPH (Informes técnicos / Vol. 4, nro. 83). Instituto Nacional de Estadística y Censos. https://www.indec.gob.ar/uploads/informesdeprensa/mautic_05_20A36AF16B31.pdf

Entonces, definiremos a los teléfonos inteligentes, como un dispositivo móvil que trabaja bajo un sistema operativo móvil (OS) y funciona como una mini computadora, ofreciéndole, al equipo, capacidades informáticas más avanzadas.

Hoy, aparte de las funciones básicas predeterminadas de fábrica, gracias a su sistema operativo que lo acerca al de las computadoras, el equipo puede instalar algunas de los millones de aplicaciones que integran una amplia gama de categorías disponibles, que pueden mejorar sus prestaciones, manteniendo a sus usuarios entretenidos, productivos, organizados, actualizados sobre noticias y socialmente conectados.

Identificándose como la nueva generación de teléfonos, estos equipos ofrecen mucho más poder, memoria, velocidad y conectividad, sumado a la aplicación de la miniaturización de todos sus componentes que facilitan su transporte. Es decir, un teléfono inteligente es capaz de ejecutar muchas tareas diferentes, además de la simple posibilidad de mantenernos en contacto telefónicamente con el resto del mundo.

1.3 Nuestro asistente personal

Desde hace un poco más de una década, el sector de la telefonía móvil se ha marcado como objetivo hacernos la vida más fácil. De forma paulatina, se fueron incorporando mejoras y actualizaciones en nuestros equipos, que los han convertido en completísimos teléfonos inteligentes.

Trayendo incorporadas funciones básicas de fábrica como llamada de voz, mensajería de texto, cámara digital, reproductor multimedia, acceso a correo electrónico, calculadora, agenda, leer documentos con diferentes formatos, fijar alarma, GPS o conexión a internet, entre otras, los teléfonos inteligentes comenzaron a desplazar a estos y muchos otros gadgets⁵ más, que a su lado se ven anticuados.

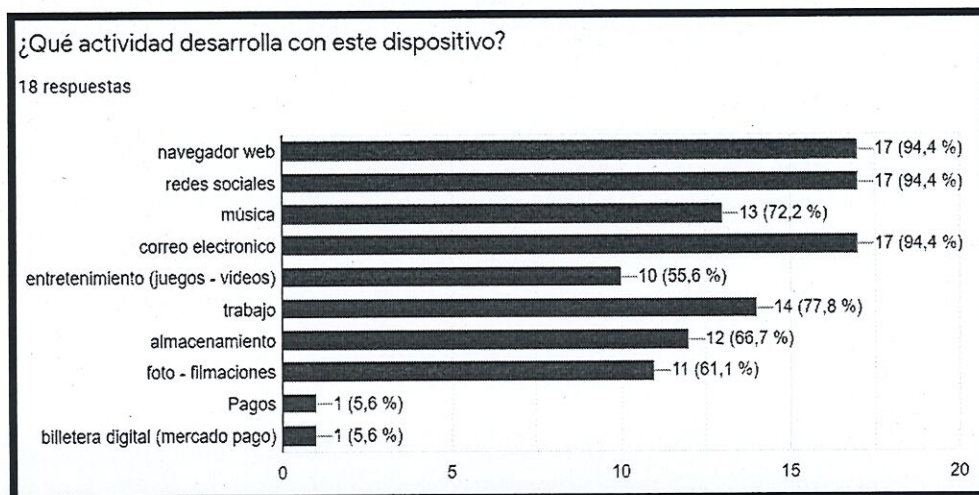
Una de las características más importante de estos equipos, es que posibilitan la instalación de aplicaciones que pueden ser desarrolladas por el fabricante del dispositivo, por el operador o por un tercero, con el objeto de incrementar sus prestaciones, como el procesamiento de datos, la conectividad e internet.

⁵ El gadgets, es un dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso

Intentar hacer referencia a las millones de aplicaciones existentes que nos pueden llevar a la compra de estos equipos, nos va a demandar mucho más que estas simples hojas, por ello, con el objeto de dimensionar qué tan amplio es este campo, destacaremos las categorías más utilizadas por los usuarios, las cuales cuentan con un abanico de miles de posibilidades cada una, como son las aplicaciones de mensajería instantánea, juegos, educativas, entretenimiento, deportes, estilo, informáticas, viaje y guías, salud, biblioteca, mapas y navegación, comerciales, financieras, noticias, herramientas y muchas otras, todas ellas con el único objetivo de satisfacer las necesidades del usuario.

Las aplicaciones móviles para redes sociales, guardan una gran cantidad de información personal. El aumento de aplicaciones destinadas a la compra – venta de productos y servicios, dieron pie a innovaciones recientes en los dispositivos, permitiendo a los usuarios realizar muchas transacciones desde su teléfono inteligente, como la billetera virtual y aplicaciones para canjear cupones y boletos, control de cuenta bancaria, procesamiento de pagos en el punto de venta e incluso pagos en cajas registradoras.

Como fuere mencionado en la introducción, al momento de definir el tema a desarrollar en el presente trabajo, se realizó una encuesta sobre los dieciocho integrantes del Curso Básico de Inteligencia del Instituto de Inteligencia de las Fuerzas Armadas, del ciclo lectivo 2020, la cual releva que, aparte de ser un elemento indispensable para el quehacer diario para la totalidad del personal, el mismo es utilizado para navegar en internet (94,4%), comunicarse (94,4%), reproducir multimedia (94,4%), leer los correos electrónicos (94,4%), entretenimiento (55,6%), almacenar información (66,7%), billetera digital (5,6%), Pagos (5,6%) y para realizar actividades laborales (77,8%).



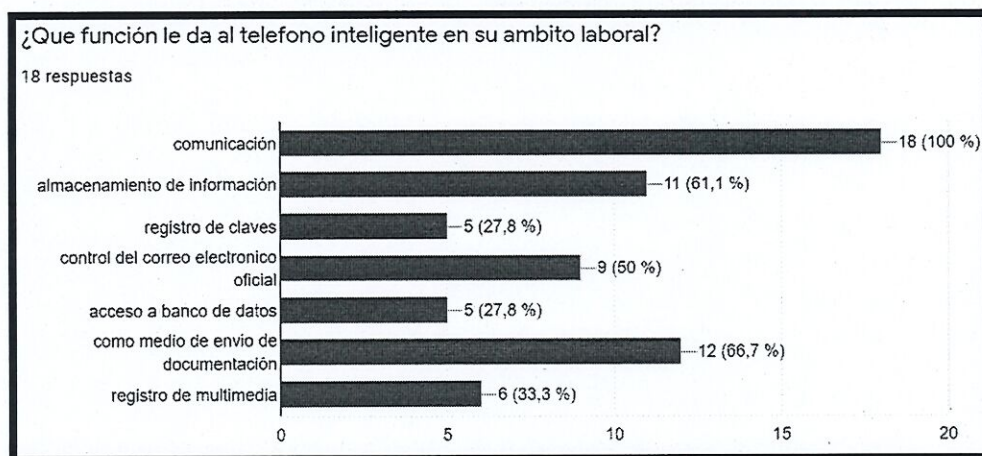
Aunque todas estas funciones nos den más de un motivo para ser usuarios de estos equipos, muchos expertos coinciden en destacar que, aunque el desarrollo tecnológico empezó mucho antes, la verdadera inteligencia llegó a nuestros móviles con la incorporación de los primeros asistentes virtuales, que nos ayudan en la realización de diferentes tareas, desde llamar a tus contactos, organizarte el calendario o aprenderse tus gustos, la lista de estos asistentes virtuales es extensa, aunque se prevé que se vaya incrementando con las mejoras de la tecnología.

