Conciencia Digital
www.concienciadigital.org

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Políticas de seguridad para dispositivos móviles en el manejo de información en PYMES

Security policies for mobile devices in the management of information in SMEs

Jenny Gabriela Vizuete Salazar. [1], Raúl Humberto Cuzco Naranjo. [2], Byron Ernesto Vaca Barahona. [3] & Carmen Elena Mantilla Cabrera. [4]

Recibido: 16-02-2021 / Revisado: 25-02-2021 /Aceptado: 17-03-2021/ Publicado: 05-04-2021

Abstract. DOI: https://doi.org/10.33262/concienciadigital.v4i2.1676

Introduction. Currently mobile devices provide great advantages for information management, if they are used within a company, it becomes a versatile tool, but, as well as offering advantages, there is also the other side in terms of security as it must maintain integrity, confidentiality, and availability of information. Knowing that in Ecuador approximately 4.39% are SMEs and that in Riobamba almost 354 are, and since there is no mobile culture in the organization of the company, it is necessary to implement strategies that promote the correct use of mobile devices to support business activity. **Objective.** Improve security in SMEs by implementing security policies on mobile devices for the safe handling of information. **Methodology.** A SWOT analysis was carried out where the strengths and weaknesses of the company with respect to the management of information through mobile devices were identified, processes were established from the surveys carried out to the members of the company, the necessary security policies were drawn up to solve the shortcomings that arose, the policies

[1] Investigador independiente, Riobamba, Ecuador, jennyvizuete@yahoo.es
[2] Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Grupo de Investigación en Seguridad Telemática (SEGINTE). Riobamba, Ecuador. rcuzco@espoch.edu.ec. https://orcid.org/0000-0002-7469-8742
[3] Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Grupo de Investigación en Seguridad Telemática (SEGINTE). Riobamba, Ecuador. bvacab@espoch.edu.ec. https://orcid.org/0000-0002-3622-0668
[4] Escuela Superior Politécnica de Chimborazo, Facultad de Recursos Naturales, Grupo de Investigación en Seguridad Telemática (SEGINTE). Riobamba, Ecuador. carmen.mantilla@espoch.edu.ec. https://orcid.org/0000-0001-5422-7073

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

developed were implemented and the validity and effectiveness of these policies in the company was verified. **Results.** The implemented policies increased the integrity of the data transmission through mobile devices, it went from 13.64% to 86.36%, the confidentiality of the data to 36.36% since before the application of the policies it did not exist, availability was obtained 18.18% on mobile devices, since previously information was obtained from these. **Conclusion.** The security policies on mobile devices for the safe handling of the information shared with the personnel allowed the improvement in the security of the company according to its initial situation.

Keywords: policies, mobiles devices, computer security, SMEs.

Resumen.

Introducción. En la actualidad los dispositivos móviles proporcionan grandes ventajas para el manejo de información, si se utilizan dentro de una empresa se convierte en una herramienta versátil, pero, así como ofrece ventajas también existe la otra cara en mira a la seguridad pues debe mantener la integridad, confidencialidad y disponibilidad de la información. Sabiendo que en Ecuador aproximadamente el 4.39 % son PYMES y que en Riobamba casi 354 lo son, y al no existir una cultura una cultura móvil en la organización de la empresa se ve necesario implementar estrategias que promueva el uso correcto de los dispositivos móviles para apoyar la actividad empresarial. **Objetivo.** Mejorar la seguridad en PYMES al implementar políticas de seguridad en dispositivos móviles para el manejo seguro de la información. **Metodología.** Se realizó un análisis FODA donde se identificó las fortalezas y debilidades de la empresa respecto al manejo de la información a través de dispositivos móviles, se establecieron procesos a partir de las encuestas realizadas a los miembros de la empresa, se redactaron las políticas de seguridad necesarias para solucionar las falencias que se presentaron, se puso en marcha las políticas desarrolladas y se verificó la validez y eficacia de estas políticas en la empresa. **Resultados.** Las políticas implementadas incrementaron la integridad de la transmisión de datos por medio de dispositivos móviles pasó de un13.64% a 86.36%, la confidencialidad de los datos a un 36.36% ya que antes de aplicación de las políticas no existía, se obtuvo una disponibilidad de un 18,18% en dispositivos móviles, pues antes se obtenía información desde estos. **Conclusión.** Las políticas de seguridad en dispositivos móviles para el manejo seguro de la información socializadas al personal permitieron la mejora en la seguridad de la empresa acuerdo a su situación inicial.

