ANÁLISIS DE RIESGOS SOBRE DISPOSITIVOS MÓVILES EMPRESARIALES

Cardona Perdomo, Rene Alejandro
rene.cardona35@gmail.com
Universidad Piloto De Colombia

Resumen—*En este artículo se expone de una forma muy elemental, un modelo de seguridad sobre los dispositivos móviles en una organización. Hoy en día, las empresas reconocen las enormes ventajas de implementar soluciones de movilidad a nivel tecnológico para fortalecer sus estrategias de negocio, sin embargo, la mayoría no lo hacen por miedo a caer en eventos de seguridad como pérdida de información corporativa que lleguen a poner en riesgo la integridad del negocio. Realizando un análisis de los riesgos más predominantes en el mundo de dispositivos móviles, y validando las funcionalidades más importantes de las herramientas de gestión y control de dispositivos existentes en el mercado, se detallan en este artículo recomendaciones sobre los criterios de control que debe implementar una organización para mitigar los riesgos de seguridad más relevantes basados en el resultado del análisis y gestión de riesgos para este entorno de movilidad al que se enfrentan las organizaciones.*

Índice de Términos—*Contenedor, Dispositivo móvil, enrolamiento, movilidad, riesgo, ruguerizado, supervisión.*

Abstract—*This article exposes in a very elementary way, a security model on mobile devices in an organization. Today, companies recognize the enormous advantages of implementing mobility solutions at the technological level to strengthen their business strategies, however, most do not for fear of falling into security events such as loss of corporate information that they get to put at risk the integrity of the business. By analyzing the most prevalent risks in the world of mobile devices, and validating the most important functionalities of the tools of management and control of devices existing in the market, it is detailed in this article recommendations on the criteria of control that must implement a organization to mitigate the most relevant security risks based on the result of the analysis and risk management for this mobility environment that organizations face.*

I. INTRODUCCIÓN

Con el avance tecnológico que se ha venido desarrollando a grandes pasos en el tiempo, enfocado especialmente sobre los dispositivos móviles de los ambientes empresariales, donde la movilidad es una prioridad importante para los empleados, en especial en las fuerzas comerciales, quienes exigen acceso a la información a través de las aplicaciones del negocio que les permiten ser más productivos cuando se encuentran fuera de la oficina fortaleciendo las estrategias de negocio; por esta razón, las auditorias de TIC, se han convertido en un escenario donde los profesionales de la seguridad deben hacer frente a las amenazas que de igual forma evolucionan significativamente en el ambiente de movilidad. En consecuencia, a nivel organizacional es de vital importancia realizar un análisis y gestión de riesgos sobre el parque de dispositivos móviles, realizando pruebas a las apps desde su concepción hasta su lanzamiento, siguiendo con un análisis de vulnerabilidades, cuyo resultado conlleve a la implementación de controles apropiados, estableciendo un modelo de seguridad de la información para movilidad. Con base a esta necesidad planteada, en este artículo se presentan recomendaciones y criterios muy elementales sobre el análisis de los factores de riesgo más relevantes a nivel de dispositivos móviles y las apps, estableciendo como resultado la implementación de controles de seguridad que permitan a la organización cumplir con las necesidades propias del negocio en sus diferentes áreas bajo un entorno seguro.

II. ANÁLISIS DE RIESGOS DISPOSITIVOS MOVILIDAD

La protección de los dispositivos móviles, es una necesidad primordial en una organización que brinde este tipo de tecnología a sus funcionarios para el desarrollo de sus actividades laborales, pues estos dispositivos funcionan como computadores pequeños que permiten llevar la información a todo lugar, brindando acceso a múltiples servicios como banca digital, redes sociales, correo electrónico, fotografía y videos que pueden comprometer en un incidente de seguridad a la organización o al funcionario que la administre.

Como fase inicial del análisis de riesgo identificamos y determinamos sobre un dispositivo móvil, las vulnerabilidades que lo vuelven débil y las amenazas que lo ponen en peligro, con el fin de posteriormente valorar su grado de riesgo. Como parte del proceso de análisis desarrollado para este artículo, se determinan a continuación los peligros más relevantes a los que se encuentran expuestos los dispositivos móviles, que pueden llegar a generar un evento de seguridad si no se aplica la protección adecuada:

1) Indisponibilidad de dispositivo y pérdida de información por daño fisico.

2) Pérdida o robo de información del dispositivo móvil.

3) Pérdida y divulgación de datos por acceso no autorizado.

4) Pérdida y divulgación de datos en transmisión por conexión de red.

5) Pérdida y divulgación de datos por software malintencionado.

6) Indisponibilidad de servicios y pérdida de datos por malware.

Teniendo definido los seis (6) riesgos más relevantes y comunes en el mundo de movilidad, se inicia el proceso de análisis de los mismos donde se valida la posibilidad de ocurrencia y el impacto que tiene cada uno de estos en el caso de que se llegue a materializar; esto con el objetivo de determinar cúal tiene mayor efecto sobre la organización; para desarrollar este análisis, se usó un método semi-cuantitativo, donde se utilizan clasificaciones de palabras como alto, medio o bajo, o descripciones más detalladas de la probabilidad y la consecuencia y su cantidad no es fija, depende de las necesidades propias de la organización, variando hasta un máximo de seis (6) condiciones.

Para el desarrollo del análisis presentado en este artículo, se definieron cuatro (4) variable (mínima frecuente – poco frecuente – frecuente – muy frecuente) para definir la probabilidad de ocurrencia de cada riesgo analizado. Para realizar el cálculo del valor cuantitativo del riesgo, se asignan los valores a cada una de las variables de la probabilidad basados en el número de veces que el evento de riesgo pueda materializarse en un periodo de un (1) año. Ver Tabla I.

TABLA I

Variables probabilidad de ocurrencia [3]

Probabilidad	*No. Eventos x Año*
Muy frecuente (4)	Más de 24 veces por año
Frecuente (3)	Menos de 24 veces por año
Poco frecuente (2)	Menos de 6 veces por año
Mínima frecuente (1)	Menos de 2 veces por año

Así mismo, para determinar el impacto, se definieron cuatro (4) variables (alto – medio – bajo) con la asignación de los valores cuantitativos respectivos basados en el porcentaje de dispositivos afectados por la materialización del evento de riesgo analizado. Ver Tabla II.

TABLA II

Variables nivel de impacto [3]

Impacto	*Magnitud Daño*
Alto (3)	100% dispositivos
Medio (2)	60% dispositivos
Bajo (1)	30% dispositivos

Estimar el impacto o la magnitud de daño, de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio complejo y extenso. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. [3]

Para desarrollar el análisis de riesgo y estimar el resultado (*riesgo*) se usa la gráfica de dos dimensiones, con la probabilidad vs el impacto, Ver Tabla III, donde se establece la operación matemática que determina un valor cuantitativo del riesgo que representa cada amenaza planteada.

