BYOD: Tendencia en Crecimiento

Parra Sterling, Jaime Addulth
jaddulth.parra@gmail.com
Universidad Piloto de Colombia

Resumen— Bring Your Own Device, también conocido bajo el término BOYD, es una tendencia masiva, donde los empleados traen sus dispositivos móviles personales especialmente para usar en el lugar de trabajo. Esto puede representar ventajas potenciales para las empresas, pero debido a que estas máquinas no están tan bien protegidas como las computadoras tradicionales, las organizaciones pueden considerar esta tendencia como un desafío que necesita una consideración estratégica. Este trabajo explora conceptualmente esta tendencia como resultado de la consumerización de tecnologías de información, revisando sus ventajas y riesgos. Entendiendo la necesidad de establecer un programa BYOD, este documento presenta el posible uso de un estándar popular y reconocido internacionalmente de buenas prácticas para tratar asuntos de seguridad de la información. Asimismo, este documento analiza una guía para seleccionar, implementar y mantener los controles de seguridad necesarios. Finalmente, este documento expone algunos controles técnicos para aumentar la seguridad de la información en un programa BYOD.

Índice de Términos—BYOD, ISO 27002, NIST, riesgos, seguridad de la información.

Abstract — Bring Your Own Device, also known under the term BOYD, is a massive trend, where the employees bring their personal mobile devices specially to use in the workplace. This can represent potential advantages for the companies, but due to these machines are not so well protected as traditional computers, the organizations can consider this tendency as a challenge that need a strategic consideration. This paper explores conceptually this trend as a result of the consumerization of information technologies, reviewing its advantages and risks. Understanding the need to stablish a BYOD program, this paper present the possible use of a popular, internationally-recognized standard of good practice to deal with information security issues. Likewise, this paper analyzes a guide to selecting, implementing, and maintaining the necessary security controls. Finally, this paper expose some technical controls to increase information security in a BYOD program.

Keywords— BYOD, ISO 27002, NIST, risks, information security.

I. INTRODUCCIÓN

Es evidente la gran capacidad de procesamiento que poseen los dispositivos móviles hoy en día, donde éstos ya pueden realizar funciones que antes estaban solo dentro del ámbito de cubrimiento de los computadores tradicionales.

Paralelamente, también se está observando una mayor popularidad en los teléfonos inteligentes y tabletas; lo que le permite a cualquier usuario acceder a diferentes servicios desde cualquier ubicación, con tan solo una conexión a Internet.

Estas facilidades de ubicuidad y capacidad, ha permitido borrar de cierta manera la división entre los ámbitos laborales y personales, facilitando que se pueda trabajar y disfrutar de sus redes sociales, utilizando un único dispositivo. Este fenómeno se analiza en las siguientes secciones, donde se identifican y analizan las tendencias de consumerización de las tecnologías de información (TI) y de Bring Your Own Device.

Debido a que la tendencia de Bring Your Own Device tiene consecuencias a nivel corporativo de consideración, en las secciones IV y V se examinan tanto las ventajas y beneficios de un programa BYOD, como los riesgos a los que se exponen las organizaciones que deseen optar por aplicar una estrategia de este tipo.

Uno de los ámbitos más fuertemente impactado dentro de un programa de BYOD es precisamente la seguridad de la información corporativa, pues el acceso y manipulación de la data corporativa se realiza sobre dispositivos que los usuarios adquieren y no poseen el mismo nivel de aseguramiento que los equipos tradicionales corporativos.

El estándar ISO 27002 utiliza un enfoque basado en riesgos, donde a través de sus controles se busca garantizar las propiedades de la seguridad de la información. Por lo anterior, en la sección VI, se identifica y analiza cada control que aplique al fenómeno de BYOD, para que sirva como apoyo a las organizaciones en el diseño de sus estrategias corporativas.

El desarrollo de los programas de BYOD representa un desafío para las organizaciones, puesto

que se deben considerar aspectos legales, regulatorios, estratégicos y técnicos. Para ello, se puede recurrir a guías documentadas por expertos como la NIST SP 800-46, analizada en el numeral VII. Esta provee recomendaciones en temas de seguridad para diferentes tipos de soluciones de acceso remoto, incluyendo las tecnologías de BYOD.

Finalmente, se presentan diferentes controles técnicos relevantes a esta tendencia y que puede apoyar el diseño de una estrategia BYOD, enfocados en el aseguramiento de la información propiamente.

II. CONSUMERIZACIÓN DE LAS TI

De acuerdo a diferentes fuentes especializadas [1],[2], la consumerización de las TI es un fenómeno el cual los usuarios utilizan recursos tecnológicos propios en sus ámbitos personales y laborales indistintamente.

Esto tiene su origen en el hecho de que los empleados encuentran en casa mejores capacidades que en sus lugares de trabajo.

Según algunos investigadores del tema [3], la consumerización es producto del vertiginoso desarrollo de cuatro tecnologías:

a. *La introducción de los teléfonos inteligentes*

Ericsson regularmente con objeto investigativo, hace mediciones sobre redes de comunicaciones en todas las mas destacadas regiones del mundo, especialmente en redes WCDMA, HSPA y LTE, donde la data es hecha anónima para su investigación.

En el informe Ericsson Mobility Report de junio de 2016 [4], se aprecia claramente cómo el tráfico de datos móviles global ha crecido evidentemente en el transcurso de los años.

Según el estudio, el aumento en el tráfico de datos obedece a la multiplicación de las suscripciones de dispositivos móviles como los teléfonos inteligentes y la ampliación de los planes adquiridos, especialmente para acceder a servicios de video.

De manera particular, se identifica que entre el Q1 de 2015 y el de 2016, dicho tráfico aumentó en un 60%.

