La tendencia "Bring Your Own Device" o el uso de información corporativa sensible en dispositivos electrónicos personales para el sector Defensa en Colombia.

Javier Orlando Betancourt Nova

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

La tendencia "Bring Your Own Device" o el uso de información corporativa sensible en dispositivos electrónicos personales para el sector Defensa en Colombia.

Mayor
Javier Orlando Betancourt Nova

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2020

Durante todo el proceso de investigación, cualquier persona que advierta una situación de plagio, dará informe de ello al Director del Programa, quien seguirá el conducto establecido por el Reglamento Académico para adelantar el correspondiente proceso, además de dar aviso a las autoridades públicas competentes de la investigación y enjuiciamiento de conductas punibles.

7. **CUMPLIMIENTOS Y REQUISITOS PARA OPTAR EL GRADO.**

El cumplimiento de todos y cada uno de los requisitos descritos en este instructivo será verificado por la Coordinación del Área de Investigaciones del Programa, rindiendo informe de su cumplimiento al Director del Programa y a la Coordinación Académica del Programa.

7.1 Las versiones finales de los trabajos, así como la sustentación serán evaluadas por tres jurados establecidos por la Maestría.

7.2 Una vez se apruebe la sustentación del trabajo de grado, el estudiante deberá entregar en la oficina de la Maestría, dos (02) copias empastadas con las siguientes características:

Pasta dura, el color depende de la maestría, letras doradas, incluyendo los siguientes datos además de un CD que contenga el trabajo de grado en Word y la presentación de la sustentación.

En la portada:

TRABAJO DE GRADO

"TITULO"

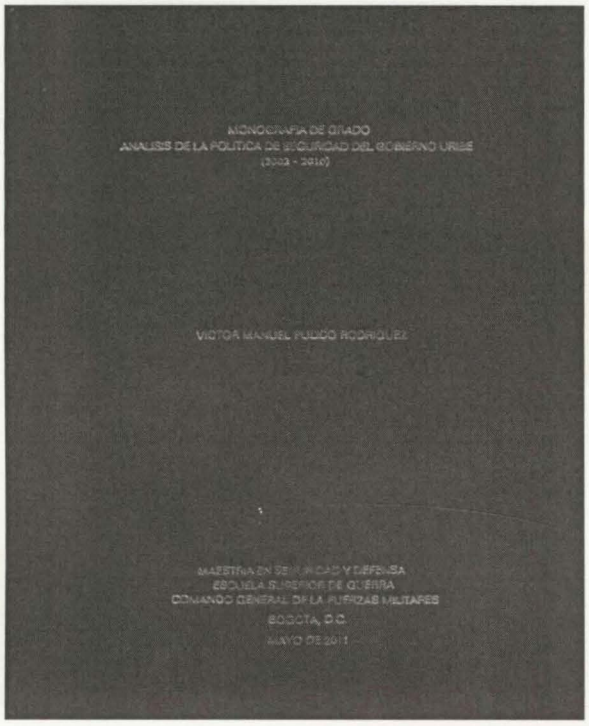
AUTOR

MAESTRÍA EN ...

ESCUELA SUPERIOR DE GUERRA

COMANDO GENERAL FUERZAS MILITARES

BOGOTÁ D.C., FECHA

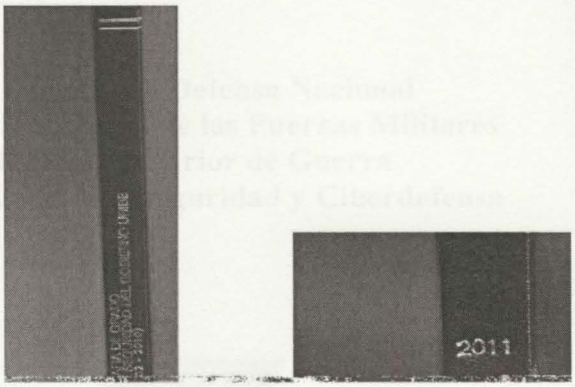


En el lomo (escritura en forma vertical):

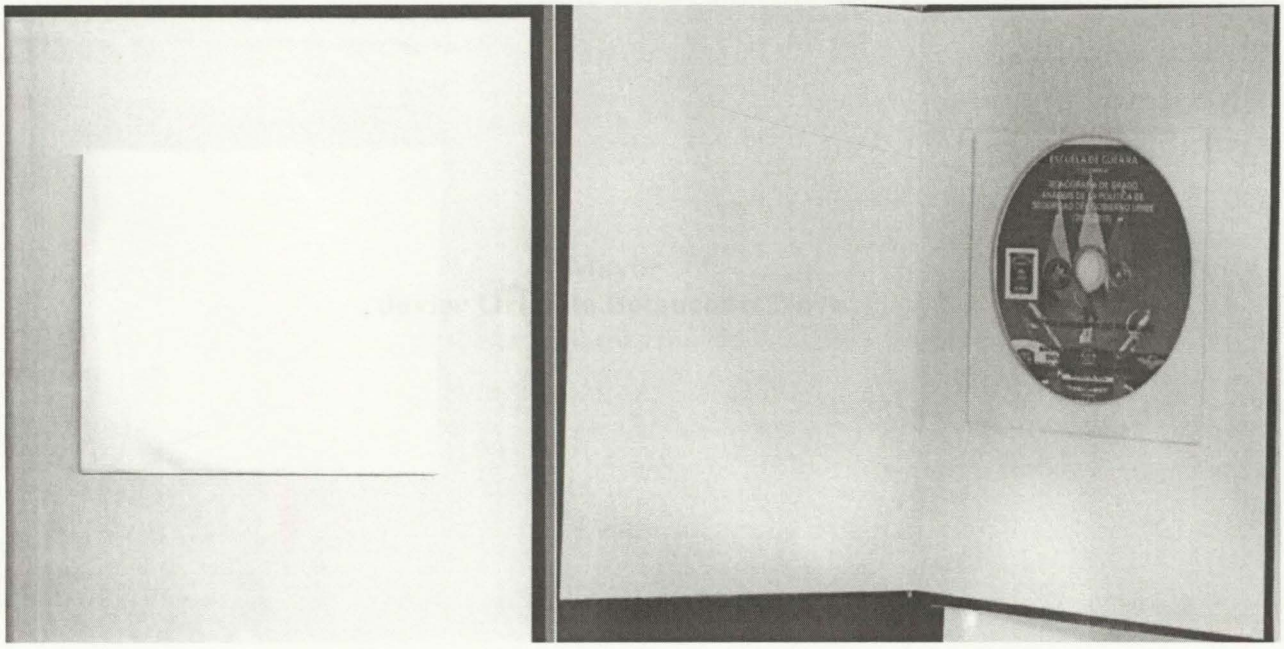
MONOGRAFÍA DE GRADO Y EL "TITULO"

En el lomo (escritura en forma horizontal en la parte inferior)

EL AÑO (2020)



En la solapa trasera va un CD:



En la contraportada: no se escribe nada.

5. BIBLIOGRAFÍA

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

La tendencia "Bring Your Own Device" o el uso de información corporativa sensible en dispositivos electrónicos personales para el sector Defensa en Colombia.

Mayor
Javier Orlando Betancourt Nova

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2020

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

Mayor
Javier Orlando Betancourt Nova

Director:
Doctor Fabio Alberto Salazar Lopera

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2020

Dedico este trabajo a Dios, quien en su infinita misericordia me permitió culminar con éxito esta etapa de mi vida.

"Como palmeras florecen los justos;
como cedros del Líbano crecen.
Plantados en la casa del Señor,
florecen en los atrios de nuestro Dios.
Aún en su vejez, darán fruto;
siempre estarán vigorosos y lozanos,
para proclamar: «El Señor es justo;
él es mi Roca, y en él no hay injusticia»".
Salmo 92:12-15

Agradecimientos

Agradezco a Dios por haberme acompañado en el camino todos los días de mi vida.

A mi esposa Mónica, quien me dio su apoyo incondicional y siempre me ofreció una palabra de aliento cuando la necesitaba. Este también es un logro tuyo.

A mis padres, Laureano y Alcira, quienes me formaron en principios y valores y me enseñaron que los límites son mentales y que de la mano de Dios todo es posible.

Al Doctor Fabio Alberto Salazar Lopera, por su valiosa orientación y asesoría en la realización del presente trabajo de grado.

Y agradezco a todos los que me brindaron su apoyo para la culminación de este trabajo.

Resumen Ejecutivo

Este trabajo de grado tiene como objetivo estudiar a profundidad el fenómeno del uso de dispositivos móviles personales para actividades laborales específicamente en el sector Defensa de Colombia. En primera instancia se analiza el estado del arte del "Bring Your Own Device" (BYOD) a nivel mundial, regional y nacional, para luego establecer su penetración en el sector Defensa de otros países. Posteriormente se analizan varias investigaciones y frameworks que diferentes autores han planteado al respecto, con el fin de identificar puntos comunes. Luego se realiza un análisis de riesgos de la implementación de este tipo de prácticas en las organizaciones, particularmente en aquellas que pueden manejar información sensible como instituciones pertenecientes al sector Defensa. Finalmente se proponen algunos aspectos a considerar y un marco de buenas prácticas para la implementación de BYOD en instituciones del sector Defensa en Colombia. El análisis de la información obtenida a través de la investigación realizada sugiere que la tendencia BYOD ha venido teniendo cada vez más aceptación, especialmente en actividades educativas y académicas. En cuanto a actividades relacionadas con el sector Defensa a nivel global, si bien es cierto que inicialmente existió bastante resistencia hacia este tipo de prácticas, la reducción de presupuestos y la aparición de nuevas herramientas tecnológicas han logrado que cada vez más se amplíe la visión de competitividad que esta tendencia puede tener y el impacto que puede lograr en cierto tipo de actividades que no comprometan información clasificada o restringida. El análisis de riesgos realizado muestra que a pesar de ser un tema delicado y de alto impacto en las organizaciones, a través de planes fuertes de mitigación es posible asumir los riesgos inherentes a esta práctica. Por último, se proponen algunas buenas prácticas y aspectos a considerar que permitan a las instituciones pertenecientes al sector Defensa en Colombia, implementar y facilitar la adopción del BYOD en cierto tipo de actividades que se fortalezcan por medio del uso de la tecnología.

Palabras claves: BYOD, política, seguridad, información, defensa, dispositivo móvil, framework, clasificación de la información.

Abstract

The aim of this graduate work is to study in depth the phenomenon of the use of personal mobile devices for work activities specifically in the defense sector of Colombia. The first step is to analyze the state of the art of the "Bring Your Own Device" (BYOD) at global, regional and national level, and then to establish its penetration in the defense sector of other countries. Subsequently, several researches and frameworks that different authors have raised in this regard are analyzed in order to identify common points. Next, a risk analysis of the implementation of this type of practices in the organizations is carried out, particularly in those that can handle sensitive information such as institutions belonging to the Defense Sector. Finally, some aspects to consider and a framework of good practices for the implementation of BYOD in institutions of the Defence sector in Colombia are proposed. The analysis of the information obtained through the research suggests that the BYOD trend has been increasingly accepted, especially in educational and academic activities. With regard to activities related to the defense sector at a global level, although it is true that there was initially considerable resistance to this type of practice, the reduction in budgets and the appearance of new technological tools have led to an increasing increase in the vision of competitiveness that this trend may have and the impact it may have on certain types of activities that do not compromise classified or restricted information. The risk analysis carried out shows that despite being a delicate and high impact issue in the organizations, through strong mitigation plans it is possible to assume the risks inherent to this practice. Finally, some good practices and aspects to be considered are proposed to allow institutions belonging to the defense sector in Colombia to implement and facilitate the adoption of BYOD in certain types of activities that are strengthened through the use of technology.

Keywords: BYOD, policy, security, information, defense, mobile device, information classification.

Lista de abreviaturas y siglas

BYOD	:	Bring Your Own Device – Trae tu propio dispositivo
BYOT	:	Bring Your Own Technology – Trae tu propia tecnología
CIO	:	Chief Information Officer – Oficial Jefe de Información
COBO	:	Company Owned, Business Only – Propiedad de la compañía
COPE	:	Corporate Owned, Personally Enabled - Propiedad de la compañía
CYOD	:	Choose Your Own Device – Elige tu propio dispositivo
DoD	:	Departamento of Defense – Departamento de defensa
EMM	:	Enterprise Mobility Management – Gestión de movilidad empresarial
GPS	:	Global Position System – Sistema de Posicionamiento Global
ICISP	:	Conferencia Internacional de seguridad de la información y privacidad
IJACSA	:	International Journal of Advanced Computer Science and Applications
ISO	:	International Standard Organization
MDN	:	Ministerio de Defensa Nacional
MDM	:	Mobile Device Management – Grstión de dispositivos móviles
NCI	:	Agencia de Comunicaciones e Información
NTC	:	Norma Técnica Colombiana
OTAN	:	Organización Tratado del Atlántico Norte
TIC	:	Tecnologías de Información y Comunicaciones
TMF	:	Trabajo de Fin de Máster
US	:	United States – Estados Unidos
USM	:	University Sains Malaysia – Universidad Sains Malasia

Contenido

Introducción

Los dispositivos electrónicos como los teléfonos inteligentes se han convertido en elementos indispensables para el desarrollo de las labores diarias de personas que se desempeñan en diferentes niveles de una organización, ya sea en el nivel operativo, gerencial o directivo. De hecho, las compañías han entendido que el uso eficiente de la tecnología puede aportar ventajas significativas frente a la competencia, por lo cual ya es una tradición que se destinen importantes recursos a la permanente actualización y adquisición de tecnología. Estas adquisiciones tecnológicas contemplan medios y métodos de protección de la información, ya que las organizaciones son conscientes de la necesidad de protección del activo más valioso de una empresa: la información.

Sin embargo, en algunos casos los recursos destinados para la adquisición de tecnología no son suficientes para otorgar a todos los miembros de la organización los dispositivos requeridos para su diaria labor. A pesar de ello, el ritmo acelerado y la necesidad de compartir información de manera inmediata, hace que los funcionarios busquen soluciones para lograr cumplir con sus metas en el tiempo requerido, por lo cual muchos de ellos optan por adquirir y emplear dispositivos de uso personal para desarrollar actividades y procesos de carácter institucional. Dichas adquisiciones de carácter personal muchas veces no contemplan la protección de los datos como prioridad.

Este escenario no es desconocido para el sector Defensa en Colombia. Debido a la gran cantidad de miembros de las fuerzas, a las limitaciones presupuestales y a la facilidad de adquisición de tecnología para los usuarios a costos cada vez menores, la tendencia ha girado vertiginosamente hacia el uso de dispositivos personales para la transmisión, procesamiento y manipulación de datos e información (en algunos casos reservada, clasificada y/o secreta), exponiendo de manera preocupante la información institucional a los peligros del ciberespacio, y sin una reglamentación que permita la integración de este tipo de dispositivos de una manera segura. Por ello, este trabajo de grado busca investigar sobre el uso de dispositivos móviles personales para actividades laborales, tendencia conocida a nivel mundial como "Bring Your

Own Device" (BYOD). En primer lugar, se identifica cómo esta tendencia ha venido creciendo a nivel mundial, regional y nacional. Posteriormente la investigación se centra en las fuerzas militares y sector Defensa a nivel mundial, analizando cuál ha sido su reacción frente al BYOD. Luego se analizan varios estudios e investigaciones que se han realizado al respecto en diferentes países, algunos de los cuales proponen diferentes marcos de referencia o frameworks para que las organizaciones adopten BYOD de manera más segura. De igual manera se desarrolla un estudio del marco normativo y legal que afecta la posible implementación del BYOD en el sector Defensa en Colombia y como complemento se incluye el análisis de una encuesta de percepción realizada con el fin de medir la percepción que se tiene sobre el BYOD en Colombia.

Luego de revisar la información encontrada, se propone una evaluación y análisis de riesgos que se deben tener en cuenta para estudiar la viabilidad de implementación de BYOD en este tipo de instituciones. Este análisis de riesgos se basa en la norma NTC/ISO 27005 y en algunos estudios y frameworks realizados al respecto.

Por último, este trabajo propone algunos aspectos a tener en cuenta para la implementación de ambientes BYOD en instituciones del sector analizado, partiendo de las ventajas y desventajas que tiene esta tendencia, pasando por los aspectos clave que debe incorporar una política de BYOD. Finalmente, se enuncian algunas buenas prácticas tanto para la creación de la política, como para la implementación de la misma y para el fomento de la seguridad en dispositivos móviles, tendiente a concientizar a los funcionarios de la importancia de proteger su información tanto personal como corporativa. En resumen, este trabajo responde a la pregunta: ¿Cuál podría ser un marco de referencia para implementar entornos BYOD para las instituciones que conforman el sector Defensa en Colombia?

Metodología

Este trabajo obedece a un tipo de investigación que utiliza el método analítico-descriptivo. Es analítico, dado que se estudia y analiza la tendencia de emplear dispositivos móviles personales en actividades laborales. Es descriptivo, puesto que se establecen aspectos a tener en cuenta para una correcta evaluación de riesgos de las entidades, así como se describen algunas de las mejores prácticas a tener en cuenta con el fin de implementar entornos BYOD en las organizaciones pertenecientes al sector Defensa en Colombia.

Con respecto a la investigación, en primera instancia se contextualiza al lector sobre qué es el BYOD, cual ha sido el impacto del mismo en las organizaciones y cuál ha sido su crecimiento a través de los años, visto desde una perspectiva global, regional y nacional. Posteriormente se analiza el comportamiento que ha tenido esta tendencia a nivel de entidades militares y organizaciones de seguridad y defensa nacional en todo el mundo. Luego se verifica que estudios e investigaciones se han realizado al respecto y se analiza el marco legal y jurídico que puede aplicar a la implementación de entornos BYOD en el país.

Con base en la información recopilada, se realiza un diseño metodológico para obtener un modelo de evaluación de riesgos. Para lograrlo, se toman como referencia varios documentos que proponen algunos frameworks y análisis de riesgos a tener en cuenta en BYOD y se adaptan al sector Defensa. Posteriormente, se establecen algunos aspectos a considerar, un análisis de ventajas y desventajas de BYOD, para finalizar presentando un conjunto de buenas prácticas para la adopción del BYOD en el sector Defensa, tanto para la creación de políticas, pasando por la implementación del entorno y terminando con algunos aspectos de seguridad en dispositivos móviles.

1. Capítulo uno. Marco teórico conceptual

Este capítulo introduce al lector en el campo de investigación, mostrando cuál ha sido el impacto de la tendencia del BYOD a nivel global. De igual manera analiza diversos estudios e investigaciones realizadas con respecto a esta tendencia, que puedan servir como referencia para el marco de buenas prácticas a desarrollar. Finalmente se analiza el contexto legal de esta tendencia en el marco legal colombiano.

1.1 Bring Your Own Device

"Bring your own device" ("trae tu propio dispositivo" en inglés), abreviado BYOD, es una política empresarial consistente en que los empleados lleven sus propios dispositivos 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. También se le conoce como *"Bring your own technology"* (BYOT, "trae tu propia tecnología"), ya que de esta manera se expresa un fenómeno mucho más amplio, que no sólo se refiere al equipo, sino que también cubre al software.

El término tiene su origen en algunos bares y restaurantes de Inglaterra a mediados de los noventa, cuanto este tipo de establecimientos, con el fin de atraer clientes jóvenes, universitarios y de presupuestos limitados, establecieron noches de "bring your own bottle (BYOB)" ("trae tu propia botella"), refiriéndose a que los clientes podían traer su propia botella de vino al restaurante para alivianar los costos de la cuenta. Posteriormente en los Estados Unidos se hicieron populares las fiestas "bring your own beer" ("trae tu propia cerveza"), las cuales eran llevadas a cabo por jóvenes universitarios con pocos recursos disponibles. Fue aproximadamente en 2009 cuando el término dio el salto hacia la tecnología, popularizando el término "Bring your own device" (BYOD) (Cabrera, J., 2013).

Es importante mencionar que existen actualmente otros modelos de movilidad empresarial además del BYOD (R. N. Akram, 2016). A continuación, se enumeran algunos de ellos:

- CYOD (Choose Your Own Device): este modelo propone que los empleados de la empresa puedan elegir el dispositivo que van a usar de un listado aprobado previamente por la entidad. Es importante mencionar que en este modelo es la compañía la que adquiere el dispositivo y asume su costo, aunque en algunos casos se permite que el mismo pase a pertenecer al empleado ya sea como un obsequio o por medio de planes de financiamiento ofrecidos por la empresa.