*Riesgo = Probabilidad * Impacto*

TABLA III

Análisis de riesgo [3]

*Riesgo = Impacto * Probabilidad*

Impacto \ Probabilidad	1	2	3	4
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4

Esta matriz es una herramienta muy útil para la gestión de riesgos, pues permite priorizar, de forma muy visual y sencilla, los riesgos definidos en la fase inicial, identificando de forma clara aquellos sobre los cuales es necesario prestar más atención y establecer medidas o controles antes de que estos se materialicen para propender mitigarlos y minimizar los daños que puedan generar.

El resultado obtenido de la operación en la matriz, determina cuantitativamente (entre 1 y 12) la prioridad con que se debe atender cada riesgo a analizar. Los resultados de esta matriz, permiten agrupar los riesgos por categorías estableciendo el nivel de atención y tratamiento que se le debe dar a cada riesgo según el resultado obtenido. Para el análisis planteado en este artículo se agrupan los riesgos en tres (3) categorías establecidas cuantitativamente según su valor y representadas cualitativamente en los colores (rojo – amarillo – verde), presentes en la matriz de análisis de riesgos: Ver Tabla III.

Rango entre 8 y 12: Riesgos intolerables por su altísima probabilidad y trascendencia; que deben ser atendidos rápidamente con prioridad alta identificados cualitativamente con el color (*rojo*).

Rango entre 3 y 6: Riesgos importantes, con menor probabilidad y repercusiones, pero importantes en atender; con prioridad media identificados cualitativamente con el color (*amarillo*).

Rango entre 1 y 2: Riesgos moderados que suceden con escasa frecuencia y relevancia, con prioridad baja identificados cualitativamente con el color (*verde*).

Con la determinación de las amenazas más comunes en el mundo de dispositivos móviles, y basados los rangos obtenidos en la matriz de análisis de riesgos, se realiza el cálculo cuantitativa del riesgo por cada una de las amenazas el cual determina el rango de clasificación en el que se enmarcan, para tal fin se definió la siguiente Tabla IV:

TABLA IV

Cálculo cuantitativo del riesgo por amenaza [3]

Análisis de Riesgos Dispositivos Móviles			*Resultados Cuantitativos*		
Componente	***Causa***	***Vulnerabilidad***	***Probabilidad***	***Impacto***	***V. Riesgo***
Dispositivo móvil	Daño físico del dispositivo.	Indisponibilidad de dispositivo y perdida de información.	4	2	8
	Pérdida o robo del dispositivo móvil.	Pérdida o robo de información del dispositivo móvil.	4	3	12
	Acceso no autorizado al dispositivo móvil	Pérdida y divulgación de datos por acceso no autorizado.	2	3	6
	Conexión a redes wifi públicas.	Pérdida y divulgación de datos en transmisión por conexión de red.	4	2	8
	Instalación de App de origen desconocido.	Pérdida y divulgación de datos por software malintencionado.	3	3	9
	Infección por malware en dispositivo móvil.	Indisponibilidad de servicios y pérdida de datos por malware.	3	3	9

Con base a los resultados obtenidos en este análisis de riesgos donde se obtuvo la clasificación del riesgo según el valor cuantitativo de cada amenaza, definida en este artículo, a la que están expuestos los dispositivo móvil en una organización, se establecen a continuación una serie de factores básicos y recomendaciones a tener en cuenta para implementar controles de seguridad elementales que deben ser parte fundamental de la gestión de riesgos y que a su vez deben ser instaurados bajo el modelo de seguridad sobre movilidad, alineados con las políticas de la organización, todo para brindar protección en un entorno seguro. Los controles establecidos para mitigar las amenazas analizadas en este artículo se basan en la implementación de soluciones de administración de dispositivos móviles existentes en el mercado con funcionalidades orientadas a mitigar un sin número de amenazas y vulnerabilidades existentes en el mundo de la movilidad y que para este caso aplica para las más comunes identificadas en este artículo.

III. SELECCIÓN DE DISPOSITIVO

Basados en la necesidad del negocio y de las expectativas de la alta gerencia, la organización en asesoría con el área de TIC, deben establecer los criterios básicos de selección de los dispositivos móviles teniendo en cuenta las siguientes recomendaciones:

1) Basados en el requerimiento funcional y el factor presupuestal que la organización tenga dispuesto para tal fin, se deben validar por parte del área TIC de la organización, la adquisición de un dispositivo de fabricantes reconocidos en el mercado como por ejemplo Samsung, Lenovo, LG Electronics o Apple Inc, entre otros, que brinden respaldo de garantía y soporte a nivel nacional sobe el producto seleccionado, así como la selección de un modelo de dispositivo que esté vigente o próximo a salir al mercado; la selección de este fabricante podría estar alineada con la misma marca del parque computacional que la organización tenga, esto para garantizar compatibilidad en los sistemas o precios a mayor escala con el mismo proveedor.

2) Determinando el sistema operativo del dispositivo, y basados en el requerimiento de la necesidad de negocio a satisfacer, se debe proceder a analizar y seleccionar un modelo de dispositivo que cumpla técnicamente con las características necesarias para desarrollar las funcionalidades que se requieren operar, dando como resultado el documento de especificación técnica que como mínimo debe contemplar tres puntos importantes correspondientes a procesamiento (CPU), memoria (RAM), almacenamiento local (ROM), los cuales deben estar estimados con base al volumen de carga que demande el proceso funcional que la organización pretende movilizar, contemplando también las plataformas o aplicaciones que la organización posea en su core de negocio.

3) Dentro de las características técnicas, de debe contemplar el sistema operativo del dispositivo el cual preferiblemente debe garantizar compatibilidad con la infraestructura de la organización y la flexibilidad para sistemas móviles y manejo de apps. Bajo este criterio, se deben tener en cuenta sistemas operativos estándar en el mercado mundial como lo son Android, iOS, BlackBerry, Mac OS, Symbian y Windows Phone, recomendados por su flexibilidad para plataformas de movilidad como es este caso.

Aunque existen dispositivos móviles (tabletas), que trabajan bajo sistema operativo windows, el criterio de selección de este sistema operativo se debe basar solo en caso de que el negocio así lo requiera o por integración con otros sistemas de la organización, esto debido a que para windows, los requisitos técnicos en el dispositivo son altos para que las aplicaciones desarrolladas para este sistema operativo corran idealmente.

IV. PROTECCIÓN FÍSICA DEL DISPOSITIVO

Una de las características importantes de protección que en ocasiones no se tiene en cuenta al momento de definir los controles de protección en los aspectos de movilidad, es la parte física del dispositivo, la cual puede llegar a generar indisponibilidad de la información o incluso perdida de la misma causando afectación en la productividad del negocio, conllevando una pérdida económica a la organización.

Riesgo: Indisponibilidad de dispositivo y pérdida de información por daño fisico.

Este factor de protección depende del tipo de labor que desempeñen los funcionarios de la organización. Para establecer un control que garantice la mitigación del riesgo de daño físico por golpes o desgastes a causas del medio donde se desarrollan las actividades, se establece el termino de ruguerizado, cuyo significado hace referencia a un adjetivo castellanizado, del verbo inglés "ruggedize", del que se ha tomado prestado su significado: To strengthen for better resistance to wear, stress, and abuse (en definición del diccionario Merriam-Webster). [5].