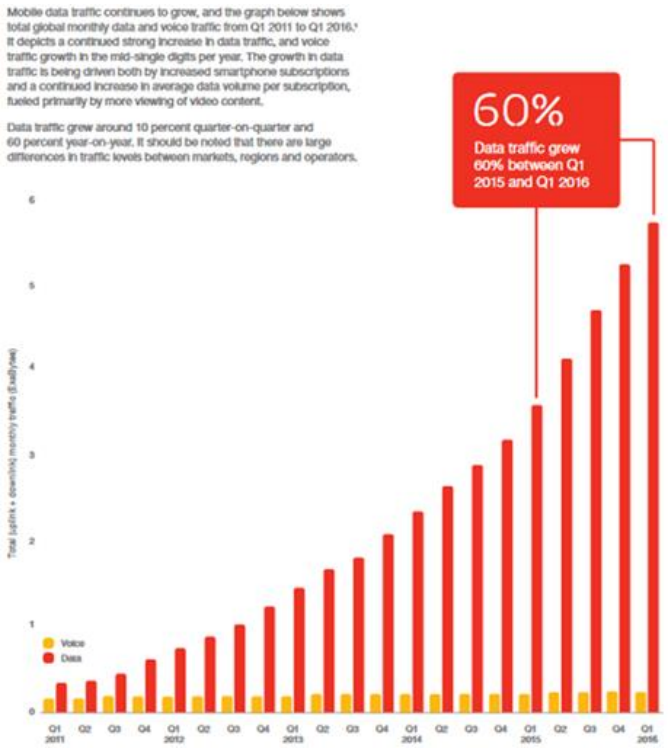

Fig. 1. Tráfico móvil entre Q1 del 2011 al Q1 de 2016. En rojo el tráfico de datos y en amarillo el tráfico de voz. Se muestran el tráfico en exabytes en el eje de las ordenadas y para cada Q desde 2011 a 2016 en la abscisa [5]

b. *La Internet como medio ideal de consumo de multimedia*

En el mismo reporte de Ericsson, se encuentra que para el año 2015 el tráfico predominante ha sido video para las diferentes plataformas de acceso.

Aquí el porcentaje de consumo en video se ubica entre el 40 y el 55% del tráfico total.

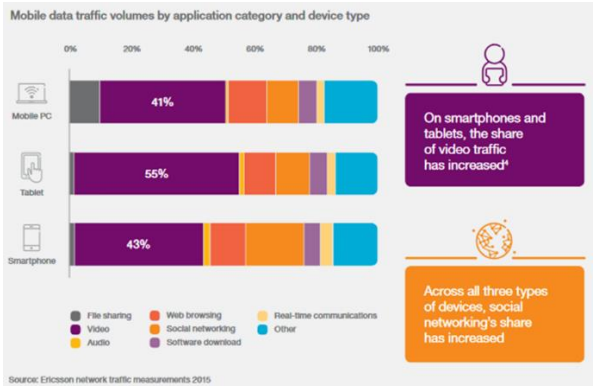

Fig. 2. Volumen de tráfico de Data en Móviles por categoría de aplicación y tipo de dispositivo. En violeta el porcentaje del tráfico de video [6]

c. El Cloud Computing, que facilita el acceso a diversos recursos, servicios o información, desde cualquier sitio y a cualquier momento

De acuerdo al estudio Cloud Security Survey Report de 2016 [7], realizado por CloudPassage; al preguntar por el modelo de servicio cloud que se encuentra usando en las organizaciones encuestadas se tiene:

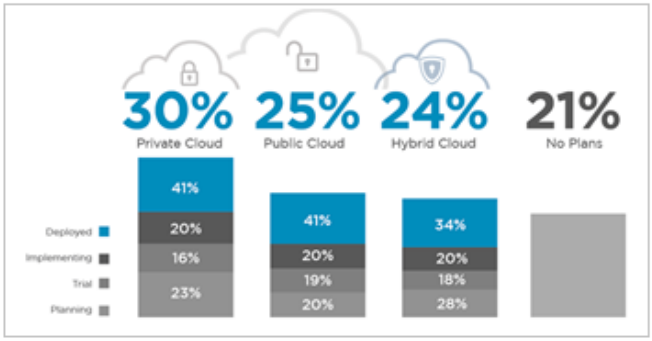

Fig. 3. Estado de adopción de Cloud Computing. Se analizaron 3 tipos de soluciones Cloud: Privada, Pública e Híbrida. En cada columna su etapa de implementación [8]

Identificando que se tiene una proporción considerable de adelanto en sus implementaciones de soluciones de Cloud Computing, versus el 21% de la totalidad que no planea realizarlo.

d. Las redes sociales, donde se puede expresar y compartir.

Este fenómeno puede ser rastreado en dos aspectos:

- A nivel de hardware propiamente dicho, al referirse a smartphones, laptops, tabletas, etc. y
- A nivel de software con servicios como almacenamiento en la nube tipo Dropbox y Google Drive; al igual que de mensajería instantánea como Skype y Google Talk.

Como consecuencia de ello, los empleados pueden obtener mejor experiencia de usuario y mayor libertad, representando finalmente en pro de la productividad para las compañías.

Esto ha facilitado el desarrollo de nuevas tendencias en entornos laborales, como el de Bring Your Own Device (BYOD), en el cual se utilizan los dispositivos personales de cómputo como smartphones, tabletas, laptops y otros en su trabajo.

A continuación, se hará una exploración más profunda al fenómeno BYOD, el cual presenta una tendencia de crecimiento que necesita ser abordado por las organizaciones.

III. BYOD

De acuerdo a diferentes fuentes [9],[10],[11], Intel fue el pionero en el desarrollo de una estrategia de Bring Your Own Device en 2009 y quien introdujo el término como tal. Luego, le siguieron otras como IBM, Unisys y Citrix en su idea de permitir a sus empleados utilizar sus propios equipos para realizar labores propias de la compañía, abriendo una nueva posibilidad, basada en la flexibilidad.

Existe una creencia popular que la aparición del iPhone [12], fue el catalizador de esta nueva tendencia, ya que les permitió a ciertos sectores de las organizaciones desarrollar tanto sus tareas corporativas, como personales a través de sus propios equipos.

Entonces, los fabricantes de tecnología comenzaron a desarrollar el mercado de los smartphones y luego el concepto de tablet; lo que representó la utilización cada vez mayor de estos en el ámbito laboral.

Ya hoy en día según Gartner [13], se entiende a Bring Your Own Device como una estrategia alternativa que permite a los empleados, socios de negocio y otros usuarios usar un dispositivo cliente comprado y seleccionado para ejecutar aplicaciones corporativas y acceder data.

Las organizaciones entonces [14], están desarrollando programas bajo esta estrategia influenciados por temas como mejora de movilidad, satisfacción y productividad del personal que opera bajo ese nivel. Sin embargo, también confirman inhibidores como problemas con seguridad y privacidad de los empleados.