- COPE (Corporate Owned, Personally Enabled): en este caso, la empresa adquiere los dispositivos para entregárselos a los empleados para el desarrollo de sus actividades laborales, sin embargo, permite el uso de algunas aplicaciones y características para actividades de tipo personal.

- COBO (Company Owned, Business Only): este modelo propone que la empresa adquiera los dispositivos para el uso de sus empleados, pero limita su uso a actividades netamente laborales. Es el modelo más restrictivo de todos.

Con el fin de establecer cuál de los modelos existentes es el que más se ajusta a las necesidades de las entidades que conforman el sector Defensa en Colombia, se realizó una valoración cuantitativa de cada uno de los modelos. Para ello se identificaron las principales variables que impactan en todos los modelos descritos y a cada una de ellas se le asignó un peso específico con base en las condiciones y relevancia que presenta desde el punto de vista del sector Defensa en Colombia. Posteriormente, se le dio a cada variable una valoración en cada modelo, establecida en tres posibles estados: Alto (equivalente a 1 punto), medio (equivalente a 2 puntos), y bajo (equivalente a 3 puntos). Luego se multiplicó el peso de cada variable por la valoración en cada uno de los modelos, y finalmente se sumaron los puntos obtenidos en cada variable para asignar un puntaje de cada modelo. Los resultados de la valoración cuantitativa de presentan en la siguiente tabla:

VARIABLES A CONSIDERAR		BYOD		CYOD		COPE		COBO	
VARIABLE	PESO	VALOR	PUNTOS	VALOR	PUNTOS	VALOR	PUNTOS	VALOR	PUNTOS
Presupuesto requerido para su instalación	10	Bajo(3)	30	Medio(2)	20	Alto(1)	10	Alto(1)	10
Autorización explicita del empleado	5	Alto(1)	5	Medio(2)	10	Medio(2)	10	Alto(1)	5
Tiempo requerido para aprendizaje	7	Bajo(3)	21	Medio(2)	14	Medio(2)	14	Alto(1)	7
Costos de mantenimiento de dispositivos	8	Bajo(3)	24	Medio(2)	16	Alto(1)	8	Alto(1)	8
Impacto legal de implementación	7	Alto(1)	7	Medio(2)	14	Medio(2)	14	Medio(2)	14
Vulnerabilidades inherentes a la implementación	4	Medio(2)	8	Medio(2)	8	Medio(2)	8	Medio(2)	8
Riesgos inherentes a la implementación	5	Alto(1)	5	Alto(1)	5	Alto(1)	5	Alto(1)	5
PUNTAJE TOTAL		100		87		69		57	

Fuente: elaboración propia

Como se puede apreciar, dadas las condiciones particulares que se presentan en las instituciones que conforman en sector Defensa en Colombia, la valoración sugiere que le modelo BYOD es el más indicado a implementar. Esto se puede evidenciar, por ejemplo, tomando como base la variable "Presupuesto requerido para su instalación". En el caso del Ejército Nacional, una institución con más de 250.000 miembros activos, es prácticamente imposible que se puedan adquirir dispositivos móviles para cada uno de sus empleados (dentro de los que se cuentan oficiales, suboficiales, soldados y personal civil) con recursos propios del Ejército. De hecho, según datos consultados al Comando de Ingenieros del Ejército (quien tiene la responsabilidad de la adquisición y suministro de teléfonos celulares institucionales), actualmente el Ejército cuenta tan sólo con aproximadamente 1500 teléfonos celulares adquiridos y pagados con recursos propios. Inclusive dicho comando manifestó que cada año se recorta un porcentaje de la partida destinada para tal fin. Tomando este ejemplo, dado que los modelos CYOD, COBO y COPE se basan en que la entidad adquiera los dispositivos, dichos modelos son más costosos de implementar, y por ende debemos optar por BYOD como alternativa para las instituciones que conforman el sector Defensa.

A continuación, se profundiza en el estado del arte del modelo BYOD, en primer lugar, en un contexto global o mundial, para pasar a analizar el contexto regional y nacional. Posteriormente se describirá la forma como el BYOD ha interactuado con entidades del sector Defensa en todo el mundo. Luego se realiza un estudio de diferentes investigaciones realizadas sobre la seguridad de BYOD y algunos marcos de referencia propuestos por expertos, para culminar con un estudio de la normatividad nacional vigente que tiene relación con el tema.

1.2 Contexto global

El portal CYBERKNOWLEDGE, en su artículo del 15 de noviembre de 2013 llamado *"Why the BYOD trend is so popular"*, indica que esta tendencia permite a las empresas lograr sus metas de producción sin necesidad de realizar grandes inversiones en hardware y software. Este artículo informa que el 38% de los CIO[1] de los Estados Unidos creían que para finales de 2012 podrían ofrecer soporte a la tendencia BYOD, mientras que el 80% de las compañías encuestadas en 2013 mencionó que permiten a sus trabajadores el uso de dispositivos móviles comprados por ellos mismos para actividades laborales.

El artículo menciona que algunas de las razones por las cuales esta tendencia está en crecimiento son:

- A los empleados les gusta, y lo toman como un incentivo.
- Ahorra dinero a las compañías, al evitar que se empleen recursos de la empresa en adquisición de dispositivos.
- Incrementa la productividad y la eficiencia, ya que se ha demostrado que esta tendencia en un entorno de trabajo realmente fomenta la productividad.
- Simplifica la infraestructura de TI. Si se permite a los empleados utilizar sus propios dispositivos, tal filosofía simplifica enormemente la infraestructura informática de la empresa. Adicionalmente, permite a los departamentos de TI centrarse más en la estrategia, mientras se reduce la gestión de dispositivos de usuario final.

---

[1] Chief Information Officers

- Es una práctica de negocios alineada con el siglo 21. Con dispositivos móviles cada vez más potentes y asequibles, no hay duda de que cada vez más empresas adopten políticas BYOD en el futuro. Y como se puede ver claramente, esta es una rara nueva "mejor práctica" que la gente está realmente dispuesta a seguir. Beneficia a empleadores y empleados por igual.

Por otra parte, el portal Facility Executive en su artículo *"Growing Bring Your Own Device (BYOD) Market Driven By Employee Behavior"*, del 23 de diciembre de 2014, nos ofrece unas cifras muy interesantes. El artículo estima que el mercado BYOD crecerá de $29,5 mil millones de dólares en 2014 a $89,6 millones de dólares en 2019, a una tasa CAGR[2] del 24% desde 2014 a 2019. También comenta que entre los años 2012 y 2013 se incrementó en un 14% el porcentaje de PYMES que tienen soporte de BYOD para sus empleados, mientras que para el año 2014 se estimaba que por cada empleado se tendrían 3.3 dispositivos conectados. El artículo finaliza informando que se esperaba que el mercado europeo de BYOD crezca de US$19,35 mil millones en 2013 a US$74.70 mil millones en 2019, a una tasa CAGR del 25,2% durante el período previsto.

La multinacional de seguridad informática Trend Micro Inc, en su informe *"The Case of Making BYOD Safe"* del 29 de mayo de 2015, advierte que, aunque es una tendencia prácticamente imparable en empresas de todo tipo, su adopción trae algunos riesgos en cuanto a seguridad informática se refiere. Para fundamentar esta afimación, nos ofrece algunas cifras interesantes: para el año 2015 en los Estados Unidos, el 82% de las compañías permiten que sus empleados usen sus propios dispositivos para el trabajo; el 90% de los empleados usan sus propios teléfonos inteligentes en el trabajo; el 70% de los empleados usa los dispositivos móviles proporcionados por las compañías para descargar y usar aplicaciones de uso personal. Por otro lado, en cuanto a brechas de seguridad, el informe muestra que el 40% de los casos de fuga de información corporativa se producen por la pérdida o robo de dispositivos móviles; el 50% de las compañías que permiten BYOD tuvieron infracciones de seguridad a través de los

[2] Compound Annual Growth Rate – Tasa de crecimiento anual compuesto

dispositivos personales de los empleados; y el 60% de las compañías no se aseguran de borrar la información corporativa de los dispositivos personales de sus exempleados.

De igual manera el grupo Crowd Research Partners, elaboró el *"BYOD & Mobile Security 2016 Spotlight Report"*, un completo documento donde se analiza el fenómeno BYOD desde varias perspectivas que van desde la adopción de esta tendencia, pasando por brechas de seguridad hasta propuestas de medidas de mitigación de riesgos. El documento menciona cinco claves principales que influyen en el BYOD empresarial y en la seguridad móvil:

- Aumento en la movilidad de los empleados (63%), la satisfacción (56%) y la productividad (55%) dominan como los promotores de BYOD. Curiosamente, estos promotores en relación con los empleados son considerados más importantes que los costos reducidos (47%).
- La seguridad (39%) y la privacidad de los empleados (12%) son los mayores inhibidores de la adopción de BYOD. En contraste, la oposición de la administración (3%) y los aspectos referentes a la experiencia del usuario (4%) son mucho menos importantes.
- Una de cada cinco organizaciones sufrió una violación de seguridad móvil, impulsada principalmente por el malware y redes Wifi maliciosas.
- Las amenazas a la seguridad de BYOD imponen una pesada carga sobre los recursos de TI de las organizaciones (35%) y las cargas de trabajo de help desk (27%).
- A pesar del aumento de las amenazas de seguridad móvil, las vulnerabilidades de la información y las nuevas regulaciones, sólo el 30% de las organizaciones están aumentando los presupuestos para seguridad BYOD en los próximos 12 meses. Mientras tanto, el 37% no tiene planes de cambiar sus presupuestos de seguridad.

Este informe nos define de manera muy completa los retos, las consideraciones y algunas medidas de control que deben tener en cuenta las empresas en cuanto a la adopción de BYOD.

Podemos concluir entonces que la tendencia BYOD viene creciendo y no se detendrá en los próximos años, por el contrario, cada vez más las empresas y los CIO de las organizaciones están entendiendo que hay que considerar seriamente la incorporación de políticas y

frameworks que permitan a los empleados el uso de sus propios dispositivos, por lo cual el reto consiste no en decidir si se autoriza su uso o no, sino en cómo se van a proteger las redes y la información corporativa en ambientes BYOD.

1.3 Contexto regional

En cuanto a Latinoamérica, el blog Pulso Social presenta el artículo "BYOD y el empleado móvil en Latinoamérica", del 13 de septiembre de 2016, mediante el cual nos da una perspectiva sobre cómo la tendencia BYOD se ha venido posicionando en la región de manera creciente, inicialmente vista como una opción y convirtiéndola casi en una obligación. El articulo menciona que:

> "Las empresas se han concientizado de las ventajas de tener empleados móviles, otorgándoles dispositivos como tabletas y teléfonos inteligentes para trabajar. Para el año 2015 se calculaba que el 35% de los empleados desempeñaban su labor desde cualquier lugar o zona de trabajo; sabiendo esto para 2016, el 45% de las compañías en Latinoamérica tiene planeado alinear sus esfuerzos hacia una estrategia definitiva de movilidad que incluya todos los procesos organizacionales (marketing, servicio al cliente, soporte técnico, etc.) y el ecosistema de la industria (proveedores, clientes, reguladores, etc.) para disfrutar los beneficios de una organización con la movilidad como base". (Silva Filho, 2016)

El artículo finaliza mencionando que la movilidad es un factor clave en el desarrollo de las empresas hoy en día, por lo cual sugiere que se realicen las acciones necesarias para implementar mecanismos eficaces y eficientes que faciliten el trabajo diario de los empleados.

Aunque de una manera un poco más lenta que a nivel global, en Latinoamérica esta tendencia se viene adoptando, dadas las grandes ventajas que su uso ofrece. Es necesario que las organizaciones entiendan la necesidad de estudiar el tema y definir políticas de seguridad claras para estar preparados para la implementación de ambientes BYOD.

1.4 Contexto nacional

En cuanto a Colombia, la tendencia no difiere mucho con respecto a lo que ocurre a nivel mundial y regional. La revista Dinero, en su artículo *"Las tendencias que nos dejarán las TICS en 2016"*, menciona el BYOD y el Teletrabajo como algunos de los motores tecnológicos que impulsarán la forma de hacer negocios en nuestro país para años próximos.

Por su parte, el portal Colombia Digital en su artículo *"Consideraciones para adoptar modelos de BYOD en las organizaciones"*, del 6 de febrero de 2017, hace referencia a que, si bien el BYOD es una práctica que se ha venido popularizando durante los últimos años a nivel global y nacional, es importante que las empresas identifiquen los retos que su adopción puedan llegar a tener. La primera consideración de la que nos habla el artículo hace referencia al nivel de madurez tecnológica de la empresa en temas de seguridad informática y de la información, especialmente teniendo en cuenta que la organización no está facultada para acceder a los dispositivos de sus empleados, por temas de privacidad y protección de datos. Por otro lado, el artículo menciona la importancia de conocer la legislación nacional en torno al tema de protección de datos personales, representada principalmente por la ley 1581 de 2012. En ella se establecen sanciones en caso de pérdida, robo, acceso y divulgación no autorizada de los datos. Adicionalmente, menciona que la legislación colombiana sobre el teletrabajo, desarrollada por la ley 1221 de 2008 y el decreto 884 de 2012, es explicita en la obligación del empleador de aportar al empleado los dispositivos necesarios para desarrollar su labor. El artículo termina recomendando la identificación de riesgos como una valiosa herramienta para determinar si una organización es lo suficientemente madura para adoptar al BYOD.

Colombia, como uno de los países pioneros en la adopción de nuevas tecnologías y tendencias a nivel Latinoamérica, ha sido escenario de la discusión generada en torno a la adopción de BYOD. De hecho, el Ministerio de las TICS dentro de su iniciativa "Fortalecimiento de las TI en la gestión del Estado y la información pública"[3] propone estudiar a fondo el uso de dispositivos móviles soportado en políticas BYOD.

[3] https://www.mintic.gov.co/portal/604/w3-propertyvalue-657.html

1.5 BYOD en el sector Defensa y Fuerzas Militares a nivel global

Debido al rápido crecimiento de la tendencia BYOD en el mundo, su difusión ha impactado en todas las áreas donde se emplee la tecnología como base fundamental del desarrollo de los procesos en las organizaciones, y el sector Defensa no podía ser la excepción. Si bien es cierto que este sector es uno de los más custodiados por los gobiernos, fue inevitable que el BYOD obligara a los militares a tomar el tema muy en serio.

Una de las primeras alertas en este sentido la generó el Inspector General del Departamento de Defensa de los Estados Unidos, en su informe *"Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices"* de marzo de 2013. En este documento, el Inspector General advierte sobre el insuficiente trabajo que ha realizado para la fecha el Oficial de Información del Ejército (Army CIO), en lo concerniente a programas efectivos de ciberseguridad para dispositivos móviles comerciales. El informe recomienda a dicha instancia el desarrollo políticas claras y exhaustivas para incluir requerimientos para el reporte y seguimiento de dispositivos móviles comerciales. De igual manera, se sugiere al CIO del Ejército que debería extender los requerimientos de seguridad de la información existentes hacia el uso de dispositivos móviles comerciales.

La empresa de ciberseguridad Trend Micro, en su artículo *"US Army having some troubles with BYOD"*, analiza el informe citado mencionando los apartes y hallazgos más significativos del mismo. Incluye también una referencia al hecho de que el Departamento de Asuntos de Veteranos del Ejército americano intentó crear una política que permitiera a sus miembros el uso de sus propios dispositivos, sin embargo, dicha política no fue posible implementarla debido a restricciones de tipo legal.

Por otro lado, el portal de tecnología InformationWeek, en el artículo titulado *"BYOD In Defense Department? Not In This Lifetime"* de enero de 2014, analiza el fenómeno desde la perspectiva del Departamento de Defensa de los Estados Unidos (DoD). El artículo menciona que, si bien es cierto que el DoD ha venido abriendo sus puertas al uso de dispositivos móviles, aún no siente la suficiente confianza en los sistemas de ciberseguridad como para dar el paso de aprobación al BYOD para la época. De hecho, de acuerdo a las declaraciones del CIO de

Defensa de la época (Teri Takai), el tema se ha mantenido en un "congelador burocrático" al cual no se le dio respuesta ni positiva ni negativa.

Es importante también mencionar el informe *"BYOD Guidance: Executive Summary"*, publicado por el gobierno ucraniano en octubre de 2014. Esta guía se constituyó en la hoja de ruta para que las entidades gubernamentales de Ucrania que deseen adoptar el BYOD tengan en cuenta algunos aspectos esenciales para establecer parámetros básicos de seguridad y protección de la información. Dentro de los aspectos resaltantes de la guía se encuentran:

- Entender los asuntos legales: la responsabilidad legal de proteger la información personal de los empleados la debe realizar el propietario de los datos, no necesariamente el propietario del dispositivo.
- Crear una política efectiva de BYOD: Asegurar que los dispositivos adquiridos por el personal solamente pueden acceder a los datos corporativos que la entidad está dispuesta a compartir sólo con el personal autorizado.
- Limitar la información compartida en los dispositivos: El personal habitualmente comparte su información con otros usuarios y a través de la nube. Las copias de seguridad automáticas de los datos de los dispositivos en plataformas basadas en la nube pueden llevar a que los datos de negocio sean divulgados.
- Establecer acuerdos con el personal: Comunicar la política BYOD por medio de capacitaciones, con el fin de que los empleados entiendan sus responsabilidades cuando usan sus propios dispositivos para propósitos laborales.
- Considerar el uso de controles técnicos: Aplicaciones y servicios técnicos como la gestión de dispositivos móviles pueden contribuir en la administración remota de dispositivos personales, pero es posible que estos medios afecten el rendimiento de los mismos.
- Anticipar un mayor soporte a los dispositivos: Los servicios deben ser accesibles por medio de diferentes tipos de dispositivos, por lo cual se debe asegurar que el área de soporte TIC de la entidad tiene la capacidad y experiencia para manejar un rango cada vez más creciente de dispositivos.
- Generar planes para los incidentes de seguridad: Cuando ocurra un incidente, la entidad debe actuar rápidamente y mitigar las pérdidas. La entidad debe considerar la posibilidad

de borrar remotamente datos sensibles de los dispositivos personales, si estos son robados o perdidos.

- Considerar modelos alternativos de propiedad: Algunos usuarios no están dispuestos a restringir sus propios dispositivos, por lo tanto, la entidad debe considerar ofrecer a su personal como alternativa algunos dispositivos que sean adquiridos y controlados por la organización.

En esta misma línea, en el 2015 el Pentágono inició una prueba piloto de BYOD para el DoD. El portal C4ISRNet publicó en marzo de ese año, en un artículo titulado *"Pentagon to launch BYOD pilot this summer"*, una entrevista al CIO del DoD de la época, Terry Halvorsen, en la cual revela el inicio de un plan piloto para BYOD, como prueba de la implementación de esta tendencia en mayor escala. Como el artículo describe en palabras de Halvorsen, "Creo que una de las cosas que serían útiles es [entender] dónde BYOD está funcionando y donde no lo hace. Muchas grandes empresas están rescindiendo sus políticas de BYOD, no estoy diciendo que sea lo correcto en todas partes", dijo Halvorsen. "Lo que sospecho que va a pasar con el Departamento de Defensa, debido a nuestro tamaño y todos los negocios en los que estamos, es que habrá algunos lugares donde BYOD va a funcionar y va a haber lugares donde no. Creo que va a ser como con la nube y otras cosas, con el tamaño y la escala del DoD, no va a ser fácil obtener respuestas claras". Halvorsen plantea que uno de los objetivos del piloto es probar dispositivos dual-persona, los cuales tienen la capacidad de emplearse para el trabajo y también para actividades personales, en un entorno seguro.

El blog del Sector Gobierno de IBM publicó en julio de 2015 un artículo llamado *"Military 'Bring Your Own Device'?"*, donde se ilustra un ejemplo ficticio en el cual se ve comprometida una base de datos del Ejército Americano por la inclusión de una tableta inteligente de un general en la red clasificada. Este ejemplo demuestra cuán vulnerable se puede ser la red más segura del mundo, por la simple negación de aceptar una política de adopción de BYOD con todas las medidas de seguridad requeridas.

