UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del artículo
Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Rendon Terreros Moises
Tutor/a:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Msc. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: **Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM**.

Elaborado por: Moises Rendon Terreros, de C.I: 0105947824, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI

Firma

APROBACIÓN DEL TUTOR

Yo, Ph.D. Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: **Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM**.

Elaborado por: Moises Rendon Terreros, de C.I: 0105947824, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

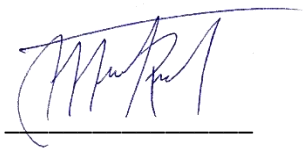
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Moises Rendon Terreros con C.I: 0105947824, autor del proyecto de titulación denominado: **Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024



Firma

https://orcid.org/0009-0001-1354-0730

Tabla de contenidos

Índice de figuras

Índice de tablas

INFORMACIÓN GENERAL

Contextualización del tema

El crecimiento de las cooperativas en el sector financiero ha ido en aumento y juega un papel importante en el sistema económico popular brindando a las comunidades diversos servicios virtuales a través de dispositivos móviles como smartphones, tablets, POS, entre otros, que pertenecen a estas cooperativas, es por este crecimiento que se ha visibilizado un aumento de amenazas. Es por ello necesario asegurar los datos sensibles, como información personal, tipos de transacción, información de la cuenta, que manejan estos dispositivos y que estén protegidos de manera efectiva.

Las herramientas de Gestión de los dispositivos Móviles (MDM) o Mobile Device Management, permite a las cooperativas financieras centralizar la administración y la supervisión de todos los dispositivos móviles utilizados en la organización, lo que facilita aplicar y hacer cumplir políticas que las cooperativas requieren para la seguridad consistentes específicas, como el cifrado de datos, autenticación de múltiples factores y restricciones de acceso, garantizando así la protección de la información confidencial, además de gestionar de manera eficiente las aplicaciones empresariales y asegurarse de que todas las actualizaciones críticas sean implementadas en todos los dispositivos de manera oportuna y tomar medidas pro activas en caso que un dispositivo se extravié o sea robado, como el borrado remoto de datos para proteger la información confidencial.

Problema de investigación

Los socios y empleados de las cooperativas de ahorro y crédito, juegan un papel importante en el empleo de productos que ofrece las instituciones financieras. Hoy en día, la interacción de estos con la cooperativa se realiza principalmente a través de dispositivos móviles de la institución, los cuales facilitan el acceso a una variedad de servicios financieros proporcionados por la cooperativa.

Sin embargo, es importante destacar que no todas estas personas cuentan con la preparación técnica en seguridad informática necesaria por lo que puede llevar a un uso potencialmente inseguro de los dispositivos que pertenecen a la cooperativa, lo cual genera un riesgo para la seguridad de los datos y las operaciones de la cooperativa financiera. Dada la accesibilidad y facilidad de uso de estos dispositivos, se ha vuelto imperativo garantizar la protección de los mismos.

Por lo tanto, es esencial contar con una gestión eficaz de estos dispositivos móviles a través de MDM y así abordar los desafíos de seguridad y eficiencia que enfrenta la cooperativa financiera en la era digital. La gestión de los dispositivos móviles no solo protege los datos sensibles, sino que también mejora la productividad y la eficiencia operativa al facilitar un entorno de trabajo móvil seguro y controlado. ¿De qué manera la gestión de Dispositivos Móviles (MDM) puede maximizar la seguridad

y eficiencia en la cooperativa financiera, reduciendo los riesgos y facilitando una gestión más controlada y centralizada?

Objetivo general

Maximizar la seguridad y eficiencia de los dispositivos móviles empleadas dentro del entorno financiero cooperativista a través de la Gestión de dispositivos móviles (MDM).

Objetivos específicos

- Explorar las características y funciones clave de la gestión de dispositivos móviles (MDM) que contribuyen a la eficiencia operativa y la seguridad de los datos de la cooperativa financiera.
- Investigar cómo las soluciones de MDM simplifican las tareas administrativas, relacionadas con la configuración, distribución de aplicaciones y actualizaciones de software en dispositivos móviles empleadas en las cooperativas financieras.
- Analizar cómo las soluciones MDM optimizan el rendimiento de los dispositivos móviles, mejorando así la productividad de los empleados y socios de la cooperativa, reduciendo los costos asociados con el mantenimiento y soporte de dispositivos.
- Validar el impacto de la implementación de MDM en la seguridad de los dispositivos móviles utilizados en la cooperativa.

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos con la realización de este artículo, son los empleados y socios de la Cooperativa, por razones de seguridad y confidencialidad, se ha decidido reservar el nombre de la cooperativa pero los datos, investigaciones y análisis son reales tomados de esta institución, quienes se beneficiarán de una mayor seguridad en el manejo de información y una mejor eficiencia operativa, indirectamente, la comunidad en general se verá favorecida por una cooperativa más sólida y segura, capaz de ofrecer mejores servicios financieros en cualquier parte de la región. No solo fortalece a la cooperativa, sino que también establece un modelo replicable para otras instituciones financieras, ampliando así el impacto positivo en la sociedad.

A través de los Objetivos de Desarrollo Sostenible (ODS) de la ONU se pretende que este artículo se vincule con el objetivo 9, que se enfoca en la industria, la innovación y la infraestructura, que permitirá a la cooperativa se beneficie de una infraestructura tecnológica más robusta y resiliente, apoyando el desarrollo económico y el bienestar de la comunidad.

Por lo antes mencionado se busca un impacto significativo en la sociedad y en la colectividad mediante la capacitación y asesoría en el uso y gestión de MDM, fortaleciendo así las capacidades

tecnológicas en el sector financiero cooperativista. El articulo también contribuirá con investigación y bibliografía que servirán como referencia para otras cooperativas y organizaciones interesadas en mejorar su seguridad y eficiencia operativa, facilitando la implementación de MDM en entornos similares.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

1.1.1. Gestión de Dispositivos Móviles - MDM (Mobile Device Management):

Según Ruesgas(2014) la gestión de Dispositivos Móviles son políticas y tecnologías que trabajan en conjuntos que están diseñadas para gestionar, controlar y proteger dispositivos móviles utilizados por empleados o clientes en entornos empresariales.

Permiten administrar de manera integral, supervisando el estado y controlando las funciones de forma remota a través de una comunicación inalámbrica (Rhee et al.,2012).

1.1.2. Amenazas en la seguridad móvil.

Rhee et al. (2012) establece que una amenaza es un ataque llevado a cabo por un agente malintencionado contra cualquier activo de una empresa, es por ello que es importante el poder identificar correctamente estos ataques.

Muchas veces las amenazas de seguridad móvil se suelen agrupar como un único riesgo en general, pero en realidad se dividen en cuatro tipos específicos principales de amenazas que las organizaciones deben abordar y protegerse a continuación se detallan estas amenazas (Guaña, 2024).

1.1.2.1. Fuentes desconocidas de aplicaciones móviles.

Esta amenaza se da cuando las personas descargan en sus dispositivos aplicaciones que creen que son de fuentes legítimas, pero en realidad son aplicaciones que extraen datos sensibles del dispositivo, roban información con el uso de spyware y malware, siendo esta información personal o comercial sin que el usuario se dé cuenta ni las personas que usan el dispositivo (Gontovnikas, 2021).

1.1.2.2. Amenazas a la seguridad de la red móvil.

Según Prensariotila(2024) indica que existen amenazas basadas en la red siendo estas frecuentes y peligrosas, ya que atacantes pueden aprovechar cuando las personas usan redes Wifi públicas y capturar datos no cifrados. Muchos de estos atacantes evitan de manera sofisticada las herramientas de seguridad convencionales a través de ciberataques dirigidos, con el objetivo de espiar a los usuarios y obtener información confidencial, enfocándose especialmente en los teléfonos móviles (Guaña, 2024).

1.1.2.3. Seguridad Física de los dispositivos móviles.

En el trabajo de Gontovnikas(2024) señala que las amenazas a nivel de la seguridad física están relacionadas con el robo o perdida del dispositivo, en estas situaciones, los criminales obtienen acceso directo al hardware donde se encuentra datos privados, esto representando un riesgo significativo para las cooperativas. Según la empresa ESET, el 58% de los usuarios de dispositivos móviles en Latinoamérica ha sido víctima de robo, esto indica que a medida que aumenta el uso de estos equipos móviles, también se incrementa el robo de estos dispositivos (Bécares, 2014).