Identificando su importancia, de acuerdo a un estudio realizado por Global Market Insights [15], analizando empresas de tamaño pequeño y mediano-grande; se espera tener un crecimiento considerable en el mercado para los próximos años para los dispositivos móviles:

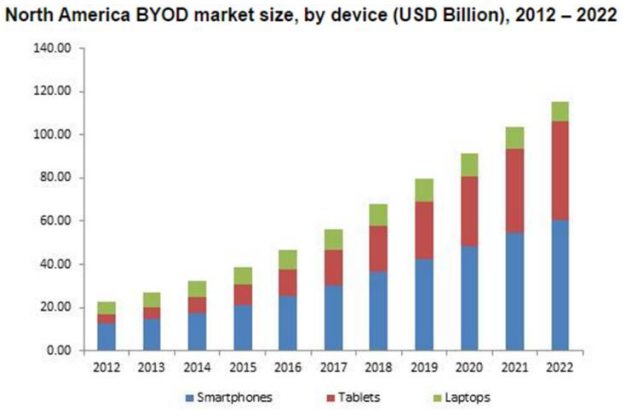

Fig. 4. Predicción de mercado para dispositivos móviles. Forecast entre 2015 a 2022. Sobre la abscisa para cada año, se relaciona el tamaño del mercado para Smartphone (Azul), Tabletas (Rojo) y Laptops (Verde) [16]

Aquí se identifica que el mercado de los smartphones y tablets se incrementará sustancialmente, al contrario de aquel de los laptops, el cual mantendrá valores similares.

Esto puede servir a las organizaciones para focalizar esfuerzos en entender los beneficios y riesgos de esta tendencia y así mismo prepararse para los retos que esto representa.

Esto incluye no solo cambios en las áreas operativas y de soporte; si no también a nivel estratégico de las organizaciones, pues puede apalancar la innovación y la manera en cómo se desarrollan sus procesos

IV. VENTAJAS Y BENEFICIOS DE BYOD

El Grupo de Soluciones Empresariales para Internet (IBSG, de sus siglas en inglés) es una organización del gigante de tecnología Cisco que presta servicios de consultoría y asesoramiento a nivel corporativo.

Éste ha realizado un importante estudio financiero que busca comprender los beneficios y costos de la tendencia global de Bring your Own Device (BYOD) [17], que resulta muy útil en niveles tanto estratégicos como de personal en las empresas que están analizando esta posible solución.

Esta publicación incluye investigaciones y análisis sobre encuestas realizadas tanto a responsables de toma de decisiones como a usuarios móviles, en compañías de Estados Unidos, Reino Unido, Alemania, Brasil, India y China. Lo anterior, aterrizado en términos de cómo los departamentos de tecnologías de información de sus empresas están tratando la problemática con los nuevos dispositivos que están siendo usados a nivel corporativo, desde el punto de vista de acceso a la red y de seguridad.

Los resultados de este estudio son los siguientes:

- Los colaboradores de las empresas reconocen el valor de usar sus propios dispositivos. Esto se refleja en el hecho de que en promedio éstos utilizan 1,7 equipos de propiedad personal para su trabajo, lo que les representa cerca de 1000 dólares norteamericanos en compra de tecnología móvil y un gasto anual superior a 700 dólares norteamericanos en planes de datos para su acceso a Internet.
- Los teléfonos inteligentes son los dispositivos móviles que más se llevan a sus labores corporativas; con un total de 81%.

Al preguntar el porqué de esta decisión de llevar sus propios dispositivos móviles a su trabajo; se identificaron las siguientes razones:

- Se tiene mayores capacidades tecnológicas con sus propios equipos o se encuentran más familiarizados con su uso. Con lo anterior se puede reconocer que haciendo uso de Bring Your Own Device se puede aprovechar este grado de libertad para mejorar la productividad corporativa.
- Se puede combinar las actividades laborales y las personales. En términos de innovación en el lugar de trabajo, hoy en día se busca que los colaboradores puedan realizar sus labores sin importar su ubicación física. Basados en lo anterior, esta movilidad está muy alineada a la oportunidad de que el empleado acceda a los ámbitos laborales y personales indistintamente desde sus equipos.
- Por iniciativa, porque sienten que los necesitan para trabajar y la compañía no los proporcionan. En una gran medida, se puede interpretar que debido a que las empresas no entregan las herramientas, los empleados se

adelantan llevando sus dispositivos. Así pues, las empresas pueden dedicar esfuerzo y recursos en seguimiento y servicios relacionados.

Al respecto de productividad, se identificó que el 35% de los encuestados ahorra dos o más horas por semana; al utilizar sus propios equipos. Esto claramente respalda a BYOD como una práctica innovadora que apoya el negocio, ya que además el 53% de los empleados aumentaron su productividad, habilitada con sus propios dispositivos.

En temas de estabilidad del personal también se tiene un diferencial con el uso de estas estrategias, ya que el 49% de los encuestados prefiere trabajar en compañías que admite Bring your Own Device y el 60% usa el dispositivo corporativo porque debe hacerlo de manera impositiva.

El uso de BYOD podría atraer y mantener recursos humanos más productivos, aplicando primas para aquellos que se lo deseen.

Finalmente, en términos financieros el estudio identifica que las compañías pueden llegar a obtener un beneficio adicional de 1300 dólares norteamericanos por año y por usuario móvil con BYOD, debido a ahorro de costos en:

- Hardware. Esto debido a que el empleado proporcionaría su propio dispositivo.
- Soporte. En cuanto se puede revalidar el esquema de soporte e implementar herramientas participativas en línea como wikis, foros y otros.
- Telecomunicaciones. Ya que ciertas empresas encuestadas lograron migrar cerca del 20% de sus colaboradores a planes de telecomunicaciones autofinanciados.

Estas cifras pueden ser alcanzables si se establece una estrategia real corporativa al respecto de BYOD, más no reactiva al enfrentarse a empleados con esta iniciativa únicamente, como es el caso del 26% de las organizaciones encuestadas.

V. RIESGOS DE BYOD

La Agencia Europea de Seguridad de las Redes y la Información (ENISA, de sus siglas en inglés) es un centro de conocimientos especializados para la seguridad cibernética en Europa que ayuda a la Unión Europea y los países que la integran a estar mejor equipados y preparados para prevenir, detectar y dar respuesta a los problemas de seguridad de la información.