En el mismo mes de Julio de 2015, la revista Nextgov publicó el artículo *"Pentagon Not Ready For Bring-Your-Own-Device Just Yet"*, en el cual informaba que el CIO del DoD Terry

Halvorsen, quien en marzo anunciaba el inicio de un plan piloto de BYOD para su agencia, advertía que dicho piloto se había aplazado debido principalmente a que había otros asuntos más urgentes que atender. El funcionario declaró que el piloto planteado inicialmente era "demasiado grande", por lo cual se iba a redimensionar. Por último, Halvorsen informó que posiblemente el BYOD se vea limitado a algunos tipos de dispositivos específicos y para funciones limitadas.

Por su parte, la revista socPub, especializada en temas de administración de contenido, medios sociales, tecnología de la información y tecnología de consumo, publicó el informe titulado *"The Challenges of Bringing BYOD to the Military"*, mediante el cual explica que aunque al inicio los militares norteamericanos fueron reacios a la adopción de BYOD, cada vez se han visto más flexibles a aprovechar las ventajas de que los militares usen sus propios dispositivos para el trabajo, sin embargo esto presenta un enorme desafío en términos de seguridad. Uno de los principales retos que plantea el autor corresponde a los costos de implementar BYOD en todo el Ejército: aunque se podría asumir que el hecho de que los militares usen sus propios dispositivos reduciría costos en este sentido, la inversión en infraestructura tecnológica de ciberseguridad sería gigantesca. Otro reto importante es el hecho de que debido a los exhaustivos controles de seguridad a los cuales deben someterse los dispositivos, el BYOD obligaría a permitir el uso de solo algunos modelos de ciertos dispositivos, los cuales contarían con limitaciones en administración y operatividad frente a los dispositivos comerciales comunes. Otro aspecto que menciona el artículo son los resultados de varias pruebas piloto de la adopción de esta tendencia, encontrando algunos fallos preocupantes que van desde el no cifrado de las comunicaciones hasta fallas humanas tan básicas como no tener activada una contraseña de ingreso en los dispositivos. El artículo finaliza concluyendo que, aunque los retos son enormes, los militares norteamericanos están decididos a apostarle al BYOD ya sea en el mediano o en el largo plazo.

Ya para febrero de 2016, el blog de tecnología FedTech publicó el informe *"Federal Agencies Turn to BYOD, Mobile Devices in the Field to Attract New Workers"*, donde se explora la situación de muchas agencias federales, las cuales están sufriendo el fenómeno llamado "the Silver Tsunami", que consiste en que se calcula que para septiembre de 2017 un

31% de sus trabajadores se podrán jubilar, debido a que cumplen la edad mínima para ello. Esto ha representado un importante desafío para el reclutamiento de jóvenes profesionales, quienes dependen de la tecnología en muchos aspectos de la vida, incluido el laboral. Gracias a este fenómeno algunas agencias federales, entre ellas la Casa Blanca, han abierto las puertas a tendencias como BYOD con el fin de atraer mentes jóvenes para que se pongan al servicio del gobierno. El informe explora varios ejemplos en los cuales se han flexibilizado las normas habituales de trabajo para adaptarse a la forma en que las nuevas generaciones conciben su desempeño laboral.

El uso de BYOD en entornos de seguridad como el militar ha sido explorado ampliamente alrededor del mundo. Un ejemplo de ello es el interés mostrado por la Organización del Tratado del Atlántico Norte (OTAN) sobre la posibilidad de que sus militares puedan emplear sus dispositivos personales para labores de su trabajo diario. Prueba de ello es el informe presentado en la Conferencia Internacional sobre Sistemas de Comunicaciones e Información Militares (ICMCIS) del 2016, titulado *"Developing a NATO BYOD Security Policy"*, de los investigadores Alessandro Armando, Gabriele Costa, Alessio Merlo, Luca Verderame y Konrad Wrona. Este informe nos dice lo siguiente:

> "Los dispositivos móviles tienen un papel importante que jugar tanto en las actividades privadas, así como las profesionales de los trabajadores. Sin embargo, su uso puede representar una seria amenaza para la seguridad del ambiente de trabajo. Por lo tanto, muchas organizaciones establecen una política específica de llevar su propio dispositivo (BYOD). En este documento se presenta una propuesta sobre cómo fomentar un ambiente de trabajo seguro y consciente de políticas. Nuestra solución implica la aplicación de políticas de seguridad detalladas para los dispositivos personales, mientras que busca la tranquilidad de los propietarios de no tener que tomar decisiones críticas y asumir la responsabilidad por el comportamiento de las aplicaciones instaladas en sus dispositivos. Reportamos nuestra experiencia en el desarrollo y aplicación de una política de seguridad basada en las directrices existentes de la Agencia de Comunicaciones e Información de la OTAN (Agencia del NCI)". (Armando, A., Costa, G., Merlo, A., Verderame, L., & Wrona, K., 2016)

Para probar su teoría, los investigadores desarrollan un caso de estudio basado en la aplicación BYODroid, diseñada para tal fin. Como conclusión, el artículo nos dice que:

> "Este artículo presenta la aplicación de BYODroid a la infraestructura de la agencia NCI e informa de nuestra experiencia con el modelado y aplicación de políticas de seguridad reales para un entorno BYOD complejo. La actividad se llevó a cabo junto con los expertos en seguridad de la Agencia NCI para identificar y codificar las políticas de seguridad BYOD. Aunque este proceso se inició a partir de la documentación del lenguaje natural, podríamos rápida y fácilmente obtener una especificación formal adecuada. Además, ampliamos la arquitectura BYODroid existente para hacer frente al sistema de políticas basado en roles de la Agencia del NCI. La adopción de un lenguaje de políticas formalmente definido fue crucial para garantizar la composición de las políticas asociadas a cada usuario. Debido a que la infraestructura subyacente es sensible a la seguridad, no pudimos ejecutar experimentos reales en el campo. Las recomendaciones para la evolución futura de esta investigación incluyen la experimentación práctica, ya sea en entornos simulados o reales, para confirmar la viabilidad de nuestro enfoque". (Ibid, 2016)

Por otro lado, en agosto de 2016 la revista GCN, especializada en evaluaciones tecnológicas, recomendaciones y estudios de casos para apoyar a los administradores de TI del sector público que son responsables de la especificación, evaluación y selección de soluciones tecnológicas, publicó el artículo *"Federal BYOD: The mobile security conundrum"*, en el cual nuevamente se aborda el tema de la renuencia de las entidades gubernamentales en la adopción de tendencias como el BYOD. Entre las razones más comunes, menciona el artículo, se encuentran amenazas como el software potencialmente no deseado, el ransomware y la fuga de información. Para solventar este tipo de problemas, el artículo ofrece algunos consejos de seguridad, entre los cuales se cuentan el uso de políticas aceptables a través de un enfoque basado en la red; la integración de funcionalidades de seguridad directamente en las soluciones de administración de dispositivos móviles; la implementación de control de aplicaciones granulares que pueden dirigir la forma en que los usuarios interactúan con aplicaciones web y móviles; el monitoreo y medición de efectividad de las políticas y controles establecidos; y la capacitación a los usuarios sobre los vectores comunes de amenazas de infección que tienen más probabilidades de encontrar. El artículo culmina diciendo que, si se hace correctamente, la tendencia BYOD

puede ayudar a las agencias federales a hacer grandes progresos en un cumplimiento más eficaz en su misión.

En mayo de 2017, Alexandra Sander, Colaboradora del blog FedTech, presenta en su artículo *"The Smart Move for the DOD on Smartphones"* la necesidad de que el Pentágono lidere el camino hacia el BYOD. Inicia la autora poniendo sobre la mesa uno de los ejemplos más recientes de esta tendencia: la renuencia del presidente Donald Trump a abandonar su teléfono Samsung y reemplazarlo por el teléfono asignado por su servicio secreto. La autora expone que existe una brecha importante entre la funcionalidad de los teléfonos comerciales y los dispositivos autorizados por el Departamento de Defensa. De igual manera plantea que, si bien las preocupaciones sobre la seguridad son válidas, los avances en la tecnología móvil hacen que el equilibrio entre funcionalidad y seguridad sea obsoleto e innecesario. Los procesadores móviles de última generación emparejados con sensores sofisticados y las opciones de almacenamiento de datos en expansión (especialmente aquellas que permiten la autenticación multifactor y la virtualización) aumentan la línea base y hacen irrelevantes las evaluaciones de riesgos pasadas. El articulo también explora la posibilidad de que BYOD se observe como una iniciativa de modernización de la infraestructura de TI. Como conclusión, el artículo plantea que no va a ser la tecnología existente, sino las decisiones políticas las que determinarán la adopción del BYOD en el entorno gubernamental.

Como podemos apreciar, dada la importancia que tiene la información de seguridad y defensa de los estados y el celo con que ésta se administra, inicialmente se consideró imposible la adopción de BYOD. Sin embargo, dado que la tendencia aumentó radicalmente en el ámbito corporativo, que ha sido probada con éxito en diferentes tipos de empresas y que trae grandes ventajas, los gobiernos y las entidades gubernamentales del sector Defensa a nivel mundial han cambiado su perspectiva y han dejado de considerar el BYOD como una amenaza, para analizarlo como una oportunidad. Ya varios gobiernos han iniciado planes piloto, algunos incluso ya tienen políticas establecidas para BYOD y su implementación segura. Por ello, este trabajo cobra gran importancia puesto que estudia y analiza la tendencia desde la perspectiva del sector Defensa en Colombia, con el fin de brindar herramientas a los jefes de TICS y a los tomadores de decisiones para definir su postura frente a BYOD.

1.6 Estudios e investigaciones realizadas sobre BYOD

En el artículo titulado *"Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments"* de marzo de 2015, explora los desafíos a los cuales se ven avocadas las organizaciones que intentan implementar ambientes BYOD. Este artículo concluye que a pesar de que esta tendencia va en aumento, muchas empresas no comprenden los desafíos de seguridad y privacidad asociados con su práctica. La falta de comprensión de BYOD por parte de las organizaciones las pone en riesgo de perder el control de sus recursos y activos de información críticos. Este artículo identificó un vacío que revela que ninguno de los mecanismos o enfoques hasta la fecha para la protección de la información confidencial en entornos BYOD ha equilibrado los objetivos contradictorios de tratar de asegurar el propio dispositivo o los datos en el dispositivo, por lo cual ocurren una de dos cosas: o se exponen los datos o se destruye la experiencia de los usuarios. Si no se puede lograr la seguridad y privacidad de los datos, entonces el enfoque BYOD es inútil. Del mismo modo, si se destruye la experiencia de los usuarios, la solución se debilita y se considera infructuosa. Entre otros hallazgos, el estudio muestra algunos de los problemas con los que se encuentran las organizaciones al tratar de implementar BYOD, como por ejemplo que diferentes dispositivos móviles con diferentes sistemas operativos causan problemas de compatibilidad y de cumplimiento de la gestión de parches. La detección de un dispositivo móvil o el seguimiento de su actividad en una red puede ser difícil. Las aplicaciones no verificadas y no confiables pueden introducir problemas de malware, virus y ancho de banda. Los dispositivos perdidos o robados provocan la pérdida y el robo de datos, ya que el dispositivo puede conectarse a la red de forma remota. Los métodos y procesos de seguridad tradicionales, como los cortafuegos móviles y el filtrado de contenidos móviles, se han convertido en herramientas anticuadas contra las amenazas emergentes en los dispositivos móviles. Esto se debe especialmente a que absorben los recursos del sistema y ralentizan el tiempo de respuesta y el rendimiento de los dispositivos. Además, dado que las soluciones antivirus funcionan internamente con el procesador central de los sistemas operativos de los dispositivos, las puertas traseras para ataques pueden abrirse fácilmente, especialmente porque los malware en la actualidad explotan las vulnerabilidades de día cero. Además, los sistemas de solución BYOD en la actualidad se

centran principalmente en las capacidades de red seguras, y no en cómo lograr un equilibrio entre la disponibilidad y protección de los recursos y activos de información, de tal manera que los objetivos de confidencialidad, integridad y disponibilidad de la seguridad de la información, junto con la privacidad, se ven comprometidos. Por lo tanto, como la tecnología para manejar BYOD es todavía inmadura y los riesgos quizás no son ampliamente conocidos, este estudio destaca la importancia de una política efectiva de seguridad y privacidad. Además, es imperativo que las organizaciones inviertan tiempo y recursos adecuados con el objetivo de obtener una comprensión más profunda de las vulnerabilidades y amenazas que rodean a BYOD, para proteger sus recursos y activos de información confidencial. En conclusión, cualquier intento por parte de las organizaciones de adoptar o implementar BYOD sin prestar la atención adecuada a los problemas o desafíos de seguridad y privacidad mencionados puede aumentar el riesgo de pérdida de información confidencial.

En junio de 2015 se publica el estudio titulado *"BYOD Security Engineering: A Framework & its Analysis"* (Zahadat, 2015). En esta investigación se propone un marco de referencia para la implementación de BYOD de manera segura en las organizaciones. Inicialmente los autores establecen la definición de BYOD y por qué es interesante esta tendencia para las entidades. Posteriormente se propone un framework de seguridad que toma como referencia el ciclo de vida de los dispositivos en ambientes BYOD, para establecer las bases del marco de referencia en ocho pasos fundamentales: Planeación, identificación, protección, detección, respuesta, recuperación, evaluación y supervisión. La investigación también propone algunos controles clave para la implementación de políticas BYOD, como los incentivos, desincentivos, las tácticas de cumplimiento y la comunicación permanente y continua. Los investigadores dan comprobación a sus 12 hipótesis a través de un cuestionario de encuesta con 60 preguntas, tomando como muestra a profesionales de seguridad e ingenieros de seguridad. El estudio concluye con algunas recomendaciones para el uso del framework, así como una descripción de los pasos para establecer un programa de seguridad en BYOD.

Por otro lado, en diciembre de 2015 en el marco de la Conferencia Internacional sobre seguridad de la información y privacidad (ICISP2015) del 2015, se presentó el estudio llamado *"Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)"*, publicado por

la revista ScienceDirect. Este estudio aborda los posibles problemas legales a los cuales se pueden ver avocados los empleadores que han permitido la adopción del BYOD en sus organizaciones. Dentro de los tópicos a considerar, el documento explora algunos aspectos como la actualización y almacenamiento de datos; la seguridad de BYOD; BYOD y la privacidad de los empleados; la respuesta, notificación e investigación de infracciones; el borrado y bloqueo remoto; y la destrucción segura de datos corporativos. El estudio ofrece recomendaciones puntuales sobre los aspectos que debería cubrir una política BYOD bien implementada, desarrollando políticas enfocadas en la seguridad de los dispositivos móviles, el cifrado y contraseñas de usuario, la categorización de datos, el uso de software antivirus, el acceso inalámbrico, el manejo de incidentes de violación de la seguridad y su respuesta, el trabajo a distancia y la protección de la privacidad. Por último, el estudio concluye que:

> "Corresponde a la empresa desarrollar una política BYOD que no sólo proteja los datos confidenciales, sino que también se ocupe de los derechos de los empleados. Para ello, las organizaciones necesitan procedimientos integrados más sistemáticos para gestionar las amenazas, así como mantener los dispositivos de los empleados y las implicaciones legales del enfoque BYOD teniendo en cuenta todos los factores relevantes para cosechar los beneficios para la organización". (Dhingra, 2016)

En noviembre de 2016 se publica la tesis de licenciatura titulada "*Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones*". Este estudio inicia describiendo la necesidad de la seguridad de la información y planteando el desafío que representan las nuevas tecnologías móviles a la misma. Luego explora las plataformas móviles más usadas en la actualidad, para luego describir las amenazas más conocidas hacia las mismas. Posteriormente describe las buenas prácticas en cuanto a seguridad de dispositivos móviles, para luego adentrarse en el campo del BYOD y su impacto en la seguridad al interior de las organizaciones. El estudio concluye que "el uso extendido de dispositivos móviles ha hecho que se conviertan de manera activa en una herramienta de trabajo, alojando en ocasiones información crítica y valiosa. La concienciación del usuario es y seguirá siendo un factor determinante para los daños y la exposición al malware. El fenómeno BYOD se presenta como una realidad difícil de restringir y controlar. A la hora de diseñar e implementar soluciones y gestionar la seguridad, se debe abordar la problemática en forma integral".

Más adelante, en febrero de 2017 se publica el artículo titulado *"BRING YOUR OWN DEVICE: Oportunidades, retos y riesgos en las organizaciones"* en el cual el autor explora las oportunidades, retos y riesgos a los que se enfrentan las organizaciones cuando de implementar BYOD se trata. El artículo concluye que esta tendencia va en aumento y no parece desacelerar en el futuro próximo, por todas las ventajas que su implementación conlleva a las organizaciones de todo tipo. Sin embargo, destaca que existen algunas preocupaciones frente a la fuga de información que se puede producir por el robo o pérdida de dispositivos móviles. Por ello recalca que es importante la capacitación y el entrenamiento que se le debe impartir a los empleados con el fin de disminuir este tipo de riesgos; el autor afirma que también es primordial concientizar a los empleados de las consecuencias laborales y legales que puede acarrear un fallo de seguridad. De igual manera, se advierte que las aplicaciones corporativas deben ser plenamente compatibles con dispositivos móviles. Por último, el artículo menciona la importancia de implementar herramientas para la gestión de dispositivos móviles, conocidas en el mercado como Mobile Device Management (MDM), con el fin de administrar la autenticación al dispositivo, el comportamiento del mismo en redes no autorizadas y el aislamiento de los datos personales de los corporativos.

Posteriormente, en junio del mismo año, se publica el artículo *"National Cyber-security Policies oriented to BYOD (Bring Your Own Device): Systematic Review"*, en el cual se propone la creación de una política nacional para la implementación de BYOD en Ecuador. Este estudio concluye que el principal problema de BYOD está en la conexión, por ello la principal recomendación del autor va encaminada a generar políticas de aseguramiento de la conexión y de la información transmitida entre dispositivos. Sin embargo, el establecimiento de políticas claras no será efectivo si los usuarios no son conscientes de la importancia de las mismas. Por ello, el factor humano es muy importante para que la ejecución de las políticas establecidas sea efectiva. Por último, el autor recomienda que el estado debe destinar recursos de inversión para la seguridad de la información, no solo para la adquisición de herramientas tecnológicas sino también para estudios de políticas y estrategias nacionales de ciberseguridad que puedan proporcionar reglas de uso o mejores prácticas, con el fin de prevenir cualquier ataque o pérdida de información.

En el mes de julio de 2017 se publica un trabajo fin de máster (TFM) titulado *"Riesgos de seguridad asociados al uso de dispositivos móviles personales (smartphone – Android) en entornos BYOD – Bring your own device"*, en la Universidad Internacional de la Rioja, de España. Este trabajo analiza la tendencia BYOD, mostrando sus ventajas y desventajas y su posible pertinencia en las organizaciones. El trabajo se centra en un análisis de riesgos tomando como base la norma ISO/IEC 27001:2013, en la cual se establecen 14 dominios de la seguridad de la información, analizando cada uno de manera detallada. Este trabajo concluye, en primer lugar, que está comprobado que los smartphones han desplazado en gran medida a los computadores personales en la realización de tareas diarias tanto personales como laborales, por lo cual las organizaciones deben considerar muy seriamente la adopción de BYOD. Para ello, el autor ofrece una propuesta metodológica que facilite la adopción de BYOD a los responsables de este tipo de implementaciones. Esta propuesta incluye un análisis de BYOD y del sector de los smartphone, incluyendo una propuesta de evaluación de riesgos, pasando por el tema de los controles de seguridad y mejores prácticas, y finalizando con una propuesta de política de seguridad.

Es importante mencionar un artículo publicado en agosto de 2017 en la revista International Journal of Advanced Computer Science and Applications (IJACSA), titulado *"Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm"*. En este artículo el autor aborda el tema del BYOD en la educación superior, analizando los posibles riesgos a los que se enfrenta la comunidad académica en la adopción del BYOD. Para ello, el autor realiza una encuesta en la University Sains Malaysia (USM) de Malasia, en la cual se analiza el conocimiento y la concienciación que tienen los estudiantes y profesores sobre el uso de dispositivos móviles personales para sus labores académicas. Los resultados de la encuesta muestran que los estudiantes encuestados de la USM tienen un conocimiento básico o fundamental de la seguridad y la privacidad, al igual que la mayoría de los estudiantes se consideran principiantes con respecto a los controles de seguridad y privacidad o medios para proteger sus dispositivos móviles y sus datos. El artículo concluye reconociendo que las investigaciones con respecto a este tema aún están iniciando, y que se debe profundizar más en aspectos como posibles ataques o vulnerabilidades que se puedan presentar para fortalecer los controles del BYOD.