1.4 Empleo de los teléfonos inteligente en el ámbito laboral

Toda organización usa algún tipo de tecnología para intentar aumentar su eficiencia, productividad, proactividad y mejora de recursos. Algunas con base en la conexión de internet, utilizan servicios como la nube, blogs, bancos de datos, páginas web, redes sociales, etc. Esto, sumado al avance de la tecnología, que permitió reducir el tamaño de los equipos, y con ello, favorecer la movilidad de las personas en comparación a una notebook, provocaron que los usuarios puedan acceder desde cualquier lugar a la información de la organización, a través de los teléfonos inteligentes.

En tal sentido, resulta necesario destacar que nuestra reglamentación vigente, define al tratamiento o gestión de la información, al conjunto de acciones que abarcan la elaboración, almacenamiento en soportes de diversa naturaleza y multiplicidad de formatos, custodia, proceso, utilización, presentación, reproducción, acceso, transporte, transmisión y/o destrucción de la información clasificada, sea cual fuere el método empleado (Capítulo III, RCG-16-02).

El cuestionario realizado, nos permitió entrever que estos dispositivos se encuentran inmersos en las actividades del ámbito laboral, desde las comunicaciones (100%), envío de documentación (66,7%), almacenamiento de información (61,1%), control del correo electrónico laboral (50%), registros multimedia (33,3%), el registro de claves (27,8%) y para el acceso a banco de datos (27,8%). Asimismo, un punto a destacar es que el 72,2% del personal, refirió poseer información laboral en sus dispositivos al momento de realizar la encuesta, la cual corresponde al corriente año y en menor medida de vieja data, es decir, de destinos militares anteriores.



La posibilidad de estar todo el tiempo conectado con el correo electrónico de la organización, acceder a sus bancos de datos de forma remota, algunos servicios de nube y otras funcionalidades especialmente atractivas, como poder ver y editar documentos de oficina (como Word y Excel), convierten a estos dispositivos en verdaderos centros multimedia de trabajo.

Entonces, podemos decir que estos equipos nos ofrecen diferentes beneficios para el ámbito laboral, atento a la intención de la organización de moverse a la par de la tecnología, resultando indispensable en muchos casos, por los siguientes motivos:

1.4.1 Servicio de nube: Posibilita la sencilla incorporación en las empresas de algunas plataformas ya existentes. De esta forma, no deben llevarse a cabo actuaciones que conlleven riesgos para la empresa al trabajar desde el propio dispositivo móvil. Por ejemplo, con Microsoft Office Mobile podemos sincronizar los documentos de la empresa con la misma plataforma usada por las estaciones de trabajo (nube). Así no necesitamos sacar datos sensibles de la empresa (USB o correo personal).

1.4.2 Aislante: Por el propio diseño del sistema operativo, ya se aíslan unas aplicaciones de otras. Esto supone que, si se produce un fallo de seguridad en una aplicación, no afecta a las demás.

1.4.3 Home office: Ofrecen la habilidad de mantener conectados a sus empleados a toda hora, permitiéndoles desarrollar sus tareas en cualquier lugar, sin importar si están en casa, en la oficina o viajando.

1.4.4 Seguridad incluida: Incluyen muchas características de seguridad por defecto que, en sistemas de escritorio, deben ser implementadas mediante herramientas de terceros, como sistemas de cifrado de disco por defecto.

En la actual era digital, cuya tendencia de conexión a internet de forma permanente a través de estos dispositivos personales es para atender asuntos laborales, personales o de ocio, las organizaciones se han visto involucradas por parte de sus empleados. Por ello, surgió una necesidad a nivel mundial de adaptar políticas, proceso y plataformas tecnológicas para permitir el uso de BYOD como tendencia de trabajo a sus empleados.

La creciente adopción de las iniciativas BOYD, aumentaron radicalmente los riesgos de la seguridad de la información, ya que los dispositivos personales incorporan una mezcla de sus datos y aplicaciones personales, además de los datos de la organización, cuentas de usuarios y contraseñas de acceso, lo que termina aumentando significativamente las brechas de seguridad. Además, considerando que los equipos son tan pequeños, estos pueden ser robados, o perdidos fácilmente por sus propietarios, lo cual supone un serio riesgo a la información, dando acceso directo a usuarios no autorizados, a información personal, correos electrónicos, redes sociales, sistemas y aplicaciones de la empresa.

Por eso, la seguridad del teléfono móvil es una de las principales preocupaciones de todas las empresas en la actualidad, el hecho de que la mayoría de los trabajadores accedan diariamente a datos de la empresa desde sus teléfonos inteligentes, provoca que cada vez sea más complicado proporcionar la seguridad a esta información.

1.5 Conclusión parcial del Capítulo I

En nuestro entorno, las tecnologías de la información han evolucionado desde ser una simple herramienta para mejorar la productividad administrativa a transformarse en un medio estratégico, en donde su empleo fue provocando que se conviertan de manera activa en un instrumento de trabajo, alojando en algunas ocasiones, información crítica y valiosa.

Esto, sumado al fenómeno BYOD que se presenta como una realidad difícil de restringir y controlar, ofrece un abanico de ventajas y desventajas, entre las cuales se imponen

los riesgos de la información de la organización, debiendo ser seriamente considerado su empleo, resultando necesario que los usuarios entiendan completamente las políticas de seguridad.

Por ello, la concientización del usuario es y seguirá siendo un factor determinante para los daños y la exposición que se tenga a los malware⁶.

⁶ Se llama malware, del inglés malicious software, programa malicioso o software malintencionado a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

CAPÍTULO II

IDENTIFICACIÓN DE VECTORES DE ATAQUE

1.1 Introducción

Los equipos a los que se hizo referencia en el Capítulo I, están apareciendo en los bolsillos, carteras y maletines de más personas. La popularidad de los teléfonos inteligentes y una seguridad relativamente laxa los han convertido en objetivos atractivos para los atacantes. De acuerdo a un informe de ventas publicado a principios de este año, los teléfonos inteligentes superaron ampliamente a las computadoras personales por primera vez, llevando a que los atacantes comiencen a explotar este mercado en expansión, utilizando técnicas antiguas junto a otras más modernas.

Si a principios de este milenio el sistema más utilizado para la infección y acceso a los sistemas de información de forma no autorizada era vía correo electrónico, hoy en día está a punto de ser superado por las aplicaciones y otros sistemas derivados del uso de los teléfonos inteligentes.

Pese al avance de la tecnología y las nuevas herramientas utilizadas por los hackers, se continúa comprobando que el usuario sigue siendo el eslabón más débil en la cadena de la seguridad. Por más que se tenga programas antivirus y dispositivos de seguridad sofisticados, políticas de seguridad, controles y demás actividades de aseguramiento de la información, no existe suficiente sensibilización para que el propio usuario no ponga en riesgo su propia seguridad y la de los sistemas informáticos en los cuales interactúa, en razón que es el mismo, el que le otorga en determinadas ocasiones, acceso completo a los delincuentes a sus dispositivos móviles y por medio de estos, a la infraestructura y plataformas tecnológicas de cualquier organización. Asimismo, les entrega a los delincuentes cuentas de acceso, contraseñas, cuentas de correos electrónicos, geolocalización, datos de la red, información de sistemas operativos, servidores de bancos de datos, etc., con lo cual los delincuentes pueden lograr sabotear, robar, dañar o modificar los sistemas informáticos de las organizaciones.

Los teléfonos inteligentes y los asistentes digitales personales, brindan a los usuarios acceso móvil al correo electrónico, internet, navegación GPS y muchas otras aplicaciones. Sin embargo, la seguridad de los teléfonos inteligentes no se mantuvo al día con la seguridad informática tradicional. Las medidas técnicas de seguridad, como cortafuegos, antivirus y el cifrado son poco comunes en teléfonos móviles, y aparte, los sistemas operativos de teléfonos inteligentes no se actualizan con tanta frecuencia como las de las computadoras personales.