Esta organización ha publicado un informe en septiembre de 2012 [18], donde identifica los riesgos originados en las tendencias de consumerización de TI y de Bring Your Own Device.

Estos fueron clasificados en tres grupos de acuerdo a las áreas de impacto:

a. Riesgos relacionados a costos

- Pérdida de valor cuando los empleados degradan la reputación de la organización por el uso incontrolado de dispositivos y servicios. Debido a la utilización de servicios de tecnologías de información no supervisadas como cloud computing, redes sociales y hasta aplicaciones instaladas en sus equipos móviles. Esto puede llegar a ocasionar que la información confidencial corporativa sea expuesta por fuera del área de control de la organización y entregada o manipulada por personal no autorizada.
- Requerimientos de administración sobre una amplia variedad y complejidad de dispositivos, sistemas y aplicaciones, podría incrementar costos. La reducción de costos considerada inicialmente como una ventaja de la consumerización de TI, podría ser opacada por la necesidad de implementar estrategias de administración de TI, debido a la necesidad de cubrir el soporte y el nivel adecuado de seguridad a las diferentes tecnologías utilizadas. Además, la heterogeneidad misma se pueden presentar costos adicionales por la continua necesidad de adaptación y revisión de las políticas.
- El incremento de uso de dispositivos móviles, se traduce en más equipos y así mismo costos mayores. Una gran cantidad de dispositivos móviles son robados o perdidos, lo cual se traduce en incrementos de costos para las

organizaciones para reemplazar no solo los equipos mismos si no la información que la contienen, la cual representa costos en términos de confidencialidad, integridad y disponibilidad.

- Gastos adicionales para garantizar que los requerimientos de seguridad no actúan evitando una consumerización apropiada o alentando un inapropiado uso de los dispositivos móviles. Las compañías necesitan hacer ajustes sobre sus arquitecturas de seguridad acorde a los equipos finales. Esto implica abandonar el esquema de perímetro rígido e introducir seguridad extremo-a-extremo, que se adapte a las características de los equipos finales. Para lograr esto, es necesario mejorar significativamente las políticas de seguridad e incrementar el entendimiento de las mismas por parte de los usuarios, a través de entrenamiento y programas de concientización a todo nivel.

b. Riesgos concernientes a cumplimiento y al ámbito legal

- El gobierno corporativo y el control de cumplimiento será de difícil sostenibilidad. Se espera que la realización de auditoría y administración de las acciones de los usuarios sea de difícil consecución. De igual manera la resolución y manejo de incidentes sobre los equipos proporcionados por los usuarios, puede volverse más complicado. Otro tema importante son las dificultades al respecto de cumplimiento con regulaciones de datos personales, por pérdida de privacidad del personal e información corporativa.
- La interoperabilidad, los modelos usados y cambios del contexto de seguridad entre aplicaciones y sistemas, hará más difícil la implementación de controles para cumplimiento regulatorios. Debido a que los colaboradores podrían comprar y operar sus equipos, resultaría complicado para las compañías asegurar que las políticas corporativas sean ejecutadas completamente, tales como las de recursos humanos, de ámbito legal y de propiedad intelectual, entre otras.
- La pérdida de distinción precisa entre data personal y aquella corporativa hará que sea más complicada el descubrimiento electrónico de información en situaciones de investigación legal. Debido a que no es evidente la separación de los dos ámbitos, es posible incurrir en intervención por parte de las compañías en la vida personal de sus colaboradores, desencadenando problemas legales para la organización.

c. Riesgos que afectan la data en términos de confidencialidad, integridad y disponibilidad

- Pérdida potencial de data corporativa, como resultado de información compartida no autorizada. Por implementaciones débiles de políticas de seguridad sobre los equipos finales y los servicios que utilizan los empleados, puede haber un riesgo alto de pérdida de información. Típicamente no se ejecutan controles sobre la data en tránsito, que representa un riesgo cuando se usan canales inseguros. La heterogeneidad e inmadurez del software en los equipos móviles es una fuente de riesgo, debido a las vulnerabilidades y bajos niveles de endurecimiento de seguridad sobre los dispositivos, aplicaciones y servicios utilizados. Así mismo, la implementación de controles de seguridad es una tarea complicada.
- Pérdida potencial de data corporativa como resultado de su acceso por parte de usuarios desconocidos y dispositivos no administrados conectados a la red corporativa. La ampliación del perímetro de seguridad para acomodarse a la tendencia de BYOD, podría facilitar una intrusión a la red. La pérdida de información podría ocurrir como resultado de acceso no autorizado de un tercero a la red o incluso el uso de un dispositivo legítimo por parte del mismo tercero.
- Pérdida potencial de data corporativa como resultado de la dificultad de controlar la seguridad en aplicaciones usadas con los equipos móviles. Este riesgo está relacionada a las características de seguridad de los componentes usados por los colaboradores, que dificulta la posibilidad de verificar, influir o controlar el software utilizado. Entonces, los controles de seguridad existentes pueden ser

comprometidos, especialmente por los comportamientos de los usuarios mismos; llegando a ocasionar pérdidas de información.

- Con el fin de obtener data corporativa, los equipos móviles pueden ser objetivo de ataque. Vectores de ataque como malware, phishing, ingeniería social y otros, pueden ser utilizados explotando los controles de seguridad débiles sobre los dispositivos, con el ánimo de robar la información corporativa que contienen. De igual manera, se puede experimentar daños colaterales como el robo de data personal igualmente.

De igual manera, a la par que se evidencian riesgos sobre la implementación de una estrategia de Bring Your Own Device; también se pueden identificar unas oportunidades resultantes.

A continuación, se presentan algunas de ellas:

- Oportunidades financieras potenciales. Con el uso de BYOD es posible incrementar la productividad, reduciendo gastos y mejorando la satisfacción de los usuarios. Esto se logra con el acceso permanente a la información corporativa por parte de los usuarios. De igual manera, el recorte presupuestal en hardware e instalaciones.
- Beneficios de recursos humanos potenciales. Mejora la satisfacción del personal por la libertad entregada, alcanzando una mejor retención de los empleados en la compañía.
- Oportunidades operacionales potenciales. Se puede obtener optimización de aspectos operacionales, debido a que se incrementa la disponibilidad del personal en temas de trato urgente. Además, se puede utilizar canales modernos como redes sociales o tele presencia para mejorar la influencia de grupo y compartir conocimiento.
- Oportunidades de manejo de data potencial. Con objeto de mejorar la disponibilidad de la data, el uso de almacenamiento en la nube resulta evidente. Esto ayudará a incrementar la interacción en línea y el acceso a la data ágilmente.