Posteriormente, en diciembre de 2017, se publica el artículo *"Survey on Access Control and Management Issues in Cloud and BYOD Environment"*, el cual se centra en una revisión de la bibliografía existente sobre el control de acceso y los temas de gestión, con un enfoque en las tendencias de BYOD. Adicionalmente, se investigan las tendencias que afectan a los problemas de control de acceso en BYOD en relación con la seguridad de la información. Este articulo concluye que la tendencia BYOD ha llegado para quedarse de manera inevitable, por ello urge que se desarrollen herramientas técnicas que permitan controlar el acceso a información privada de las compañías. Finalmente, el autor plantea que cualquier solución futura debe crear técnicas para autenticar, hacer cumplir las políticas de control de acceso y proteger las políticas de control de acceso durante las fases de transferencia, proceso y almacenamiento en una plataforma independiente para dispositivos BYOD.

Los mismos autores del anterior estudio, posteriormente en febrero de 2018 presentan otro artículo titulado *"A proposed framework for access control in the cloud and BYOD environment"*, en el cual profundizan aún más en el tema con la propuesta de un marco de arquitectura que pretende controlar los riesgos de BYOD. Según los autores, la arquitectura propuesta busca reducir las restricciones y aplicar políticas de control de acceso en la nube y en el entorno BYOD de una manera fácil y segura con una plataforma independiente. El estudio busca proteger la privacidad del usuario evitando el uso de soluciones de gestión de dispositivos móviles (MDM). De igual manera, el artículo da cuenta del primer prototipo del sistema implementando y probando el framework propuesto en entornos reales, informando que los resultados de la verificación y validación muestran excelentes resultados y retroalimentación positiva.

El análisis de los estudios e investigaciones descritas anteriormente ofrecen una fuente confiable de análisis de la tendencia BYOD desde diferentes perspectivas. Cada autor da relevancia en mayor o menor medida a diversos aspectos a tener en cuenta, que van desde las políticas, pasando por las personas y culminando en la tecnología, para proponer mejores prácticas y marcos de referencia que se ajusten a las necesidades particulares de cada estudio. Por ello, en el capítulo 3 se desarrolla una propuesta de marco de mejores prácticas que busca

establecer medidas preventivas frente a diferentes aspectos de la tendencia, comunes en las investigaciones tomadas de referencia, que brindan herramientas a las entidades del sector Defensa que decidan implementar entornos BYOD seguros.

1.7 Marco normativo nacional sobre el tema

Uno de los aspectos más importantes a tener en cuenta en la implementación del BYOD, de acuerdo a la información consultada, corresponde a las implicaciones legales que esta tendencia pueda tener sobre los datos de los usuarios. Es necesario que exista un equilibrio perfecto entre la seguridad y la privacidad de los datos, básicamente porque BYOD utiliza un activo tecnológico adquirido por el propio usuario. Por ello, antes de proponer e implementar políticas del uso de BYOD en las organizaciones, es necesario hacer un estudio del marco normativo que esté vigente en el país de implementación, puesto que la regulación va a ser determinante al momento de establecer las limitaciones de las políticas propuestas.

En el caso colombiano, es importante contemplar la legislación referente al teletrabajo y la protección de datos personales. El teletrabajo se encuentra reglamentado inicialmente mediante la ley 1221 del 16 de julio de 2008 "Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones". En esta ley en su artículo 6°, Numeral 7, reza:

> "7. Los empleadores deberán proveer y garantizar el mantenimiento de los equipos de los teletrabajadores, conexiones, programas, valor de la energía, desplazamientos ordenados por él, necesarios para desempeñar sus funciones. Los elementos y medios suministrados no podrán ser usados por persona distinta al teletrabajador, quien al final del contrato deberá restituir los objetos entregados para la ejecución del mismo, en buen estado, salvo el deterioro natural". (Ley 1221 de 2008)

Para el caso de la protección de datos personales, un primer acercamiento se dio por medio de la sentencia C-748 de 2011 de la Corte Constitucional, mediante la cual se realizó el control de constitucionalidad del proyecto de ley estatutaria de Habeas Data y protección de datos personales. Para el año 2012, se promulgó la ley estatutaria 1581 del 7 de octubre de 2012 "Por

la cual se dictan disposiciones generales para la protección de datos personales", cuyo objeto, como reza en su artículo primero, es:

> "Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma". (Ley 1581 de 2012)

Posteriormente se promulga el decreto 1377 del 27 de junio de 2013 "Por el cual se reglamenta parcialmente la ley 1581 de 2012". Este decreto se motiva dado que, como reza el mismo:

> "Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas".

Dado que el presente trabajo de grado hace referencia en particular al sector Defensa en Colombia, es importante señalar que el documento rector en cuanto a políticas de seguridad de la información es la Directiva Permanente No. DIR2014-18 "Políticas de seguridad de la información para el sector Defensa", emitida por el Ministerio de Defensa Nacional, la cual rige desde el año 2014. Es necesario señalar que antes de la expedición de la directiva señalada, cada una de las fuerzas que componen el sector Defensa en Colombia (Ejército Nacional, Fuerza Aérea, Armada Nacional y Policía Nacional) emitían sus propias directivas de seguridad de la información, cada una con las características propias requeridas para cada fuerza de acuerdo a su naturaleza. Sin embargo, dado que un gran porcentaje del contenido era común entre todas, en el año 2013 se tomó la decisión de unificar la directiva para todo el sector, facilitando de esta manera su implementación y control por parte del Ministerio de Defensa Nacional (MDN).

La directiva 2014-18 parte del principio de que los activos de información de las instituciones y entidades que conforman el sector se van a acceder a través de equipos y dispositivos de propiedad del Ministerio de Defensa Nacional, y solo en algunos casos específicos establece la posibilidad de emplear equipos de terceros, haciendo referencia especialmente a contratistas y empresas que trabajen en proyectos del sector. Por ello, el tema del BYOD no se ve plasmado específicamente en la directiva, sin embargo, de manera taxativa se pueden extraer algunos apartes del documento de los cuales se infiere que en primera instancia el uso de dispositivos móviles personales para acceder a información laboral no estaría permitido. Algunos de los apartes encontrados sobre el tema son los siguientes:

En el numeral 4, que hace referencia a las acciones que afectan la seguridad de la información, se encuentran los siguientes dos ítems:

> "k. Enviar información no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
> l. Almacenar y mantener información clasificada en dispositivos de almacenamiento de cualquier tipo que no sean de propiedad de las respectivas instituciones y entidades del sector Defensa". (MDN, 2014)

En el numeral 5.4, referente a los acuerdos de intercambio de información y software, el ítem a) menciona lo siguiente: "Todo funcionario y/o tercero es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada".

El numeral 5.6, referente al uso adecuado de los activos de información, dice: "las instituciones y entidades que conforman el sector Defensa podrán monitorear y supervisar la información, sistemas, servicios y equipos que sean de su propiedad, de acuerdo con lo establecido en esta política y la legislación vigente".

El numeral 5.6.5, referente a computación en la nube (cloud computing), menciona explícitamente que "Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos".

El numeral 5.24, referente a computación móvil, en el ítem a), dice que: "Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se debe implementar controles de acceso y técnicas criptográficas para cifrar la información crítica almacenada en estos". En el ítem b menciona: "La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser debidamente autorizada por la oficina de tecnología, o la que haga sus veces, previa verificación de que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura".

De los extractos anteriores, que son los más relevantes en cuanto al tema de esta investigación, podemos concluir en primer lugar que los controles propuestos hacen referencia a dispositivos y equipos institucionales, entendidos como elementos adquiridos por las entidades que conforman el sector Defensa con recursos públicos entendidos para tal fin, por lo cual se excluyen aquellos dispositivos adquiridos por los propios funcionarios. En segundo lugar, la directiva en general y en los diferentes apartes transcritos anteriormente, es clara en hablar de las limitaciones en cuanto al tratamiento de la *información clasificada*. Para entender el concepto de información clasificada, debemos remitirnos a algunos documentos que reglamentan la clasificación de la información.

En primer lugar, la ley 1712 del 06 de marzo de 2014, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones", en su artículo 5 *Ámbito de aplicación*, establece:

> "Las disposiciones de esta ley serán aplicables a las siguientes personas en calidad de sujetos obligados:
>
> a) Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital.
>
> b) Los órganos, organismos y entidades estatales independientes o autónomos y de control.
>
> c) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público.

d) Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función.

e) Las empresas públicas creadas por ley, las empresas del Estado y sociedades en que este tenga participación.

f) Los partidos o movimientos políticos y los grupos significativos de ciudadanos.

g) Las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público.

Las personas naturales o jurídicas que reciban o intermedien fondos o beneficios públicos territoriales y nacionales y no cumplan ninguno de los otros requisitos para ser considerados sujetos obligados, solo deberán cumplir con la presente ley respecto de aquella información que se produzca en relación con fondos públicos que reciban o intermedien.

PARÁGRAFO 1o. No serán sujetos obligados aquellas personas naturales o jurídicas de carácter privado que sean usuarios de información pública."

En el artículo 6 *Definiciones*, de la misma ley, se establecen entre otras, las siguientes definiciones:

"a) Información. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen;

b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;

c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;

d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley".

Adicionalmente, en el título III *Excepciones acceso a la información*, se transcriben los artículos 18 y 19 así:

"ARTÍCULO 18. INFORMACIÓN EXCEPTUADA POR DAÑO DE DERECHOS A PERSONAS NATURALES O JURÍDICAS. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011.

b) El derecho de toda persona a la vida, la salud o la seguridad.

c) Los secretos comerciales, industriales y profesionales.

PARÁGRAFO. Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable.

ARTÍCULO 19. INFORMACIÓN EXCEPTUADA POR DAÑO A LOS INTERESES PÚBLICOS. Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

a) La defensa y seguridad nacional;

b) La seguridad pública;

c) Las relaciones internacionales;

d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;

e) El debido proceso y la igualdad de las partes en los procesos judiciales;

f) La administración efectiva de la justicia;

g) Los derechos de la infancia y la adolescencia;

h) La estabilidad macroeconómica y financiera del país;

i) La salud pública.

PARÁGRAFO. Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos".

De la ley 1712 de 2014 se entiende que toda información que un funcionario público genere, obtenga, adquiera, o controle en su calidad de tal, se considera como información pública. Sin embargo, se establecen algunas excepciones con respecto a la información pública clasificada y a la información pública restringida.

Por otro lado, la ley 1621 de 2013, "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", en el capítulo VI "Reserva de la información de inteligencia y contrainteligencia", establece lo siguiente:

> "ARTÍCULO 33. RESERVA. Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus documentos, información y elementos técnicos estarán amparados por la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada.
>
> Excepcionalmente y en casos específicos, por recomendación de cualquier organismo que lleve a cabo actividades de inteligencia y contrainteligencia, el Presidente de la República podrá acoger la recomendación de extender la reserva por quince (15) años más, cuando su difusión suponga una amenaza grave interna o externa contra la seguridad o la defensa nacional, se trate de información que ponga en riesgo las relaciones internacionales, esté relacionada con grupos armados al margen de la ley, o atente contra la integridad personal de los agentes o las fuentes.
>
> PARÁGRAFO 1o. El Presidente de la República podrá autorizar en cualquier momento, antes del cumplimiento del término de la reserva, la desclasificación total o parcial de los documentos cuando considere que el levantamiento de la reserva contribuirá al interés general y no constituirá una amenaza contra la vigencia del régimen democrático, la seguridad, o defensa nacional, ni la integridad de los medios, métodos y fuentes.
>
> PARÁGRAFO 2o. El organismo de inteligencia que decida ampararse en la reserva para no suministrar una información que tenga este carácter, debe hacerlo por escrito, y por intermedio de su director, quien motivará por escrito la razonabilidad y proporcionalidad

de su decisión y la fundará en esta disposición legal. En cualquier caso, frente a tales decisiones procederán los recursos y acciones legales y constitucionales del caso.

PARÁGRAFO 3o. El servidor público que tenga conocimiento sobre la recolección ilegal de información de inteligencia y contrainteligencia, la pondrá en conocimiento de las autoridades administrativas, penales y disciplinarias a las que haya lugar, sin que ello constituya una violación a la reserva.

PARÁGRAFO 4o. El mandato de reserva no vincula a los periodistas ni a los medios de comunicación cuando ejerzan su función periodística de control del poder público, en el marco de la autorregulación periodística y la jurisprudencia constitucional, quienes en cualquier caso estarán obligados a garantizar la reserva respecto de sus fuentes".

Adicionalmente encontramos el decreto 1070 de 2015, "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa", en el Título 3 "Normas para fortalecer el marco legal que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional", en el Capítulo 6 "Reserva legal, niveles de clasificación, sistema para la designación de los niveles de acceso a la información y desclasificación de documentos", encontramos los siguientes artículos:

ARTÍCULO 2.2.3.6.1. Reserva Legal. En los términos del artículo 33 de la Ley 1621 de 2013, los documentos, información y elementos técnicos de los organismos de inteligencia y contrainteligencia estarán amparados por la reserva legal y se les asignará un nivel de clasificación de acuerdo con lo establecido en el siguiente artículo.

ARTÍCULO 2.2.3.6.2. Niveles de Clasificación de la Información. Los niveles de clasificación de seguridad de la información que goza de reserva legal serán los siguientes:

a) Ultrasecreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.

b) Secreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.

c) Confidencial. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.
d) Restringido. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes.

PARÁGRAFO. Los documentos de inteligencia y contrainteligencia que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.

Sin perjuicio de lo establecido en el artículo 34 de la Ley 1621 de 2013, a mayor nivel de clasificación de seguridad de la información, mayores serán las restricciones y controles para el acceso a la misma por parte de los receptores, las autoridades, los servidores públicos y asesores que deban conocer de ella. Estas restricciones deberán quedar establecidas en actos administrativos, manuales, protocolos, tarjetas de autorización para manejo y acceso a la información y contratos respectivos en cada uno de los organismos de inteligencia y contrainteligencia.

ARTÍCULO 2.2.3.6.3. Criterios para dar Acceso a La Información. Los organismos de inteligencia y contrainteligencia para dar acceso interno y externo a la información que goza de reserva legal y tenga nivel de clasificación, cumplirán con los siguientes criterios:
a) Mantener el principio de compartimentación a partir de la necesidad de saber y conocer estrictamente lo necesario para el desempeño de la función que le es propia. Así mismo, establecerán un mecanismo interno que determine los niveles de acceso para cada funcionario o asesor del organismo de inteligencia y contrainteligencia.
b) Entre mayor sea el nivel de clasificación de la información, mayores serán las restricciones como los controles que se deben aplicar para tener acceso a ella.
c) Identificar a los receptores de productos de inteligencia y contrainteligencia, estableciendo su nivel de acceso.

d) Desarrollar guías y/o protocolos, cuando sea el caso, para recibir, compartir e intercambiar información de inteligencia y contrainteligencia.
e) Implementar de forma física y/o mediante la utilización de herramientas tecnológicas, el sistema de acceso a los diferentes niveles de clasificación, con capacidades de administración, monitoreo y control, con base en los cargos, perfiles y funciones determinadas en la estructura de cada organismo de inteligencia y contrainteligencia.
f) Suscribir acuerdos, protocolos o convenios, en los términos de la Constitución y la Ley, para recibir, compartir o intercambiar información que goce de reserva legal con agencias de inteligencia y contrainteligencia extranjeras.

Cada organismo documentará sus procedimientos, en sus manuales o protocolos, para asegurar la reserva legal, los niveles de clasificación y dar acceso a la información a las autoridades o receptores competentes".

De la información obtenida por medio de los documentos legales anteriormente mencionados, podemos inferir que:

1. Toda información generada, obtenida, adquirida o controlada por un funcionario público en su calidad de tal, se considera como información pública.
2. La información clasificada, a la cual se refiere la directiva 2014-18 de Seguridad de la información del Ministerio de Defensa Nacional, se entiende como toda información que tiene una o varias de las siguientes condiciones:
    a. Información con reserva legal.
    b. Información generada, obtenida, adquirida o controlada por organismos de inteligencia y contrainteligencia.
    c. Información que pueda generar daño de derechos a personas naturales o jurídicas
    d. Información que pueda generar daño a los intereses públicos.
3. Dado que la directiva mencionada establece prohibiciones específicas en cuanto a la información clasificada, se puede entender que un entorno de aplicación de la tendencia BYOD sería viable para el sector Defensa siempre y cuando se limite o prohíba el tratamiento de información clasificada.

4. La información generada por organismos de inteligencia, al igual que la correspondiente al desarrollo de operaciones militares, dada su criticidad, quedaría excluida categóricamente de cualquier entorno BYOD.
5. Toda información considerada como pública no tendría limitaciones para el uso en entornos BYOD.
6. Dado que una gran cantidad de documentos que generan las instituciones y entidades pertenecientes al sector Defensa son de carácter público, limitando a un pequeño porcentaje de documentos clasificados, es viable la implementación de proyectos BYOD en las instituciones pertenecientes a este sector.

Teniendo en cuenta las aclaraciones anteriores, podemos concluir que si bien es cierto que las instituciones del sector Defensa en muchos casos tienen autorización para el tratamiento de información clasificada, este tipo de información corresponde a un porcentaje realmente pequeño del total de información que se genera. Por ello, dado que la excepción no debe convertirse en norma, la implementación de entornos BYOD en el sector Defensa es un avance legalmente viable, siempre y cuando se cumpla con la normatividad vigente. Adicionalmente, este podría ser el momento oportuno para que el Ministerio de Defensa Nacional impulse un proyecto de ley que vaya encaminado a estudiar con mayor profundidad los alcances legales del BYOD y sus implicaciones, para de esta manera generar jurisprudencia en este aspecto que sea utilizable no solamente para el sector Defensa sino para todos los sectores gubernamentales, públicos y privados del país, lo cual colocaría al país a la vanguardia en cuanto a legislación en este aspecto.

1.8 Encuesta de percepción del BYOD

Dado que existen pocos estudios e investigaciones sobre el fenómeno BYOD en Colombia, y aún menos en el sector Defensa, se desarrolló una encuesta con el fin de, por un lado, medir la percepción que se tiene sobre el BYOD en organizaciones de todo tipo en Colombia, y por otro lado, demostrar la necesidad e importancia de desarrollar investigación que permita la

creación de políticas para aplicar el BYOD en las empresas y/o entidades del sector Defensa, basados en la idea que sobre el tema tienen los encuestados.

La encuesta fue orientada a estudiantes de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra de Colombia, pertenecientes a las cohortes 2, 3 y 4, que en total suman 96 personas. Dado que la encuesta fue de carácter voluntario, 55 estudiantes accedieron a ser encuestados. La encuesta se realizó entre el 13 y el 19 de julio de 2018, por medio de la herramienta Google Forms, la cual permite generar encuestas en línea para ser resueltas vía Internet desde computadores o dispositivos móviles. La difusión de la misma se realizó a través de correo electrónico académico de los estudiantes y por medio de grupos de Whatsapp.

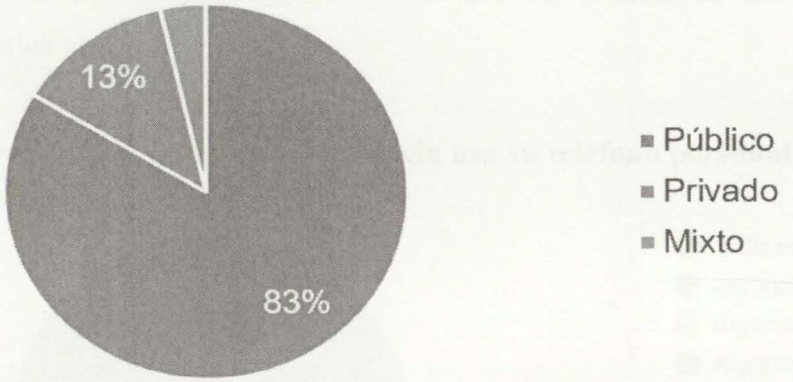
La encuesta constó de 17 preguntas, una de respuesta corta y las demás de selección múltiple con única respuesta. De igual manera, a pesar de que la tendencia BYOD involucra todo tipo de dispositivos como computadores portátiles, smartphones, tablets y relojes inteligentes entre otros, la encuesta se centró en los teléfonos inteligentes, puesto que hoy en día son la principal herramienta de comunicación e interacción digital en Colombia y el mundo. A continuación, se describen los resultados de la encuesta por cada una de las preguntas realizadas.