Desafortunadamente, muchos usuarios de teléfonos inteligentes no reconocen estas deficiencias de seguridad. Algunos no habilitan el software de seguridad que viene con sus teléfonos, y creen que navegar por Internet en sus teléfonos es igual de seguro, que navegar en las computadoras.

Aunque el malware móvil no ha alcanzado completamente a la computadora personal en cuanto a volumen o complejidad, los profesionales de seguridad están observando más malware específico de móviles diseñado para aprovecharse de las funciones de estos dispositivos, direccionando los ataques directamente al sistema operativo, al operador o a una aplicación específica del equipo. Asimismo, por el hecho de cumplir con funciones que los hacen similares a las computadoras personales, también son pasibles de muchas de sus vulnerabilidades, agravadas por la propia portabilidad del equipo, que lo expone a otros tipos de ataques:

2.1.1 Portabilidad: La ventaja que ofrece la portabilidad de los teléfonos inteligentes, lo puede convertir en el blanco de un simple robo. El propietario de un teléfono robado podría perder todos los datos almacenados en él, desde información personal, datos financieros y corporativos. Se debe considerar que un atacante sofisticado con suficiente tiempo, puede anular la mayoría de las funciones de seguridad de los teléfonos móviles y obtener acceso a cualquier información que almacenan.

2.1.2 Aplicaciones: Muchas aplicaciones de software aparentemente legítimas, en realidad pueden contener un código malicioso. Cualquiera puede desarrollar aplicaciones para algunos de los sistemas operativos móviles más populares, esto es en razón que por ejemplo Google, liberó Android con licencia, motivando que los proveedores puedan ofrecer aplicaciones de terceros con poca o ninguna evaluación de seguridad. Fuentes

que no están afiliados a proveedores de servicios móviles también pueden ofrecer aplicaciones no reguladas, las cuales una vez instaladas en los dispositivos, pueden acceder a la información del mismo. Algunos usuarios "rootean" o "liberan" sus dispositivos, omitiendo las funciones de bloqueo del sistema operativo para instalar estas aplicaciones.

2.1.3 Software: Posibilidad de explotar el software legítimo de teléfonos inteligentes. El software de estos dispositivos y los servicios de red tienen vulnerabilidades, al igual que sus contrapartes de las computadoras personales. Durante años, los atacantes han explotado el software de los teléfonos móviles para escuchar a escondidas, bloquear el software del teléfono o realizar otros ataques. Un usuario puede desencadenar un ataque de este tipo mediante alguna acción explícita, como por ejemplo hacer "clic" en un enlace diseñado con fines malintencionados que aprovecha una vulnerabilidad en una web del navegador. Un usuario también puede estar expuesto a un ataque pasivamente, simplemente usando un dispositivo que tiene una aplicación vulnerable o un servicio de red ejecutándose en segundo plano.

2.1.4 Phishing: Los ataques de phishing utilizan comunicaciones electrónicas para engañar a los usuarios haciendo que instalen software o revelen información confidencial. El phishing por correo electrónico es un ataque común en los ordenadores, y es igualmente peligroso en teléfonos móviles con correo electrónico.

Mientras tanto, los teléfonos móviles son cada vez más valiosos como objetivos de ataque. Las personas utilizan los teléfonos inteligentes para un número cada vez mayor de actividades y, a menudo, almacenan datos confidenciales, como correo electrónico, calendarios, información de contacto y contraseñas en los dispositivos.

2.2 Vectores de ataque

Al referirnos a ataques informáticos, solemos nombrar a los malware, spyware, códigos maliciosos o virus informáticos, aunque en realidad, estamos hablando de lo mismo, pero existen ciertos matices que los diferencian. Cuando hablamos de amenazas de seguridad a los sistemas de información, hay una entre todas ellas que es recurrente y que ha logrado sobrevivir a más de tres décadas. Ha crecido, evolucionado y se ha adaptado conforme ha ido

avanzando la tecnología, es el código malicioso (malware), que hace referencia a cualquier sistema de software que afecta los intereses del usuario.

El malware puede afectar no solo a la computadora o a los teléfonos inteligentes, sino también a cualquier otro dispositivo con el que este pueda comunicarse, entonces en lenguaje coloquial es más conocido como “virus”. A continuación, se enumerarán los malware más comunes con los que uno puede lidiar diariamente, describiendo una breve reseña del mismo, para entender a qué nos enfrentamos, lo que no significa que sean los únicos softwares maliciosos que nos encontremos en el ciberespacio ya que, tristemente, el avance de la tecnología no trajo únicamente cosas positivas.

- 2.2.1 Por orden de antigüedad, debemos empezar por el “*virus informático*”, este suele estar oculto en diferentes softwares, pasando desapercibido hasta ser ejecutados por su creador o de forma involuntaria por la víctima. Una vez activado puede alterar el funcionamiento normal de cualquier tipo de dispositivo, borrar datos almacenados o simplemente ralentizar el equipo.
- 2.2.2 Las historias griegas (Guerra de Troya), hablaban de un caballo de madera gigante utilizado para ocultar a los atacantes y así, permitirles ingresar a la ciudad sin ser detectados, este concepto del caballo de Troya fue traído a la actualidad para identificar el malware “*troyano*”, ya que este se infiltra en el dispositivo u ordenador de una víctima como un software legítimo, pero una vez instalado este virus se activa para darle el control del sistema al atacante o ejecutando la descarga de otros malware.
- 2.2.3 Los “*gusanos*”, fueron diseñados con el objetivo de proliferarse; por ende, buscará infectar un dispositivo y después replicarse y extenderse a otros dispositivos digitales, permaneciendo activos de forma permanente en todas las máquinas infectadas. Aunque en su mayoría, estos no buscan causar algún daño al ordenador anfitrión, atestan las redes con demandas de ancho de banda, ocasionando una mayor lentitud en el servicio. Alguno de estos malware, puede actuar de mensajero para la instalación de otro adicional.
- 2.2.4 Uno de los métodos para extraer información, son los “*spyware*”, herramienta utilizada por los hackers o crackers, que afectan el dispositivo de la víctima a través de

adware, programas gratuitos o barra de herramientas de navegación, para supervisar la actividad de la persona en internet, recopilar sus datos personales, credenciales de inicio de sesión, número de tarjetas o simplemente información financiera, para luego, enviársela al atacante y con ella, cometer fraudes o robo de identidad.

2.2.5 El *“adware”*, busca someter a la víctima a publicidad no deseada sobre juegos, software gratuitos o barras de herramientas para el navegador, a través de anuncios en la web o ventanas emergentes. Aunque la gran mayoría de estos adwares se instalen de forma legal, buscan recabar información del anfitrión para después emplearla en personalizar los anuncios, con el único fin de crear ingresos para su desarrollador.

2.2.6 Aunque no sea un malware, resulta necesario señalar a la *“red de robots”* (botnet), tratándose de la red de equipos que fueron infectados con un software malicioso conocido como robot, que es capaz de recibir órdenes desde su controlador; es decir, por parte del atacante. Una vez infectados, todos estos equipos conforman una red que le proporcionará al controlador, el acceso a una capacidad de procesamiento sustancial, permitiéndole coordinar ataques, robar datos o enviar spam.

2.2.7 El *“phishing”* es un delito cibernético, en el que un objetivo u objetivos son contactados por correo electrónico, teléfono o mensaje de texto por alguien que se hace pasar por una institución legítima para atraer a las personas a proporcionar datos confidenciales, como información de identificación personal, datos bancarios y de tarjetas de crédito, o contraseñas. La información se utiliza para acceder a cuentas importantes y puede provocar el robo de identidad y la pérdida financiera.

A diferencia de las computadoras personales, los usuarios de teléfonos móviles son también vulnerables a llamadas de voz de phishing (*“vishing”*) y mensajes SMS / MMS (*“Smishing”*). Estos ataques se dirigen a teléfonos de funciones (teléfonos móviles sin datos avanzados y capacidades inalámbricas), así como teléfonos inteligentes, y en ocasiones intentan engañar a los usuarios para que reciban cargos fraudulentos en su factura de teléfono móvil. Estos a menudo aumentan su ataque después de importantes eventos actuales, elaborando sus comunicaciones para que parezcan noticias o solicitudes de donaciones caritativas.