1.1.2.4. Malos hábitos de contraseñas.

Es bien conocido que la mayoría de los usuarios no establecen contraseñas robustas para el acceso a sus dispositivos, se emplean muchas veces combinaciones débiles o reutilizan contraseñas para varias cuentas (Bécares, 2014). Adicional muchas políticas de seguridad deficientes que no exigen cambios periódicos ni contraseñas robustas, sumando a un entorno en el que se manejan una gran cantidad de móviles se vuelve complejo administrar estas contraseñas, aumentando el riesgo de vulnerabilidades (Gontovnikas, 2021).

1.1.3. BYOD (Bring Your Own Device):

Política que permite a los socios, empleados de una cooperativa financiera utilizar sus propios dispositivos personales para trabajar, como el uso de los dispositivos móviles (Pierer, 2016)

1.1.4. ISO/IEC 27001:2022

Define criterios y requisitos para los sistemas de gestión de seguridad de la información, que puede incluir la gestión de dispositivos móviles como parte de las medidas de seguridad de una organización, incluye recomendaciones para el uso de dispositivos móviles y su gestión, como políticas de seguridad, gestión de activos, control de accesos y mantenimiento de software (ISO27001, 2024)

1.1.5. NIST SP 800-30

El “Instituto Nacional de Estándares y Tecnología” (NIST). Proporciona documentación detallada sobre la orientación, selección, implementación y gestión de tecnologías MDM, para mejorar la gestión, seguridad de dispositivos móviles en entornos empresariales, establece directrices para la gestión de dispositivos móviles de seguridad (NIST, 2023).

1.1.6. OWASP Mobile Security Project:

El Proyecto de Seguridad Móvil de OWASP (Open Web Application Security Project) ofrece pautas y buenas prácticas para asegurar aplicaciones móviles y dispositivos. Esto puede ser útil para

comprender las vulnerabilidades comunes en dispositivos móviles y cómo mitigar riesgos de seguridad (Owasp, 2023).

1.1.7. GSMA

La Asociación Global System for Mobile Communications(GSMA) publica documentos y guías de seguridad para dispositivos móviles que abordan aspectos como la autenticación, protección de datos y seguridad de la red móvil. Estos documentos son especialmente relevantes para operadores móviles y fabricantes de dispositivos (GSMA, 2023).

1.2. Proceso investigativo metodológico

El presente trabajo se basa en una ruta de enfoque cualitativo para proporcionar una visión integral del impacto de la Gestión de Dispositivos Móviles (MDM) en la seguridad y eficiencia operativa de la Cooperativa.

Dentro del enfoque cualitativo, se pretende recopilar información de diversas fuentes bibliográficas, tesis, reseñas, artículos científicos o revistas tecnológicas, para luego sintetizarlos eficientemente y poder presentarlo de una manera clara y organizada. De esa manera ofrecer una solución a la problemática planteada que se centra en la necesidad de maximizar la seguridad y la eficiencia de los dispositivos móviles utilizados en la cooperativa financiera, mediante el uso efectivo de la gestión de dispositivos móviles (MDM).

Se realizará una revisión exhaustiva de la información existente relacionada con la gestión de dispositivos móviles en entornos financieros, la seguridad de la información, las mejores prácticas en ciberseguridad, y cualquier otra área relevante para el tema de estudio.

Esta revisión proporcionará el marco teórico y contextual necesario para fundamentar la investigación, así como dejar una documentación que permita comprender la eficacia de las soluciones de MDM y proponer recomendaciones para mejorar la seguridad y eficiencia de los dispositivos móviles en cooperativas financieras a través de la gestión de MDM.

La investigación tendrá como objeto de estudio la cooperativa que, por razones de seguridad y confidencialidad se ha reservado el nombre de la cooperativa, y de los dispositivos móviles que se emplean para realizar sus operaciones diarias que incluyen teléfonos inteligentes, POS, tabletas y otros dispositivos portátiles utilizados tanto para empleados y socios de la cooperativa financiera para realizar transacciones diarias.

Pretendiendo documentar todo el proceso investigativo en un artículo de investigación y que esta pueda servir como material para comunicar los hallazgos y permita maximizar la seguridad y eficiencia de los dispositivos móviles en cooperativas financieras a través de la gestión de MDM.

Como se detalla en el Anexo 1, se realizará una entrevista según Jiménez (2012) indica que la entrevista cualitativa se distingue por ser más personal, adaptable y manejable, actuando como un intercambio de información entre dos personas, esta entrevista se hará al responsable de servicios tecnológicos de la Cooperativa de Ahorro y Crédito, estará diseñada con preguntas, previamente establecidas, para medir la percepción y satisfacción respecto a la implementación de MDM, así como su impacto en la seguridad y eficiencia operativa, las preguntas se enfocarán en la gestión de dispositivos móviles, el uso de MDM, seguridad de sus dispositivos móviles, despliegue de sus aplicaciones y los desafíos específicos que enfrenta a nivel de seguridad de dichos dispositivos.

La combinación de estos enfoques cualitativos permitirá una evaluación exhaustiva de la problemática planteada. Los resultados obtenidos de la revisión bibliográfica proporcionarán el marco teórico y contextual necesario, mientras que los datos de la entrevista ofrecerán evidencia sobre la efectividad y aceptación de las soluciones MDM en la cooperativa.

Este proceso investigativo metodológico permitirá tener una comprensión holística y detallada del impacto de la Gestión de Dispositivos Móviles en la Cooperativa de Ahorro y Crédito, proporcionando tanto la fundamentación teórica como la evidencia empírica necesarias para ofrecer soluciones efectivas y bien fundamentadas.

1.3. Análisis de resultados

Luego de la entrevista realizada al responsable del área de servicios tecnológicos de la Cooperativa, se ha identificado aspectos importantes sobre cómo se gestiona y protegen los dispositivos móviles que emplean en la cooperativa. A continuación, se realiza un análisis con los datos obtenidos de cada sección que agrupa las preguntas con más importantes:

1.3.1. Sección 1 “Conocimiento y Uso de MDM”

Se pudo constatar que el responsable del área de servicios tecnológicos de la cooperativa conoce el concepto de MDM, aunque la cooperativa no usa ninguna solución de gestión de dispositivos móviles, debido a temas de costo y compatibilidad con la variedad de dispositivos que usan para sus servicios.

Este dato es importante porque demuestra que lo que podría estar limitando a maximizar la eficiencia y seguridad de los dispositivos móviles es la brecha que existe entre el conocimiento de las herramientas disponibles y del costo beneficio de esta implementación.

1.3.2. Sección 2 “Gestión y Administración de Dispositivos Móviles”

La cooperativa, actualmente administra alrededor de 1500 dispositivos móviles, distribuidos entre 3 modelos: “PZ90”, “New9220” y “Sunmi T2”, se encontró que requieren manejo manual para configuraciones y actualizaciones.

Esta alta cantidad de dispositivos que se gestionan de manera manual indica una posible ineficiencia y vulnerabilidad a errores humanos, lo que indica que una solución centralizada para gestionar los dispositivos móviles sería lo más adecuado para optimizar los procesos que se requieren.

1.3.3. Sección 3: “Despliegue y Actualización de Aplicaciones”

Según la entrevista aproximadamente cada seis meses se realiza despliegues masivas de aplicaciones contando también que entre este lapso pueden existir otros despliegues por cambios de la normativa o para corregir algún incidente notificado, con esto teniendo que hacerlo de manera manual muchas veces accediendo al equipo para descargar el instalador generando muchas veces asistencia técnica en sitio, no teniendo un repositorio de aplicaciones automatizada que permita liberar versiones de manera controlada o sectorizada de manera automática.

La implementación de un gestor de administración de dispositivos MDM podría minimizar estos procesos, permitiendo simplificar los despliegues haciéndolos más eficientes y así minimizando los fallos, de esta manera maximizando así la operatividad y seguridad.

1.3.4. Sección 4: “Seguridad y Auditorías”

Actualmente la cooperativa para sus dispositivos móviles cuenta con medidas de seguridad básicas como el bloqueo por patrón y limitando el uso de aplicaciones para evitar la instalación o acceso de aplicaciones no autorizadas, aunque mencionan dificultades en la homogeneidad de las configuraciones para los diferentes modelos de dispositivos que cuentan.

Como se indicó estas medidas son muy básicas que para la cantidad y modelos que emplean, siendo estas insuficientes para la cooperativa que maneja información sensible. La implementación de un gestor de administración de dispositivos MDM mejoraría notablemente la seguridad, podría generar políticas más robustas y un control centralizado de configuraciones para cada modelo de dispositivo que emplean para sus servicios.

1.3.5. Sección 5: “Percepción General y Futuro”

En la entrevista quedo claro que la cooperativa reconoce que una solución MDM puede mejorar la gestión de sus dispositivos móviles, aunque por el momento no es una prioridad y no le ven viable por el costo operativo y técnico.