Pregunta 1: Por favor escriba el nombre de la organización a la que pertenece.

Dentro de las entidades a las que pertenecen los encuestados se encuentran algunos ministerios como el Ministerio de Defensa, el Ministerio de Justicia y el Ministerio de Agricultura y Desarrollo Rural; en cuanto a las Fuerzas Militares, tenemos encuestados pertenecientes al Comando General de las Fuerzas Militares, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea; algunos órganos de control como la Contraloría General de la República y la Fiscalía General de la Nación; Algunas otras entidades estatales como el ICFES, el ICBF, la Agencia de Desarrollo Rural, la Dirección Nacional de Inteligencia, entre otros. De igual manera, algunos encuestados pertenecen a empresas del sector privado como Softtek, Thomas Greg Colombia, Telefónica Movistar, entre otros. Esta gran variedad de organizaciones nos permite obtener una visión general de la percepción del BYOD tanto en el sector público como en el sector privado, de entidades el sector Defensa, pero también de otras

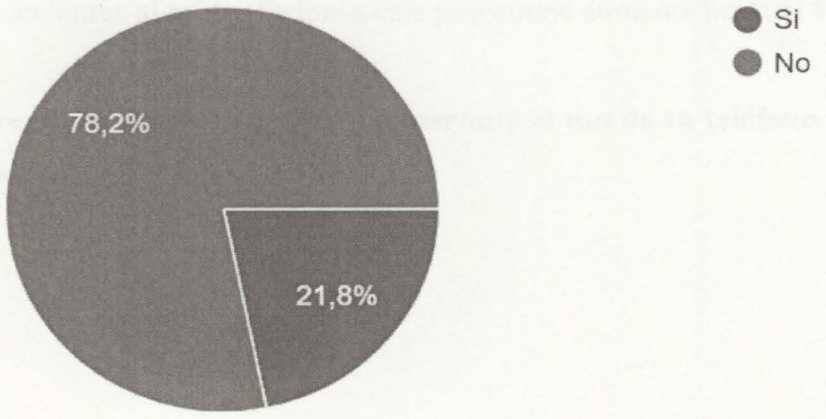
entidades de otros sectores de gran importancia para el país. Es importante resaltar que el 58.2% de los encuestados pertenecen al sector Defensa en Colombia.

Pregunta 2: La compañía o institución a la que pertenece es de carácter:



El 83.6% de los encuestados pertenece el sector público, frente a un 12.7% que pertenece al sector privado, y sólo un 3,6% pertenece al sector mixto. Esto nos permite ver que la mayoría de nuestros encuestados pertenecen a entidades del gobierno, y como vimos en la pregunta anterior, el 58.2% de los encuestados pertenece al sector Defensa específicamente.

Pregunta 3: La compañía o institución a la que usted pertenece, ¿le asignó un teléfono corporativo para realizar las actividades laborales?



La encuesta nos indica que solo al 21,8% de los encuestados le ha sido entregado un teléfono en su trabajo, mostrando que son relativamente pocas las organizaciones que destinan rubros específicos para dispositivos corporativos. En cuanto a los encuestados pertenecientes al sector Defensa, tan solo 12,5% tiene un teléfono corporativo, por lo cual más del 87% de los funcionarios encuestados debe hacer uso de su teléfono móvil personal para actividades laborales.

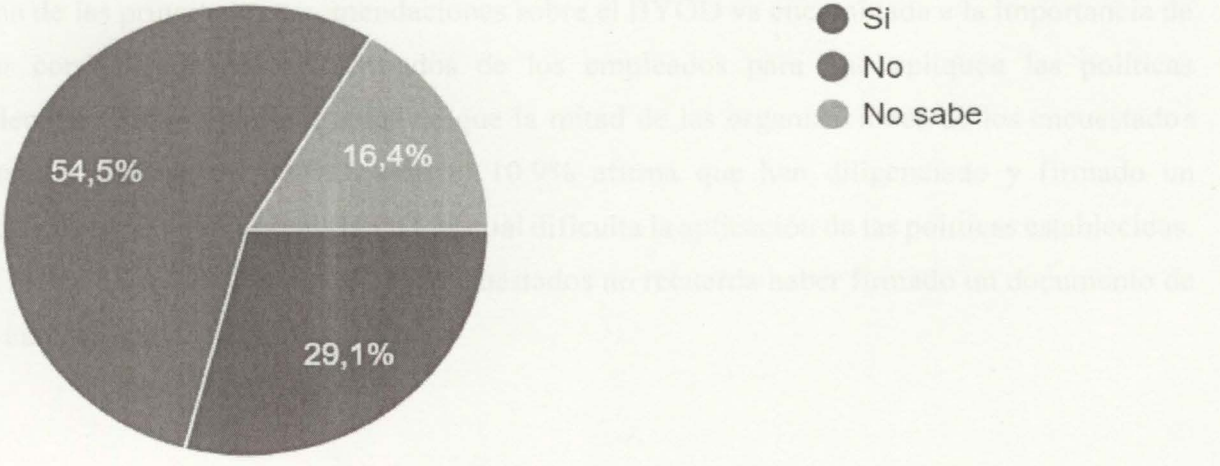
Pregunta 4: ¿Con que frecuencia usa su teléfono personal para actividades laborales?

Con respecto a la frecuencia con que los encuestados utilizan su teléfono personal en actividades laborales, el 83,6% de los encuestados manifiestan usarlo todo el tiempo o al menos algunas veces al día. Esto indica que con alta frecuencia se accede a información corporativa desde teléfonos personales, con los riesgos que esto conlleva. En cuanto a los encuestados pertenecientes al sector Defensa este porcentaje aumenta hasta el 93,8%.

Pregunta 5: ¿Su organización permite el uso de su teléfono personal para actividades laborales?

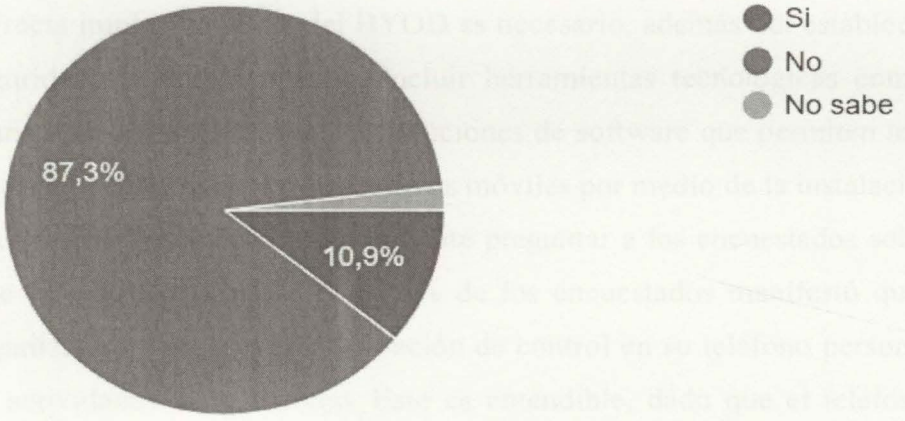
Esta pregunta muestra que cerca de la mitad de los encuestados manifiestan que sus organizaciones no tienen ningún reparo en cuanto al BYOD. El 40%, a pesar de permitirlo, lo hace con algunas restricciones, y tan solo el 5% no lo permite. En cuanto al sector Defensa la tendencia es muy similar, donde encontramos que el 50% puede emplear sus dispositivos personales sin ningún tipo de restricción, frente al 47% que lo permite con restricciones. Es importante anotar que las restricciones que manifiestan los encuestados en su mayoría vienen de la interpretación de las normas emitidas en la Directiva 2014-18 de Seguridad de la Información, del Ministerio de Defensa Nacional.

Pregunta 6: ¿Su organización tiene establecida una política formal para regular el uso de teléfonos personales en actividades laborales?



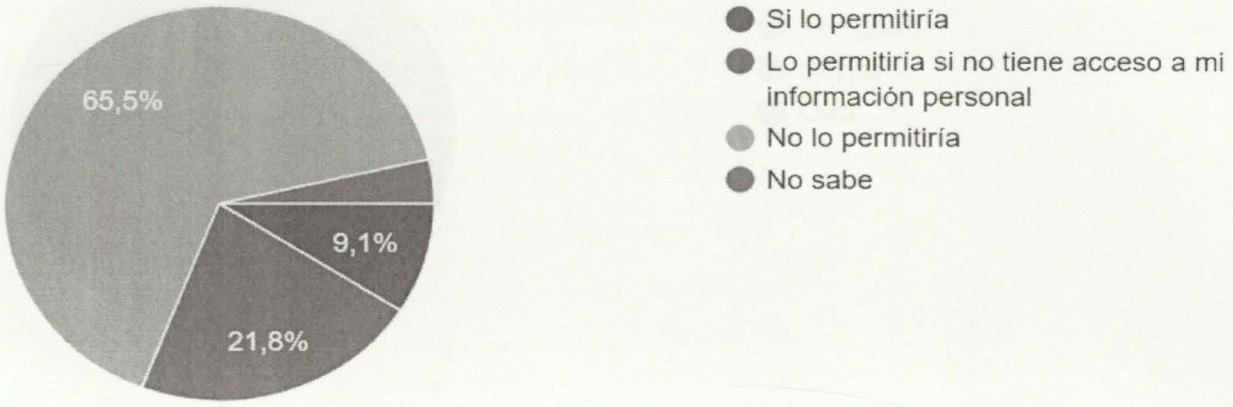
Esta pregunta nos permite identificar si las organizaciones tienen una política de BYOD establecida, o si la misma es de conocimiento de los funcionarios. Se observa que el 54,5% manifiesta que no existe tal política, frente al 29,1% donde si existe. Estos datos coinciden con los diferentes estudios a nivel global sobre BYOD, donde se ha encontrado que aún las empresas no han dado pasos decisivos en esta dirección a pesar de que la tendencia crece año a año. En cuanto al sector Defensa, solo el 25% de los usuarios manifiestan que conocen una política BYOD en sus instituciones, frente al 60% que dice que no existe tal política. Esto indica que algunas instituciones del sector han hecho algunos avances en la materia, sin embargo, es necesario que estas políticas se apliquen a todo el sector.

Pregunta 7: ¿Su organización lo obliga a diligenciar y firmar algún documento para poder usar su teléfono personal en actividades laborales?



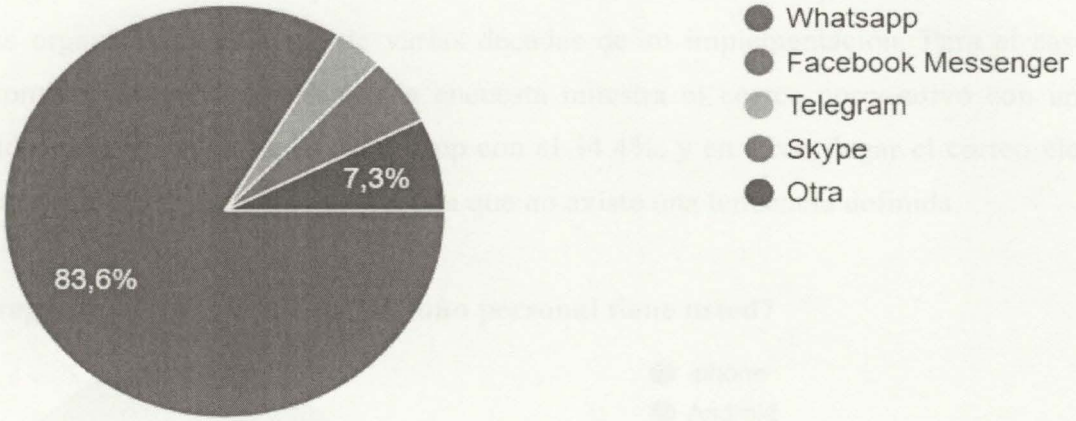
Una de las principales recomendaciones sobre el BYOD va encaminada a la importancia de contar con consentimientos firmados de los empleados para que apliquen las políticas establecidas. Sin embargo, a pesar de que la mitad de las organizaciones de los encuestados tienen una política de BYOD, solo el 10.9% afirma que han diligenciado y firmado un documento para poder usar el BYOD, lo cual dificulta la aplicación de las políticas establecidas. En el sector Defensa el 90.6% de los encuestados no recuerda haber firmado un documento de estas características.

Pregunta 8: ¿Permitiría usted que su organización instale una aplicación de control en su teléfono personal para poder usarlo en actividades laborales?



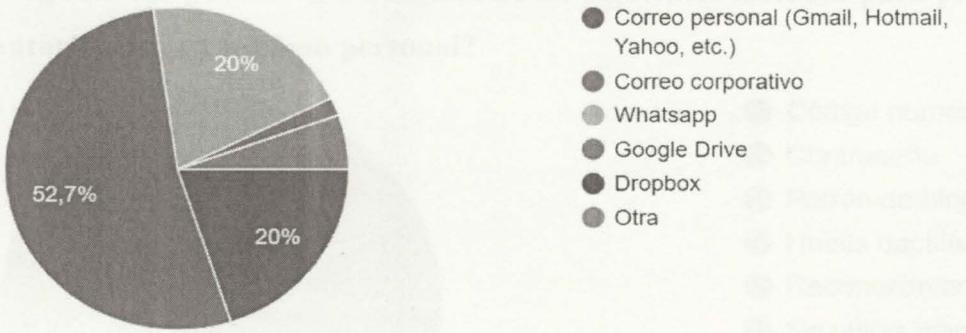
Dado que los estudios e investigaciones que se consultaron recomiendan que para una correcta implementación del BYOD es necesario, además del establecimiento de políticas de seguridad de la información, incluir herramientas tecnológicas como los Mobile Devices Management (MDM), que son soluciones de software que permiten tener una administración y control centralizado de dispositivos móviles por medio de la instalación de una aplicación en el dispositivo, se consideró pertinente preguntar a los encuestados sobre su posición frente a este tipo de tecnologías. El 65.5% de los encuestados manifestó que no permitiría que su organización instalara una aplicación de control en su teléfono personal para poder utilizarlo en actividades de su trabajo. Esto es entendible, dado que el teléfono es de propiedad del empleado, y además existe el miedo de que su información personal pueda ser monitoreada por su empleador. En el caso del sector Defensa específicamente, este porcentaje aumenta al 72% de negativas. El 22% de los encuestados permitiría la instalación siempre y cuando el empleador no tenga acceso a su información personal. Solo un 3% estuvo de acuerdo en instalar la aplicación sin condiciones.

Pregunta 9: ¿Cuál de las siguientes aplicaciones utiliza usted con mayor frecuencia para comunicarse con personas de su organización?



En vista de que muchos de los encuestados utilizan BYOD (algunos de manera inadvertida), es necesario conocer cuáles son las aplicaciones preferidas para comunicarse con sus compañeros de trabajo, con el fin de medir que tan expuesta está la información con base en la seguridad de la aplicación. El 83.6% de las encuestados utilizan la aplicación de mensajería instantánea Whatsapp, la plataforma de chat más usada en el mundo occidental. En el caso de los miembros del sector Defensa, el 94% manifestó usar Whatsapp como su aplicación preferida para comunicarse con personas de su organización.

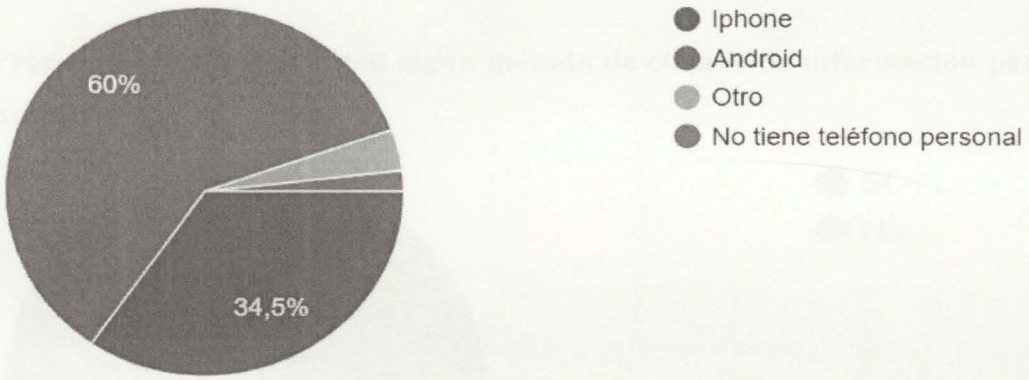
Pregunta 10: ¿Cuál de las siguientes aplicaciones utiliza usted con mayor frecuencia para compartir documentos y archivos con personas de su organización?



Además de la comunicación, es necesario conocer qué aplicaciones se utilizan para compartir documentos. Un poca más de la mitad de los encuestados dijo utilizar el correo electrónico corporativo para dichos fines, seguido por el correo electrónico personal y

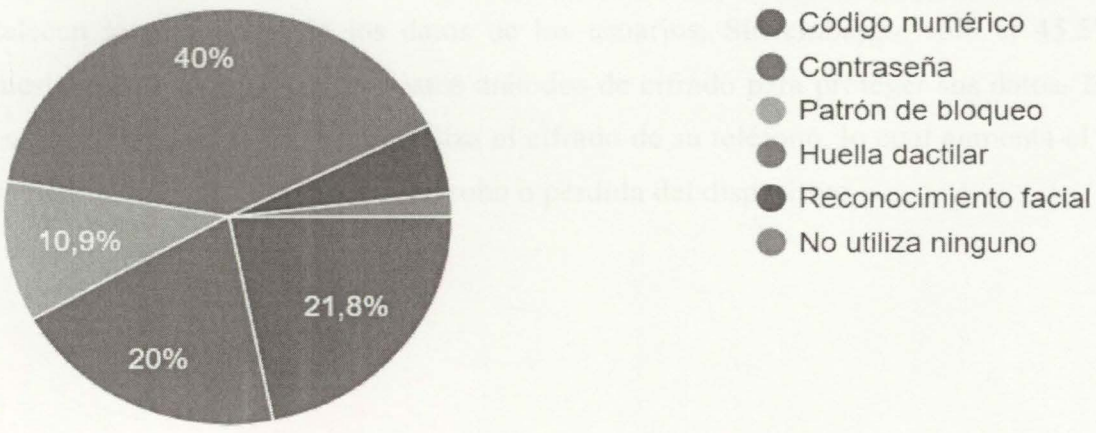
Whatsapp. Esto se puede explicar debido a la madurez que ha adquirido el correo electrónico en las organizaciones, luego de varias décadas de su implementación. Para el caso de los funcionarios del sector Defensa, la encuesta muestra el correo corporativo con un 37.5%, seguido muy de cerca por el Whatsapp con el 34.4%, y en tercer lugar el correo electrónico personal con un 25%, lo que demuestra que no existe una tendencia definida.

Pregunta 11: ¿Qué tipo de teléfono personal tiene usted?



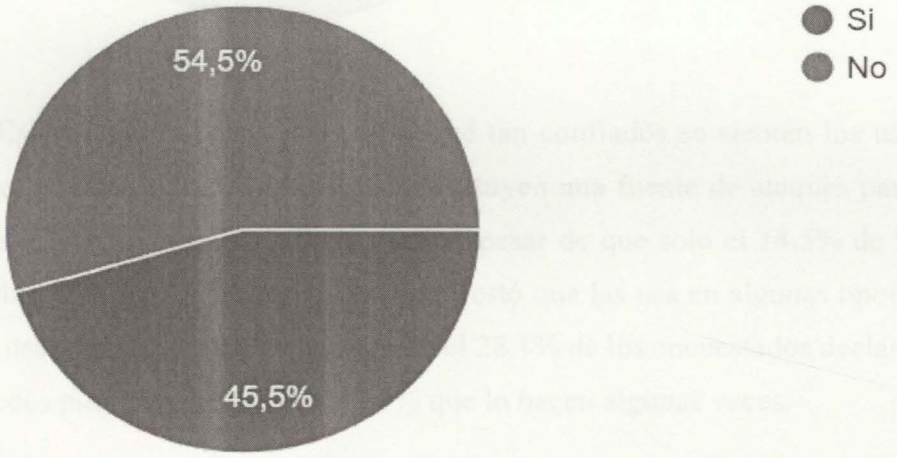
Con respecto al sistema operativo de los teléfonos personales de los encuestados, el 60% tiene teléfono con Android, frente al 34,5% que tiene un iPhone. En el sector Defensa la tendencia es similar, con un 62.5% de teléfonos Android frente al 34.4% de teléfonos con iOS.