En términos de dispositivos móviles lo rugerizado corresponde a una carcasa o chasís diseñado especialmente para absorber la energía de un impacto protegiendo los componentes electrónicos internos del dispositivo, brindando al funcionario tranquilidad y seguridad en su manipulación.

Hoy en día en el mercado hay grandes marcas que fabrican tabletas rugerizadas con características especiales, llamadas tabletas todoterreno o tabletas robustas, [4]. resistentes a impactos, resistentes a partículas de polvo, resistentes al agua y hasta sumergibles. Ver Fig. 1. Este tipo de producto es muy poco conocido y limitado en el mercado y con un costo bastante elevado, lo cual hace que sea de difícil adquisición para pequeñas y medianas organizaciones.

Fig. 1. Dispositivo móvil rugerizado. [6]

Llevando este factor a términos más técnicos, se está hablando de dispositivos que cumplen con la certificación IP67 o IP68 o a niveles más extremos a la certificación militar MIL-STD-810G o MIL-STD-810F. El grado de protección IP, de la norma IEC 60529, hace referencia al sistema de codificación para indicar los grados de protección provistos por un encerramiento contra acceso a partes peligrosas, entrada de cuerpos sólidos extraños, entrada de agua y para dar información adicional en conexión con tal protección, [7]. Este estándar ha sido desarrollado para calificar de una manera alfa-numérica los grados de protección provistos por los encerramientos de equipo eléctrico en función del nivel de protección que sus materiales contenedores le proporcionan contra la entrada de materiales extraños. Mediante la asignación de diferentes códigos numéricos, el grado de protección del equipamiento puede ser identificado de manera rápida y con facilidad mediante los dos dígitos del estándar como muestra la siguiente Fig. 2:

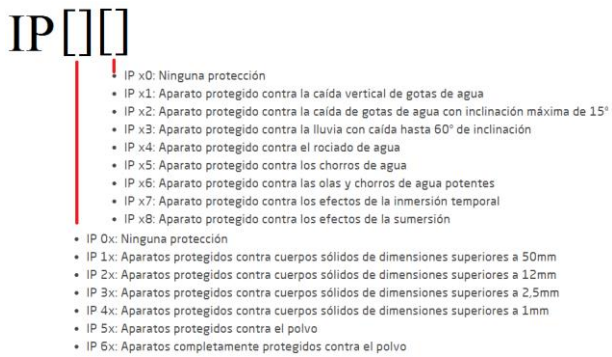

Fig. 2. Nomenclatura norma IEC 60529. [10]

Como recomendación, a la hora de elegir el tipo de protección en el dispositivo móvil, la organización debe tener en cuenta estas certificaciones basados en la necesidad y el medio donde se desarrollarán las actividades del personal que las tendrá en uso.

V. MODELO DE ADMINISTRACIÓN DE DISPOSITIVOS

Cada dispositivo de movilidad que se entregue a los funcionarios de la organización bien sea en los niveles gerenciales o a las fuerzas comerciales, debe contener un marco de control y administración de forma segura y centralizada mediante el cual se puedan realizar los ajustes y configuraciones que permita aplicar las diferentes políticas de seguridad de la información definidas en la organización.

Para garantizar este propósito, en la era de los dispositivos móviles se habla de los sistemas de gestión de movilidad empresarial, correspondiente al control y administración de tres elementos fundamentales en movilidad (dispositivos, aplicaciones y datos) enfocados al mundo empresarial; de ahí nace el concepto de MDM, correspondiente al acrónimo de ***Mobile Device Management***, en español "gestión de dispositivos móviles" [8]. correspondiente a una solución de software que ofrece una funcionalidad de gestión, control y soporte a los dispositivos móviles de la organización, todo desde una única consola y sin importar el operador de telefonía o proveedor de servicios. Con la implementación de un MDM, la organización podrá brindar a los empleados que operan fuera de la oficina, un acceso coherente a los recursos y datos corporativos desde cualquier ubicación y con cualquier dispositivo, permitiendo mejorar la productividad con ahorros en tiempos y costos en un entorno confiable; garantizando la protección de los recursos corporativos frente a un acceso no autorizado.

No hay que confundir los conceptos respecto al MDM, pues existe en el mercado y en las redes de internet el concepto de MDM como (***Master Data Management***) el cual corresponde a un método integral que permite a una organización unificar todos sus datos críticos en un solo repositorio bajo el nombre de fichero maestro [9]. exclusivamente enfocado a la información, algo muy diferente a la administración de dispositivos móviles (***Mobile Device Management***).

La arquitectura de un MDM está estructurada sobre tres componentes básicos que interactúan de forma coordinada para la ejecución de sus funciones, conformando así la herramienta de administración de dispositivos móviles [11]. Ver Fig. 3.

1) Plataforma centralizada: La organización debe disponer dentro de su infraestructura tecnológica, un servidor integrado con las características técnicas exigidas, donde se implementará el core de la solución del *mobile device management* (MDM), que soportará toda la administración de los dispositivos que la organización pretende distribuir a sus funcionarios.

2) Base de datos: Como parte integral de la solución del MDM, se contempla una base de datos que permite el almacenamiento de toda la información de la administración procesada por el MDM a través de los diversos dispositivos móviles de la organización.

3) Agente local: Es una aplicación que se instala en cada uno de los dispositivos que se desean administrar; este agente mantiene una conexión directa con el servidor central a través de redes wifi, GPRS, 4G o cualquier otro medio de transmisión de datos lo cual le permite a la consola central del MDM tomar control del dispositivo y aplicar las configuraciones y reglas definidas.

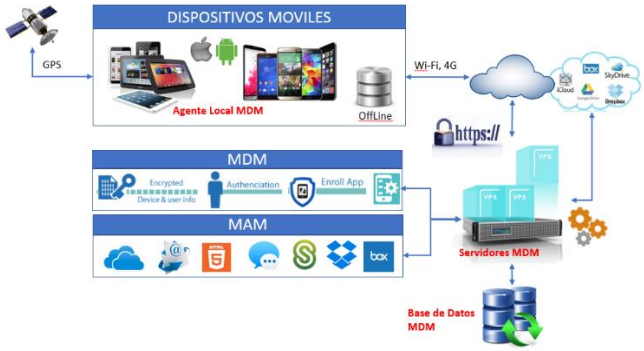

Fig. 3. Arquitectura MDM. [20]

En muchas organizaciones los dispositivos son adquiridos y suministrados a los funcionarios, por ellas misma, modelo que garantiza mayor seguridad, sin embargo, existen casos donde los empleados utilizan su propio dispositivo como herramienta de trabajo, promoviendo así la tendencia conocida como BYOD acrónimo de (***Bring Your Own Device***) en español "traiga su propio dispositivo", otro concepto que se enmarca dentro del mundo del MDM. [12].