La cooperativa podría cambiar de parecer respecto a esta percepción si se destacan los beneficios tangibles de MDM, adicional de la reducción de costos operativos que se generarían a futuro y el incremento de la seguridad, lo que es importante para una expansión futura de la cooperativa.

1.3.6. Conclusión de los resultados

La entrevista permitió tener una mejor visión sobre la gestión que tienen la Cooperativa, actualmente de sus dispositivos móviles y aunque están consciente de las ventajas de una gestión de dispositivos móviles MDM, aún no ha dado el paso hacia su implementación debido a preocupaciones de costos y compatibilidad. Sin embargo, la creciente escala en cantidad y modelos la administración de estos dispositivos y los problemas recurrentes en la actualización y seguridad indican que la adopción de MDM es necesaria de esta manera maximizando así la operatividad y seguridad de sus dispositivos permitiendo administrar sus múltiples dispositivos y podrían gestionarlos de manera íntegra, permitiendo actualizaciones en segundo plano de forma autónoma, un mejor control de inventario, así como tener mayor control en las configuraciones y políticas para sus dispositivos de manera automática.

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1. Resumen

Dentro de las cooperativas financieras el uso de dispositivos móviles ha ido en aumento, esto provoca nuevos desafíos en cuanto a la seguridad y eficiencia en la gestión de estos dispositivos. La falta de control centralizado sumando las amenazas de seguridad a las que están expuestos estos dispositivos, se ha convertido en un problema constante, lo que compromete la integridad de la información, así como la operatividad de los servicios que ofrecen las cooperativas.

La propuesta del artículo se centra en maximizar la seguridad y eficiencia de los dispositivos móviles empleadas en la Cooperativa través de la "Gestión de dispositivos móviles" (MDM), A través del enfoque cualitativo, se recopilo datos mediante entrevistas dirigidas al personal de servicios tecnológicos de la cooperativa.

Los resultados sugieren que mediante una Gestión de dispositivos móviles MDM no solo facilitara el control remoto y la seguridad de los dispositivos, sino que también optimiza la administración de aplicaciones como su despliegue e implementación, además de tener un mejor control del inventario.

Conclusiones preliminares indican que la implementación efectiva de una gestión de dispositivos MDM, puede mitigar riesgos y mejorar la eficiencia operativa, siendo una herramienta clave para enfrentar los desafíos tecnológicos actuales en el entorno cooperativo.

a. Palabras clave:

Gestión de dispositivos móviles, MDM, Seguridad, Amenazas, Dispositivos Móviles, Cooperativas.

2.2. Abstract

Within financial cooperatives, the use of mobile devices has been on the rise, leading to new challenges in terms of security and efficiency in managing these devices. The lack of centralized control, combined with the security threats that these devices are exposed to, has become a persistent issue, compromising both the integrity of information and the operational services provided by cooperatives.

This article's proposal focuses on maximizing the security and efficiency of mobile devices used in the Cooperative through "Mobile Device Management" (MDM). Using a qualitative approach, data was collected through interviews with the cooperative's technology services staff.

The results suggest that implementing MDM not only facilitates remote control and security of devices but also optimizes the management of applications, including their deployment and implementation, as well as providing better inventory control.

Preliminary conclusions indicate that the effective implementation of MDM can mitigate risks and improve operational efficiency, making it a key tool for addressing current technological challenges in the cooperative environment.

a. Keywords

Mobile Device Management, MDM, Security, Threats, Mobile Devices, Cooperatives.

2.3. Introducción

En los últimos años el uso de dispositivos móviles se ha convertido en algo importante, ya que su uso ha incrementado de manera exponencial sobre todo en el área bancaria como lo indica Parra et al.(2019), por las diferentes funciones que estos dispositivos ofrecen, así en el entorno cooperativista esta tendencia ha sido aprovechada para ofrecer diferentes servicios ofreciendo mayor comodidad y eficiencia en la transaccionalidad entre los socios y las cooperativas, este aumento en el uso de dispositivos móviles también ha hecho que aumenten los riesgos y amenazas a la seguridad de los datos que se manejan en los dispositivos móviles de estas cooperativas, por lo que una implementación de una gestión de dispositivos móviles MDM, es necesaria para proteger estos dispositivos de esta manera maximizando la eficiencia y seguridad de estos equipos para asegurar la integridad, disponibilidad y confidencialidad de la información de los socios de las cooperativas.

La gestión de dispositivos móviles conocido por sus siglas en ingles MDM, se encarga de proteger, monitorear, administrar y brindar soporte a los dispositivos móviles utilizados dentro de una empresa (Pierer, 2016).

Las soluciones MDM permite administrar una gran variedad de dispositivos móviles, como teléfonos, smartphones, tabletas, dispositivos POS, etc. Siendo su objetivo principal maximizar la eficiencia y seguridad de los dispositivos, al mismo tiempo reducir costos y minimizar los procesos o tareas manuales de administración, aplicando configuraciones o políticas que aplican tanto a los dispositivos propiedad de la empresa como a aquellos pertenecientes a los empleados (Pierer, 2016).

La arquitectura en la que se basa la gestión de Dispositivos Móviles MDM, se basa en dos componentes principalmente, en un servidor MDM y en un Agente MDM (IBM, 2023). Esta arquitectura se puede apreciar en la Figura 1.

Figura 1.
Arquitectura de la Gestión de Dispositivos Móviles

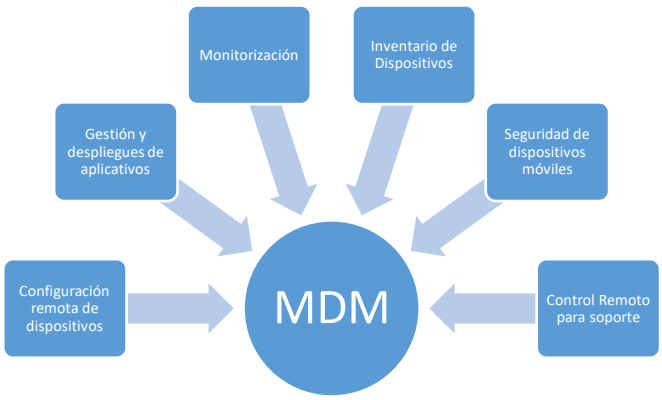
Nota. Figura explica como los diferentes dispositivos móviles se pueden comunicar con el Servidor MDM.

Funciones Principales de la Gestión de Dispositivos Móviles (MDM):

Según describe en su artículo García(2024), entre las funcionalidades principales cuenta con la configuración remota de dispositivos, gestión de aplicaciones, despliegues de aplicaciones, monitorización, inventario de dispositivos y seguridad de dispositivos móviles.

Estas funciones permiten que se puedan atender diferentes incidentes, además que se atiendan las necesidades de los usuarios en diferentes dispositivos y ubicaciones. A continuación, en la figura 2 se destacan algunas de las capacidades que ofrece una gestión de dispositivos móviles MDM (Couto, 2023).

Figura 2.
Funciones Principales de la Gestión de Dispositivos Móviles



Nota. Las funciones principales que ofrece una gestión de dispositivos móviles (Couto, 2023).

Componentes de funcionamiento para la gestión de dispositivos móviles.

En la Tabla 1, se detalla el funcionamiento para una correcta gestión de dispositivos móviles se basa en 5 componentes que se relacionan entre sí para un correcto funcionamiento (Rhee et al.,2012).

Tabla 1.
Componentes para el Sistema de gestión de dispositivos móviles

Componentes	Descripción
Inscripción/Configuración	Se proceden a registrar en el sistema MDM los datos del dispositivo móvil y los datos del usuario de la organización, luego se realiza la configuración de políticas para aplicarlos a los dispositivos móviles.
Distribución	Se distribuye el agente MDM a través de tiendas de aplicaciones o internamente en los dispositivos móviles, para luego proceder con la instalación del mismo.
Autenticación	Al ejecutarse el agente MDM instalado en el dispositivo móvil procede a validar que sea el dispositivo que este inscrito en la consola lo valida a través de los datos como: IMEI, Dirección MAC, Dirección IP, se envían al servidor MDM esta validación verifica que coinciden los datos registrados en la fase de inscripción.
Instrucción	La herramienta MDM envía las políticas y configuraciones realizadas en el portal MDM, según el dispositivo móvil inscrito, dependiendo el modelo o grupo de configuración (se repite periódicamente, según sea necesario).
Control/Informe	El agente MDM gestiona las funciones del dispositivo móvil de acuerdo con las políticas o comandos recibidos y está constantemente reportando el estado de los dispositivos móviles

	controlados (se repite periódicamente y según sea necesario).