- 2.2.8** Se conoce como *“snooping”*, a la técnica que permite efectuar el control sobre la actividad de un usuario en su dispositivo, mediante la cual se podrá obtener determinada información que resulte de interés, como datos o contraseñas. Esto, se podrá llevar a cabo mediante la utilización de software espía.
- 2.2.9** Los *“rogueware”*, son softwares maliciosos que simulan ser un antivirus o programas de ayuda, con el objeto que la víctima realice una acción concreta o que instale una falsa solución ofrecida por este software, ejecutando en realidad un malware más evolucionado para que infecte el dispositivo.
- 2.2.10** Por último, pero no menos importante es el *“ransomware”*, aunque esta práctica lleva reuniendo varios millones de dolares, ha sido el centro de atención de estos últimos años. Con el pasar del tiempo, se han desarrollado virus y otros programas dañinos para facilitar las extorsiones y estafas a usuarios de internet; este es el caso del ransomware, ya que trata de un software malicioso que funciona bloqueando o denegando el acceso de la víctima a su dispositivo y archivos, hasta que la víctima pague un rescate. En pocas palabras, es la versión malware de la nota de rescate de un secuestrador.

Los objetivos de un ataque de ransomware, pueden variar desde una persona, empresas u organizaciones públicas o privadas. Lo único que interesa es que tengan información esencial en sus dispositivos y estén en condiciones de pagar el rescate. El software puede propagarse a los teléfonos por intermedio de enlaces o archivos en correos electrónicos y por descarga de programas de fuentes no oficiales.

Se debe comprender que estos son diferentes, que cada uno explota diferentes brechas en los sistemas, y que el pago del rescate no asegura que se devuelva la información, por el contrario, existen antecedentes de empresas que pagaron el rescate y poco después, los secuestradores le pidieron dinero para no exponer al público dicha información.

2.3 ¿Cómo nos atacan?

Desde el inicio de internet, existen este tipo de personas que ingresan a diferentes webs a través de fallos de seguridad por el simple hecho de demostrar que pueden hacerlo. Hoy en día, existe una competencia en las sombras, en donde miles de expertos intentan entrar en sistemas informáticos que presentan una destacada importancia, que van desde empresas locales hasta organismos gubernamentales o grandes conglomerados internacionales.

Al advertir que nuestro dispositivo móvil se encuentra infectado, nos preguntamos qué artimañas o sistemas avanzados habrán utilizado para hackear el sistema; bueno, mucho tenemos que ver nosotros, ya que como lo remarcan los diferentes portales de firmas antivirus o expertos en la materia, *"el usuario es el eslabón más débil"*, y no por nada miles de sitios web se hicieron eco de esas palabras.

En la actualidad, no resulta tan simple poder detectar si el dispositivo está infectado, la existencia de un mensaje en la página web, que nos alerta que estamos siendo víctimas de un ataque ya es anticuado, relegado únicamente a algunos grupos de hacktivistas⁷, que intentan demostrar que todavía están activos.

Aunque parezca extraño o increíble, uno debe comprender que si le hackearon el equipo, es muy probable que el atacante no tenga ningún interés en la persona o información que pueda llegar a tenerse, ya que lo más seguro es que no los conozcan. Como lo fuimos mencionando anteriormente, con el tiempo, estos intrusos entendieron que el anonimato resultaba ser mucho más rentable, ya que si no se enteran que están siendo hackeados, podrán ser controlados, es decir; que podrán acaparar recursos, como nuestro teléfono, el cual les permitirá posteriormente realizar acciones mucho más grandes y que les darán un mayor rédito.

Si uno está interesado en tirar abajo una web importante para conseguir su minuto de gloria, debe considerar la cuantiosa suma de dinero que representa costear una granja de servidores para realizar algún ataque de denegación de servicio (haciendo que miles de servidores intenten acceder a la vez a la web atacada, sobrecargando sus servidores con

⁷ Hacktivismo (acrónimo de hacker y activismo también conocido como ciberactivismo) se entiende normalmente "la utilización no-violenta de herramientas digitales persiguiendo fines políticos"

peticiones). Para evitar estos gastos, encontraron una solución mucho más rentable, basándose en hackear miles de sistemas previamente, para controlar sus recursos y preparar este ataque.

Cada ataque deja una serie de huellas de las que se puede aprender y utilizar para comprender a los adversarios y estudiar cómo realizan sus acciones. Esto permitirá diseñar defensas cada vez más efectivas y comprobar si las que tenemos son las más adecuadas.

Pero al tratarse de una secuencia de fases (cadena), una mitigación en cualquiera de ellas romperá la cadena, y, por lo tanto, frustrará el ataque. Por ello, la clave para detectar, detener, interrumpir y recuperarse ante un ciberataque radica en comprender cuál es su ciclo de vida y así desarrollar e implementar todas las operaciones necesarias que garanticen el mayor grado de seguridad y protección

Con esta premisa, las diferentes empresas de antivirus y tecnología, comenzaron a estudiar todos los ataques que se llevaron a cabo en los últimos años, pudiendo entrever que los ataques contra redes de dispositivos y sistemas informáticos suelen constar de etapas o fases, aunque muchas varían en su cantidad o procesos. A continuación, se presentará un modelo que consta de cinco fases, que para el fin que intenta perseguir este ensayo, estimo que resultan pertinente:

2.3.1 Fase 1 – Reconocimiento

Como su nombre lo señala, este es el momento en que el atacante busca a su futura víctima, que puede ser una persona o empresa, realizando una recopilación de información utilizando recursos de internet como por ejemplo el buscador de Google, trabajando mayormente sobre fuente abiertas. Esta es una fase preparatoria, en donde se obtiene la información necesaria y se elige una estrategia antes de lanzar un ataque.

En esta etapa, el hacker se vale de diferentes técnicas para reunir la información, que va desde los **sniffing**, que como dijimos se encargaban de rastrear la información que circula por la web, almacenarla y descifrarla, o el **dumpster diving** (buscar en la basura), en donde buscan el tipo de sistema operativo o aplicaciones de software que utiliza la víctima, localizar los routers, identificar los host más accesibles, buscar en internet

registro de dirección IP, información de contacto, información DNS⁸, cómo toda otra información que imaginemos.

Cómo vimos, la explotación de fuentes abiertas que uno puede llegar a hacer, sumado a la aplicación de estas dos técnicas u otras que están siendo creadas en este momento, nos llegan a ofrecer la suficiente información para dar por superada esta fase, pero si la persona o empresa presenta un nivel de seguridad superior al de los atacantes. No es un misterio que algunas empresas cuentan con equipos de hackers propios que dan respuesta a amenazas de seguridad. En estos casos, ¿qué hacen los atacantes?, cesan la actividad, cambiando de objetivo o resueltos a prevalecer, buscan otra alternativa para ingresar al sistema.

Así es, buscan otra alternativa para extraer información, pero viendo que por el lado del ciberespacio la empresa se encuentra bien protegida, redireccionaron sus técnicas al espectro físico, dando luz a la *“Ingeniería social”*, de la cual diremos es una metodología de investigación, de influencia y de acciones clandestinas que tienen por objetivo comprometer un sistema de información explotando principalmente sus fallos humanos.

Es decir, el ataque de ingeniería social consiste básicamente, en provocar en un objetivo un comportamiento preciso o previsto, explotando cuatro principios: “todos queremos ayudar”, “el primer movimiento es siempre de confianza hacia el otro”, “no nos gusta decir que no” y “a todos nos gusta que nos alaben”. Esta práctica, es usada como elemento de seducción para que, por ejemplo, un empleado por sus propios medios nos otorgue la información que requerimos.