Además de un control y una buena gestión corporativa del personal en movilidad, los sistemas MDM brindan numerosas ventajas con las múltiples funcionalidades que poseen, a nivel de accesos, restricciones, manejo de apps, localización, sincronización, reportes, entre otras; todas enfocadas al proceso de administración y control; nombrando las más relevantes tenemos:

- Establecimiento de una contraseña de bloqueo desde el servidor.
- Instalación masiva de aplicaciones en los dispositivos conectados a la red.
- Rastreo satelital sobre los dispositivos para el seguimiento, monitoreo y localización.
- Control de gastos en el consumo telefónico y red de datos.
- Integración con el directorio activo LDAP de la organización para unificar usuarios y procesos de autenticación unificados.
- Bloqueo de funciones sobre los periféricos integrados al dispositivo.
- Sincronización de archivos.
- Borrado remoto de los datos de cualquier dispositivo.

La característica más importante, es que todo está manejado desde una consola centralizada de administración; garantizando una seguridad unificada de todos los dispositivos móviles que acceden a los sistemas corporativos; sin embargo, para establecer un buen modelo de seguridad de la información se deben tener en cuenta las siguientes funcionalidades más relevantes e imprescindibles a implementar como criterios de control a través de un sistema MDM para garantizar un modelo se seguridad de la información confiable:

A. El control de acceso de los dispositivos:

Riesgo: Pérdida y divulgación de datos por acceso no autorizado.

Una opción básica que nos brindan los sistemas MDM, corresponde a la obligatoriedad de una contraseña de bloqueo para acceso al dispositivo, permitiendo parametrizar un tipo de contraseña que este alineada con las políticas de seguridad establecidas en la organización, como la longitud, si es alfanumérica o numérica, el usos de caracteres especiales, el histórico de contraseñas, el número de intentos y las acciones a ejecutar como borrado total del dispositivo, en caso de que el número de intentos sobrepase el límite establecido. Este parámetro de seguridad es uno de los primeros y más básicos a implementar en el modelo de seguridad de dispositivos móviles. Esta contraseña de autenticación se almacena de forma segura localmente dentro del dispositivo en un token inteligente, lo que facilita la seguridad, la portabilidad y las operaciones tanto en modo online como offline y como seguridad adicional, se activa el cifrado del dispositivo completo.

B. Integración con directorio activo:

Riesgo: Pérdida y divulgación de datos por acceso no autorizado.

Con el objetivo de unificar usuarios y contraseñas de acceso, se recomienda implementar las paramétricas de integración del MDM con el directorio activo de la organización, para la administración de cuentas de usuarios y autenticación basadas en las políticas del mismo directorio.

C. Suscripción de dispositivos:

Riesgo: Pérdida y divulgación de datos por acceso no autorizado.

Estableciendo contraseña de acceso físico al dispositivo, como primer control de seguridad, y activando la integración con el directorio activo, se deriva el tercer control correspondiente al proceso de suscripción. Cuando el dispositivo es registrado por primera vez a la plataforma MDM, esta toma todos los datos tanto de usuario como del dispositivo suscrito. Este proceso de suscripción se ejecuta con un usuario y contraseña, que, como recomendación, debe corresponder a las credenciales del directorio activo o la solución de inicio de sesión único de la organización. El proceso de suscripción del MDM, permite asociar el id del dispositivo con el usuario, de esta forma se debe establecer

un criterio de control donde no se permite la suscripción de dispositivos que no estén previamente relacionados en la lista blanca de dispositivos autorizados. Este control garantiza que ningún dispositivo externo de origen desconocido se enrole y haga uso de los sistemas de la organización.

D. Borrado remoto de los datos:

Riesgo: Pérdida y divulgación de datos por acceso no autorizado.

Esta opción es una función imprescindible en la implementación del modelo de seguridad mediante los sistemas MDM, para prevenir la fuga de los datos que residen en el dispositivo móvil; permite de forma remota a través de un comando dirigido desde la consola central ejecutar un proceso de borrado total de la información del dispositivo y aplica en los casos de perdido o robo, evitando así la posibilidad de extracción de información valiosa por parte de los delincuentes o de quien llegue a encontrar el dispositivo.

Esta opción está asociada a otra serie de funciones que permiten hacer un rastreo, bloqueo con mensaje de pantalla indicando la devolución del dispositivo, esto en caso de perdida, pero si el dispositivo es robado, no se recomienda recuperarlo por cuenta propia de la organización, para no enfrentar una situación de riesgo peor; en ese caso lo recomendado es limitarse a ejecutar el proceso de borrado total de los datos, poner la correspondiente denuncia a la policía y llamar al operador para bloquear el acceso a la red móvil y la SIM con la información del número IMEI y el serial del dispositivo existente en los registros de la consola del MDM. [14].

E. Bloqueo de funciones en el dispositivo móvil:

Riesgo: Pérdida y divulgación de datos.

Una característica importante en los sistemas de MDM, es la opción de habilitar o deshabilitar de forma remota, funciones en los dispositivos móviles tales como el micrófono, la cámara, el GPS, y el más importante el puerto USB o micro USB, impidiendo la conexión de unidades de almacenamiento a través de este puerto previniendo la fuga de información. El bloqueo de este puerto, es un criterio de control que debe estar implementado dentro del modelo de seguridad de la información en los dispositivos móviles de la organización, brindando al funcionario únicamente la opción de trabajar la información localmente o través del modelo de repositorio central mediante nube privada o la administración de contenido, donde estén aplicadas las políticas de protección de datos corporativos.

F. Restricción de usuarios:

Riesgo: Pérdida y divulgación de datos por acceso no autorizado.

El manejo perfiles dentro de la plataforma de administración del sistema MDM, es una característica que debe tomarse como un criterio de control importante y debe estar incluida dentro del modelo de seguridad de la información en dispositivos móviles, definiendo parametrizaciones de perfiles que permitan establecer acceso o restricción a las diferentes funcionalidades del dispositivo o al uso de las aplicaciones apps, con base a las funciones que desarrolle cada funcionario en la organización.

G. Supervisión del estado de los dispositivos en relación con el cumplimiento de políticas:

Riesgo: Acceso no autorizado a los sistemas, pérdida y divulgación de datos por acceso no autorizado, fraude.

El sentido de ser de los sistemas MDM, es el control y la administración centralizada de todos los dispositivos móviles de la organización, garantizando la aplicación de políticas de seguridad para mitigar los riesgos de seguridad analizados, y para que este sentido se cumpla, un criterio importante que se debe contemplar en el modelo de seguridad, es la activación de la funcionalidad del manejo de inventario, que nos permita tener una información completa y en tiempo real del estado de los dispositivos enrolados al sistema, garantizando que las políticas y controles de seguridad estén habilitadas y aplicadas correctamente en cada dispositivo, por consiguiente, un criterio de control que debe estar habilitado, es la parametrización de alertas y reportes que avisen e informen al administrador de la plataforma central, cuando un dispositivo pierde el control o cual no tiene las políticas activas para tomar acciones y prevenir que quede expuesto a cualquier riesgo. En los sistemas MDM, es de vital importancia mantener constantemente actualizado este inventario, con el objetivo de brindar una visión lo más precisa posible de la situación real de los dispositivos de la organización.

H. Administración de certificados:

Riesgo: Pérdida y divulgación de datos en transmisión por conexión de red.