Palabras claves: políticas, dispositivos móviles, seguridad informática, PYMES.

Introducción.

Hoy en día, los dispositivos móviles juegan un papel relevante dentro de las empresas debido a que proporciona grandes ventajas como acceder de manera instantánea a

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

información actualizada en el momento oportuno (Baz, 2013), permitiendo tomar decisiones acertadas y no dejando escapar oportunidades (Macías, 2016).

Por supuesto el uso de los dispositivos móviles para el manejo de la información también supone la presencia de riesgos para las empresas. Entre los principales peligros tenemos: la pérdida de los terminales, acceso no autorizado o fuga de información, infecciones de software maliciosos, etc. Consecuentemente la seguridad es uno de los pilares principales para las empresas que apuestan por implementar la movilidad dentro de las mismas (D'Angelo et al., 2014).

Para poder desarrollar una cultura móvil en la organización es importante definir una estrategia que promueva el uso correcto de los dispositivos y delimite su alcance. El reto de las empresas es como aprovechas estas ventajas según sus necesidades, pero siempre manteniendo la integridad, confidencialidad y disponibilidad de la información (Carrasco, 2015).

Hay varias ventajas que ofrecen los dispositivos móviles en una empresa como: portabilidad a través de la cual se puede tener una comunicación digital desde cualquier parte sin estar dentro de la empresa, generando participación activa de los empleados, la disponibilidad donde los dispositivos móviles ayudan a la visualización de cualquier información sobre productos o servicios en el momento requerido, y la captura de datos en tiempo real permite que los dispositivos móviles capturen información y se envíen datos recolectados a cualquier sistema necesario (Siniša, 2016).

En Ecuador el 4.39 % son medianas y pequeñas empresas, existe un total de 21864 PYMES que tienen RUC. En Riobamba, el total de micro, pequeña, mediana y grande empresa es de 8071, según Slusarczyk, 2015 diagnóstica en la aplicación de las NTIC en las PYMES de Riobamba que el 3.72 % de las empresas son pequeñas y el 0.64% son medianas, aproximadamente 354 PYMES en la ciudad de Riobamba (Slusarczyk, María, 2015).

Por lo expuesto anteriormente, el presente trabajo se centra en la aplicación de políticas de seguridad al momento de acceder a la información a través del uso de los dispositivos móviles, para lo cual se realizó un análisis de la situación actual de la PYME y el análisis de indicadores que intervienen en la seguridad de dispositivos móviles para el manejo de la información, el análisis de datos permitió obtener resultado para la implementación de políticas en la empresa (Vizuete, 2020).

Metodología.

A. Análisis FODA Dispositivos móviles

El estudio de la empresa PYME permitió analizar las principales debilidades en seguridad de la información que se presentan al momento del manejo de la información a través de dispositivos móviles (Antosz, 2015).