2.3.2 Fase 2 – Escaneo

En esta etapa, es donde se recogerá la información obtenida en la fase anterior y se examina, con el objetivo de buscar huecos de seguridad en los sistemas del objetivo, ya que se puede obtener detalles sobre el sistema operativo que utilizan, los puertos de comunicación abiertos, vulnerabilidades de las aplicaciones y cuentas de usuarios.

⁸ DNS es el acrónimo para “Domain Name System” (sistema de nombre de dominio), es una tecnología fundamentada en una base de datos distribuida que sirve precisamente para traducir estos nombres de dominio en las redes. Es decir, para conocer la dirección IP de la máquina donde está alojado el servicio al que queremos acceder.

En esta segunda fase, el atacante puede emplear diferentes herramientas durante la exploración, como network scanners, network mappers, port scanners, port mappers, y vulnerability scanners.

2.3.3 Fase 3 – Acceso

Tras el análisis de la información recolectada, es en esta fase donde se comenzará a materializar el ataque. Aquí es donde empieza la magia del atacante, ya que este comienza a explotar cada vulnerabilidad que fuera detectada en el sistema durante las fases de reconocimiento y escaneo. Para la explotación de dichas vulnerabilidades, se suelen utilizar herramientas específicas construidas para este fin, las cuales son identificadas como *“exploits”*.

Esto se lleva a cabo, con el objeto de tener acceso al sistema o causar daños en el mismo, ya sea llevándolo a una saturación de los recursos y por ende generando un ataque DoS (Denial of Service): ataques de fuerza bruta para poder adivinar o romper las credenciales de acceso al sistema o secuestro de sesión (Hijacking), a fin de tener el control del sistema y poder explotarlo.

2.3.4 Fase 4 – Explotación

Una vez que el atacante logró ingresar al sistema, se torna primordial mantenerse en el mismo, es decir, mantener la puerta abierta para entrar y salir por el mayor tiempo posible. Para ello buscará implantar herramientas que le permitan volver a ingresar en el futuro desde cualquier lugar donde tenga acceso a Internet, recurriendo a utilidades como rootkits, backdoors y trojanos.

A través de dichas herramientas, se modificarán programas y ficheros del sistema para dejar instaladas determinadas puertas traseras, trojanos o creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado.

2.3.5 Fase 5 – Eliminación de rastros

En esta instancia, y con extrema vinculación al punto anterior, al efecto de poder seguir entrando y saliendo del sistema comprometido, el atacante buscará borrar toda la evidencia que pueda ser utilizada para rastrear su actividad, para no ser detectado por el equipo de seguridad o administradores de la red (software instalados o modificaciones). Para lograr su objetivo, los atacantes utilizan diferentes técnicas, entre las cuales se puede remarcar la “esteganografía”, la cual le proporciona un modo para ocultar esta información (huellas) o para no percibirse su existencia en la red.

En consecuencia, los atacantes tratarán de eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). Asimismo, muchos atacantes llegan incluso a parchar la vulnerabilidad descubierta en el sistema para que no pueda ser utilizada por otros intrusos.

2.4 Conclusión parcial del Capítulo II:

A lo largo del presente capítulo, fui demostrando el riesgo que representa permitir el libre acceso al dispositivo y su conexión a internet, materializados en el robo del dispositivo o la inyección de un programa malicioso. Aunque existan muchas otras prácticas que permiten acceder al equipo de forma física o remota, se debe considerar que las amenazas futuras serán proporcionales a los adelantos de las tecnologías informáticas.

Además, la presencia permanente de diferentes actores que, motivados por intereses políticos, económicos, por simple reconocimiento o venganza, intentarán vulnerar la seguridad de las personas, empresas o Estados, nos presentan el sustento necesario, para considerar al ciberespacio como un nuevo ambiente operacional.

Por ello, solo me resta concluir, que se debe aprender de los incidentes de seguridad, cuyas lecciones darán origen a nuevas propuestas para la implementación de mejoras en los protocolos de seguridad, los cuales deberán complementar los objetivos, políticas y líneas de acción que deberá adoptar la Institución, para reducir significativamente estas vulnerabilidades.

CAPÍTULO III

MEDIDAS DE SEGURIDAD A PRUEBA DE FALLOS

3.1 Doctrina

Muchos usuarios pueden considerar que la seguridad de los teléfonos móviles es menos importante que la seguridad de su computadora personal, pero las consecuencias de los ataques a teléfonos móviles pueden ser igualmente graves. La posibilidad de acceso a la información que brinda la tecnología informática hace que no pueda considerarse que una situación de debilidad en la seguridad informática de un equipo aislado, pueda no tener efectos sobre el conjunto de los sistemas informáticos de una organización.

Entonces, a través del presente capítulo, se evidenciará las medidas de seguridad empleadas para disminuir el grado de vulnerabilidad de la información por parte de la Institución, utilizando como base, el reglamento de Medidas de Seguridad de Contrainteligencia, ya que como bien lo refiere en su alcance, involucrará a toda la Fuerza. No por nada su instrucción se encuentra contemplada en los diferentes planes de estudio en la formación de los Oficiales, Suboficiales y Gendarmes.

En términos generales, dicho documento establece que toda información que posee clasificación de seguridad, no puede ser tratada en equipos que tengan una conexión a la red de internet. Esto representa el primer eslabón en una cadena de fallas a la seguridad, porque existe el concepto erróneo en la identificación de la información con clasificación de seguridad; debiendo entender que no siempre la misma se encuentra acondicionada en una carpeta de color o almacenada en algún dispositivo, dentro de una caja fuerte, pasando completamente desapercibido los artículos que hacen referencia a la imposición de la clasificación de seguridad.

Por otro lado, las limitaciones de materiales por lo general, suelen complicar más la situación, ya que no solo esta información es tratada en equipos que poseen conexión a internet, y que además carecer de toda barrera de seguridad, sino que también, el personal al no contar con medios materiales necesarios para cumplir con sus actividades diarias, suelen

emplear sus propios equipos para poder cumplir con las mismas, lo que conlleva que esa información salga de las instalaciones de la unidad, aumentando significativamente el grado de amenaza.

Pese a esto, el reglamento establece dos grandes vulnerabilidades: la primera es que está sujeto a riesgos de *hardware*, entendiendo que la portabilidad de estos equipos, los hacen susceptibles ante un robo o pérdida, lo cual supone que los atacantes puedan robar, revelar públicamente o vender cualquier información personal o laboral extraída del dispositivo, y si el dispositivo contiene el nombre de usuario y la contraseña del propietario para el servidor, el atacante tendría todo lo necesario para acceder a nuestro sistema.

La segunda es que existe la violación de la seguridad sujeta al *software*, en relación al empleo de softwares maliciosos, que pueden enviar información del dispositivo a los atacantes y realizar otros comandos dañinos, que pueden ser propagados a otros dispositivos al ser vinculados. En tal sentido, el código de Android es abierto, Google liberó Android bajo licencia Apache⁹ permitiendo que cualquier persona pueda diseñar una aplicación para Android y ofrecerla para descargar, careciendo de cualquier tipo de regulación, creando esa falsa seguridad para los usuarios, de creer que, si está en la lista del “play store”, esta aplicación es segura.

3.2 Implementación de regulación Internacional

Además del citado reglamento, considerando que la mayor parte de la seguridad de los teléfonos inteligentes depende de que el usuario haga elecciones cautelosas, la Institución emite de forma paulatina, directivas asociadas a las normas ISO 27001¹⁰, en lo referente a la seguridad de la información, dando un conjunto de buenas prácticas que nos permitan aumentar el grado en la seguridad de los dispositivos y reducir la probabilidad de un ataque, encontrándose entre ellas las que se detallan a continuación:

⁹ La licencia Apache (Apache License o Apache Software License para versiones anteriores a 2.0) es una licencia de software libre permisiva creada por la Apache Software Foundation (ASF). Esta licencia requiere la conservación del aviso de derecho de autor y el descargo de responsabilidad, pero no es una licencia copyleft, ya que no requiere la redistribución del código fuente cuando se distribuyen versiones modificadas.