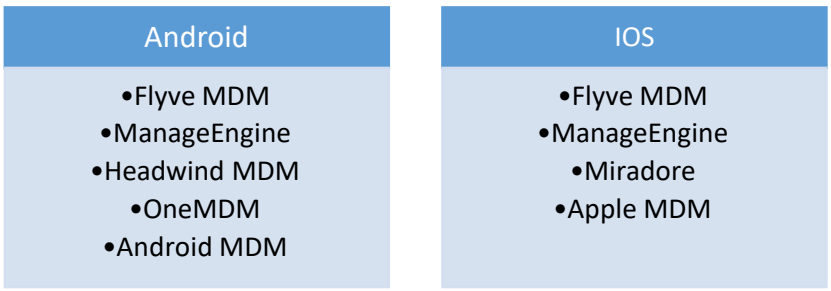
Nota. La tabla muestra los componentes principales para el funcionamiento correcto de la gestión de dispositivos móviles (Rhee et al.,2012).

Soluciones MDM

Dentro de las soluciones MDM, se pueden encontrar diferentes herramientas que permiten una administración y gestión de los dispositivos móviles sin importar el sistema operativo que posean ya sean estos: Android, IOS, etc (Venosa et al.,2016).

Como indica Pierer (2016) la mayoría de herramientas MDM trabajan con la misma arquitectura Servidor-Agente, además que funciona de la misma manera empleando una inscripción del dispositivo para poderlo gestionar desde un portal, muchas de estas soluciones pueden trabajar con diferentes Sistemas operativos como se detalla en la Figura 3, solo cambia el agente de instalación.

Figura 3.
Soluciones MDM, en diferentes Sistemas Operativos.



Nota. La figura muestra algunas soluciones MDM que se pueden encontrar.

Cumplimiento Normativo en la Gestión de Dispositivos Móviles: ISO, NIST y OWASP

Como indica (Preciado, 2021) el cumplimiento de las normativas en empresas es muy importante ya que estas pueden ayudar a minimizar el riesgo a las que se enfrentan, la gestión de dispositivos móviles (MDM) está vinculada con estándares de seguridad como la ISO 27001, NIST 800-30 y OWASP.

La ISO 27001:2022 se enfoca en establecer políticas que protegen la confidencialidad, integridad y disponibilidad de los datos que se manejan en los dispositivos móviles (Bazán, 2024), cumpliendo los anexos que presenta la ISO 27001:2022 se puede maximizar la seguridad de los equipos, la gestión de dispositivos móviles posee funcionalidades que ayuda a cumplir con estos anexos.

Tabla 2.
Anexos Normativa ISO 27001 relacionado con la seguridad de dispositivos móviles.

Norma ISO Anexo	Descripción
6.2.1 Política de dispositivos móviles	Adopción de una política y medidas para soportar la seguridad con el fin de manejar los riesgos introducidos por el uso de dispositivos móviles.
8.1.1 Inventario de activos	Identificar los activos asociados con la información y las instalaciones de procesamiento de la información y se creará y mantendrá un inventario de estos activos.
8.1.2 Propiedad de los activos	Reconocer la propiedad de los activos mantenidos en el inventario.
8.1.3 Uso aceptable de los activos	Se identificarán, documentarán e implementarán las reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de información.
12.5.1 Instalación de software en los sistemas operativos	Procedimientos para controlar la instalación de software en los sistemas operativos.
12.6.2 Restricciones en la instalación de software	Se establecerán e implementarán reglas que rigen la instalación de software por parte de los usuarios.

Nota. Tomado de Familia de Normas ISO 27000 (ISO27001, 2024).

Dentro de los dispositivos móviles se deben evaluar riesgos, ayudando a identificar y reducir vulnerabilidades en los sistemas de información aquí es donde nos apoya la NIST 800-30 (Gavidia, 2024), y la OWASP, que se centra en la seguridad de aplicaciones, subraya la necesidad de proteger los dispositivos móviles contra amenazas específicas (Owasp, 2023).

La gestión de dispositivos móviles (MDM), puede hacer cumplir estas normativas y guías si se establece políticas de seguridad sólidas, controlar el acceso a los datos y equipos, así como garantizar que las aplicaciones y dispositivos cumplan con los estándares de seguridad.

Esto también implica la capacidad de realizar auditorías, aplicar actualizaciones de seguridad y control de inventario, restricción de aplicaciones, seguridad física de los dispositivos, asegurando que se sigan las mejores prácticas continuamente ya que se debe seguir protocolos adecuados para maximizar la seguridad de los dispositivos móviles de la cooperativa (Erreyes, 2017).

Tabla 3.
Problemas de seguridad de dispositivos móviles

Problema de seguridad en los dispositivos móvil	ISO 27001	NIST 800-30	OWASP
Seguridad Física del dispositivo móvil	x		x
Autentificación Fuerte	x		x
Aislamiento de aplicaciones	x		
Protección contra Virus, gusanos, troyanos, spyware y malware	x	x	x
Proceso de parchado/actualización	x		x
Localización de privacidad / seguridad	x	x	x
Aseguramiento de los sistemas operativo	x	x	

Nota. Problemas de seguridad vinculados con la ISO 27001, NIST 800-30 y OWASP.

2.4. Metodología

La metodología empleada para la realización de este trabajo se basa en una ruta de enfoque cualitativo para proporcionar una visión integral del impacto de la Gestión de Dispositivos Móviles (MDM) en la seguridad y eficiencia operativa de los dispositivos móviles que emplea la Cooperativa que por razones de seguridad y confidencialidad, se ha decidido reservar el nombre, pero los datos, investigaciones y análisis son reales tomados de esta institución, se recopilo información de diversas fuentes bibliográficas, tesis, reseñas, artículos científicos y revistas tecnológicas, para sintetizarlos eficientemente y poder presentarlo de una manera clara y organizada.

De la misma manera se realizó una entrevista al responsable de servicios tecnológicos de la Cooperativa de Ahorro y Crédito, esta entrevista consta de 17 preguntas distribuidas en 5 secciones que sirven para conocer sobre la gestión y seguridad de los dispositivos móviles dentro de la cooperativa. Las respuestas obtenidas de la entrevista permitieron analizar información importante, sobre la cantidad dispositivos móviles empleados, como sus modelos y sistemas operativos utilizados en estos, adicional la frecuencia con el despliegue de aplicaciones además de las medidas de seguridad implementadas como manejan el inventario y la gestión de estos dispositivos. Además, se obtiene información importante, sobre la posibilidad de implementar soluciones de gestión de dispositivos móviles (MDM) para mejorar la seguridad y eficiencia operativa.

Basado en la entrevista y la información recopilada, el artículo propone que una gestión de Dispositivos Móviles (MDM), ofrece herramientas que solucionaran los problemas actuales que enfrenta la cooperativa, como se puede visualizar en la comparativa que presenta la Tabla 4.

Tabla 4.
Comparativa entre Situación Actual vs Propuesta de MDM

Problemas Actuales	Situación Actual	Propuesta de Gestión de Dispositivos móviles
Gestión de Inventario	Descentralizada, manual, no se tienen en tiempo real datos de específicos de los dispositivos móviles.	Centralizada, automatizada, se puede obtener datos específicos de cada dispositivo.
Seguridad del dispositivo	Políticas de seguridad insuficientes, en caso de robos no hay plan de bloqueo o formateo de la información del dispositivo.	Aplicación de políticas robustas como encriptación, control de acceso, perfiles de usuario, bloqueo en caso de robos.
Actualización de Software	Actualización manual y poco frecuente, se debe hacer de manera local no remotamente.	Actualización automatizada y periódica, además que se puede ejecutar remotamente.
Gestión de Contraseñas	Política de contraseñas débil sin cambios periódicos, no es robusta, muchas veces mismo patrón en los equipos.	Política de contraseñas estricta cambios periódicos, muy robusta, se puede personalizar por dispositivo.
Monitoreo en tiempo Real	Monitoreo inexistente, no se tiene datos en tiempo real de los dispositivos móviles, sin reportes.	Monitoreo en tiempo real, automatizado, generación de reportes.

Nota. Tabla que presenta una comparativa entre la situación actual de los problemas que enfrenta la cooperativa y como ayudaría la propuesta de Gestión de Dispositivos Móviles.

Adicional en la Tabla 5, se establece una comparativa, sobre si actualmente se cumplen normativas o guías como ISO 27001, la NIST 800-30 y OWASP que nos brindan buenas prácticas para la seguridad en los dispositivos móviles.