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Fortalezas

- Acceso fácil y rápido a la información y contactos
- Las aplicaciones han mejorado las plataformas y la interconectividad
- Ahorro de tiempo y dinero por la múltiple oferta del mercado
- Rapidez en el desarrollo de aplicaciones que permiten el intercambio de información rápida entre los usuarios
- Posibilidad de bloquear los dispositivos móviles para asegurar la información en ellos

Oportunidades

- Se presentan actualizaciones continuamente que pueden mejorar las protecciones del dispositivo.
- A nivel global se puede compartir información rápidamente

Debilidades

- Hay muchas aplicaciones inseguras en la red
- Los sistemas operativos presentan muchas fallas en su estructura interna, lo que los hace vulnerables a hackeos y robo de información.
- No existe un control en la mayoría de PYMES de los dispositivos que se conectan a la red
- No se utiliza software de seguridad en los dispositivos móviles que impida el acceso de información del teléfono
- Los dispositivos móviles se conectan a redes inalámbricas
- Configuración incorrecta de permisos que permiten acceso a funciones controladas
- Falta de protocolos para comunicación internas. La información o mensajes internos se transfiere a través del dispositivo a otras aplicaciones
- Uso excesivo del consumo de aplicaciones corriendo continuamente en segundo plano, las que drenan la batería, por lo tanto, reduciendo la disponibilidad del sistema

Amenazas

- Existe una gran cantidad de virus malware que pueden atacar a los dispositivos y robar los datos
- Los usuarios no utilizan las contraseñas y protecciones para sus equipos
- Las trasmisiones de datos inalámbricas no siempre están encriptadas
- Los dispositivos móviles constituyen una forma fácil de ingresar

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

- Los servicios disponibles para utilizar por el dispositivo pueden sufrir ataques como: de fuerza bruta, ataques DoS, ataques de XSS, SQL Inyección, etc
- Son más susceptibles a robo o hurto
- Filtración involuntaria de datos.
- Conexión a Wi-Fi no asegurada

B. DISEÑO DE ESTUDIO

Para la implementación las políticas de seguridad para dispositivos móviles al momento de manejar la información (Ramos, 2011), se aplicó una investigación cuasi experimental, esto logró por medio de la evaluación con la norma NTE INEN-ISO/IEC 27001:2011 en una empresa de la ciudad Riobamba, el nombre de la empresa no se menciona para mantener su integridad.

Se consideró como población el personal que trabaja en la empresa, por medio de la aplicación de una encuesta, se pudo conocer las principales falencias de seguridad de los dispositivos móviles que requieran de políticas para contrarrestar su efecto negativo (Castro,2015).

Se utilizó el método científico, el modelo general, que contiene la formulación del problema, formulación de la hipótesis, la recolección de información, el análisis e interpretación de resultados, demostración de la hipótesis y la publicación de los resultados de la investigación, el método que principalmente se aplica en el presente trabajo es el inductivo, que permite encontrar generalidades a partir de conocimientos particulares, en el caso que se está tratando dará como resultado un conjunto de políticas destinadas a mejorar la seguridad de dispositivos móviles en PYMES.

Se utilizó una encuesta, aplicada a los diferentes actores de la investigación, que ayudó a entender la calidad de seguridad que tienen actualmente los dispositivos en las PYMES (ISO, 2019).

C. APLICACIÓN DEL MÉTODO

Los dispositivos móviles poseen una serie de propiedades que le vuelven un blanco fácil para los hackers, por tanto, una fuente poco segura para el manejo de información importante (Betancur,2015).

El estudio incluye una serie de políticas de seguridad que serán de aplicación necesaria a las PYMES de la ciudad de Riobamba, de acuerdo con la normativa NTE INEN-ISO/IEC 27001:2011, convirtiéndose en una herramienta de apoyo para las empresas para buscar seguridad en la información que se administra por dispositivos móviles (Vieites,2017).

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

En primer lugar, se revisó las normativas vigentes para verificar la base legal que deben cumplir las empresas respecto a sus seguridades en la información (INEN, 2016).

De las encuestas y observación obtuvo la situación actual de los niveles de seguridad de la empresa y las políticas que se aplican para el manejo de la información (Solarte, 2015).

De estos dos procesos se obtuvieron los datos necesarios para desarrollar las políticas que se adecúen a la realidad empresarial, basada en la normativa NTE INEN-ISO/IEC 27001:2011.