¹⁰ ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa, permitiendo el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

- a. Al momento de elegir un teléfono, debemos tener en cuenta las características de seguridad, establecer si el dispositivo ofrece cifrado de archivos, identificar la capacidad del proveedor de servicios de buscar y borrar el dispositivo de forma remota, la capacidad de eliminar aplicaciones maliciosas conocidas de forma remota, y la calidad de las funciones de autenticación como contraseñas de acceso al dispositivo.
- b. Si realiza una copia de seguridad de los datos de su teléfono a una PC, resultara necesario buscar una opción para poder cifrar la copia de seguridad.
- c. Si planea usar el dispositivo para acceso VPN¹¹, como suelen hacer los usuarios para acceder a redes de trabajo, se debe preguntar al proveedor si el dispositivo admite autenticación basada en certificados.
- d. Al momento de adquirir un teléfono inteligente, se debe configurar para que sea más seguro, ya que muchos dispositivos poseen funciones de contraseña, que bloquea el dispositivo hasta que se ingresa el PIN o la contraseña correctos. Por ello, el primer paso deberá ser la habilitación de esta función y elegir una contraseña que cumpla con los parámetros de seguridad. Además, servirá de utilidad, habilitar el cifrado, las capacidades de borrado remoto y software antivirus si está disponible.
- e. Se deberá configurar las cuentas web para poder utilizar conexiones seguras. Las cuentas de ciertos sitios web pueden configurarse para utilizar conexiones seguras y cifradas. Habilitar esta función disuade a los atacantes de espiar en la web sesiones. Muchos sitios populares de correo y redes sociales incluyen esta opción.
- f. Siempre dude de los mensajes provenientes de fuentes desconocidas, los mismos pueden contener enlaces que llevan a páginas web maliciosas.
- g. Limitar la exposición de sus datos y número de teléfono. La creciente tendencia de las sociedades, a compartir sin discreción una cantidad significativa de los actos de sus vidas y número de teléfono en diferentes sitios web, permite que los atacantes puedan recopilar esta información y utilizarla para efectuar los ataques.

¹¹ Una VPN (por las siglas en inglés de Virtual Private Network), o red privada virtual, es un túnel seguro entre su dispositivo y la internet. Las VPN protegen su tráfico de internet contra espías, interferencias y censura.

- h. Considerar cuidadosamente qué información se desea almacenar en el dispositivo. Se deberá tener en cuenta que, con suficiente tiempo, sofisticación y acceso al dispositivo, cualquier atacante podría obtener la información almacenada.
- i. Inspeccionar las aplicaciones antes de proceder a su instalación. Se recomienda hacer una investigación previa sobre cualquier aplicación antes de instalarla. Verificar los permisos que requiere la aplicación o si estos pesan más de lo que debería requerir la aplicación.
- j. Mantener el control físico del dispositivo, especialmente en lugares públicos o semipúblicos. La portabilidad de los teléfonos móviles hace que sea fácil perderlos o robarlos.
- a. Desactivar las interfaces que no estén en uso actualmente, como por ejemplo Bluetooth, infrarrojos o Wi-Fi. Los atacantes pueden aprovechar las vulnerabilidades del software que utiliza estas interfaces.
- b. Configurar los dispositivos habilitados para Bluetooth en no detectables. Cuando está en modo visible para otros dispositivos cercanos, puede alertar a un atacante o vincularse con algún dispositivo infectado.
- c. Evitar unirse a redes wi-fi desconocidas y utilizar puntos de acceso wi-fi públicos. Los atacantes pueden crear puntos de acceso wi-fi falsos diseñados para atacar teléfonos móviles o pueden acceder a dispositivos no seguros que estén conectados a redes públicas de wi-fi.
- d. Eliminar toda la información almacenada en un dispositivo antes de descartarlo. Consultar el sitio web del fabricante del dispositivo para obtener información sobre cómo eliminar datos de forma segura. El proveedor de telefonía también puede tener información útil sobre cómo borrar de forma segura su dispositivo. Tenga cuidado al utilizar aplicaciones de redes sociales. Estas aplicaciones pueden revelar más información personal de la prevista y a terceros no deseados. Tener especial cuidado cuando se utilizan servicios de rastreo.

- e. Informar de forma inmediata la pérdida o extravió del teléfono inteligente, ya que esto le permitirá a la Institución bloquear los usuarios que posea para ingresar al sistema o banco de datos de la organización. Además, será conveniente comunicarse con su proveedor de servicios de telefonía móvil lo antes posible, para disuadir el uso malintencionado de su dispositivo y minimizar los cargos fraudulentos. Por último, se deberá radicar la correspondiente denuncia ante la autoridad policial, ya que esto puede evitar futuros problemas judiciales, en caso de su uso malintencionado.
- f. Cambiar las credenciales de la cuenta. Si usó su teléfono para acceder a redes corporativas o sitios de redes sociales, habrá que revocar todas las credenciales que se almacenaron en el dispositivo perdido.
- g. En estos casos, será necesario efectuar la limpieza del equipo. Algunos proveedores de servicios ofrecen un borrado remoto, lo que nos permite eliminar de forma remota todos los datos del teléfono.

3.3 Conclusiones parciales del Capítulo III

La Institución, cumple un papel protagónico en el establecimiento de una necesidad de seguridad en el tratamiento de la información, ya que le recae la responsabilidad de generar esas políticas y procedimientos de seguridad, que garanticen la protección de los sistemas e información.

Para ello, deberán capacitar al personal para forjarle una verdadera cultura de ciberseguridad, la cual les impondrá el compromiso a los diferentes usuarios del sistema de información y todos aquellos integrantes de la organización, de participar de forma activa para que el sistema cumpla con los requerimientos, manteniendo en todo momento su integridad.

CONCLUSIONES GENERALES

El impacto de la globalización que va acompañando la creciente implantación de nuevas tecnologías, materializado en el avance del fenómeno de la BYOD, se transformó en una tendencia que puede traer grandes beneficios relacionados con la disminución de gastos en infraestructura, la comodidad del personal para el manejo de la información y por tanto el incremento de la productividad.

Como hemos visto, cuando se habla de BYOD se hace referencia a una tendencia consolidada y ante la cual, la Institución debe hacer un análisis de riesgo para tomar una posición al respecto. La sinergia entre la persona, proceso y tecnología, resulta difícil de controlar y restringir, convirtiendo su adopción en grandes problemas de seguridad y de protección de datos y privacidad con los cuales la organización tendrá que enfrentarse.

Entonces, se puede concluir a través del análisis efectuado a lo largo del presente ensayo, que los activos de información de áreas consideradas críticas y el empleo de las medidas de seguridad destinadas a tal fin, reflejan un potencial índice de riesgo, ya que dejan expuesta la información a cualquier tipo de robo, daño o alteración que pueda sufrir el usuario y que puedan traer consecuencias catastróficas en la organización, vulnerando los principios de confidencialidad, integridad o disponibilidad de la información.

En consecuencia, la Institución se enfrenta a estas nuevas amenazas que deben ser gestionadas, exigiendo por parte de ella una actitud proactiva, desde la implementación de análisis de riesgos, cuya evaluación permitirá definir medidas y contramedidas que garanticen poder reducir, mitigar o evitar estas amenazas, hasta la adopción de políticas de seguridad como estrategia general, para establecer controles de seguridad acorde a la realidad y necesidad actual de la Fuerza, sin dejar de lado la educación del personal para que logren percibir el verdadero riesgo que esto representa y sepan cómo enfrentarlo.