Tabla 5.
Cumplimiento Normativo de la Situación Actual vs. MDM

Normativa seguridad en los dispositivos móvil	Situación Actual	Propuesta de Gestión de Dispositivos móviles con MDM
Seguridad Física del dispositivo móvil	Ocasionalmente	Muy Frecuentemente
Autentificación Fuerte	Raramente	Muy Frecuentemente
Aislamiento de aplicaciones	Frecuentemente	Muy Frecuentemente
Virus, gusanos, troyanos, spyware y malware	Raramente	Muy Frecuentemente
Proceso de parcheo/actualización	Raramente	Muy Frecuentemente
Localización de privacidad / seguridad	Nunca	Muy Frecuentemente
Seguramiento de los sistemas operativo	Nunca	Muy Frecuentemente

Nota. Se califica la normativa cumplida entre una escala de: Muy Frecuentemente, Frecuentemente, Ocasionalmente, Raramente, Nunca.

Además en la Tabla 6, se establece una comparativa de métricas principales basadas entre la eficiencia y seguridad, de los resultados obtenidos de la entrevista realizada, se analiza aspectos como la gestión de dispositivos, el control de aplicaciones, y las prácticas de seguridad actuales, comparándolos con las expectativas de mejora mediante la implementación de un sistema de gestión de dispositivos móviles, así identificar áreas críticas que pueden mejorar con una gestión más robusta, centralizada así como automatizada.

Tabla 6.
Métricas de Eficiencia y Seguridad

Métricas	Situación Actual	Propuesta de Gestión de Dispositivos móviles con MDM	Mejora Esperada
Tiempo de Configuración de Dispositivos	Lento, manual	Rápido, automatizado	Reducción tiempos de configuración
Incidencias de Seguridad Registradas	Frecuentemente	Raramente	Reducción de Incidencias registradas
Frecuencia de Actualizaciones de Software	Raramente	Frecuentemente, automatizada	Incremento de despliegues de

			actualización o parches de seguridad
Cumplimiento de Políticas de Contraseñas	Raramente	Muy Frecuentemente	Incremento en el cumplimiento y eficiencia de políticas de contraseñas.
Auditorías de Seguridad	Raramente	Frecuentemente, continua	Incremento en las auditorias de seguridad de los dispositivos móviles

Nota. En la tabla se muestra la mejora esperada que se obtiene con la propuesta de gestión de dispositivos móviles frente a la situación actual que presenta la Cooperativa.

Este análisis comparativo resalta cómo la implementación de un sistema MDM no solo mejoraría las operaciones actuales, sino que también alinearía a la cooperativa con las mejores prácticas y estándares internacionales en seguridad.

Con el análisis de las respuestas se puede encontrar que existe una la posibilidad de maximizar la seguridad y la eficiencia de los dispositivos móviles utilizados en la cooperativa financiera, mediante el uso efectivo de la gestión de dispositivos móviles (MDM).

2.5. Resultados – Discusión

Luego del análisis de las respuestas de la entrevista realizada, se llega a la conclusión que se puede maximizar la seguridad y la eficiencia de los dispositivos móviles utilizados en la cooperativa financiera, mediante la gestión de dispositivos móviles (MDM).

Las funciones que brindan las soluciones MDM permiten una mejor gestión de los equipos que poseen actualmente se pueden automatizar muchas tareas que lo realizan de manera manual, algunos de los componentes que pueden ayudar a maximizar la eficiencia está dentro de las funciones como:

- **Inventario de dispositivos:**

La herramienta de administración de dispositivos móviles ayudaría a la cooperativa a tener un mejor control de sus dispositivos actualmente cuenta con más de 1500 dispositivos y esto hace que no tengan a la mano información detallada de cada equipo y que los registros se lo hagan de manera manual, además esto les permitiría tener una recopilación actualizada de toda la información requerida sobre programas y hardware de cada dispositivo inscrito en el portal de administración de la solución MDM.

- **Restricciones y configuraciones:**

Actualmente la cooperativa tiene establecidos configuraciones básicas para sus equipos, esto se lo hace de manera local y por dispositivo, pero si se desea configurarlos remotamente, no se lo puede hacer. Se debe solicitar asistencia generando costos operativos y de traslado o solicitar soporte técnico a distancia, lo que se traduce en pérdidas de tiempo y recursos. Una solución MDM permite generar configuraciones por cada dispositivo que se requiera además que se pueden agrupar dispositivos específicos para configuraciones particulares y así tener un perfil por modelo o un catálogo de configuraciones, que se pueden desplegar en cualquier momento reduciendo el proceso manual además de poderlo realizarlo a distancia.

- **Gestión de aplicaciones y contenido:**

La Cooperativa realiza despliegue de aplicaciones cada 6 meses, sin contar que pueden existir tiempos en los que se requiera más despliegues para corregir algún incidente o actualización de alguna normativa financiera, se encontró que se debe hacerlo de manera manual descargando el aplicativo desde un repositorio para proceder con la instalación y de existir alguna novedad se realiza asistencia técnica para revisar el dispositivo, provocando tiempos altos en la distribución de actualizaciones o de la instalación de nuevas aplicaciones. Dentro de las herramientas MDM las aplicaciones se pueden gestionar de forma centralizada además de restringir aplicaciones maliciosas estas se pueden bloquear o eliminarse de los dispositivos. Además, que los despliegues se pueden realizar a distancia, así como instalar nuevas aplicaciones o actualizaciones del mismo de manera controlada y sin intervención manual.

Las Soluciones MDM también brindan herramientas que permiten mejorar la seguridad en los dispositivos móviles, para así gestionar las políticas y corregir observaciones de auditorías o normativas de seguridad, permitiendo maximizar la seguridad, las herramientas que permiten mejorar la seguridad están presentes como:

- **Seguridad Física de los dispositivos móviles:**

Las soluciones MDM permite que, en caso de robo de algunos de los dispositivos, estos se puedan rastrear por medio de la geolocalización, y en caso de pérdida poder formatear el equipo o restablecer a un punto inicial, hasta bloquear el equipo y todas estas herramientas se puede realizar a distancia.

Además, proporcionan herramientas que permiten el cifrado de discos, así como bloqueo del equipo si detecta algún cambio en el hardware como lectoras de tarjetas, sensores de huella, etc.

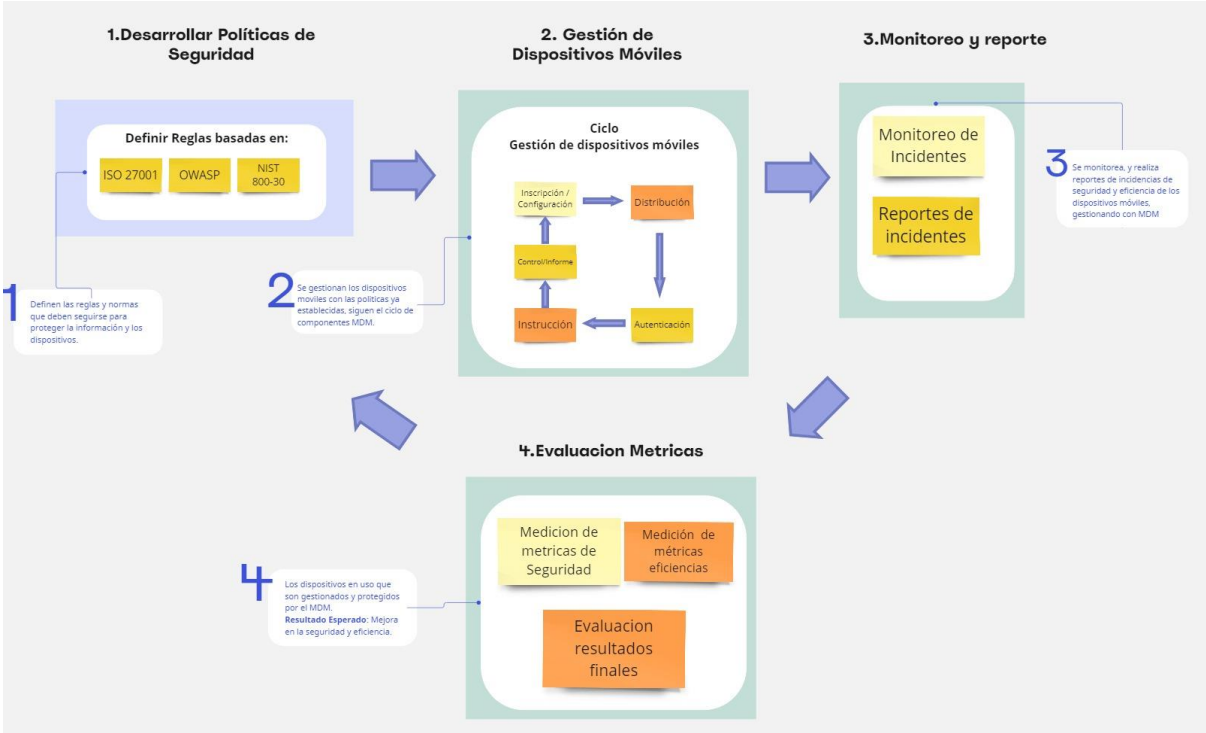
- **Implementación de políticas:**

Las políticas son la parte esencial de la seguridad de los dispositivos, estos deben cumplir con normativas, reglamentos o estándares que cuenta la cooperativa, y son los que establecen las configuraciones, restricciones, así como que aplicaciones son permitidas, cuales restringidas, implementar estas políticas de forma masiva sin importar el modelo o la cantidad de dispositivos ahorran tiempo y garantizan que los dispositivos cumplan siempre la normativa. Esto permitirá que la cooperativa tenga actualizado sus políticas y se lo pueda implementar controlada y masivamente, algo que actualmente no cuentan.