VI. MARCO ISO 27002

ISO 27002:2013 [19] es un estándar globalmente aceptada publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Esta proporciona una guía para la selección, implementación y mantenimiento de controles al respecto de seguridad de la información en para las organizaciones. Aunque esta norma no contempla específicamente la regulación sobre la utilización de Bring Your Own Device, es posible aplicar esta guía para gestionar adecuadamente esta tendencia.

A continuación, se presentan la relación de dominios, objetivos de control y controles seleccionados (Indicados entre paréntesis) que podría apoyar la implementación de una estrategia de Bring Your Own Device:

- Directrices de la Dirección en seguridad de la información (5.1). Con la definición de una política de seguridad de seguridad corporativa por parte de la alta dirección al respecto de Bring Your Own Device, se establece con claridad el alcance del uso de dispositivos dentro de la estrategia organizacional. Esta política necesita ser definida en el contexto de negocio y tiene que ser revisada y evaluada periódicamente.
- Dispositivos para movilidad y teletrabajo (6.2). Aquí se define puntualmente una política formal al respecto del uso de recursos de informática móvil y de teletrabajo, al igual que se debe desarrollar medidas de seguridad de apoyo para proteger la información misma.
- Seguridad ligada a recursos humanos (7). Es necesario una adecuada gestión del personal de la organización que hace uso de Bring Your Own Device durante todo el ciclo de vida dentro de la organización. Incluyendo establecer lineamientos en la vinculación, durante el empleo; donde se deberá garantizar que los colaboradores conozcan las amenazas y riesgos del uso de BYOD y al término de la relación laboral, cuando se tiene que cumplir con procedimientos para la devolución de los activos de información de la organización como la cancelación de permisos de acceso.
- Gestión de Activos (8). Es preciso realizar una adecuada identificación y clasificación de los

activos de información, que permita cumplir con una adecuada gestión de los mismos, aplicando de acuerdo a su criticidad esquemas de seguridad suficientes.

- Control de Accesos (9). Resulta indispensable identificar de acuerdo al negocio y las características de la estrategia Bring Your Own Device adoptada, cuáles serían los requerimientos de control de acceso necesarios, para así mismo establecer el conjunto de procedimientos para controlar la asignación de derechos de acceso.
- Criptografía (10). Con objeto de preservar la confidencialidad e integridad de la información corporativa, hay que declarar e implementar una política de seguridad sobre controles criptográficos y procedimientos para el manejo de claves, aun cuando se trate de dispositivos de propiedad de los usuarios; debido a la naturaleza de propiedad de la información que utilizan.
- Seguridad de los equipos (11.2). Aquí se incluye la debida protección de los equipos de Bring Your Own Device para reducir el riesgo de acceso no autorizado a la información que presentan y su protección contra pérdida o robo.
- Protección contra código malicioso (12.2). Pese a la heterogeneidad de dispositivos que puede presentarse en una estrategia de Bring Your Own Device, es necesario implementar medidas para evitar y detectar la introducción de códigos de programación maliciosos, tal como la instalación de software antimalware y levantamiento de barreras de seguridad local.
- Copias de seguridad (12.3). Mediante el establecimiento de una justa estrategia de respaldo, es posible mantener la integridad y la disponibilidad de la información que es accedida y transportada por dispositivos por dentro y fuera de un ambiente corporativo.
- Registro de actividad y supervisión (12.4). Basado en el axioma de que no se puede controlar lo que no se puede medir, es necesario aplicar esquemas de monitoreo sobre el acceso y tratamiento de la información desde los equipos móviles, para prevenir y detectar cualquier afectación de la misma, al igual que oportunidad de mejora sobre el sistema.
- Gestión de la vulnerabilidad técnica (12.6). Esto permitirá identificar las vulnerabilidades que se presenten sobre los activos de información, cuando son accedidos desde los equipos de Bring Your Own Device, para así mismo poder mitigarlas oportunamente.
- Gestión de la seguridad en las redes (13.1). Se debe garantizar la protección de la información sensible en las redes de la organización y desde accesos externos a la misma, a través de los dispositivos de BYOD.
- Requisitos de seguridad de los sistemas de información (14.1). Es necesario identificar los requisitos relacionados con la seguridad de la información dentro del contexto de Bring Your Own Device, lo mismo que protegerla cuando se usan redes públicas.
- Gestión de incidentes en la seguridad de la información (16). Con esto se busca que se garantice que los eventos de seguridad de la información y las debilidades de los sistemas de información sean correctamente reportados para aplicar las medidas respectivas de manera oportuna.
- Cumplimiento de los requisitos legales y contractuales (18.1). Debido a la débil separación de los ámbitos laborales y personales al interior de los dispositivos BYOD; es indispensable identificar e implementar medidas que garanticen los requisitos estatutarios, normativos y contractuales legislativos para evitar riesgos de tipo legal.
- Revisiones de la seguridad de la información (18.2). Su objetivo es garantizar que la seguridad de la información se mantiene pese a la dinámica de las tecnologías y contexto del negocio.

Con la revisión de los controles identificados previamente, le es posible a las organizaciones trazar una hoja de ruta ante la necesidad de implementar una estrategia Bring Your Own Device de manera estructurada y organizada.

VII. RECOMENDACIONES NIST

El Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en ingles); es una reconocida agencia del Departamento de Comercio de Estados Unidos, la cual promociona la innovación y competitividad industrial de los Estados Unidos.

En julio de 2016 realizó publicación NIST Special Publication 800-46, denominada "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security" [20], donde presenta recomendaciones para mejorar la seguridad en los programas Bring Your Own Device y reducir los riesgos sobre la información utilizando dispositivos móviles.

Aquí se reconoce a la tendencia Bring Your Own Device como una expansión del concepto de teletrabajo, permitiendo que los equipos que llevan sus usuarios se conecten directamente a la red corporativa. Ahora, debido a que estos dispositivos no presentan el mismo nivel de aseguramiento que los equipos corporativos tradicionales, se recomienda proporcionarles una red de acceso separada y externa que permita contener los posibles riesgos.