Pregunta 12: ¿Utiliza usted alguno de los siguientes métodos para proteger el ingreso no autorizado a su teléfono personal?



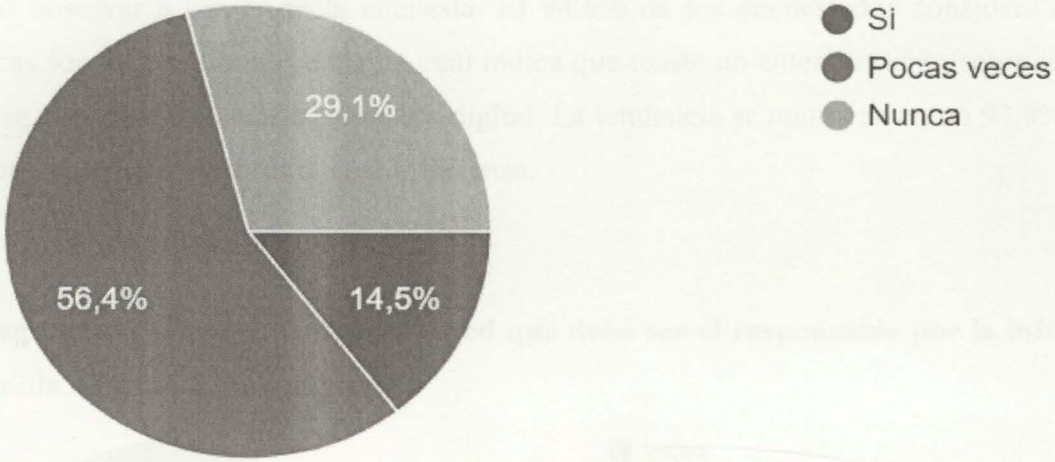
Es importante conocer cómo los encuestados protegen el acceso a su dispositivo. Para el caso, el 40% manifestó utilizar el sensor de huella dactilar, seguido de un 21,8% que utiliza un código numérico, un 20% protege a través de contraseña y un 10,9% que emplea un patrón de bloqueo. En cuanto a los encuestados que pertenecen al sector Defensa, encontramos un 43,8% que utiliza la huella dactilar, seguido por un 25% con código numérico, un 15.6% utilizan el patrón de bloqueo y un porcentaje muy pequeño que usa contraseñas y otros métodos, como el reconocimiento facial.

Pregunta 13: ¿Utiliza usted algún método de cifrado de información para su teléfono personal?



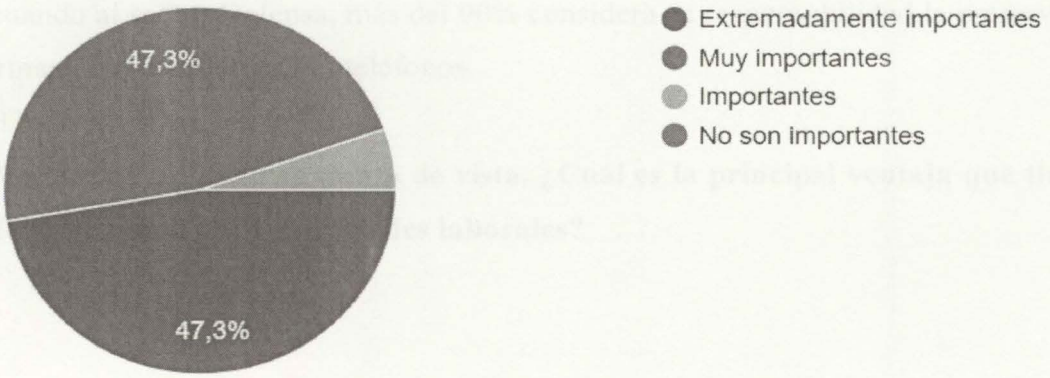
Hoy en día tanto el sistema operativo Android como iOS incluyen herramientas nativas de cifrado de los medios de almacenamiento utilizados (memoria interna o tarjetas micro SD) que fortalecen la protección de los datos de los usuarios. Sin embargo, sólo el 45.5% de los encuestados afirmó que utilizan estos métodos de cifrado para proteger sus datos. En el caso del sector Defensa, el 53.1% no utiliza el cifrado de su teléfono, lo cual aumenta el riesgo de filtración de información en caso de robo o pérdida del dispositivo.

Pregunta 14: ¿Utiliza usted redes públicas (como las de aeropuertos, tiendas de café, restaurantes, etc.) con su teléfono personal?



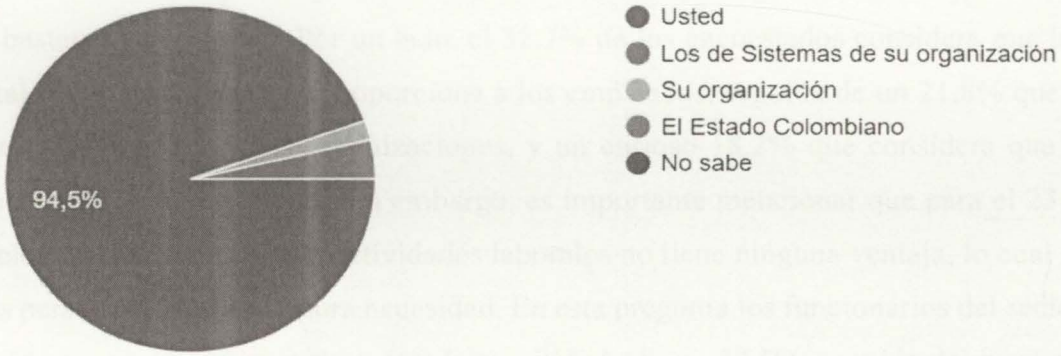
Esta pregunta buscó identificar qué tan confiados se sienten los usuarios en cuanto a las redes públicas, puesto que éstas constituyen una fuente de ataques para robo de información más utilizadas por los delincuentes. A pesar de que solo el 14.5% de los encuestados afirmó utilizar redes públicas, el 56,4% manifestó que las usa en algunas oportunidades. En cuanto a los usuarios del sector Defensa, solo el 28.1% de los encuestados declaró que nunca se conecta a redes públicas, frente a un 62.5% que lo hacen algunas veces.

Pregunta 15: ¿Qué tan importantes son para usted las políticas de seguridad de la información?



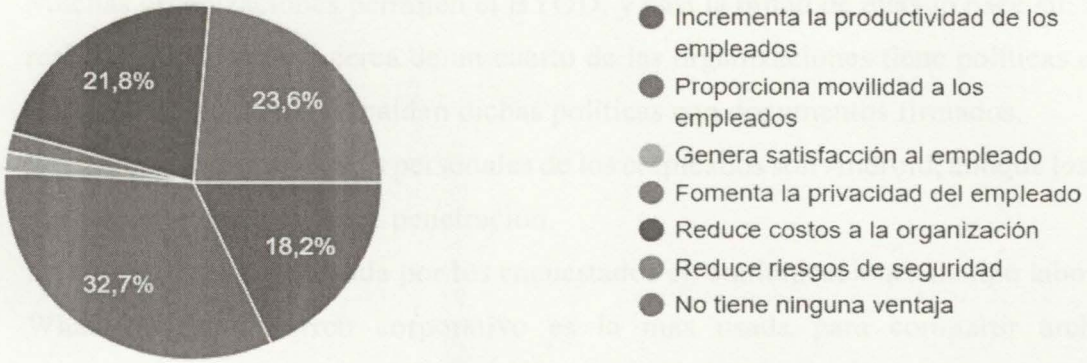
Los encuestados son muy conscientes de la importancia de las políticas de seguridad de la información, a pesar de que incumplen muchas de ellas de manera consciente, como se ha podido observar a través de la encuesta. El 94.6% de los encuestados considera que éstas políticas son de vital importancia, lo cual indica que existe un entendimiento sobre los riesgos a que se exponen los usuarios en la era digital. La tendencia se mantiene en un 93.8% para los funcionarios pertenecientes al sector Defensa.

Pregunta 16: ¿Quién considera usted que debe ser el responsable por la información contenida en su teléfono personal?



Esta pregunta se realizó con el fin de medir el nivel de responsabilidad que asumen los encuestados sobre la información contenida en sus dispositivos. Casi todos coinciden de que es su propia responsabilidad el proteger sus dispositivos y la información contenida en ellos, a pesar de que han demostrado que no utilizan todas las herramientas a su alcance para este fin. En cuando al sector Defensa, más del 90% considera su responsabilidad la preservación de la información contenida en sus teléfonos.

Pregunta 17: Según su punto de vista, ¿Cuál es la principal ventaja que tiene usar el teléfono personal para actividades laborales?



La última pregunta de la encuesta se realizó con el fin de conocer lo que piensan los encuestados sobre las ventajas o desventajas de la tendencia BYOD. Las respuestas obtenidas son bastante interesantes. Por un lado, el 32.7% de los encuestados considera que la principal ventaja es la movilidad que proporciona a los empleados, seguida de un 21,8% que cree en la reducción de costos a las organizaciones, y un curioso 18.2% que considera que el BYOD reduce riesgos en seguridad. Sin embargo, es importante mencionar que para el 23.6% el uso de teléfonos personales para actividades laborales no tiene ninguna ventaja, lo cual indica que estas personas lo usan por pura necesidad. En esta pregunta los funcionarios del sector Defensa consideraron como principal ventaja la movilidad con un 37.5%, seguida del incremento de la productividad (21.9%) y la reducción de costos para las instituciones (12.5%). Al igual que el total de los encuestados, un 25% de los funcionarios considera que la tendencia BYOD no aporta ninguna ventaja.

En resumen, de la aplicación de esta encuesta podemos obtener algunas conclusiones, que nos facilitan la labor de entender la percepción que tienen los encuestados sobre la tendencia BYOD:

1. Un número reducido de organizaciones está dispuesta a asumir los costos de asignar teléfonos corporativos a sus empleados. Este número es aún más reducido en el caso de las entidades del sector Defensa.
2. La gran mayoría de nuestros encuestados admitió que usa su teléfono personal para actividades laborales.

3. Muchas organizaciones permiten el BYOD, y casi la mitad de ellas lo hace sin ninguna restricción. De hecho, cerca de un cuarto de las organizaciones tiene políticas claras al respecto y muy pocas respaldan dichas políticas con documentos firmados.
4. La mayoría de los teléfonos personales de los empleados son Android, aunque los iPhone han venido aumentando en penetración.
5. La aplicación más utilizada por los encuestados en comunicaciones de tipo laboral es el Whatsapp, y el correo corporativo es la más usada para compartir archivos y documentos.
6. Dado que los encuestados son conscientes de la propiedad de sus equipos, muy pocos estarían dispuestos a permitir que la organización a la que pertenecen pueda tener un comando y control de su teléfono, lo cual hace que exista cierta resistencia a la implementación de los MDM.
7. Los usuarios son muy conscientes de la importancia de la seguridad de su información, de hecho, asumen esa responsabilidad y utilizan las herramientas que tienen disponibles para evitar el acceso no autorizado a sus dispositivos. Casi la mitad de ellos cifra su teléfono para proteger su información, y evita conectarse a redes públicas.
8. La mayoría de los encuestados considera que el BYOD trae algunas ventajas en sus actividades laborales, principalmente que proporciona movilidad a los empleados.

Como conclusión final, basados en lo observado a través del instrumento encuesta, podemos observar que a pesar de que no se ha estudiado este fenómeno en profundidad en Colombia, la investigación es muy pertinente para identificar todas las aristas a tener en cuenta para enfrentar la problemática del BYOD. Si a esto le sumamos una propuesta sobre la manera como se pueden implementar este tipo de entornos en las organizaciones, podemos situar el BYOD como una posibilidad real en cualquier organización, trabajando conjuntamente en aspectos legales, técnicos, organizacionales y procedimentales que brinden las herramientas adecuadas para la implementación.

2. Capítulo Dos. Evaluación de riesgos propuesta para las entidades del sector Defensa

Con el fin de dar alcance a uno de los objetivos específicos del presente trabajo de grado, se presenta una evaluación de riesgos propuesta como punto de partida para evaluar la viabilidad de la implementación de BYOD en las instituciones que componen el sector Defensa. Esta propuesta se desarrolla tomando como referencia diferentes frameworks analizados en el numeral 1.6 del presente trabajo, los cuales fueron estudiados y contextualizados para el sector Defensa en Colombia, por lo cual se extrajeron los aspectos más relevantes que aplican al contexto definido.

2.1 Consideraciones para la evaluación de riesgos

El sector Defensa en Colombia está conformado por todas las instituciones que participan de una u otra manera en la seguridad y defensa del país. El sector está dividido en Sector Central, conformado por las Fuerzas Militares y de Policía, y los institutos descentralizados, los cuales tienen fines y particularidades de acuerdo a su misión y que conforman el Grupos Social y Empresarial de la Defensa (GSED). En la siguiente tabla se ilustran las entidades que componen el sector Defensa:

SECTOR	INSTITUCIÓN
SECTOR CENTRAL	Ministerio de Defensa Nacional (MinDefensa)
	Comando General de las Fuerzas Militares de Colombia (CGFM)
	Ejército Nacional (EJC)
	Armada Nacional (ARC)
	Fuerza Aérea Colombiana (FAC)
	Dirección Policía Nacional
	Dirección de Policía Judicial e investigación (DIJIN)
GSED – APOYO LOGÍSTICO	Agencia Logística de las Fuerzas Militares (AGLO)
	Industria Militar- INDUMIL

	Corporación de la Industria Aeronaútica de Colombia (CIAC)
	Fondo Rotatorio de la Policía Nacional
	Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial (COTECMAR)
GSED - BIENESTAR	Caja de Retiro de las Fuerzas Militares (CREMIL)
	Caja de Sueldos de Retiro de la Policía Nacional (CASUR)
	Club Militar
	Caja Promotora de Vivienda Militar y Policía (CAJAHONOR)
	Hospital Militar Central
	Instituto de Casas Fiscales del Ejército (ICFE)
	Universidad Militar Nueva Granada (UMNG)
	Círculo de Suboficiales de las Fuerzas Militares
	Sociedad Hotelera Tequendama S.A
	Corporación Matamoros
GSED – APOYO SEGURIDAD	Superintendencia de Vigilancia y Seguridad Privada (SuperVigilancia)
	Defensa Civil Colombiana
	Servicio Aéreo a Territorios Nacionales (SATENA)
	Corporación de Alta Tecnología (CODALTEC)

Fuente: Página web del Ministerio de Defensa Nacional (www.mindefensa.gov.co)

Dada la variedad de instituciones que conforman este sector, además de los diversos grados de complejidad del manejo de la seguridad de la información de cada una en función de la cantidad de personal y las funciones que se desempeñan, resulta muy complejo establecer un análisis de riesgos general para todo el sector. Por ello, se propone que cada una de las entidades adelante su propia evaluación de riesgos, para lo cual se propone que se utilice como pnto de partida la tabla que se incluye en el numeral 2.3.

2.2 Riesgos de carácter general a tener en cuenta

En general, podemos atribuir los riesgos del BYOD a dos aspectos: los dispositivos móviles y los usuarios de los mismos. A continuación, se enumeran algunos riesgos generales a

considerar para las entidades que quieran estudiar la posible implementación de ambientes BYOD en el sector Defensa, discriminados en estos dos aspectos.

Riesgos referentes a la naturaleza de los dispositivos móviles personales:

- Pérdida, daño o robo de los dispositivos móviles.
- Falta de actualizaciones de parches seguridad y de los sistemas operativos de los dispositivos móviles, lo cual facilita la explotación de vulnerabilidades asociadas a las diferentes versiones de los sistemas operativos desactualizados.
- Vulnerabilidades asociadas a la conexión e interceptación de comunicaciones vía Wi-Fi, NFC, Bluetooth, etc.
- Vulnerabilidades asociadas a arquitecturas de comunicación 2G, 2.5G, 3G y 4G.
- Acceso no autorizado a información almacenada en medios de almacenamiento extraíble o interno de los dispositivos móviles.
- Dispositivos con sistemas operativos modificados (root, jailbreak, etc.)
- Adquisición y uso de dispositivos móviles de segunda mano.
- Explotación de vulnerabilidades asociadas a fabricantes, modelos y partes específicas.
- Explotación de vulnerabilidades de los métodos de acceso a los dispositivos.
- Explotación de vulnerabilidades de los circuitos integrados y de la arquitectura de hardware y software con el que vienen de fábrica los dispositivos móviles.
- Acceso de personas no autorizadas a la información de los dispositivos móviles por medio de interconexión de los dispositivos con otros sistemas y sincronizaciones.
- Falta de sensibilización de los funcionarios en cuanto a seguridad y privacidad de la información en este tipo de dispositivos.

Riesgos referentes a malas prácticas de los usuarios de los dispositivos móviles personales:

- Ataques de Ingeniería Social enfocados a los usuarios.
- Instalación de aplicaciones de terceros, no autorizadas por las tiendas de aplicaciones.

- No utilización de controles de acceso a los dispositivos, o uso de contraseñas y patrones débiles.
- Almacenamiento de información sensible sin cifrar, tanto personal como laboral, en los dispositivos móviles.
- Ataques por medio de direcciones URL falsas, códigos QR, URL en mensajes de texto, descarga y ejecución de archivos dañinos.
- Aprobación no verificada de los permisos para las aplicaciones.
- Omisión del cifrado de los medios de almacenamiento de los dispositivos.
- Cesión o préstamo de los dispositivos móviles a terceras personas.
- Intercambio de información sensible sin utilización de canales cifrados adecuados (VPN)
- Uso indiscriminado de redes Wifi públicas.
- Activación permanente de medios de conectividad inalámbrica como Wi-Fi, Bluetooth, NFC, a pesar de no requerirse todo el tiempo.
- Conexión de los dispositivos móviles a computadores desconocidos y dispositivos de carga de baterías en sitios públicos.
- Uso indiscriminado del GPS por parte de aplicaciones que no requieren su utilización.

2.3 Evaluación de riesgos propuesta para las entidades del sector Defensa

Con base en la caracterización de riesgos analizada, a continuación, se presenta una tabla que resume los aspectos más relevantes a considerar para realizar una evaluación de riesgos sobre la implementación del BYOD en las entidades que componen el sector Defensa. Esta tabla se elaboró con base en la propuesta presentada en el estudio "Riesgos de seguridad asociados al uso de dispositivos móviles personales (smartphone - Android) en entornos BYOD" (Cadena-Herrera, 2018) y complementada con las recomendaciones obtenidas por el Modelo Nacional de Gestión de Riesgos de Seguridad Nacional del MinTIC de Colombia y de la norma NTC-ISO/IEC 27005:2009.