Para maximizar la seguridad y eficiencia de los dispositivos móviles usadas en la cooperativa, se ha diseñado un esquema que integra la gestión de dispositivos móviles (MDM) con políticas de seguridad, monitoreo y reportes constantes de los incidentes detectados, para una evaluación de métricas con los datos obtenidos. Este esquema, describe cómo las políticas de seguridad, basadas en normativas y guías como la, ISO 27001, NIST 800-30, y OWASP, son implementadas y gestionadas, esto no solo asegura que todos los dispositivos móviles cumplan con los estándares de seguridad establecidos, sino que también optimiza su rendimiento y funcionalidad, permitiendo una administración más eficiente de los dispositivos móviles. El flujo entre las políticas de seguridad, la gestión de dispositivos móviles con un monitoreo constante además de una evaluación periódica, basadas en métricas de los reportes obtenidos, demuestra que puede resultar en una mejora significativa tanto en la seguridad como en la eficiencia operativa, ya que al estar en un constante ciclo, con la evaluación de métricas de seguridad y eficiencia se puede nuevamente desarrollar políticas de seguridad basadas en normas y guías que permitirán una mejor gestión de dispositivos móviles. En la Figura 4, visualiza de una manera simple permitiendo una comprensión integral de cómo esta propuesta puede alcanzar los objetivos planteados.

Figura 4.

Esquema Conceptual para maximizar seguridad y eficiencia móvil a través de MDM.



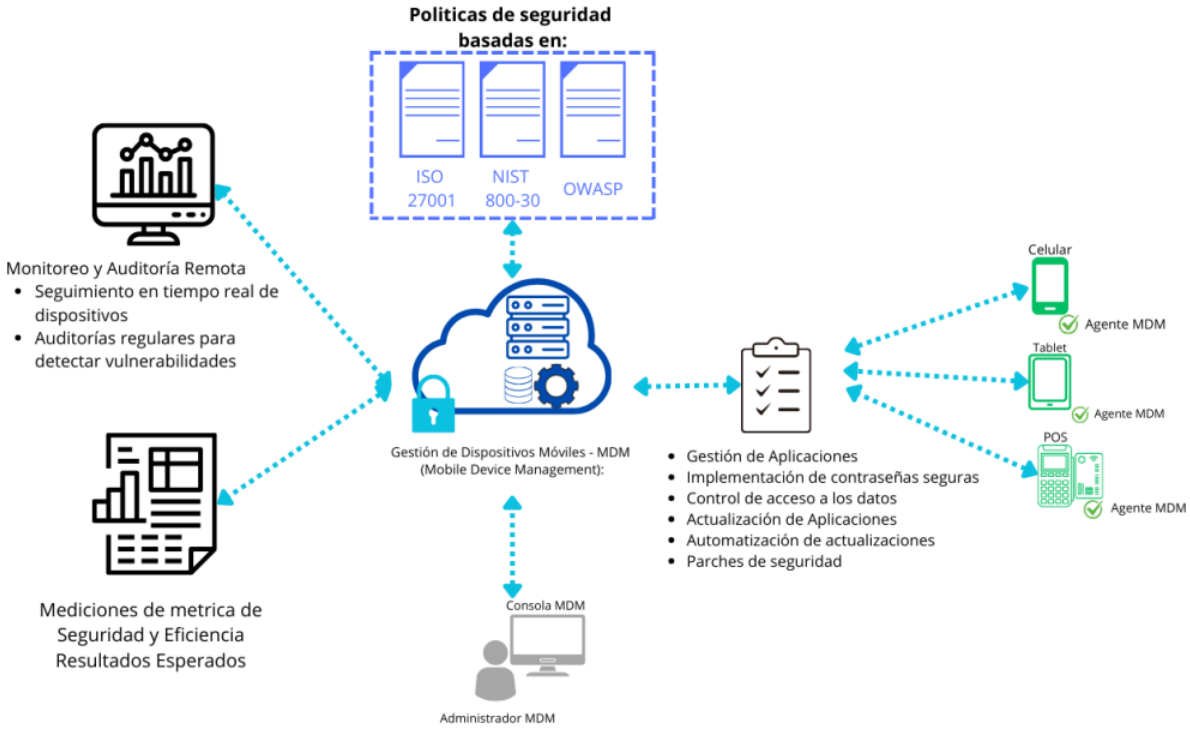
Nota. Esta figura muestra la integración de la gestión de dispositivos móviles con políticas de seguridad basadas en normativas, guías, estándar, resaltando el flujo de administración y control de dispositivos, con monitoreo y evaluación constante.

La gestión de dispositivos móviles interactúa con políticas de seguridad, para garantizar la protección y eficiencia de los equipos de la cooperativa, actúa de manera centralizada, que no solo gestiona la configuración y el acceso de los dispositivos móviles, sino que también garantiza el cumplimiento de estándares de seguridad al implementar actualizaciones automáticas, parches de seguridad, y monitoreo en tiempo real.

Adicional la gestión de dispositivos móviles interactúa con diversos componentes como la aplicación de políticas de seguridad hasta la administración remota y la auditoría de los dispositivos, este enfoque incluye la medición de métricas de seguridad y eficiencia, maximizando tanto la seguridad de los datos como el rendimiento de los dispositivos móviles.

La Figura 5, es una representación visual clara y simplificada del proceso, indicando cómo se interrelacionan los componentes para cumplir con los objetivos de maximización de seguridad y eficiencia.

Figura 5.
Diagrama Funcional de la gestión MDM para la seguridad y eficiencia móvil.



Nota. Este diagrama funcional describe cómo el MDM interactúa con los dispositivos móviles y cómo se implementan las políticas de seguridad para garantizar la protección y eficiencia de los sistemas dentro de la cooperativa.

Después, de realizar la recolección, análisis y preparación de información sobre las herramientas, componentes y funcionalidades que presenta la Gestión de Dispositivos Móviles MDM, y revisar los resultados de la información obtenidas de la entrevista realizada sobre la situación actual de la gestión de equipos que cuenta la cooperativa, se puede determinar que si se puede maximizar la seguridad y eficiencia de los dispositivos móviles de la cooperativa financiera, reduciendo así los riesgos y facilitando una gestión más controlada y centralizada de sus dispositivos, aunque esto también dependerá de que la implementación se lleve a cabo conforme a los parámetros adecuados y específicos que requiere la organización.

CONCLUSIONES

Luego del desarrollo de este artículo se puede identificar la importancia de la gestión de Dispositivos Móviles (MDM) para maximizar la seguridad y eficiencia en el entorno financiero cooperativista. Con el análisis realizado y la comparativa, entre de la situación actual de la cooperativa considerando los resultados de la entrevista y la propuesta de gestión de dispositivos móviles, se concluye que:

La gestión de dispositivos (MDM), ofrece un conjunto de herramientas que no solo mejoran la eficiencia operativa, sino que también fortalecen significativamente la seguridad de los datos en la cooperativa, ofrece características como la gestión remota de dispositivos, que permiten una mejor administración y protección de los equipos usados.

Permite simplificar muchas tareas administrativas, relacionadas con la configuración, distribución de aplicaciones y actualizaciones de software, esto permitiría la reducción de procedimientos manuales, además asegura que los dispositivos móviles estén alineados con las políticas de seguridad y operativas establecidas por la cooperativa, minimizando errores humanos y brechas de seguridad.

Se optimiza el rendimiento y reducción de costos asociados al mantenimiento y soporte de dispositivos, gestionándolos de manera centralizada los dispositivos reduce el tiempo de inactividad y los costos derivados de la resolución de problemas y reemplazo de dispositivos.