Al respecto de los dispositivos BYOD, se identifica que el equipo final utilizado es controlado por el colaborador y es éste quien tiene responsabilidad de la seguridad del mismo.

Debido a que los equipos finales de teletrabajo están expuestos a amenazas externas a la infraestructura de la organización, resulta necesario la implementación de medidas complementarias a las que se imponen a los equipos que se mantienen dentro del perímetro de la red corporativa. Ahora, si no es posible cumplir con lo anterior, se podría recurrir a ambientes locales seguros como las tecnologías VDI o VMI. De igual manera, se puede adoptar soluciones de MDM (Mobile Device Management) o MAM (Mobile Application Management).

Para tratar con más exactitud, los dispositivos utilizados por los usuarios son divididos en dos tipos: Los computadores personales (PC, de sus siglas en inglés personal computer) y los dispositivos móviles como tal. En los primeros se incluyen computadores tradicionales, como los PC de escritorio y los laptops; en los segundos se listan teléfonos inteligentes (smartphones) y tabletas (tablets).

Para los PC, se recomienda cubrir las siguientes actividades:

- Una correcta utilización del firewall del equipo; donde se ajusten las políticas del mismo para que sea aplicadas de acuerdo al nivel de seguridad de la red donde se conecta. Debido a que, en muchos casos, esta configuración es automática, luego de que el mismo sistema hace una verificación de las condiciones ambientales; resulta buena práctica que se revise administrativamente si correcta elección y llegado el caso, permitir ajustes apropiados.
- Mantener actualizados los sistemas operativos y aplicaciones, pese a que la conexión con la red de la organización sea breve o de poca constancia.
- Utilizar cuentas de usuario con privilegios limitados para el trabajo normal y solo hacer uso de aquellas con capacidades administrativas cuando se requiera.
- Activar bloqueo automático de acceso al PC. Con esto, cuando se deje desatendido este por un periodo considerable, se evite que personal no autorizado pueda utilizar la sesión abierta.
- Físicamente, se recomienda la utilización de cables o seguros, que reduzcan la oportunidad de ser objeto de robo.
- Debido a que existen herramientas que permiten correr desde medios extraíbles e iniciar PC, sin que se utilice el sistema operativo del mismo; resulta útil el bloqueo de este tipo de funcionalidades en los equipos de teletrabajo, para evitar el robo de información alojada en el disco duro. También es viable el uso de soluciones que evite el almacenamiento de información en diferentes destinos y así limitar la fuga de data corporativa.
- Una opción que evita el uso de recursos de la máquina de los empleados es correr las aplicaciones corporativas directamente con medios extraíbles y cuya integridad pueda ser gestionada más apropiadamente.

Al respecto de los dispositivos móviles, se recomienda:

- La implementación de soluciones de administración de equipos móviles centralizadas, que permitan gestión sobre las aplicaciones permitidas o configuraciones aceptadas.

- Por cuanto los equipos móviles cada vez son más similares a los PC tradicionales, es viable la aplicación de las mismas políticas de seguridad para ambos tipos; con lo cual se guarda consistencia en temas de seguridad. Si no es posible, hay que documentar con suficiencia esta desviación.

La data corporativa que es manipulada, creada y accedida en los equipos cliente necesita ser controlada y asegurada adecuadamente. Para ello se pueden utilizar las siguientes estrategias:

- Cifrado de información que reposa sobre los equipos y medios extraíbles que presente. Esto se podría lograr haciendo uso del mismo sistema operativo o a través de aplicaciones específicas para tal fin. La creación y uso de las llaves criptográficas para el cifrado remoto, deberán seguir las mismas políticas corporativas de los demás sistemas.
- Uso de máquinas virtuales. Para dispositivos BYOD es poco factible la ejecución de políticas de seguridad. Entonces, se puede controlar el ambiente, haciendo que el colaborador emplee una máquina virtual para sus labores corporativas. Para ello, se utiliza un software denominado hypervisor; sobre el cual se instala y corre la máquina virtual que la organización distribuye y sobre la cual se pueda garantizar la aplicación de las políticas de seguridad adecuadas. Existen dos tipos de hypervisores, uno que correo sobre el sistema operativo de la máquina del trabajador y otro no necesita, disponiendo directamente de los recursos de hardware de la máquina física. Se recomienda el uso del segundo tipo, por considerarse de mejor seguridad, pues reduce su superficie de ataque. Las imágenes de las máquinas virtuales distribuidas deben estar cifradas, igualmente.
- Es necesario extender las políticas de respaldo de información corporativas a los equipos móviles. Así pues, si se utiliza un repositorio dentro de red de la organización, será necesario utilizar esquemas de cifrado durante la transferencia de la información. Pero, si se almacena localmente, se tendrá que proteger al menos en la misma forma como es la data, ya sea cifrada o en texto plano.

Ahora, en lo respecta a cómo abordar el ciclo de vida del teletrabajo y acceso remoto, incluyendo BYOD; se presenta un modelo compuesto de cinco fases, a saber:

a. Fase 1: Inicio

Incluye acciones preparatorias, como identificar las necesidades actuales y futuras, requerimientos de desempeño, funcionalidad y seguridad; que finalmente apoya la construcción de una política propiamente dicha. Esta debe especificar cómo se permite el acceso a la red de la organización y cómo manejar el aprovisionamiento de cuentas de usuario.

Aquí se puede confirmar qué características deben tener los dispositivos dentro de la estrategia BYOD y de acceso remoto. De igual manera, es posible establecer el nivel de confianza en el cumplimiento de las políticas de seguridad; como, por ejemplo, confirmando que los usuarios partícipes de esta estrategia sean conscientes de sus responsabilidades frente a los temas de seguridad.

b. Fase 2: Desarrollo

Aquí se determina qué tecnologías utilizar para desarrollar la estrategia. Esto incluye consideraciones como arquitectura, métodos de autenticación, esquemas de cifrado y de control de acceso, como también decisiones de seguridad sobre los equipos finales. Estos aspectos deben alimentar un plan de seguridad del sistema, el cual también debe incluir el plan de gestión de incidentes.

c. Fase 3: Implementación

En esta etapa se despliega y prueba un prototipo del diseño, antes de ponerlo en producción. Con esto, se logrará evaluar y revisar aspectos como:

- Conectividad: Cómo se conecta y a qué recursos accede.
- Protección: Al respecto del flujo de tráfico.
- Autenticación: Confirmando que se ejecute correctamente e identificando brechas de seguridad.
- Aplicaciones: evitando que se tenga interferencia entre software de conexión y la operación propia.
- Administración/Gestión: Ratificando que los administradores pueden configurar y gestionar la solución segura y efectivamente.