Dentro de la arquitectura de los sistemas MDM, en cada uno de los dispositivos que se desean administrar, existe un agente que mantiene una conexión directa con el servidor central a través de redes Wifi, GPRS, 4G o cualquier otro medio de transmisión de datos utilizando generalmente comunicaciones encriptadas de protocolo tipo SSL, SSH a través de HTTPS para conectarse de forma segura. Bajo este modelo, los sistemas MDM permiten habilitar la suscripción de certificados tipo CA para conexiones por Wifi o VPN y perfiles de correo electrónico, por esta razón, es de vital importancia activar este tipo servicio de certificados para la protección de acceso a redes. Este servicio es suscrito una vez que se inscribe un dispositivo móvil en el MDM, y de esta forma, los usuarios pueden tener acceso sin problemas a los recursos corporativos con las configuraciones de seguridad adecuadas garantizando un control para mitigar el riesgo de secuestro de una sesión debido a un protocolo de conexión inseguro.

I. El control de acceso a las apps:

Riesgo: Pérdida y divulgación de datos por software malintencionado, indisponibilidad de servicios y pérdida de datos por malware.

Los sistemas MDM permiten establecer un contenedor para las apps públicas y las apps desarrolladas exclusivamente para la organización, integrándose con el

MAM para establecer reglas de seguridad que permiten otorgar o denegar desde la consola central permisos de ejecución sobre estas. Esta funcionalidad, debe estar habilitada como un criterio de control dentro del modelo de seguridad en dispositivos móviles de la organización que, en conjunto con la definición de perfiles, permite establecer una política de control importante para evitar la ejecución y utilización de aplicaciones no autorizadas en la organización, mitigando así el riesgo de infección por malware o accesos no autorizados a causa del uso de aplicaciones de origen desconocido.

J. Contenedor, área protegida para aplicaciones empresariales que se articula con el principio BYOD:

Riesgo: Acceso no autorizado a los sistemas, pérdida y divulgación de datos por acceso no autorizado, fraude, pérdida y divulgación de datos por software malintencionado, indisponibilidad de servicios y pérdida de datos por malware.

Este modelo donde la organización permite a los trabajadores llevar a cabo tareas del trabajo, conectarse a la red, a los recursos corporativos y centralizando información empresarial todo desde su dispositivo personal (portátiles, smartphone o tableta), es una tendencia que aún tiene muchas implicaciones para la organización, pues la ausencia de políticas de seguridad adecuadas puede poner en riesgo información confidencial de la compañía. Para las organizaciones que adopten esta modalidad, es importante definir el concepto de contenedor, que hace referencia a las tecnologías que permiten crear entornos autenticados y cifrados de confianza MCM, utilizados para almacenar, utilizar y compartir datos empresariales. [12].

La mayoría de los sistemas de gestión de movilidad empresarial incluyen varias opciones de contenedores para diferentes casos de uso y la implementación de estos, ayuda a TIC a crear un espacio seguro en cualquier dispositivo, al cual se le pueden definir y aplicar políticas de cifrado y autenticación secundaria que refuerzan la protección de datos corporativos.

Por esta razón, si la organización acoge este modelo BYOD, debe establecer como mínimo un contenedor o área protegida, que permita compartir datos de negocios, pero manteniendo aisladas las aplicaciones y datos personales y al cual se le deben aplicar todos los controles mencionados dentro de la zona del contenedor, para garantizar la seguridad de la información corporativa que estará anidada dentro del dispositivo personal del funcionario.

Adicionalmente se debe tener en cuenta otra serie de factores que involucra el modelo BYOD, como mayor proliferación de todo tipo de terminales y aplicaciones que aumentan el consumo de recursos tecnológicos centralizados de infraestructura, generando mayor incidencia sobre los departamentos de soporte y mantenimiento de TIC.

Todo lo mencionado en los puntos anteriores, representa un reto de gestión importante para los administradores de TIC, quienes son los responsables de garantizar una adecuada configuración de los dispositivos móviles bajo un buen modelo de seguridad de la información corporativo, todo para facilitar a los funcionarios el ingreso al ambiente empresarial por fuera de la organización. Sin embargo con la implementación de un sistema MDM es claro que definiendo y parametrizando detalladamente cada configuración de estas diez (10) funcionalidades básicas de un sistema MDM, validadas como criterios de control , se puede establecer un modelo básico inicial de seguridad de la información para dispositivos móviles de la organización; donde el administrador desde su consola central, podrá enviar a cada dispositivo móvil la configuración inicial para que puedan ser usados apropiadamente bajo un modelo de seguridad que garantice mitigar los riesgos a los que claramente están expuestos.

En el mercado existe un gran número de proveedores que ofrecen sistemas MDM para la administración de dispositivos móviles, tales como Citrix, Microsoft, Bixpe, Aranda Software, Escanda, por mencionar algunos; que permiten parametrizar las funcionalidades descritas en este artículo, pero deberá ser el área de TIC, quien, mediante un estudio de mercado, defina cuál es la que más se adapta a las necesidades que la organización demanda.

VI. ADMINISTRACIÓN DE APLICACIONES MÓVILES

El objetivo de una solución móvil no es sólo hacer posible que los usuarios finales trabajen en dispositivos móviles, sino ayudarlos a ser lo más productivos posible, para tal fin, en las diferentes tiendas de aplicaciones apps para Android y iOS, existentes en la red de internet, hay un sin número de desarrollos de todo tipo y para todo propósito posible, expuestas al público sin ninguna garantía de seguridad en cuanto al verdadero propósito en su código fuente, generando un riesgo latente en el esquema de movilidad.

Riesgo: Acceso no autorizado a los sistemas, pérdida y divulgación de datos por acceso no autorizado, pérdida y divulgación de datos por software malintencionado, indisponibilidad de servicios y pérdida de datos por malware.

Validando este riesgo, dentro del mundo de los dispositivos móviles, se enmarca otro concepto importante a tratar en este artículo correspondiente a la administración y control de las aplicaciones móviles apps en los dispositivos, denominado (***MAM***) acrónimo de ***Mobile Application Management***, que en español hace referencia a gestión de aplicaciones móviles, que también hace parte integral de los sistemas de gestión de movilidad empresarial, y que permite garantizar una protección más selectiva y eficaz sobre la seguridad en las apps de uso corporativo. [16].

De todas las tareas que desempeña un complejo sistema de gestión de movilidad empresarial, está la gestión de aplicaciones a través de MAM encargada de administrar y controlar todas las aplicaciones que la organización determine indispensables para el desarrollo de las funciones de los empleados según el modelo de negocio.

MAM juega un papel importante en el modelo de gestión de las aplicaciones móviles, optimizando efectivamente este proceso para garantizar la seguridad de la información mediante la definición de controles de acceso, restricciones y condicionamientos de ejecución de las apps, que conlleven a

mitigar los riesgos presentes en el uso de aplicaciones de origen desconocido.