La gestión de dispositivos móviles tiene un impacto positivo en la seguridad de los equipos utilizados en la cooperativa, las políticas de seguridad aplicadas mediante MDM, junto con la posibilidad de auditar y realizar seguimiento de los dispositivos, reducen los riesgos asociados con amenazas, así como a la pérdida o robo de dispositivos, la capacidad de ejecutar comandos de seguridad como borrado remoto de datos en caso de robo, mejoran la capacidad de respuesta ante incidentes de seguridad.

El monitoreo remoto constante, con la capacidad de realizar auditorías de seguridad, la distribución automática de actualizaciones parches o políticas de seguridad, son herramientas fundamentales para mantener la integridad, seguridad y eficiencia de los equipos de la cooperativa.

En resumen, este articulo confirma que la gestión de dispositivos móviles MDM en la cooperativa, es esencial para mejorar la seguridad y eficiencia operativa de la institución. La implementación adecuada de estas soluciones puede ofrecer beneficios sustanciales tanto en términos de protección de datos como en la optimización de recursos, alineándose con las mejores prácticas y estándares internacionales en seguridad de la información.

RECOMENDACIONES

Este artículo documenta una base para comprender de mejor manera los conceptos de gestión de dispositivos móviles, su funcionamiento y componentes, así como las ventajas del uso mediante esta gestión MDM, y pretende servir como punto de partida para futuros artículos, proyectos dentro de la cooperativa, así como en otras organizaciones similares.

Se recomienda desarrollar guías o metodologías específicas para evaluar herramientas MDM, así como diseñar y establecer políticas de seguridad adaptadas a las necesidades de la cooperativa. También se recomienda crear una metodología para definir métricas de evaluación que consideren los parámetros específicos requeridos para una implementación adecuada, todas estas basadas en lo realizado en este artículo.

Este trabajo de investigación recomienda realizar evaluaciones periódicas de la efectividad de la gestión de dispositivos móviles y de las políticas de seguridad implementadas. Esto permite ajustar y optimizar las estrategias establecidas para maximizar la seguridad y la eficiencia de los dispositivos.

Las recomendaciones proporcionadas no solo ayudarán a la cooperativa a mejorar su infraestructura tecnológica, sino que también establecerán una base sólida para enfrentar futuros desafíos de seguridad.

BIBLIOGRAFÍA

Bazán, M. (02 de 05 de 2024). *Repositorio Uisrael*. Propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A: https://repositorio.uisrael.edu.ec/bitstream/47000/4071/3/UISRAEL-EC-MASTER-SEG-INF-PRO-%20378.242-2024-002.pdf

Bécares, B. (30 de 10 de 2014). *El robo de celulares en América Latina: un problema aún por resolver.* siliconweek: https://www.siliconweek.com/e-enterprise/el-robo-de-celulares-en-america-latina-un-problema-aun-por-resolver-55123

Couto, M. E. (15 de 01 de 2023). *Gestión moderna del puesto de trabajo.* Barcelona, España: Creative Common.

Erreyes, D. (2017). METODOLOGÍA PARA LA SELECCIÓN DE HERRAMIENTAS EFICIENTES Y PROTOCOLOS ADECUADOS PARA MEJORAR LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES. Cuenca, Azuay, Ecuador: Universidad de Cuenca.

García, J. (2024). Estudio de plataformas MDM en arquitecturas distribuidas. *Universidad Autonoma de Barcelona, 1*, 12.

Garcia, M. G. (2020). Análisis de riesgos de vulnerabilidades y auditorias de dispositivos. Barcelona, España: Universidad Oberta de Barcelona.

Gavidia, J. (10 de 08 de 2024). *Repositorio Uisrael*. Modelo de seguridad informática en el control de accesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NIST: https://repositorio.uisrael.edu.ec/bitstream/47000/3360/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-003.pdf

Gontovnikas, M. (25 de 07 de 2024). *Las 9 amenazas de seguridad .* https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

GSMA. (05 de 11 de 2023). https://www.gsma.com/latinamerica/es/

Guaña, J. M. (2024). Seguridad, amenazas y mecanismos de protección de los dispositivos móviles. *REVISTA MULTIDISCIPLINARIA DE DESARROLLO AGROPECUARIO, TECNOLÓGICO, EMPRESARIAL Y HUMANISTA., 6*(1), 9.

IBM. (2023). *Guía de configuración de Endpoint.* IBM.

ISO27001. (11 de 08 de 2024). *ISO/IEC 27001:2022*. https://www.iso.org/standard/27001

Jiménez, I. V. (5 de 2012). LA ENTREVISTA EN LA INVESTIGACIÓN CUALITATIVA: NUEVAS. Costa Rica: Universidad Nacional.

NIST. (05 de 11 de 2023). *The National Institute of Standards and Technology (NIST)*. https://www.nist.gov/

Onu. (2023). Informe de los Objetivos de Desarrollo Sostenible 2023. *Naciones Unidas, Edicion Especial*, 30 -31. https://www.un.org/sustainabledevelopment/es/infrastructure/

Owasp. (05 de 11 de 2023). https://owasp.org/www-project-mobile-top-10/

Parra, D., & Cubides, A. (21 de 05 de 2019). *Cienca Universidad La Salle*. https://ciencia.lasalle.edu.co/administracion_de_empresas/1587/

Pierer, M. (2016). *Mobile Device Mobility Evaluation in Small and Medium-Sized Enterprises*. Springer Vieweg. https://doi.org/10.1007/978-3-658-15046-4

Preciado, K. (06 de 2021). IMPORTANCIA DE LA ISO 27001 EN LAS PYMES DE GUAYAQUIL. Guayaquil, Guayas, Ecuador: UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL.

Prensariotila. (25 de 07 de 2024). https://prensariotila.com/33106-informe-de-seguridad-movil-2021-de-check-point/

Rhee, K., Woongryul, J., & Dongho, W. (2 de 04 de 2012). Security Requirements of a Mobile Device Management System. *International Journal of Security and Its Applications, 6*, 6. https://www.researchgate.net/profile/Dongho-Won-2/publication/267227402_Security_Requirements_of_a_Mobile_Device_Management_System/links/55ca889508aeca747d69ea6e/Security-Requirements-of-a-Mobile-Device-Management-System.pdf

Ruesgas, B. S. (Julio de 2014). Desarrollo de una política de seguridad para el uso de aplicaciones Android en un contexto empresarial. Madrid, España: Universidad Autonoma de Madrid.

Venosa, P., Macia, N., Piazza, O., & Pacheco, S. (2016). Dispositivos móviles y el fenómeno del BYOD. *XXII Congreso Argentino de Ciencias de la Computación, 1*, 1125-1134.

ANEXOS

ANEXO 1

REPUESTAS DE LA ENTREVISTA

Explorando la Seguridad y Eficiencia en la Gestión de Dispositivos Móviles: Entrevista con el Responsable de Tecnología en la Cooperativa [redacted]

Estimado [redacted]

Le agradezco de antemano por tomarse el tiempo para participar en esta entrevista. Las preguntas que siguen están dirigidas a usted como Responsable del Área de Servicios Tecnológicos, de la Cooperativa de Ahorro y Crédito [redacted] y están diseñadas para ser respondidas de forma abierta.

Esta entrevista consta de 15 preguntas agrupadas en 5 secciones, se espera que se pueda contestar de manera abierta y con la mayor sinceridad posible, ya que sus respuestas serán fundamentales para la elaboración de mi artículo titulado "Maximizando la Seguridad y Eficiencia de Dispositivos Móviles Empleadas en la Cooperativa Financiera [redacted] a través de la Gestión de MDM(Sistema de gestión de dispositivos móviles - Mobile device management)", como parte de los requisitos para la obtención de mi Maestría en Seguridad Informática.

Su participación contribuirá significativamente a la investigación y ayudará a identificar oportunidades para mejorar la seguridad y eficiencia en la gestión de dispositivos móviles dentro de la cooperativa.

Agradezco su colaboración y honestidad al completar esta encuesta.

Atentamente,

Moises Rendon Terreros

Estudiante de la Maestría en Seguridad Informática
Universidad Israel

¿Está de acuerdo en participar en esta entrevista y en que sus respuestas sean utilizadas para la elaboración de un artículo académico sobre la gestión de dispositivos móviles en la Cooperativa ■ ■ ■ ■ ■ ?