- Auditoría: Permita realizar registro de actividad adecuadamente.
- Desempeño: Corroborando que se tiene disponibilidad de servicio tanto en horas valle como en horas pico.
- Seguridad de Implementación: Confirmar que se cumplen con los requisitos de seguridad.
- Configuraciones por Defecto: Identificar si los valores por defecto son viables o si es necesario realizar los ajustes correspondientes.

d. Fase 4: Operación y Monitoreo

Etapa que busca mantener el nivel de acceso y de seguridad apropiado, haciendo labores como:

- Verificando actualizaciones y parcheo de los componentes de software.
- Confirmando sincronización de relojes a una fuente única.
- Reconfigurando características de control de acceso, producto de cambio de políticas o tecnologías, como también por ajuste en requerimientos de seguridad.
- Identificando y documentando anomalías detectadas.
- Ejecutando análisis periódicos sobre las políticas, los procesos y los procedimientos, para corroborar que están funcionando correctamente. Estos pueden ser pasivos, analizando registros; o activos como escaneo de vulnerabilidades y con pruebas de penetración.

e. Fase 5: Terminación

Antes de que un equipo final permanentemente deje la organización, es necesario garantizar que toda la información corporativa es removida del mismo. Para el caso de dispositivos BYOD, donde sobre el mismo también se tiene data personal; es indispensable tener especial cuidado con esta y no llegar a afectarla. Esto se puede alcanzar mediante soluciones especializadas con tal fin.

Esta guía proporciona otra referencia útil en la consecución de un programa Bring Your Own Device bien estructurado, que requiere ser complementado con otras más técnicas y otras desde el punto de vista de gobierno corporativo.

VIII. CONTROLES TÉCNICOS

La implementación adecuada de un programa de Bring Your Own Device, requiere no solo la aplicación de buenas prácticas en temas de gobierno, también resulta necesario incluir tecnologías que le permitan a las áreas de TI operar, controlar y asegurarlas de manera justa a las necesidades del negocio y eficientemente.

De acuerdo a Gartner [21], de manera general en el mercado especializado se tiene un conjunto de tecnologías denominadas como EMM (Enterprise Mobile Management), que conecta los dispositivos móviles a la infraestructura empresarial y las organizaciones utilizan las siguientes funciones en sus programas de movilidad, incluyendo Bring Your Own Device:

- Aprovisionamiento: Configuración de dispositivos y aplicaciones para el despliegue y uso corporativo, gestionar actualizaciones y asistencia en el retiro de producción.
- Auditoría, seguimiento y Reporte: Gestión de inventarios, verificación de cumplimiento de las políticas corporativas y manejo de activos.
- Protección de data corporativa: Mitigación de pérdida y robo de información, mediante cifrado, control de acceso, contención y bloqueo de equipos.
- Soporte: Haciendo uso de inventario, analítica y conexión remota, las áreas de TI pueden dar soporte técnico a los dispositivos del programa.

Estas cinco capacidades pueden ser rastreadas en tres diferentes enfoques básicos no excluyentes, que requieren ser analizados sobre el criterio de la necesidad a cubrir y así proceder con la implementación de alguno(s) de ellos.

A continuación, se presenta un resumen de las características propias de cada enfoque [22],[23],[24],[25],[26]:

- Gestión de Dispositivos móviles (MDM, Mobile Device Management). Típicamente haciendo uso de APIs (Application Programming Interface) sobre el sistema operativo; estas soluciones pueden obtener control completo sobre los dispositivos gestionados. Con esto, se logra estableces

restricciones como bloqueo, cifrado y controlar el acceso al equipo. Son considerados muy intrusivos para estrategias de Bring Your Own Device, ya que puede llegar a afectar la data y configuraciones personales del usuario.

- Gestión de Aplicaciones Móviles (MAM, Mobile Application Management). Permite el control de las aplicaciones instaladas y utilizadas en los dispositivos, mediante la definición de listas blancas (permitidas) y listas negras (prohibidas) e identificación geográfica de uso o de conexión a Internet para restringir dependiendo el ámbito de uso. Por lo anterior, es posible dar mayor libertad y control sobre el dispositivo al usuario mismo.
- Gestión de Contenido en Móviles (MCM, Mobile Content Management). Usualmente mediante métodos de autenticación multi-factor, restringe el acceso a contenido controlando habilidades como edición, lectura, borrado o compartir.

Existen otras tecnologías que apoyan la mitigación de riesgos en la implementación de una estrategia Bring Your Own Device como:

- Escritorios remotos. Aquí el usuario desde su equipo se conecta a un servidor remoto, sobre el cual corre las aplicaciones corporativas, realizando toda actividad sobre la data en el mismo server.
- Máquinas virtuales. La organización distribuye entre sus colaboradores imágenes de máquinas virtuales que los usuarios pueden utilizar para realizar sus labores en un ambiente seguro y dedicado para estos temas.
- Soluciones de cifrado en los equipos. Mediante esto se logra mitigar posibles afectaciones sobre la información corporativa, por robo, pérdida o desatención de los equipos. Se puede usar las mismas capacidades de cifrado del sistema operativo o disponer de aplicaciones específicas para este tema.

IX. CONCLUSIONES

La consumerización de las TI es una realidad cada vez más predominante y la tendencia de Bring Your Own Device consecuentemente, tiene más presencia al interior de las organizaciones, aunque no se desarrolle dentro de un programa formal corporativo.

A lo largo del documento se identificaron diferentes ventajas y consecuencias negativas, producto del fenómeno. Éstas deberían ser analizados desde el punto de vista estratégico, para poder tomar una posición frente a su inminente masificación, gestionando de manera oportuna sus riesgos y oportunidades.

Para abordar el reto de implementar un programa de BYOD, es necesario combinar políticas, seguridad y tecnología, que entregue un producto acorde a los requerimientos del negocio y que garantice el cumplimiento regulatorio y normativo. Para ello, se puede recurrir a guías como las entregadas por la NIST, buenas prácticas como la norma ISO 27002, apoyadas en tecnologías que se ajusten al dinamismo de las amenazas circundantes.