D. IMPLEMENTACION DE POLÍTICAS DE SEGURIDAD.

Se implementaron políticas de seguridad en:

Disposiciones generales

Artículo 1: Las normativas tienen por objeto estandarizar y normar el uso de los dispositivos móviles respecto a las redes de la empresa

Artículo 2: Para los efectos de este documento, se entiende por Políticas de seguridad en dispositivos móviles al conjunto de reglas obligatorias que deben seguir los miembros de la empresa respecto al uso de dispositivos móviles; siendo responsabilidad de la administración vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Artículo 3: La instancia rectora del sistema informático es la Gerencia, y su aplicación dependerá de la designación que realice el Gerente o Junta de Accionistas por escrito.

Artículo 4: Las normas que se presentan serán únicamente para regular el uso de los dispositivos móviles dentro de la empresa, a fin de cuidar la información que pueda ser vulnerable a través de estos medios.

Artículo 5: Será importante nombrar por escrito a personas responsables para el manejo y divulgación de los procedimientos que deberán seguirse para el uso de dispositivos móviles

Artículo 6: Será responsabilidad de RRHH o Gerencia la contratación del personal adecuado para las labores en las diferentes áreas de la empresa.

Uso general de dispositivos

Artículo 7: Se prohíbe el uso de los dispositivos móviles personales en horas de trabajo para realizar o recibir llamadas, excepto en casos de emergencia en cuyo caso deberá darse conocimiento al supervisor o encargado del área responsable.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Artículo 8: No se puede utilizar redes sociales u otros medios de mensajería en horas de trabajo desde los dispositivos móviles.

Artículo 9: Los contactos hacia proveedores o jefes de la empresa se realizarán con un teléfono móvil de la empresa exclusivo para el efecto, el cual tendrá un custodio que se asegure de su manejo y preservación adecuada.

Responsabilidad

Artículo 10: Los gerentes o la persona que tiene a cargo la red de internet de la empresa es la única que puede otorgar claves el acceso de los dispositivos móviles siempre y cuando se necesite acceder al sistema de la empresa.

Artículo 11: No se permite a los empleados compartir las claves de acceso a la red bajo ningún concepto. Esta particularidad será exclusiva del responsable de las redes de la empresa.

Artículo 12: En caso de que el empleado necesite llevarse consigo el dispositivo móvil de la empresa debe informar al personal responsable y llenar el registro de responsabilidad. Este artículo aplica cuando el empleado se ausente por enfermedad o calamidad doméstica.

Seguridad

Artículo 13: El acceso a los sistemas de información, deberá contar niveles de seguridad de acceso suficiente para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

Artículo 14: Se deberá establecer claves de accesos a las redes WIFI de la empresa, además es necesario registrar la MAC del dispositivo móvil, el encargado de redes será el único que tenga la autorización de ingresar las direcciones para el uso de la red.

Artículo 15: Debe llevarse un listado de los dispositivos móviles que se conectan a la red cada día a fin de controlar el acceso y la velocidad de conexión.

Artículo 16: El acceso a programas de la compañía por medio de dispositivos móviles que requieran información deberá limitarse al cargo que tenga cada empleado.

Artículo 17: Se deben implantar rutinas periódicas de auditoria a la confidencialidad, integridad y disponibilidad de los datos y de los programas de la empresa, para garantizar su confiabilidad.

Artículo 18: Si se desea acceder a la red de la empresa mediante el dispositivo móvil desde una red externa se lo debe realizar mediante una VPN que maneje protocolos

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

seguros (L2TP/IPSec), siempre se debe cerrar la sesión de VPN una vez terminado cualquier actividad.

Artículo 19: Todos los dispositivos móviles deben estar enlazados a una cuenta de correo electrónico de la empresa y la sincronización activada, las credenciales de esta cuenta deben ser manejadas por el responsable de la seguridad de la información.