ÍTEM	Riesgo	Objetivos de Control	Controles	Pruebas de Cumplimiento
R1 - Gobierno	Incumplimiento de normatividad legal con respecto a la protección de datos personales y al tratamiento de información reservada, o de desconocimiento de amenazas asociadas a BYOD	Proteger a la entidad contra la materialización de incumplimientos de tipo legal, jurídico y normativo.	Procedimiento de verificación de leyes nacionales, internacionales e internas de la entidad que debe aplicar.	Verificar la documentación existente, de la normatividad vigente aplicada a BYOD.
		Proteger a la entidad contra la materialización de ataques de código malicioso desde los dispositivos móviles.	Procedimiento de estudio de amenazas, asociadas a los dispositivos móviles.	Verificar la documentación de las amenazas asociadas a los dispositivos móviles, en particular a los teléfonos inteligentes
R2 - Gobierno	Desconocimiento de las políticas y directrices de la entidad.	Proteger a la entidad de la materialización de riesgos de seguridad por desconocimiento de las medidas de seguridad, por parte de los empleados y usuarios.	Procedimiento de verificación de campañas de sensibilización y de divulgación oportuna de políticas, directrices e información relevante.	Verificar la documentación que la entidad ha elaborado, actualizado y divulgado respecto al uso de los dispositivos móviles y de BYOD.
R3 - Gobierno	Accesos no autorizados a las redes y sistemas de información de la entidad	Proteger los sistemas de información, los sistemas y la infraestructura de la entidad del robo, modificación, pérdida y/o secuestro de información.	Procedimiento de verificación de documentación de usuarios con acceso por BYOD, dispositivos, permisos y procesos de autorización y revocatoria de acceso a servicios.	Verificar la documentación que la entidad ha elaborado, divulgado y publicado respecto al alcance, restricciones y revocatoria de acceso a BYOD.
R4 - Gestión de Dispositivos	Ausencia de consentimiento informado de la Privacidad de la Información de los Dispositivos Móviles, firmado por los funcionarios y/o usuarios.	Proteger la seguridad y privacidad de la información corporativa y personal de los dispositivos móviles.	Procedimiento de verificación de existencia, aceptación y firma de los consentimientos informados, en los cuales se permita el monitoreo de los dispositivos móviles y acciones de respaldo y/o eliminación de información	Verificar la existencia y funcionalidad de procesos y procedimientos de monitoreo, respaldo y/o eliminación de información de los dispositivos móviles.
R5 - Gestión de Dispositivos	Desactualización de listas blancas de dispositivos permitidos que acceden a la red y a los sistemas de información	Garantizar la disponibilidad de acceso de los dispositivos permitidos.	Procedimiento de verificación de control de acceso de dispositivos y usuarios.	Verificar la existencia de herramientas de monitoreo de acceso de dispositivos a la red.

ÍTEM	Riesgo	Objetivos de Control	Controles	Pruebas de Cumplimiento
	Desactualización de listas negras de dispositivos rechazados que no están autorizados para acceder a la red y a los sistemas de información	Proteger la red de la entidad de accesos no autorizados.	Procedimiento de monitoreo de actividades de los dispositivos y verificación de listas blancas y negras de dispositivos.	Verificar la existencia de herramientas de monitoreo de registro de actividad de los dispositivos.
R6 - Gestión de Dispositivos	Ausencia de Políticas de seguridad y de uso de BYOD	Proteger la información, los sistemas de información de la entidad y los dispositivos móviles e información de los usuarios de BYOD.	Procedimiento de verificación de existencia, aplicabilidad, actualización concientización y divulgación de las políticas de BYOD.	Verificar la existencia y aplicación de políticas para el acceso de usuarios y dispositivos al BYOD.
R7 - Gestión de Dispositivos	Instalación de software ilegal o inseguro que facilite el robo o pérdida de información	Proteger la entidad del uso de software o aplicaciones ilegales, posibles violaciones de seguridad y violación de derechos de autor, así como también de la instalación y uso de aplicaciones de terceros que no han sido comprobadas y autorizadas por la entidad	Validar la gestión del software por medio de herramientas automatizadas de gestión, instalación y desinstalación de software, en los dispositivos permitidos.	Verificar la existencia de los procedimientos de administración y gestión de dichas plataformas para el monitoreo y reporte de aplicaciones permitidas y no permitidas.
		Proteger los dispositivos de instalación de código malicioso.	Validar la existencia de lineamientos de prohibición de instalación y uso de aplicaciones no avaladas por la entidad.	Verificar reportes de aplicaciones detectadas en los dispositivos.
R08 - Red de datos	Fallo o interrupción en las comunicaciones.	Mantener la conectividad de los dispositivos entre ellos y hacia los aplicativos y servicios.	Procedimiento de implementación de dispositivos de conectividad redundantes.	Verificar que se cuenta con un plan de contingencia de conectividad LAN – WAN
				Verificar la documentación y pruebas del procedimiento de alta disponibilidad de comunicaciones.

ÍTEM	Riesgo	Objetivos de Control	Controles	Pruebas de Cumplimiento
R9 - Software Antivirus	Propagación de Virus por la Red y/o Instalación de código malicioso que tenga privilegios de robo de información.	Proteger la plataforma tecnológica de la organización de propagaciones de virus por medio de la red.	Procedimiento de gestión y administración de herramientas Antivirus y políticas.	Verificar las estadísticas o reportes de los últimos 60 días en cuanto a infección y desinfección.
				Verificar que las actualizaciones de la consola Antivirus no sean superiores a 30 días.
R10 - Gestión de autorizaciones	Acceso de usuarios no autorizados a BYOD.	Prevenir el ingreso de usuarios no autorizados a la plataforma BYOD.	Procedimiento de aprobación o denegación de acceso a BYOD.	Verificar que existe una política de control y denegación de acceso.
	Cambios no autorizados o sin adecuado seguimiento.	Validar las actividades que realizan los usuarios y dispositivos móviles en BYOD.	Procedimiento de monitoreo, revisión de control de acceso y verificación de cambios realizados.	Comprobar que se lleva un registro de accesos y actividades sobre los servicios BYOD y un registro detallado de control de cambios.
R11 - Seguridad de los dispositivos	Vulnerabilidades asociadas a cada versión de iOS y Android	Mantener la confidencialidad disponibilidad e integridad de la información en los dispositivos móviles.	Procedimiento de verificación y pruebas de seguridad en los dispositivos móviles.	Verificar la documentación relacionada con incidentes de seguridad de los dispositivos móviles.
R12 - Seguridad de los dispositivos	Obsolescencia de actualizaciones y parches de seguridad de los sistemas operativos iOS y ANDROID así como de las aplicaciones de los dispositivos móviles.	Actualización y parches de seguridad de los sistemas operativos iOS y ANDROID y aplicaciones de los dispositivos móviles.	Procedimiento de verificación de actualización y parches de seguridad de los sistemas operativos iOS y ANDROID y aplicaciones de los dispositivos móviles.	Verificar las evidencias de actualizaciones y parchado de seguridad y que los modelos de dispositivos que se admiten puedan contar con actualizaciones por parte del fabricante (Apple, Samsung, Sony, Huawei, HTC, LG, Motorola, otros)
R13 - Seguridad de la información	Fallas de los controles de autenticación.	Evitar la suplantación de usuarios y accesos no autorizados.	Procedimiento de autenticación de usuarios, control de acceso a los sistemas de información y conectividad, autenticación en dos pasos.	Verificar la documentación de cuentas de usuario, permisos de acceso y métodos de autenticación.

ÍTEM	Riesgo	Objetivos de Control	Controles	Pruebas de Cumplimiento
R14 - Seguridad de la información	Conexión de los dispositivos móviles a redes inseguras (redes públicas).	Proporcionar adecuados niveles de seguridad mediante el cifrado de comunicaciones y certificados que garanticen la autenticación.	Procedimiento de control de acceso a BYOD de los dispositivos móviles por medio de VPN, Cifrado, canales seguros u otros.	Verificar la documentación de las herramientas de seguridad de los dispositivos móviles.
			Campañas de sensibilización de los peligros de la conexión a redes públicas.	Verificar la documentación, temas y periodicidad de las campañas de sensibilización de seguridad informática.
R15 - Seguridad Física	Cesión o préstamo de los dispositivos móviles.	Proporcionar a los usuarios adecuada información sobre los peligros de facilitar sus dispositivos móviles a otras personas.	Procedimiento de publicación y divulgación de campañas de sensibilización.	Verificar la documentación, temas y periodicidad de las campañas de sensibilización de seguridad informática.
			Procedimiento de cifrado de la información en los dispositivos móviles.	Verificar las directrices de la organización acerca del cifrado de la información en los dispositivos móviles
R16 - Contingencia	Desastre Natural, asonada, terrorismo.	Plan de contingencia en caso de desastres naturales, asonadas, terrorismo.	Procedimiento de recuperación en caso de desastres naturales, asonadas, terrorismo.	Verificar que exista un proceso y procedimientos de recuperación.

Dado que esta es una propuesta de evaluación de riesgos de carácter general, cada entidad o institución deberá incluir los riesgos que a su juicio considere que deben tenerse en cuenta, por la naturaleza de la misma entidad y su misión y otros factores que se considere deben ser tenidos en cuenta. De igual manera, es imprescindible que esta evaluación de riesgos esté alineada con los parámetros y órdenes plasmadas en la Directiva DIR2014-18 de Seguridad de la información, emitida por el Ministerio de Defensa Nacional.

3. Capítulo Tres. Aspectos a considerar y buenas prácticas para la implementación de BYOD en instituciones del sector Defensa en Colombia

3.1 Generalidades

El presente capítulo busca ofrecer a las entidades del sector Defensa en Colombia algunos de los aspectos más importantes a considerar en el evento de que las instituciones decidan abordar la adopción de BYOD para sus funcionarios. En primer lugar, se enumeran algunas ventajas y desventajas encontradas en el BYOD, que apoyen la labor de toma de decisiones frente al BYOD en cada entidad. Posteriormente se establecen algunos aspectos a considerar por las entidades para generar una política de implementación de BYOD. Por último, se presenta un marco de buenas prácticas para la implementación de BYOD en las entidades, observadas para la creación de la política BYOD, la implementación del ambiente BYOD y la seguridad de dispositivos móviles bajo las premisas expuestas.

Esta propuesta es el resultado de la investigación realizada para obtener el estado del arte de BYOD, además del análisis de diferentes estudios e investigaciones que proponen diferentes framework para la implementación de BYOD y la generación de políticas para este tipo de ambientes.

3.2 Ventajas y desventajas del BYOD

De acuerdo a la investigación realizada, podemos deducir que las principales ventajas de la implementación de entornos BYOD en organizaciones son, entre otras, las siguientes:

Ventajas

- BYOD ofrece movilidad y flexibilidad a los funcionarios, permitiendo que éstos sean menos dependientes de sus puestos de trabajo y puedan realizar actividades laborales donde se encuentren.

- Los funcionarios portan menos cantidad de dispositivos, al no tener que cargar un teléfono personal y uno laboral.
- Los funcionarios se sienten más satisfechos con el uso de la tecnología, ya que trabajan con dispositivos escogidos por ellos mismos.
- Los funcionarios están habituados al uso de sus propios dispositivos, lo cual acelera la curva de aprendizaje y por lo tanto genera mayor productividad.
- Al tener la tecnología y los medios a la mano, se reducen los tiempos de respuesta de requerimientos laborales, mejorando el aprovechamiento del tiempo.
- Existe una reducción de costos para las entidades en dispositivos, software, licencias, seguros de hurto, etc. ya que los funcionarios asumen dichos costos.
- La entidad aprovecha dispositivos con tecnología de punta, puesto que los usuarios mismos se encargan de la renovación.
- Las entidades reducen costos en mantenimiento preventivo y correctivo de dispositivos.
- Se presenta una menor inversión económica de las entidades en capacitaciones para el manejo de nuevas tecnologías móviles, pues los funcionarios evolucionan constantemente en temas tecnológicos por su propia cuenta.
- Las entidades pueden iniciar con la implementación de herramientas o aplicaciones libres o gratuitas conocidas por los usuarios, lo cual reduce costos de licenciamiento y desarrollo.

Desventajas

- Dado que el dispositivo pertenece al funcionario, existen ciertas limitaciones legales que pueden impedir a la entidad tener un control total de los dispositivos conectados.
- Las empresas pierden cierta capacidad de control, al tener limitaciones para el acceso a los dispositivos.
- La entidad debe asumir que los dispositivos que se conectan a sus redes y consumen sus servicios son 'no seguros', lo cual obliga a reforzar la seguridad.
- El BYOD expone a las entidades a riesgos latentes con la seguridad de las redes, los sistemas de información, las infraestructuras y demás componentes tecnológicos y humanos externos.

- Se abren puertas para nuevos tipos de amenazas asociados a los dispositivos móviles.
- Requiere una constante monitoreo y seguimiento a los informes, estadísticas, boletines de seguridad y de nuevas vulnerabilidades o amenazas relacionadas con dispositivos móviles.
- Se requiere fortalecer la seguridad perimétrica de las entidades y establecer muchas nuevas políticas de seguridad, aumentando el margen de error.
- Se incurre en nuevos costos para la implementación de software de tipo Mobile Device Management (MDM), que son herramientas específicas para la administración y gestión de los dispositivos móviles.
- Se requiere dar soporte a los dispositivos móviles y sus aplicaciones, el cual demanda personal con conocimientos avanzados en este tipo de dispositivos.
- Se debe incrementar el personal y capacitación del mismo de las áreas de TI, para hacer frente a los nuevos retos administrativos, documentales, de sensibilización, de soporte y personal específico para la administración de las herramientas de gestión de dispositivos móviles.
- Los dispositivos de los funcionarios no son homogéneos, por lo cual su soporte se dificulta en gran medida.
- Los funcionarios deben dar consentimientos de autorización aceptados y debidamente firmados para poder tener acceso a la gestión y administración de sus dispositivos móviles y de su información. Algunos de los funcionarios no estarán dispuestos a firmar.
- Aumenta la exposición de la seguridad de la información y la posibilidad de explotación de vulnerabilidades en servicios web, aplicativos y otros.
- Los dispositivos de los funcionarios se vuelven un blanco de la delincuencia para extraer información clasificada o corporativa.
- El BYOD requiere de servicios en la nube (ya sea privada, púbica o híbrida) que aumenta el riesgo de exposición de la información.

3.3 Aspectos propuestos a considerar para la creación de una política del BYOD para sector Defensa

Dado que el presente trabajo de grado se centra en las entidades del sector Defensa en Colombia, es necesario establecer algunos parámetros que sirvan como punto de partida para la creación de una política de BYOD para este tipo de instituciones. Los puntos que se enumeran a continuación buscan complementar lo establecido en la Directiva Permanente DIR 2014-18 "Políticas de Seguridad de la Información para el sector Defensa". Las nuevas políticas que se creen no deben ir en contraposición con las establecidas en la directiva mencionada, por el contrario, deben complementar aquellos aspectos donde éstas no son lo suficientemente claras en cuanto al BYOD se refiere. A continuación, se proponen algunos puntos a tener en cuenta, cuya implementación y adopción quedan a discrecionalidad de la entidad que desea implementar BYOD.

- La plataforma BYOD es suministrada por la entidad para proveer al funcionario acceso a la información corporativa, así como a la utilización de los servicios proporcionados por la misma, para lo cual el funcionario acepta cumplir integra y completamente la presente política, de lo contrario su dispositivo móvil y su acceso será rechazado para los servicios BYOD.
- Los funcionarios que deseen la plataforma BYOD, deben entregar a la entidad un consentimiento firmado donde conste que se comprometen a cumplir con todos los puntos establecidos en la política BYOD de la entidad, al igual que permiten a la misma el monitoreo remoto de su dispositivo.
- En ningún caso se autoriza el BYOD para funcionarios miembros de unidades de inteligencia y/o contrainteligencia de las diferentes fuerzas, ni para funcionarios que por su cargo deban realizar actividades laborales que incluyan la lectura, modificación o manipulación de información o documentos producidos por unidades de inteligencia y/o contrainteligencia.
- Los funcionarios se hacen completamente responsables de todas las actividades realizadas con sus dispositivos móviles y de los accesos concedidos a estos.

- El funcionario acepta cumplir las políticas y restricciones de uso en su dispositivo móvil para cada uno de los servicios a los cuales tendrá acceso de acuerdo a su cargo y función.
- El funcionario no debe prestar, facilitar y/u ofrecer su dispositivo móvil a personas no autorizadas, su acceso es exclusivo del cargo, funcionario y/o dependencia y no es transferible; de llegar a presentarse y/o detectarse este tipo de situaciones, la entidad procederá a la suspensión del servicio según la normatividad de la misma, acuerdos de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.
- Sólo se permitirá el acceso BYOD a los dispositivos móviles que cumplan con los requerimientos técnicos mínimos establecidos por la entidad (estos se deben establecer por medio de un anexo técnico a la presente política).
- El funcionario autoriza a la entidad la instalación de la o las aplicaciones en su dispositivo móvil personal, que la entidad considere pertinentes para el monitoreo y control del mismo. Estas herramientas son conocidas como clientes MDM.
- El almacenamiento del dispositivo móvil autorizado deberá estar cifrado y protegido por contraseña, tanto para la información clasificada como para la del funcionario. Las demás configuraciones que el área de TI defina, podrán ser enviadas remotamente a los dispositivos.
- Se prohíbe expresamente la modificación o alteración del sistema operativo de los dispositivos móviles, por métodos como el rooteo o jailbreak.
- No se permite almacenar información clasificada en los dispositivos móviles, diferente a la asignada a su cargo y función. Si la entidad detecta este tipo de actividades, se procederá a la suspensión del servicio según la normatividad de la entidad, acuerdo de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.
- Está completamente prohibida la instalación y el uso de las aplicaciones mencionadas en anexo a esta política (se entiende que debe crearse un anexo con la 'lista negra' de aplicaciones no permitidas, establecidas por el área de TICS de la entidad), mientras el dispositivo se encuentre conectado a la red corporativa o esté siendo usado con fines laborales. Si la entidad detecta este tipo de actividades, se

procederá a la suspensión del servicio según la normatividad de la entidad, acuerdo de confidencialidad, consentimiento informado, términos de uso de BYOD y/o lo estipulado en el contrato laboral.

- El dispositivo móvil será cifrado o encriptado en su totalidad por parte del usuario antes de ingresar a BYOD, procedimiento que se realizará de forma manual o de forma remota por el administrador de los servicios BYOD de la entidad.
- Los funcionarios cuyos dispositivos móviles cuentan con acceso permitido a BYOD, deben asistir obligatoriamente a las campañas de sensibilización, capacitación y participar de las pruebas de seguridad que establezca la entidad.
- Está completamente prohibido a los funcionarios deshabilitar o desinstalar los sistemas de seguridad, aplicaciones, clientes o agentes implementados por la entidad en los dispositivos móviles.
- El funcionario acepta expresamente la política de la entidad sobre los casos de pérdida, daño total o parcial y/o robo de los dispositivos móviles con BYOD autorizado.
- La entidad se reserva el derecho de revisar y monitorear a través de los medios que estime pertinentes, la trazabilidad y seguimiento de las acciones realizadas por los funcionarios y los dispositivos móviles, con respecto a los servicios BYOD. En caso de encontrarse incumplimiento total o parcial de alguna de las políticas establecidas, se procederá a desactivar el acceso a BYOD y se enviará una comunicación de las actividades realizadas al área responsable del funcionario para que se apliquen las acciones correspondientes, correctivos, suspensión del servicio, e incluso hasta la destitución del cargo.
- En caso de pérdida o robo del dispositivo móvil, el funcionario propietario del mismo y responsable del servicio BYOD debe dar aviso inmediato a la entidad, usando los datos de soporte asociados a la presente política, para que se realice el procedimiento de baja del dispositivo de la plataforma BYOD y lanzar el proceso de borrado seguro de información del dispositivo. En dicho caso, la entidad no se hace responsable por la pérdida o borrado de información personal del funcionario, quien es el responsable de contar con copias de respaldo y medios de protección de su información personal,

entre la que se cuentan fotografías personales, videos, archivos de audio, documentos, historiales de conversaciones, etc.

- Cada funcionario es responsable de los procedimientos de copias de respaldo de su información (tanto corporativa como personal), por lo cual se sugiere que cada funcionario efectúe sus respectivos backup con una periodicidad mensual, como mínimo.
- En caso de que el funcionario borre de forma accidental su información, la entidad no se hará responsable de la información perdida por este incidente.
- Si por cualquier motivo el funcionario sospecha o detecta que la seguridad de su dispositivo móvil se ha visto comprometida de cualquier forma, debe reportarlo de forma inmediata a la entidad. Debido a este incidente, la entidad deberá solicitar el cambio de las contraseñas de las cuentas y accesos que considere comprometidos, de manera inmediata, o las acciones que considere pertinentes.
- La entidad se compromete a no ceder, ni vender a terceros la información privada que almacena, posee, trata o administra de sus funcionarios, contratistas, y demás personas que accedan a la plataforma BYOD.
- En ningún caso la entidad podrá retener o almacenar información personal de los funcionarios con acceso a BYOD, sin la debida autorización escrita y firmada por el funcionario. De igual manera, deberá garantizar que la información personal de los funcionarios no será divulgada por ningún motivo, y será eliminada de acuerdo a lo establecido a la Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".

3.4 Buenas prácticas de seguridad en BYOD

Se entiende por buenas prácticas al conjunto coherente de acciones que han rendido buen o excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados. Con base en esto, y dada la investigación realizada sobre el BYOD en diferentes organizaciones y múltiples contextos, se puede extraer un conjunto de buenas prácticas que se recomienda tener en cuenta para aquellas entidades del sector Defensa que deseen implementar ambientes BYOD para sus funcionarios. Este conjunto de buenas prácticas

ha sido condensado por el autor con base en el análisis de diferentes estudios e investigaciones desarrolladas para estudiar esta tendencia.