Basados en el resultado del análisis de riesgos en dispositivos móviles, se recomienda establecer y habilitar como criterios de control las siguientes opciones más relevantes dentro del MAM de un sistema de gestión de movilidad empresarial:

- Mediante la definición de listas negras y blancas, restringir el acceso y ejecución de las aplicaciones para evitar que los usuarios instalen aplicaciones no permitidas en la organización.
- Restringir el descargue de aplicaciones apps de tiendas no oficiales, determinando solo acceso a las tiendas certificadas como Play Store para Android o App Store para iOS.
- Establecer una regla de aprovisionamiento automático de las apps contenidas en el catálogo de aplicaciones permitidas, durante el proceso de enrolamiento del dispositivo.
- Crear un contenedor de uso app, para exponer una tienda privada de la organización donde se publiquen las aplicaciones apps desarrolladas in-house, aplicaciones de terceros y públicas, estableciendo un catálogo empresarial de las aplicaciones apps permitidas en la organización.
- Un criterio de control fundamental es permitir que únicamente las aplicaciones aprobadas accedan a los datos corporativos. MAM, puede configurar y hacer cumplir que el acceso a los datos lo realicen solo aquellas aplicaciones presentes en el catálogo de la empresa, logrando así que los datos empresariales interactúen libremente entre aplicaciones del catálogo, pero impidiendo la fuga hacia aplicaciones no autorizadas. [15].
- Crear cuentas oficiales en las tiendas de apps Play Store para Android y Apps Store para iOS, y establecer como política de seguridad, que la descarga y actualización de las apps públicas que la compañía determine utilizar, se realicen exclusivamente desde estas tiendas avaladas y certificadas como sitios seguros para adquirir aplicaciones, parametrizando, como criterio de control, que el sistema MDM, sea el encargado de descargar y actualizar las apps que se exponen en el contenedor de aplicaciones definido en la arquitectura.

Garantizando la implementación de estas funcionalidades a través del MAM, y definiéndolas dentro del modelo de seguridad de la información en los dispositivos móviles, una organización puede garantizar con tranquilidad que sus aplicaciones desarrolladas in-house o públicas, estarán expuestas de forma segura para uso exclusivo de los funcionarios y que no habrá forma de que apps de origen desconocido afecten el negocio a través de la plataforma de movilidad.

VII. ALMACENAMIENTO DE DATOS

Los dispositivos móviles son cada vez más económicos y tecnológicamente avanzados, brindando mayor capacidad de almacenamiento, lo que facilita tener gran cantidad de información de negocios como información de clientes, proveedores, cuentas de correo, redes sociales, banca electrónica, fotografías y videos todo contenido en un solo dispositivo, generando así un riesgo para la organización. Hoy en día estos datos se consideran confidenciales lo que convierte a los dispositivos en presa de interés para los ciberdelincuentes. Enfocando el tema en la información de negocio en términos legales, todas las empresas tienen la responsabilidad de proteger la privacidad de clientes, empleados y proveedores de una forma adecuada porque de no hacerlo, puede significarle sanciones legales como multas, la suspensión de actividades y hasta el cierre definitivo de las operaciones de la organización.

Riesgo: Pérdida o robo de información del dispositivo móvil.

Por esta razón este punto referente al manejo del almacenamiento en los dispositivos móviles es una responsabilidad que la organización debe asumir garantizando un modelo de almacenamiento seguro para los dispositivos móviles que distribuya a sus funcionarios.

Existen diversos modelos de protección de la información para almacenar los datos de forma segura y así evitar la extracción maliciosa por parte de aplicaciones cuando los datos estén almacenados localmente en el dispositivo. Para mitigar este riesgo, la organización puede optar por implementar los siguientes controles básicos en su modelo de seguridad de la información:

1) Cifrado del dispositivo: Alguna de las opciones en el mercado permite a los dispositivos almacenar datos en un formato cifrado – utilizando un estándar de cifrado avanzado (*Advanced Encryption Standard*: AES) de 128, 192 o 256 de forma local. Este tipo de cifrado de la información guardada en el dispositivo es la forma más segura para que los datos no sean vistos por ningún ladrón o ciberdelincuente, incluso en caso de que logran extraer copia de los datos del dispositivo almacenados localmente.

A nivel de sistemas operativos, todas las versiones de Android a partir de Gingerbread 2.3.4 y en versiones iOS superiores a 9.5 permiten habilitar el cifrado de disco completo, esto significa que todos sus datos almacenados localmente en el dispositivo, estarán mezclados por un algoritmo AES de 128, 192 o 256, lo que impide que puedan ser puestos en orden y comprendidos sin introducir la contraseña establecida por el funcionario; y a nivel de hardware este modelo en algunos dispositivos ya viene habilitado de fábrica.

Desde la consola de administración de dispositivos MDM se presenta la opción de habilitar el cifrado como política de seguridad, activando y estableciendo el pin o contraseña segura de cifrado, la cual estará administrada directamente por la organización sin que el funcionario intervenga en la elección o definición de este pin, garantizando así el cifrado automáticamente de la información local del dispositivo, estableciendo esta opción como una de las políticas obligatorias en el modelo de seguridad de la organización.

2) Almacenamiento en servidor centralizado: Otra opción en el mercado imprescindible en la era de los

dispositivos móviles para brindar protección a los datos, está orientada al manejo de la información a través del almacenamiento en un servidor centralizado de un tercero como servicio (nube). Existen muchas empresas que ofrecen este servicio con almacenamiento de datos cifrados y transmisión segura de gran capacidad a nivel organizacional como Dropbox, OneDrive, Box, Icloud, entre otros; brindando todas las funcionalidades de sincronización de información en línea, no solo para guardar datos, sino para el trabajo sincronizado en archivos, accediendo a ellos desde los múltiples dispositivos que posea la organización mediante las apps oficiales para acceder al contenido de la cuenta organizacional establecida. [17]. Ver siguiente Fig. 4.

Fig. 4. Modelo Servicio Almacenamiento en Nube. [18]

El inconveniente en este tipo de almacenamiento, es que, si el proveedor del servicio recibe un ataque o un hackeo a sus bases de datos, entonces los datos de la organización entran a estar comprometidos y en peligro. Para mitigar este riesgo bajo esta modalidad de almacenamiento en nube, la organización debe optar por adquirir el servicio de nube privada de tipo convergente, concepto nuevo en el mercado basado en virtualización, donde el hardware de infraestructura incluye recursos de computación, red y almacenamiento, junto con el software de gestión todo en un solo paquete, donde la infraestructura de almacenamiento es propia, administrada y controlada por la organización garantizando así un nivel de seguridad en los datos a través de su propio modelo de seguridad y con la información almacenada directamente en su propio datacenter.

3) Gestión de contenido móvil: Dentro de los sistemas de gestión de movilidad empresarial, se enmarca otro concepto denominado gestión de contenido Móvil o (MCM) acrónimo del inglés ***Mobile Content Management***, enfocado exclusivamente al manejo y control sobre los datos utilizados a través de los dispositivos móviles, proporcionando acceso móvil seguro a los datos empresariales compartidos de una manera controlada y supervisada. [16].