Artículo 20: Establecer un método y período de bloqueo para acceso al dispositivo y su memoria (contraseña, biometría, patrones gráficos, u otras opciones) para los dispositivos móviles institucionales que serán entregados a los usuarios. Además, las contraseñas deben ser cambiadas cada tres meses.

Artículo 21: Se procederá a realizar cambios de claves de las redes en un período máximo de 6 meses por parte de la administración

Instalaciones y mantenimiento de los dispositivos móviles

Artículo 22: Se debe realizar el mantenimiento de los equipos móviles de la empresa cada tres meses con el objetivo de verificar el funcionamiento de hardware y software de este.

Artículo 23: La Administración deberá contar con el diagrama de la red interna y de los dispositivos móviles instalados en red.

Artículo 24: El personal responsable de los dispositivos móviles se encargará de instalar las actualizaciones del sistema operativo, actualización de programas, parches, etc.

Artículo 25: El personal responsable de los dispositivos móviles se encargará de instalar y mantener actualizado el antivirus de cada dispositivo móvil.

Información

Artículo 26: Los responsables de la información, delimitarán las responsabilidades de sus empleados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes desde sus dispositivos móviles.

Artículo 27: Si se requiere, se autorizará el uso de otros dispositivos móviles para realizar alguna operación emergente en caso de no poder utilizar el dispositivo móvil que se asignó para dicho efecto. Sin embargo, deberá eliminarse el acceso al programa una vez que se ha completado la operación.

Artículo 28: No se podrá conectar ningún dispositivo móvil a las computadoras por medio de cables o de forma alámbrica. La carga de los dispositivos solo se permitirá a través de la toma de corriente.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Artículo 29: A pesar de que se otorga permisos específicos a las personas que poseen dispositivos móviles, es responsabilidad del administrador de la red verificar los accesos y modificaciones que han realizado los usuarios a las bases de datos.

Artículo 30: Los encargados de los servidores y bases de datos deberán respaldar la información de los celulares en el servidor al menos una vez a la semana.

Uso personal

Artículo 31: Los usuarios son responsables de toda actividad relacionada con el uso de sus credenciales y claves a los dispositivos móviles.

Artículo 32: Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 33: Si un usuario tiene sospechas de que su acceso autorizado (identificador usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

Artículo 34: Proteger con contraseña y respaldar, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Artículo 35: Los usuarios tienen terminantemente prohibido almacenar los datos personales en los dispositivos móviles de la empresa.

Conectividad a internet

Artículo 36: Los dispositivos móviles tienen autorización de acceso a internet exclusivamente para actividades de trabajo.

Artículo 37: Sólo puede haber transferencia de datos o a Internet para realizar actividades propias del trabajo desempeñado.

Artículo 38: Toda configuración y cambio de la red en donde se conectan los dispositivos móviles debe estar debidamente respaldada, además se debe llenar el documento en donde se describe los cambios realizados y la persona que los realizó.

Artículo 39: Si se tiene problemas de conectividad de internet a través del plan de datos se debe reportar al personal encargado con el fin de corregir el problema con el proveedor.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Pérdidas y robos

Artículo 40: Cada persona es responsable del uso y cuidado de su dispositivo móvil, por tanto, la empresa no se responsabiliza del cuidado y pérdida que se haya dado del equipo tanto dentro como fuera de sus instalaciones.

Artículo 41: La administración deberá capacitar a los empleados en temas de uso correcto de sus dispositivos móviles, y como cuidarlos incluyendo vinculación a cuentas que permitan rastrearlos, denuncias por pérdida de dispositivos, entre otros procedimientos.

Artículo 42: Es obligación de los empleados comunicar a la administración la pérdida o robo de su dispositivo móvil que se haya vinculado a la red de la empresa o a sus programas.

Artículo 43: La administración desvinculará y eliminará claves de acceso de los dispositivos móviles que se hayan extraviado una vez que se haya sacado respaldo de estas.