Bibliografía

- ✚ Auditoría, consejo, instalación y seguridad de sistemas de información ACISSI (septiembre de 2015), Seguridad Informática: Hacking ético, conocer el ataque para un mejor defensa, Barcelona, Editorial ENI.
- ✚ Avast Software S.R.O. (28 de septiembre del 2019). Seguridad de los Sistemas, <https://www.avast.com/es-es/c-category-security>.
- ✚ Avast Software S.R.O. (19 de mayo del 2020). ¿Qué es un Malware?. <https://www.avast.com/es-es/c-malware#topic-1>.
- ✚ GOMEZ VIEITES, Álvaro (2014), Gestión de incidentes de seguridad informática, Madrid, editorial RA-MA.
- ✚ GARCÍA FERNÁNDEZ, Fernando (2007), Ética e Internet – Manzanas y serpientes. Madrid, editorial RIALO S.A.
- ✚ HERNÁNDEZ, Claudio (2001), Hackers – Los piratas del chip y de internet. Barcelona. editorial VLex.
- ✚ MERINO DABA, Cristina y CAÑIZARES SALES, Ricardo (2014), Auditoria de sistemas de la gestión de la seguridad de la información, Madrid, editorial FC.
- ✚ Observatorio Argentino de Ciberespacio (25 de junio del 2018). Ciberseguridad, Elecciones e infraestructura critica en el hogar y en el exterior. <http://www.esgcffaa.edu.ar/esp/oac-boletines.php>.
- ✚ Oficina de lucha contra el terrorismo de las Naciones Unidas (2019), La seguridad cibernética. <https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity>.
- ✚ Observatorio ciberseguridad (2020), Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y El Caribe, <https://www.observatoriociberseguridad.com>.
- ✚ PEIRANO, Marta (enero de 2015), El pequeño libro rojo del activista en la red, Barcelona, Editorial Rocaeditorial.
- ✚ RCG-16-02 (2000), Reglamento de Contrainteligencia y Medidas de Seguridad de Contrainteligencia de Gendarmería Nacional Argentina.

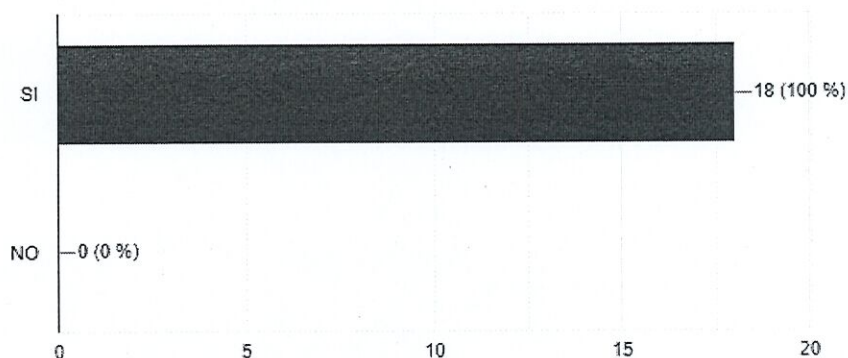
Anexo I

Encuesta

Anexo I: Resultado de la encuesta formulada al personal de cursantes del Instituto de Inteligencia de las Fuerzas Armadas, ciclo lectivo 2020, en relación al empleo de los teléfonos inteligentes particulares en el ámbito laboral. -----

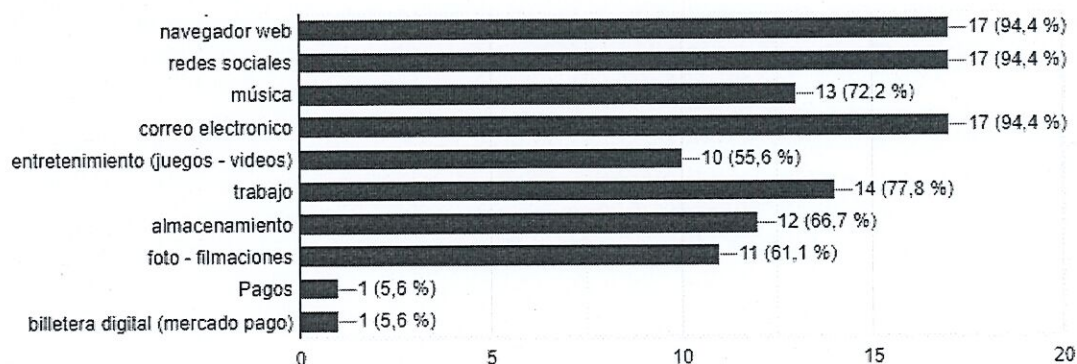
¿Posee un telefono inteligente?

18 respuestas



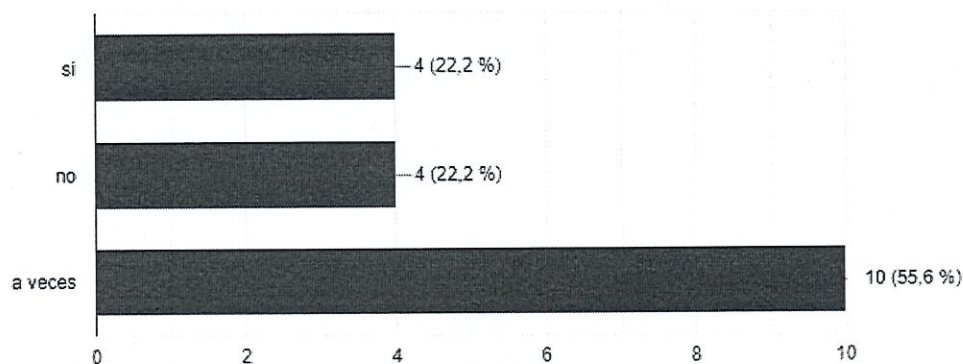
¿Qué actividad desarrolla con este dispositivo?

18 respuestas



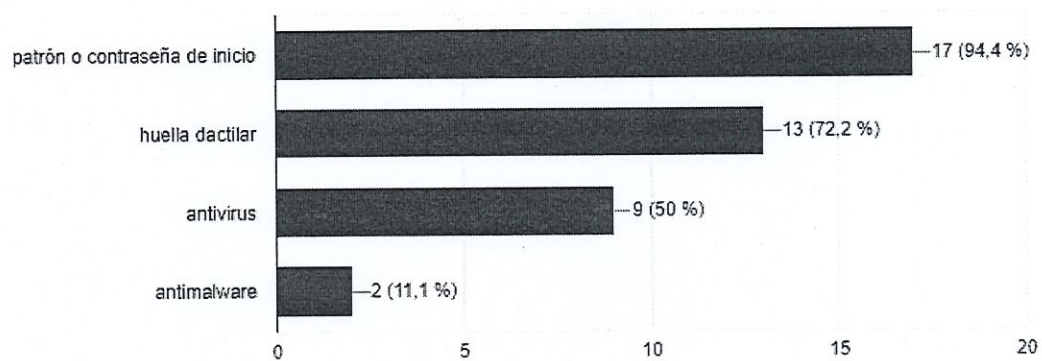
¿Suele navegar por sitios web que no estan protegidos?

18 respuestas



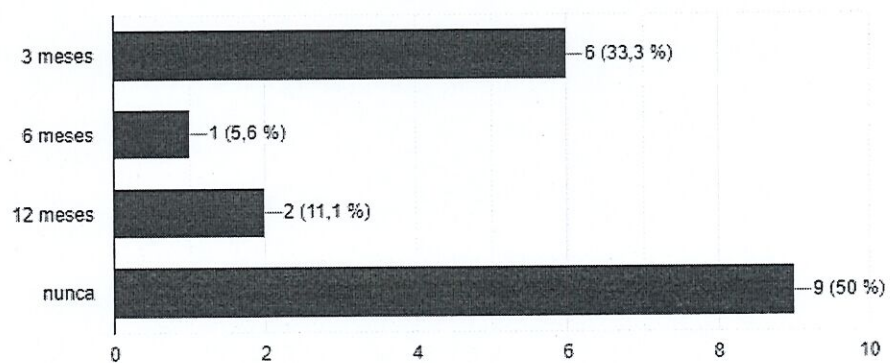
¿Como protege su dispositivo?