Como criterio de control, se debe realizar la creación de una caja de seguridad cifrada mediante el MCM, donde los usuarios pueden almacenar documentos de negocios, imágenes, archivos adjuntos de correo electrónico, mensajes y más. Para las organizaciones que acojan el modelo BYOD, la caja de seguridad, permite aislar los datos corporativos de los datos personales, garantizando protección ante cualquier amenaza que pudiera estar presente en el dispositivo o evitando fugas de información que a menudo generan los usuarios por errores en la manipulación.

Se recomienda, como otro criterio de control, establecer mediante el MCM, políticas de seguridad que impiden copiar y pegar, imprimir, enviar y compartir archivos no autorizados, permitiendo asegurar constantemente el cumplimiento de las leyes de protección de datos a través de diversas plataformas móviles. [23].

La mayoría de los sistemas de gestión de movilidad empresarial, permiten integrar MCM con los almacenamientos de datos empresariales o los datos almacenados en la nube; integración que brinda un nivel de proyección bastante robusto sobre los datos de la organización.

Implementando cualquiera de estos esquemas o los tres al tiempo, como criterios de control bajo un solo modelo de seguridad, la organización garantiza la mitigación de los riesgos relacionados a la perdida y divulgación de datos por robo o perdida de los dispositivos móviles que entregue a sus funcionarios; ofreciendo todas las ventajas relacionadas a las funcionalidades que brinda el modelo de almacenamiento en nube complementado con el concepto de gestión de contenido (MCM) en los sistemas de gestión de movilidad empresarial.

VIII. TRANSMISIÓN DATOS EN LA RED MÓVIL

Otro de los retos importantes que deben asumir las áreas de tecnología en las organizaciones, es la de brindar protección en la transmisión de datos según el modelo de conexión que utilizan sus dispositivos móviles. En la actualizada, como factos estándar, el principal método de conexión de los dispositivos móviles a las redes corporativas se realiza a través de conexiones de tecnología wifi. Por esta razón es de vital importancia revisar y mejorar la infraestructura wifi de la organización para proporcionar comunicaciones seguras con mecanismos avanzados de control de acceso a la red (NAC, ***Network Access Control***), sistemas de detección/protección de intrusos inalámbricos (WIPS, ***Wireless Intrussion Protection System***) y soluciones de filtrado de contenidos web (*proxies*); todo esto para los casos donde la organización brinda desde su infraestructura servicios de conexión wifi. [27].

Mientras los dispositivos se encuentren enlazados a las redes wifi de la organización el modelo de seguridad se garantiza con el mejoramiento de sus redes, sin embargo la mayoría de los empleados, requieren consumir los servicios internos desde una ubicación externa a su organización; para estos casos se recomienda que la conexión de los dispositivos se realice a través del uso de servicios de la internet por planes corporativos contratados con operadores de cobertura nacional y mediante la implementación de una conexión por VPN entre la organización y el cliente móvil, modelo que garantiza una protección eficaz de la red entre los sistemas de información corporativos y los dispositivos móviles.

Entendiendo un poco lo que es VPN sigla que proviene del acrónimo en inglés ***Virtual Private Network***, que traducida al español significa red privada virtual, donde el concepto real es básicamente una red segura de navegación privada que permite que los equipos y dispositivos se

conecten por medio de una extensión del internet, sin estar vinculados ciertamente a la red, lo que permite una transmisión segura de los datos. [28]. como se muestra en la siguiente Fig. 5.

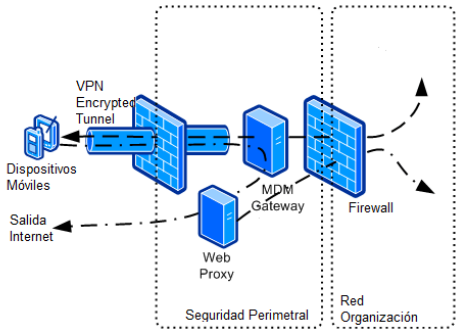

Fig. 5. Esquema de la conexión dispositivo / organización. [27]

Como primera medida a nivel de comunicaciones, la organización debe establecer como criterio de control dentro de la política de seguridad en los dispositivos móviles, la utilización de este tipo de conexión por medio de una red privada virtual VPN, para acceder a los servicios internos de la organización. Como segunda medida es necesario definir el tipo de redes de comunicaciones a las que podrán tener acceso los dispositivos móviles, cuya primera recomendación es través del uso de servicios de la internet por planes corporativos contratados con operadores de cobertura nacional mediante tecnología de tipo redes móviles LTE 3/4G.

Mientras los dispositivos se mantengan fuera de la cobertura de las rede wifi de la organización, el funcionario podrá optar por utilizar la red de internet mediante conexiones a redes wifi de la casa o redes wifi de terceros en entornos públicos, por tal motivo, como tercera medida, es de vital importancia socializar y ofrecer a los funcionarios la documentación necesaria con las políticas de seguridad que establecen las responsabilidades y la rendición de cuentas de un funcionario cuando se trata de fugas de información confidencial, para concientizarlos sobre la importancia del uso exclusivo de los canales establecidos por la organización y el no uso de estas redes públicas que pueden poner en riesgo la seguridad de la organización.

Dentro de los sistemas de gestión de movilidad empresarial, los MDM permiten establecer un acceso al sistema mediante la exposición de un servicios público con certificados digitales y la autenticación mediante la integración con la plataforma de control de accesos establecida en la organización como el directorio activo por ejemplo, adicionalmente, la comunicación que establece en dispositivo móvil con la plataforma de administración del MDM se realiza a través de una conexión VPN con protocolo SSL y para cada servicio interno que este expuesto a través de los dispositivos móviles, se recomienda habilitar como criterio de control, una paramétrica de conexión denominada micro VPN de tipo tunneling, que se refiere a la creación de un túnel de navegación dentro de otra conexión VPN, también se le denomina como protocolo de red encapsulador, esto permite crear nuevas conexiones a la red privadas dentro de las existentes como por ejemplo para redireccionar IP sin modificar su contenido, además puedes enviar informaciones de manera simultánea a diferentes equipos [28], todo esto con el objetivo de enrutar a los diferentes servicios a través de los diferentes servidores de cada uno de las plataformas internas de la organización.

IX. CONCLUSIONES

Aunque los sistemas de gestión de movilidad empresarial brindan muchas funcionalidades sobre la administración y seguridad en el uso de dispositivos móviles, estas soluciones por sí solas no son suficientes, si no existe un modelo de seguridad definido; por esta razón antes de implantar una de ellas (MDM, MAM o MCM) es requisito indispensable disponer o definir una estrategia con políticas de seguridad corporativa centrada en la utilización de los dispositivos móviles de la organización. Para definir esta estrategia de seguridad, se requiere realizar un análisis de riesgos como el detallado en este artículo evaluando como primera medida los escenarios y las amenazas principales de seguridad que afectan a estos elementos en el entorno de operación de la organización; posteriormente desarrollar un análisis de riesgos sobre estas amenazas y como resultado de este análisis, la organización deberá establecer procedimientos de seguridad con definición e implementación de controles acordes a los objetivos institucionales.