Con lo anterior, las organizaciones podrán obtener la promesa de valor que tiene el fenómeno BYOD.

REFERENCIAS

[1] Moschella, D., Neal, D., Opperman, Piet y Taylor, J. (2004). The 'Consumerization' of Information Technology. Position Paper [Online]. Disponible en: https://www.smaele.nl/documents/Taylor-Consumerization-2004.pdf

[2] Unisys. (2010). Unisys Consumerization of IT. Benchmark Study [Online]. Disponible en: http://blogs.unisys.com/cit/files/2010/08/10-0190-CIT-SUMMARY_web.pdf

[3] Zamora, Javier. (2011). TIC, de la consumerización a la customización [Online]. Disponible en: http://www.ieseinsight.com/fichaMaterial.aspx?pk=7657&idi=1&origen=1&idioma=1

[4] Ericsson. (2016, Junio). ERICSSON MOBILITY REPORT. ON THE PULSE OF THE NETWORKED SOCIETY [Online]. Disponible en: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

[5] Ericsson. (2016, Junio). ERICSSON MOBILITY REPORT. ON THE PULSE OF THE NETWORKED SOCIETY [Online]. Disponible en: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

[6] Ericsson. (2016, Junio). ERICSSON MOBILITY REPORT. ON THE PULSE OF THE NETWORKED SOCIETY [Online]. Disponible en: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

[7] CloudPassage. (2016). CLOUD SECURITY. 2016 SPOTLIGHT REPORT [Online]. Disponible en: https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf
[8] CloudPassage. (2016). CLOUD SECURITY. 2016 SPOTLIGHT REPORT [Online]. Disponible en: https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf
[9] Buchholz, d., Dunlop, J. y Ross A. (2012). Improving Security and Mobility for Personally Owned Devices [Online]. Disponible en: http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/improving-security-and-mobility-for-personally-owned-devices-paper.pdf
[10] Maxwell, K. (2013, Enero). BuzzWord BYOD [Online]. Disponible en: http://www.macmillandictionary.com/buzzword/entries/byod.html
[11] Jensen, M. (2015, Noviembre). Is BYOD Trend Fading? [Online]. Disponible en: https://technivorz.com/is-byod-trend-fading/
[12] Jones, J. (2012, Julio). Beginner's Guide to BYOD (Bring Your Own Device) [Online]. Disponible en: https://blogs.microsoft.com/microsoftsecure/2012/07/17/beginners-guide-to-byod-bring-your-own-device/
[13] Willis, D. (2013, Abril). Bring Your Own Device: The Facts and the Future [Online]. Disponible en: https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf
[14] Crowd Research Partners. (2016). BYOD & MOBILE SECURITY. 2016 SPOTLIGHT REPORT [Online]. Disponible en: http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf
[15] Punekar, D. (2016, Noviembre). Increasing usage of mobile devices is predicted to drive bring your own device (BYOD) market growth [Online]. Disponible en: https://gminsights.wordpress.com/2016/05/17/bring-your-own-device-byod-market-size/
[16] Punekar, D. (2016, Noviembre). Increasing usage of mobile devices is predicted to drive bring your own device (BYOD) market growth [Online]. Disponible en: https://gminsights.wordpress.com/2016/05/17/bring-your-own-device-byod-market-size/
[17] Louks, J., Medcalf, R., Buckalew, L. y Faria F. (2013). The Financial Impact of BYOD. A Model of BYOD's Benefits to Global Companies [Online]. Disponible en: https://www.cisco.com/web/about/ac79/re/horizons.html
[18] Clarke, J., Gomez, M., Lioy, A., Petkovic, M., Vishik, C. y Ward, J. (2012, Septiembre). Consumerization of IT: Top Risks and Opportunities [Online]. Disponible en: https://www.enisa.europa.eu/publications/consumerization-of-it-top-risks-and-opportunities/at_download/fullReport
[19] International Organization for Standardization. ISO/IEC 27002:2013. Octubre, 2013
[20] Souppaya, M y Scarfone, K. (2016, Julio). NIST Special Publication 800-46. Revision 2. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security [Online]. Disponible en: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
[21] Smith, R., Taylor, B., Silva, C., Bhat, M., Cosgrove, T y Girard, J. (2016, Junio). Magic Quadrant for Enterprise Mobility Management Suites [Online]. Disponible en: https://www.gartner.com/doc/reprints?id=1-39B6K6A&ct=160613&st=sb
[22] Madden, B. (2012, Mayo). What is MDM, MAM, and MIM? (And what's the difference?) [Online]. Disponible en: http://www.brianmadden.com/opinion/What-is-MDM-MAM-and-MIM-And-whats-the-difference
[23] Steele, C. Management technologies to ensure mobile data security and compliance [Online]. Disponible en: http://searchmobilecomputing.techtarget.com/feature/Management-technologies-to-ensure-mobile-data-security-and-compliance
[24] Techtarget. Evaluating mobile device management products and services [Online]. Disponible en: http://searchsecurity.techtarget.com/essentialguide/Evaluating-mobile-device-management-products-and-services
[25] Hess, K. (2014, Marzo). How To Evaluate Mobile Management Solutions [Online]. Disponible en: http://www.tomsitpro.com/articles/evaluating-mobile-management-solutions,2-708-2.html
[22] Kane, C. (2015, Diciembre). The Forrester Wave™: Enterprise Mobile Management, Q4 2015. The 11 Providers That Matter Most And How They Stack Up [Online]. Disponible en: https://cdn2.hubspot.net/hubfs/478588/Forrester_MDM.pdf?t=1472171913033

Parra Sterling, Jaime Addulth. Ingeniero Electrónico de la Universidad Surcolombiana, con Máster en Dirección y Gestión de Proyectos, Título Propio de la Universidad Camilo José Cela conjuntamente con Bureau Veritas Centro Universitario. De igual forma, tiene conocimientos y certificaciones en diversos ámbitos de Redes y Seguridad, como Cisco, HP y A10, al igual que la Gestión del Servicio con ITIL.

Desde 2005 ha tenido experiencia en áreas de consultoría, diseño y gestión de soluciones de redes y seguridad.