18 respuestas



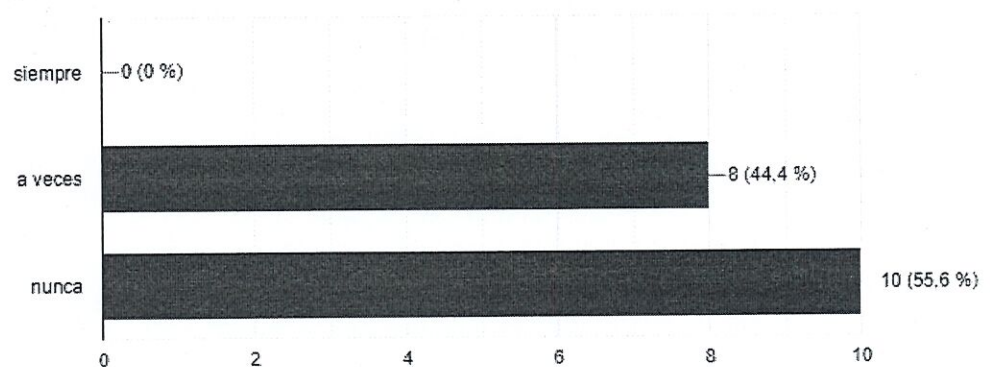
¿Cambia la contraseña de su dispositivo con regularidad?

18 respuestas



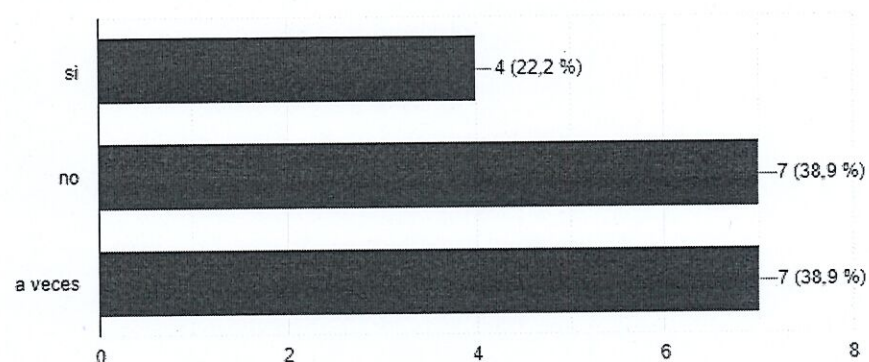
Al instalar una aplicacion, ¿lee los terminos y condiciones?

18 respuestas



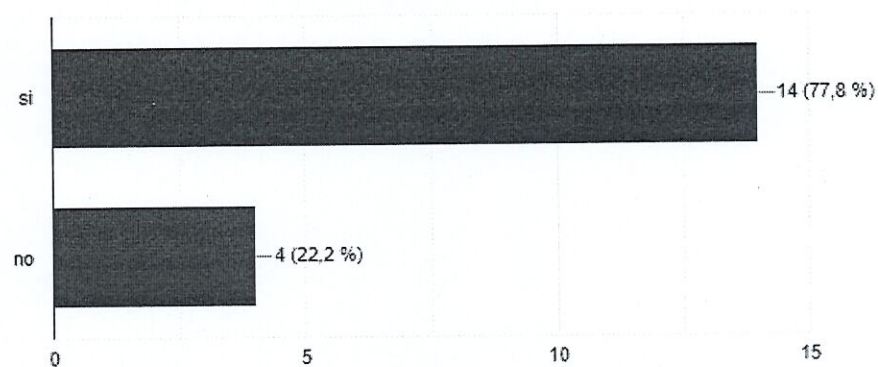
¿Suele descargar aplicaciones de fuentes no oficiales?

18 respuestas



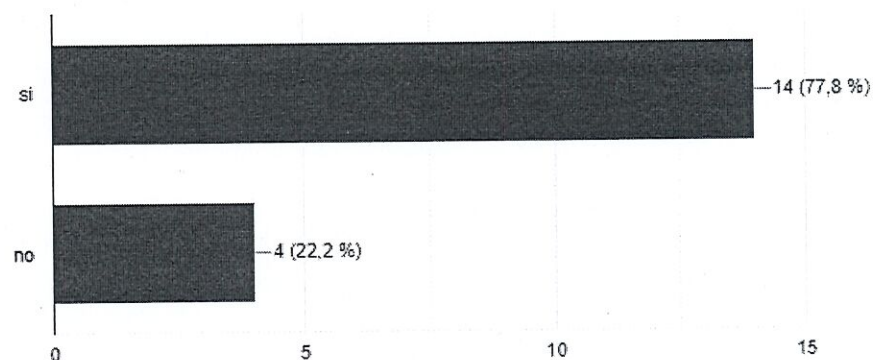
¿Se conectó alguna vez a una red pública?

18 respuestas



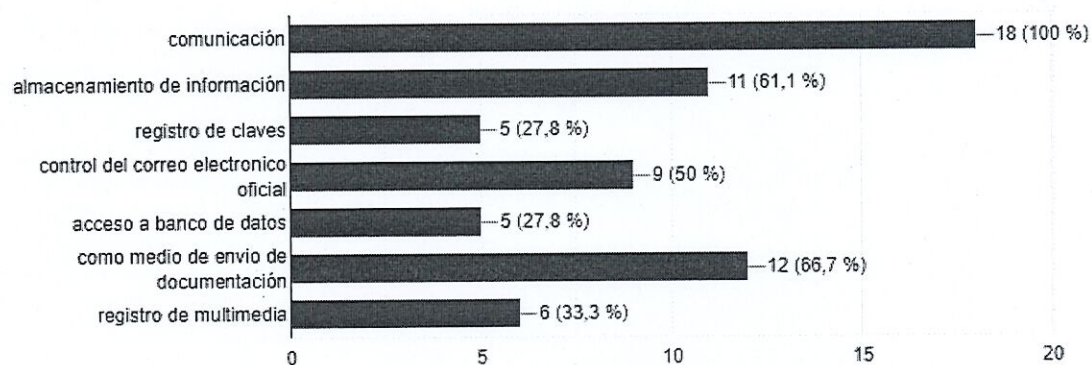
¿Se conecta asiduamente a la red privada de su entorno laboral?

18 respuestas



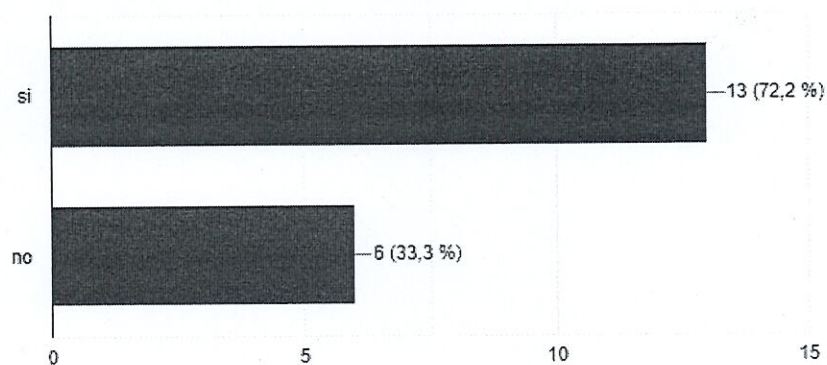
¿Que función le da al telefono inteligente en su ambito laboral?

18 respuestas



¿Fue victima o tiene conocimiento de alguien en su entorno que haya sido victima de Phishing?

18 respuestas



Al momento de realizar esta encuesta, ¿Posee información laboral en su dispositivo?

18 respuestas