Buenas prácticas para la creación de política BYOD

- **Involucrar a todas las áreas de la entidad.** Para la creación de una política BYOD acorde con las necesidades de toda la entidad, es necesario involucrar a todas las áreas de la misma, con el fin de que expongan sus preocupaciones y requerimientos específicos. Ello dará un panorama mucho más amplio sobre los verdaderos alcances que el BYOD debe tener.

- **Políticas claras y de obligatorio cumplimiento.** Es necesario que las políticas establecidas estén diseñadas en un lenguaje claro y entendible, y que todos los funcionarios las entiendan. De igual manera se deben crear políticas de obligatorio cumplimiento, con el fin de que sean lo más concretas posible.

- **Establecer diferentes roles de acuerdo a cargo.** Aunque es posible que todos los funcionarios quieran acceder a las bondades de BYOD, hay que establecer quienes realmente lo necesitan. Igualmente, hay que identificar cuales roles de la organización deben tener características especiales, o quienes por tener un perfil demasiado crítico definitivamente no pueden acceder a BYOD.

- **Tipos de dispositivos a conectar.** Se debe identificar muy bien qué tipos de dispositivos pueden acceder a BYOD: computadores portátiles, teléfonos inteligentes, etc. En algunos casos es también necesario establecer marcas y modelos específicos de dispositivos que se autorizan, o un listado de especificaciones técnicas que deben cumplir para poder acceder, dado que algunos pueden tener vulnerabilidades de fábrica.

- **Criticidad de la información a manejar.** Es necesario establecer qué información puede ser accedida a través de BYOD y cuál está expresamente prohibida. En el caso del sector Defensa, no se debe autorizar BYOD para información pública clasificada, información púbica reservada o las clasificaciones de información generada por unidades de inteligencia y/ contrainteligencia.

- **Grado de exposición de los dispositivos.** Se debe analizar cuál es el grado de exposición que pueda presentar los dispositivos que se pretenden autorizar y con base en ello definir el rol adecuado y los permisos que se van a otorgar.

- **Tenga en cuenta la infraestructura de la entidad.** El BYOD trae como ventaja principal la reducción en costos del mantenimiento de dispositivos de la entidad. Sin embargo, hay que tener en cuenta la capacidad de la infraestructura tecnológica, con el fin de que no se sobrecargue la misma y haya que invertir en ampliaciones más costosas que la inversión en dispositivos.

Buenas prácticas para la implementación de un ambiente BYOD

- **Implementación de MDM.** Es imprescindible contar con una herramienta Mobile Device Management, que permita el monitoreo y control de los dispositivos que aceden a BYOD. Este tipo de herramientas permite analizar el comportamiento de cada dispositivo, verificar los accesos a los cuales tiene permiso, verificar comportamientos anómalos, así como la instalación remota de aplicaciones y parámetros de seguridad, actualización de parches de seguridad, entre otros. Además, en caso de robo o pérdida de un dispositivo, MDM permite bloquearlo remotamente e incluso borrar toda la información del dispositivo de manera remota. Hoy en día el concepto de MDM ha evolucionado a EMM (Enterprise mobility management), que contempla un conjunto mucho mayor de soluciones para la gestión de dispositivos móviles empresariales o personales.

- **Revisión periódica de las políticas de seguridad y BYOD.** Al menos cada año debe hacerse una revisión de las políticas de BYOD y de las políticas de seguridad de la información en general, con el fin de ajustar vacíos o modificar políticas con base en los diversos incidentes de seguridad que se vayan presentando.

- **Realizar pruebas de vulnerabilidad de los servicios.** Junto con la revisión de políticas, es necesario realizar pruebas de vulnerabilidad permanentemente, con el fin de identificar posibles fallas y corregirlas cuanto antes. Es una buena práctica realizar pruebas aleatorias a dispositivos y servicios para verificar la robustez de las políticas y herramientas.

- **Sensibilización y capacitación a los funcionarios.** El factor humano es determinante en todos los aspectos relacionados con la seguridad de la información. Por ello se deben realizar permanentemente campañas de sensibilización, capacitaciones y diversas actividades cuyo fin sea concientizar a los usuarios de su rol fundamental en la protección de la información personal y corporativa.

- **Funcionarios que dejan entidad.** Debe haber una estrecha comunicación entre el área de TI y el área de Recursos Humanos de la entidad con el fin de verificar permanentemente cuáles funcionarios han dejado la entidad, para realizar las actividades necesarias de sanitización de dispositivos y revocación de permisos. Debe establecerse un protocolo claro para estos casos.

Buenas prácticas de seguridad con dispositivos móviles

- **Bloqueo de pantalla.** Los funcionarios deben establecer un método para evitar accesos no autorizados a sus dispositivos, ya sea a través de contraseñas, patrón de bloqueo, huella dactilar, Face ID, o cualquier otro disponible. En general, no debe haber algún dispositivo sin contraseña.

- **Bloqueo remoto, tracking y borrado remoto.** Hoy en día tanto los teléfonos Android como los iPhone cuentan con plataformas que ayudan a encontrar el dispositivo en caso de robo o pérdida, e incluso a realizar un borrado remoto de la información. Es una buena práctica que los funcionarios conozcan y utilicen estas herramientas, complementadas por el MDM o EMM de la entidad.

- **Cifrado de datos.** De igual manera, los sistemas operativos más comunes incluyen herramientas de cifrado de los datos de manera nativa, por lo cual es una buena práctica que los funcionarios activen el cifrado de los medios de almacenamiento interno y/o externo de sus dispositivos.

- **Control de aplicaciones.** Es recomendable que periódicamente se verifiquen los permisos que tienen las aplicaciones instaladas en el dispositivo, con el fin de verificar posibles amenazas. Por ejemplo, una aplicación como la calculadora no debería tener acceso a nuestros contactos, o a los archivos almacenados o al GPS, puesto que su función no requiere de dichos recursos. En el momento de la instalación, el funcionario debe verificar muy buen que permisos está requiriendo la aplicación y si en realidad son necesarios, o por el contrario le parecen sospechosos. Esta verificación debe hacerse incluso cuando la aplicación se instala desde la tienda oficial de aplicaciones. Igualmente, cada cierto tiempo es necesario revisar estos permisos en las aplicaciones instaladas, puesto que en algunos casos las actualizaciones de las mismas solicitan permisos adicionales que no tenían anteriormente.

- **Técnicas y aplicaciones para reforzar la seguridad.** Existen algunas aplicaciones que fortalecen la seguridad de los dispositivos, que pueden proteger en gran medida la información corporativa y personal. Los antivirus permiten el escaneo en tiempo real de todas las aplicaciones e interacciones que tiene el usuario en busca de virus o malware. Otras aplicaciones permiten almacenar y centralizar la gestión de contraseñas de manera segura, con el fin de salvaguardar el acceso a servicios y

aplicaciones. Algunas aplicaciones permiten la autenticación de dos pasos, que además de la contraseña piden la inclusión de un código de verificación obtenido por otro medio para garantizar el acceso autorizado al servicio. Todas estas herramientas contribuyen a proteger y asegurar la información de la entidad y del funcionario.

- **No instalación de aplicaciones fuera de la tienda.** Las tiendas de aplicaciones generalmente realizan muchas pruebas y verificaciones para que las aplicaciones que allí se alojan tengan unos niveles de seguridad aceptables y que no contengan código malicioso que pueda vulnerar la información del usuario. Por ello es una buena práctica instalar aplicaciones únicamente en las tiendas autorizadas, y por ningún motivo instalar aplicaciones de fuentes desconocidas. De hecho, esta opción viene desactivada por defecto en los teléfonos Android, por ejemplo.

- **No permitir rooteo o jailbreak**. Existen algunos sistemas operativos modificados que permiten al usuario tener control total sobre su dispositivo, e incluso saltarse los controles de seguridad del fabricante para poder instalar aplicaciones ilegales y acceso a servicios de pago de manera gratuita y/o fraudulenta. Estos sistemas operativos modificados vienen también con código malicioso, virus y puertas traseras que facilitan el robo de información por parte de hackers o personas inescrupulosas. Debido a ello, se debe prohibir el acceso a BYOD a dispositivos que tengan estos sistemas operativos modificados, ya sea rooteados (Android) o con jailbreak (iPhone).

Conclusiones

Dado que la tendencia BYOD cada día crece más en entornos empresariales y corporativos, en parte debido a las grandes ventajas que trae para las empresas, es necesario plantearse este escenario para instituciones gubernamentales. Si bien es cierto que aún existen algunos riesgos a los que se incurre por la utilización de dispositivos móviles personales en actividades laborales, más aún en sectores tan delicados en cuanto al manejo de la información como lo es el sector Defensa en Colombia, es viable establecer para algunas entidades entornos BYOD controlados como un primer paso de acercamiento a esta tendencia.

Mundialmente se puede observar como cada vez las compañías están acercando sus activos de información hacia la tendencia, de hecho, el mercado de soluciones BYOD ha ido aumentando tanto en inversión como en actores. En nuestro país esta tendencia ya se observa como una posibilidad de reducir costos a las compañías, por lo cual es vista con optimismo. Ahora, en cuanto a los cuerpos de seguridad y fuerzas militares, algunos países han actuado en consecuencia, generando políticas BYOD a nivel estatal. Algunas instituciones han venido haciendo pruebas piloto en este aspecto, incluso en instituciones de inteligencia. Por otro lado, las investigaciones realizadas en este campo sugieren que la tarea primordial es dar soluciones seguras para que las organizaciones adopten la tendencia con el menor riesgo posible. Por ello, se han desarrollado algunas pruebas de campo en entornos controlados, para probar software y políticas acordes con las necesidades de los entornos BYOD.

En cuanto al marco legal y normativo colombiano, es posible la implementación de este tipo de entornos en entidades gubernamentales, siempre y cuando se informe debidamente a los funcionarios sobre el tratamiento que se va a dar a su información personal y los posibles riesgos que se incurran. Particularmente en el sector Defensa, se pueden implementar ambientes BYOD, pero siendo muy enfáticos en excluir cualquier información catalogada como información pública clasificada, información pública reservada y cualquier información perteneciente o producida por organismos de inteligencia. Ahora, la Directiva de Seguridad de

la Información del Ministerio de Defensa Nacional, permite la implementación de dichos entornos únicamente para información considerada como pública. En conclusión, es posible implementar ambientes BYOD en entidades del sector Defensa, siempre y cuando se establezca una política particular para BYOD que contemple la protección de datos personales de los usuarios, que cumpla a cabalidad con la Política de Seguridad de la Información del Ministerio de Defensa, que no se comprometa información clasificada y que se cumpla con toda la normatividad legal colombiana en este aspecto.

En cuanto a la evaluación de riesgos, es necesario que cada institución realice una evaluación de riesgos de implementación de BYOD de manera individual, puesto que, dadas las características del sector y las necesidades de cada entidad, esta evaluación puede cambiar sustancialmente. Sin embargo, existen unos puntos en común que deben considerarse, estudiarse y conceptuarse a profundidad antes de sugerir la implementación de entornos BYOD, los cuales corresponden a los propuestos en este trabajo.

Es importante señalar también las ventajas y desventajas de esta tendencia. Como principal ventaja se encuentra la reducción de costos a las organizaciones y la flexibilidad que da a los usuarios. Como principal desventaja se observa que las organizaciones se ven muy dependientes de factores externos como el conocimiento de los usuarios y las vulnerabilidades de los sistemas operativos, para proteger su información corporativa. De igual manera se ofrecen algunas recomendaciones y aspectos a considerar para la creación e implementación de políticas BYOD en las entidades del sector Defensa, junto con algunas buenas prácticas para la seguridad de dispositivos móviles, con el fin de proteger tanto la información personal de los funcionarios como la información corporativa de la entidad.

Una vez alcanzados los objetivos y analizado este documento, es importante realizar una prueba de campo consistente en la creación e implementación de una política BYOD en alguna de las entidades que conforman el sector Defensa, con el fin de medir el comportamiento de los funcionarios y de la infraestructura TIC de la institución. Adicionalmente, se puede realizar una prueba de implementación de un MDM o un EMM en los dispositivos personales de los usuarios y observar las implicaciones e impacto que esto tiene en la información personal del

funcionario. Por último, es pertinente estudiar la viabilidad de este tipo de entornos en unidades militares comprometidas con operaciones militares y de inteligencia, puesto que son los ambientes más riesgosos en términos de información clasificada.

Referencias

Armando, A., Costa, G., Merlo, A., Verderame, L., & Wrona, K. (2016, mayo 24). Developing a NATO BYOD Security Policy. DOI: 10.1109/ICMCIS.2016.7496587

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2017). Survey on Access Control and Management Issues in Cloud and BYOD Environment. International Journal of Computer Science and Mobile Computing, 6, 44-54.

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2018). A Proposed Framework for Access Control in the Cloud and BYOD Environment. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18(2), 144-152.

Bailey, A. (2013, noviembre 15). Why The BYOD Trend Is So Popular. Recuperado el 25 de agosto de 2017, dehttp://www.cyber-knowledge.net/blog/why-the-byod-trend-is-so-popular/

Balanta, H. (2017, febrero 6). Consideraciones Para Adoptar Modelos De BYOD En Las Organizaciones. Recuperado el 25 de agosto de 2017, de https://colombiadigital.net/opinion/columnistas/derecho-y-economia-digital/item/9503-consideraciones-para-adoptar-modelos-de-byod-en-las-organizaciones.html

Cabrera, E. (2013, Abril 5). US Army Having Some Troubles with BYOD -. Recuperado el 25 de agosto de 2017, de http://blog.trendmicro.com/us-army-having-some-troubles-with-byod/

Cabrera, J. (2013, Noviembre 18). 'BYOD': una historia de vinos, cervezas y teléfonos móviles. [online] El Huffington Post. Recuperado el 25 de septiembre de 2017, de https://www.huffingtonpost.es/juan-cabrera/byod-una-historia-de-

vino_b_4251144.html [Accessed 27 Sep. 2018].

Cadena-Herrera, A. G. (2018). Riesgos de seguridad asociados al uso de dispositivos móviles personales (smartphone-Android) en entornos BYOD-Bring Your Own Device (Tesis de Maestría).

Centre for the Protection of National Infrastructure, UK. (2014, octubre 6). BYOD Guidance: Executive Summary. Recuperado el 25 de agosto de 2017, de https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary

Colombia, Congreso de la República (2008) Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. Bogotá: En Diario Oficial, 16 de julio de 2008.

Colombia, Corte Constitucional (2011) Sentencia de Constitucional 221 con ponencia de la Magistrada María Victoria Calle Correa, Bogotá. Recuperado el 28 de agosto de 2017 en: www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Colombia, Congreso de la República (2012) Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: En Diario Oficial, 07 de octubre de 2012.

Colombia, Congreso de la República (2013) Ley Estatutaria 1621 de 2013, Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. Bogotá: En Diario Oficial, 17 de abril de 2013.

Colombia, Presidencia de la República (2013) Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá: En Diario Oficial, 26 de junio

de 2013.

Colombia, Congreso de la República (2014) Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Bogotá: En Diario Oficial, 06 de marzo de 2014.

Colombia, Ministerio de Defensa Nacional (2014) Directiva Permanente DIR2014-18, Políticas de seguridad de la información para el sector Defensa. Bogotá: En Página Intranet, 19 de junio de 2014.

Colombia, Presidencia de la República (2015) Decreto 1070 de 2015, Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa. Bogotá: En Diario Oficial, 26 de mayo de 2015.

Colombia, Ministerio de las TIC (2017) Modelo Nacional de Gestión de Riesgos de Seguridad Digital. Recuperado el 01 de julio de 2018, de https://mintic.gov.co/portal/604/articles-61854_documento.docx

Corrin, A. (2015, marzo 18). Pentagon to Launch BYOD Pilot This Summer. Recuperado el 25 de agosto de 2017, de http://www.c4isrnet.com/c2-comms/mobility/2015/03/18/pentagon-to-launch-byod-pilot-this-summer/

Crowd Research Partners, (2015, diciembre 15). BYOD & Mobile Security Report. Recuperado el 25 de agosto de 2017, de http://crowdresearchpartners.com/portfolio_item/byod-mobile-security-report/

Delgado, R. (2015, Agosto 12). The Challenges of Bringing BYOD to the Military. Recuperado el 25 de agosto de 2017, de https://www.socpub.com/articles/the-challenges-of-bringing-byod-to-the-military-11272

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device

(BYOD). Procedia Computer Science, 78, 179-184.

FedTech Staff. (2016, Ferrero 23). Federal Agencies Turn to BYOD, Mobile Devices in the Field to Attract New Workers. Recuperado el 25 de agosto de 2017, de https://fedtechmagazine.com/article/2016/02/federal-agencies-turn-byod-mobile-devices-field-attract-new-workers

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. Journal of Information privacy and security, 11(1), 38-54.

Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In Information Systems and Technologies (CISTI), 2017 12th Iberian Conference on (pp. 1-4). IEEE.

ISO (International Standard Organization). (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Estándar de Seguridad ISO/IEC 27001.

ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

Konkel, F. (2015, Julio 9). Nextgov. Pentagon Not Ready for Bring-Your-Own-Device Just Yet. Recuperado el 25 de agosto de 2017, de http://www.nextgov.com/mobile/2015/07/pentagon-not-ready-byod-pilot-just-yet/117406/

Larkins, T. (2014, Nero 14). BYOD In Defense Department? Not In This Lifetime - InformationWeek. Recuperado el 25 de agosto de 2017, de http://www.informationweek.com/government/mobile-and-wireless/byod-in-defense-

department-not-in-this-lifetime/d/d-id/1113418

Onetto, C. (2016, enero 13). Las Tendencias Que Nos Dejarán Las TIC En 2016. Recuperado el 25 de agosto de 2017, de http://www.dinero.com/opinion/columnistas/articulo/opinion-sobre-las-nuevas-tendencias-de-las-tic-en-empresas-en-2016-en-colombia/218015

Pacheco Veliz, S. E., & Piazza Orlando, C. D. (2016). Estudio y análisis de seguridad en dispositivos móviles (Doctoral dissertation, Facultad de Informática).

Palfreyman, J. (2015, Julio 7). Military "Bring Your Own Device"?. IBM Government Industry Blog. Recuperado el 25 de agosto de 2017, de https://www.ibm.com/blogs/insights-on-business/government/military-bring-your-own-device/

R. N. Akram and K. Markantonakis (2016). Challenges of security and trust of mobile devices as digital avionics component. Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, 2016, pp. 1C4-1-1C4-11.

Rojas, D. L. M. (2015). BRING YOUR OWN DEVICE: oportunidades, retos y riesgos en las organizaciones. Revista TECNIA, 25(1), 5-5.

Sander, A. (2017, mayo 4). The Smart Move for the DOD on Smartphones. Recuperado el 25 de agosto de 2017, de https://fedtechmagazine.com/article/2017/05/smart-move-dod-smartphones

Schwartz, H. (2014, December 23). Growing Bring Your Own Device (BYOD) Market Driven by Employee Behavior. Recuperado el 25 de agosto de 2017, de https://facilityexecutive.com/2014/12/growing-byod-market-driven-by-employee-behavior/

Silva Filho, M. (2016, agosto 25). BYOD y el empleado móvil en Latinoamérica. Recuperado el 25 de agosto de 2017, de http://pulsosocial.com/2016/09/13/byod-empleado-movil-latinoamerica/

Singh, M. M., Chan, C. W., & Zulkefli, Z. (2017). Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. International Journal of Advanced Computer Science and Applications, 8(2), 53-62.

Townsend, C. (2016, Agosto 18). Federal BYOD: The mobile security conundrum. Recuperado el 25 de agosto de 2017, de https://gcn.com/Articles/2016/08/18/BYOD-security.aspx

Trend Micro USA, (2015, Mayo 29). The Case for Making BYOD Safe. Recuperado el 25 de agosto de 2017, de https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-case-for-making-byod-safe

United States Departament of Defense, I. (2013, Marzo 26). Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices. Recuperado el 25 de agosto de 2017, de http://www.dodig.mil/pubs/documents/DODIG-2013-060.pdf

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. Computers & Security, 55, 81-99.