- (●) Si Acepto
- ( ) No Acepto

Sección 1: Conocimiento y Uso de MDM

¿Está familiarizado/a con el término "Gestión de Dispositivos Móviles (MDM)"? *

- (●) SI
- ( ) NO

¿La cooperativa utiliza alguna solución de MDM para la gestión de sus dispositivos móviles? Si no es así, ¿cuáles son las razones para no utilizarlo? *

No, Por los costos que conlleva y porque la herramienta que se implemente deber ser compatible con la variede de dispositivos que contamos

Sección 2: Gestión y Administración de Dispositivos Móviles

¿Cuántos dispositivos móviles están actualmente bajo la administración de la mesa de servicio? *

sobre los 1500 dispositivo

¿Cuáles son los tipos de dispositivos móviles más comunes que se administran en la cooperativa? *

trabajamos con 3 modelos de equipos: Z90, New9220 y Sunmi T2

¿Qué tan complejo considera el proceso de administrar todos estos dispositivos sin una solución de MDM? *

Es bastante complejo pues en la preparación, despliegue o actualizaciones se lo debe realizar de forma manual, adicional la implementación de políticas de seguridad no son personalizadas, el inventario actual que se lleva se lo hace de forma manual

¿Qué limitaciones o desafíos ha encontrado al implementar o utilizar esta tecnología? *

Costos, Verificaciones de pruebas error, no todas las aplicaciones son compatibles con los dispositivos que actualmente disponemos en operación.

Sección 3: Despliegue y Actualización de Aplicaciones

¿Cuáles son los sistemas operativos que se utilizan en los dispositivos móviles de la cooperativa y cuál es la razón detrás de la elección de estos sistemas? *

Los dispositivos son sobre la plataforma Android, pues la implementación realizada se lo orienta para dispositivos móviles

¿Con qué frecuencia realiza el despliegue de aplicaciones (APPS) en los dispositivos móviles de la cooperativa? *

Se lo realiza en un lapso aproximado de 6 meses, dependiendo mucho de los incidentes que se pueda generar en los postproduccion.

¿Ha enfrentado algún problema al desplegar o actualizar aplicaciones en los dispositivos móviles? Si es así, ¿cuáles han sido esos problemas? *

Si, al no contar con una herramienta que la centralice, las aplicaciones no siempre se logran actualizar de forma homogénea, lo cual provoca que esos dispositivos presenten novedades en su funcionamiento lo cual se solventa con asistencia en sitio por personal técnico.

¿Considera que el uso de MDM podría facilitar el despliegue y gestión de aplicaciones en los dispositivos móviles? *

Si

Sección 4: Seguridad y Auditorías

¿Ha tenido novedades o problemas durante auditorías de seguridad relacionadas con los dispositivos móviles? *

- (●) SI
- ( ) NO

En el caso de tener una respuesta afirmativa indíquenos cuales han sido *

Por las configuraciones que se aplican no son homogéneas lo cual provoca que se den novedades en su verificación, asumiendo muchas veces que no se aplican los instructivos generados.

¿Qué medidas de seguridad se implementan actualmente para proteger los dispositivos móviles, y cómo cree que estas podrían mejorarse? *

Actualmente, a nivel del equipo, se tiene un bloqueo de seguridad en el dispositivo mediante patron, adiciona a esto se cuenta con aplicaciones que bloquen las funcionalidades y accesos a las diferentes aplicaciones y funcionalidades que brinda el equipo.

¿Cree que la implementación de una solución MDM podría ayudar a mejorar la seguridad de los dispositivos móviles en la cooperativa? *

- (●) SI
- ( ) NO

Sección 5: Percepción General y Futuro

¿Cómo percibe la efectividad de las soluciones actuales para la gestión de dispositivos móviles en la cooperativa? *

Por el momento cumplen ya que no hemos tenido incidencias mayores pero estamos consientes que un cambio de modelo o un despliegue masivo nos representaría el uso elevado de recursos operativos ampliando el tiempo que se podrían operativos los dispositivos, además que al seguir creciendo con los servicios se requerirán de mas dispositivos y su administración seria costosa a nivel operativo, y si se requiere cambios de o implementación de nuevas políticas costaría mucho en desplegarlas

¿Está interesado/a en recibir más capacitación o información sobre MDM y sus beneficios potenciales para la cooperativa? *

- (●) SI
- ( ) NO

¿Qué sugerencias tendría para mejorar la gestión de dispositivos móviles en la cooperativa? *

Contar con una herramienta que permita alojar a los múltiples dispositivos, poderlos gestionar de manera integra, permitir actualizaciones en segundo plano de forma autónoma.

ANEXO 2
Validación de especialistas

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Christian Flores
Título obtenido: Máster en seguridad de la información y las comunicaciones
C.I.: 0105500227
E-mail: chris.ft1993@gmail.com
Institución de Trabajo: Banco Pichincha
Cargo: Arquitecto Senior de Ciberseguridad
Años de experiencia en el área: 5 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	x				
Factibilidad	x				
Novedad		x			
Fundamentación pedagógica	x				
Fundamentación tecnológica	x				
Indicaciones para su uso	x				
TOTAL	**30**	**4**			

Observaciones: El documento incluye una explicación correcta de una solución de MDM, el impacto en la gestión y el riesgo con los dispositivos móviles. Considero importante sobre todo la comparativa contra estándares internacionales ya que generalmente las instituciones se apegan a estos estándares y es válido que este trabajo tome en cuenta los mismos.

Recomendaciones: Se recomienda el poder implementar la metodología planteada previamente gestionando una metodología para el desarrollo de políticas y enfocarse en una herramienta que se adapte a la cooperativo u organización que requiera esta gestión.

Lugar, fecha de validación: Quito, 25 de agosto de 2024.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista
Christian Flores

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM".** Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Tania Jhomara Palacios Crespo
Título obtenido: MSc. Information Security at University College London
C.I.: 0104155619
E-mail: tania20palacios@gmail.com
Institución de Trabajo: Banco del Austro S.A.
Cargo: Gerente de Seguridad de la Información
Años de experiencia en el área: 12 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	x				
Factibilidad	x				
Novedad	x				
Fundamentación pedagógica	x				
Fundamentación tecnológica	x				
Indicaciones para su uso	x				
TOTAL	35				

Observaciones: El tema del artículo es de gran interés para el sector financiero en general, ya que actualmente el uso de dispositivos móviles es un riesgo de seguridad que tiene un impacto en el confidencialidad, integridad y disponibilidad de la información.

Recomendaciones: Se recomienda el uso de este proyecto como paso inicial para el desarrollo de políticas y guía de implementación en cooperativas o entidades similares para protección de los dispositivos móviles empleando la gestión de dispositivos móviles.

Lugar, fecha de validación: Cuenca, 26 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos

personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Tania Palacios

Firmado digitalmente por Tania Palacios
Fecha: 2024.08.26 09:49:13 -05'00'

Firma del especialista
Tania Jhomara Palacios Crespo

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM".** Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Paúl Andrés Montesdeoca Méndez
Título obtenido: Magister en Seguridad de la Información
C.I.: 0105745335
E-mail: paul.montesdeoca@outlook.com
Institución de Trabajo: Cooperativa de Ahorro y Crédito Jardín Azuayo
Cargo: Especialista de Mesa de Servicios Tecnológicos
Años de experiencia en el área: 1 año

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Maximizando la seguridad y eficiencia de dispositivos móviles empleadas en una cooperativa financiera, través de la Gestión de MDM"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad		x			
Factibilidad		x			
Novedad	x				
Fundamentación pedagógica		x			
Fundamentación tecnológica	x				
Indicaciones para su uso	x				
TOTAL	**20**	**12**			

Observaciones: Se considera que la propuesta es completamente viable, con un alto potencial de implementación exitosa dentro del marco establecido, el permitir la administración y gestión de los equipos de manera remota en conjunto con la aplicación de mecanismos de seguridad garantiza que el servicio sea óptimo, adecuado y seguro para el entorno financiero cooperativista, reduciendo principalmente brechas de seguridad.

Recomendaciones: Para una implementación efectiva, se sugiere seguir las recomendaciones descritas en la propuesta como planes, procedimientos o guías que permitan establecer políticas de seguridad, gestión y administración adaptadas a las necesidades específicas de la cooperativa.

Lugar, fecha de validación: Cuenca, 26 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firma del especialista
Paúl Andrés Montesdeoca Méndez

ANEXO 3

Reporte de similitud

Moises Rendon Terreros

INFORME DE ORIGINALIDAD

6%	7%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.manageengine.com Fuente de Internet	1%
2	dspace.ucuenca.edu.ec Fuente de Internet	1%
3	searchdatacenter.techtarget.com Fuente de Internet	1%
4	dateh.es Fuente de Internet	1%
5	www.endpointprotector.es Fuente de Internet	1%
6	repositorio.uisrael.edu.ec Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		