No hay duda de que el modelo BYOD se está afianzando y a futuro terminará siendo una opción atractiva para las organizaciones, pero para disfrutar de las ventajas de esta tendencia, hay que tener en cuenta diversos criterios para garantizar la seguridad en este modelo. Por esta razón, para dar el primer paso en el mundo de la movilidad con BYOD, las organizaciones deberán inicialmente trabajar con dispositivos propios e ir madurando y mejorando el manejo y administración de estos, con un entorno protegido sin perder de vista las políticas de seguridad y posteriormente a futuro contemplar la incorporación BYOD.

Por último, es muy importante asegurar la transmisión de datos a través del cifrado de la información a nivel de comunicación, establecer contraseñas robustas para el acceso a los dispositivos, definir e implementar métodos de cifrados seguros para la protección de la información corporativa y en fin los demás criterios ya identificados y modelados en muchos manuales y guías de seguridad, sin embargo la mayoría de fuga de datos confidenciales se deba a las acciones ejecutadas por los mismos funcionarios, bien sea por causas accidentales o intencionales, por esta razón la conclusión más relevante de este análisis realizado, es la recomendación de brindar a los funcionarios, la información y documentación necesaria para la toma de conciencia sobre la seguridad de datos entre los empleados, las responsabilidades y la rendición de cuentas cuando se trata de la revelación de información confidencial, contribuyendo a la adopción de las políticas y estrategias de seguridad establecidas para el acceso a los datos y recursos de la compañía. Esta recomendación es una acción que aumenta considerablemente el nivel de seguridad de los datos corporativos.

REFERENCIAS

[1] Cartilla de seguridad para internet. https://cartilla.cert.br/

[2] PUBLICATIC - Factores de riesgo en las aplicaciones móviles y algunos controles básicos con los que abordarlos. https://blogs.deusto.es/master-informatica/factores-de-riesgo-en-las-aplicaciones-moviles-y-algunos-controles-basicos-con-los-que-abordarlos/

[3] Protejete - Gestión de Riesgo en la Seguridad Informática. https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

[4] Especialistas en telefonía móvil. https://www.telefonostodoterreno.es

[5] Facet Box Cajas Rugerizadas. http://cajasrugerizadas.com/que-es-rugerizado

[6] Tablet y Smartphone rugerizado https://elchapuzasinformatico.com/2017/02/archos-101-saphir-50-saphir-tablet-smartphone-rugerizado/

[7] NORMA TÉCNICA COLOMBIANA IEC 60529- Grado de Protección IP. https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-IEC60529.pdf

[8] ORBIT - GESTIÓN DE DISPOSITIVOS MÓVILES ¿QUÉ ES UNA SOLUCIÓN MDM?. https://www.orbit.es/gestion-de-dispositivos-moviles-que-es-una-solucion-mdm/

[9] POWERDATA - Qué es MDM y razones por las que lo necesitas. http://blog.powerdata.es/el-valor-de-la-gestion-de-datos/que-es-mdm-y-razones-por-las-que-lo-necesitas

[10] Intertek - Ensayos de Protección IP (Ingress Protection) en Productos de Iluminación: Norma IEC 60529. http://www.intertek.es/iluminacion/ip-ingress-protection-iec-60529/

[11] TUYU TECHNOLOGI - Arquitectura del software de administración de dispositivos móviles. https://gestiondispositivosmoviles.com/arquitectura/

[12] Computer Hoy - ¿Qué es BYOD?, ventajas e inconvenientes. http://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250

[13] Aranda software Mobile Device Management. http://arandasoft.com/aranda-mobile-device-management/

[14] XATAKANDROID – Cómo localizar, bloquear y borrar nuestro dispositivo Android perdido o robado. https://www.xatakandroid.com/tutoriales/como-localizar-bloquear-y-borrar-nuestro-dispositivo-android-en-caso-de-perdida-o-robo

[15] ManageEgine – Gestión de aplicaciones móviles (MAM). https://www.manageengine.com/es/mobile-device-management/gestion-aplicaciones-moviles.html

[16] Telecomunicaciones para Gerentes – ¿Por qué MDM ya no es suficiente para la gestión y seguridad móvil?. http://www.telecomunicacionesparagerentes.com/por-que-mdm-ya-no-es-suficiente-para-la-gestion-y-seguridad-movil/

[17] Almacenamiento Seguro en tu Dispositivo Móvil. https://latam.kaspersky.com/blog/almacenamiento-seguro-en-tu-dispositivo-movil/1472/

[18] muycomputer – almacenamiento en nube. http://www.muycomputer.com/2015/02/03/almacenamiento-en-nube-precios/

[19] Empresas.entel.cl - Administración de dispositivos Móviles MDM. http://empresas.entel.cl/PortalEmpresas/appmanager/entel/entel?_nfpb=true&_pageLabel=P79200186281404313613089

[20] Citrix - MDM: Los diez líderes según Gartner. https://cioperu.pe/fotoreportaje/13653/mdm-los-diez-lideres-segun-gartner/?foto=4

[21] FERMU – ADMINISTRACIÓN DE CERTIFICADOS Y CLAVES DE MANTENIMIENTO. http://www.fermu.com/40-windows/los-servicios-de-windows/651-administracion-de-certificados-y-claves-de-mantenimiento

[22] FERMU – ADMINISTRACIÓN DE CERTIFICADOS Y CLAVES DE MANTENIMIENTO. http://www.fermu.com/40-windows/los-servicios-de-windows/651-administracion-de-certificados-y-claves-de-mantenimiento

[23] Search data center – Cinco formas de impulsar la seguridad de aplicaciones móviles. http://searchdatacenter.techtarget.com/es/cronica/Cinco-formas-de-impulsar-la-seguridad-de-aplicaciones-moviles

[24] revista.seguridad – DISPOSITIVOS MÓVILES: UN RIESGO DE SEGURIDAD EN LAS REDES CORPORATIVAS. https://revista.seguridad.unam.mx/numero-21/dispositivos-moviles-un-riesgo-de-seguridad-en-las-redes-corporativas#_ftn5

[25] PublicaTIC – Gestión de aplicaciones móviles. https://blogs.deusto.es/master-informatica/gestion-de-aplicaciones-moviles/

[26] BIXPE - MDM ¿QUÉ ES LA GESTIÓN DE DISPOSITIVOS MÓVILES?. https://www.bixpe.com/blog/mdm-que-es-la-gestion-de-dispositivos-moviles/

[27] pdatungsteno - Configurar una conexión VPN en un teléfono o PDA Windows Mobile. http://www.pdatungsteno.com/2009/09/07/configurar-una-conexion-vpn-en-un-telefono-o-pda-windows-mobile/

[28] taringa.net - ¿ Qué es una VPN y para que sirve ?. https://www.taringa.net/posts/info/19467894/Que-es-una-VPN-y-para-que-sirve.html

Rene Alejandro Cardona P. Autor ()

Ingeniero Electrónico Graduado en la Universidad Manuela Beltrán en el año 2005. Cursó un posgrado en seguridad de la información en la Universidad Piloto de Colombia. Ejerce laboralmente como profesional Senior en el proyecto de seguimiento en inversiones agropecuarias de la entidad financiera Banco Agrario de Colombia.