Artículo 44: Se repondrá la clave y todos los accesos al usuario que extravió o fue víctima de robo de su dispositivo móvil una vez que se haya cumplido el artículo 42 y previa petición.

Resultados.

A continuación, se presentarán los resultados que se obtuvieron en la empresa por medio de la encuesta aplicada a sus integrantes según:

Normativas

4. ¿Conoce algún tipo de regulación que limite el uso o conexión de dispositivos móviles en la empresa?

5. ¿Se necesitan de claves para acceder a las redes de la empresa?

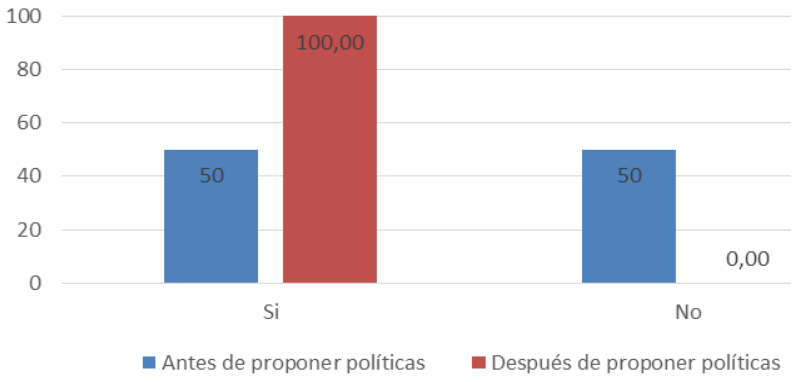

Figura 1: Resultados de encuestas para normativas

Fuente: Elaboración propia.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Según los datos recolectados, se puede observar en la figura 1, que el indicador normativas ha subido en un 50%, pasando de 50% a 100%

Antes de la propuesta de políticas el 50% de los encuestados menciona que existían normativas o regulaciones para los dispositivos móviles.

Después de la propuesta de políticas el 100% de los encuestados menciona que existen normativas o regulaciones para los dispositivos móviles.

Políticas

6. ¿Existen políticas específicas en el uso de dispositivos móviles?

9. ¿Existen algún proceso de solicitud para la asignación de dispositivos móviles corporativos?

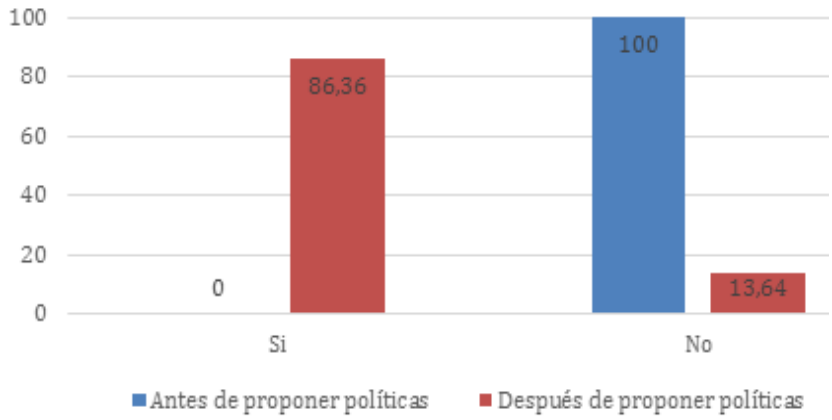

Figura 2: Resultados de encuestas para políticas

Fuente: Elaboración propia.

Como se puede observar en la figura 2, las políticas reguladoras para dispositivos móviles se elevaron en un 86,36%.

Antes del establecimiento de políticas, no existía conocimiento de políticas escritas o verbales acerca de los dispositivos móviles.

Integridad

10. ¿Mantiene un registro de los dispositivos móviles asignados (qué dispositivo móvil y a quién se le asigna además del software y hardware que son requeridos por el empleado)?

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

12. ¿Se almacena información corporativa que sea estrictamente necesaria para el desarrollo del trabajo?

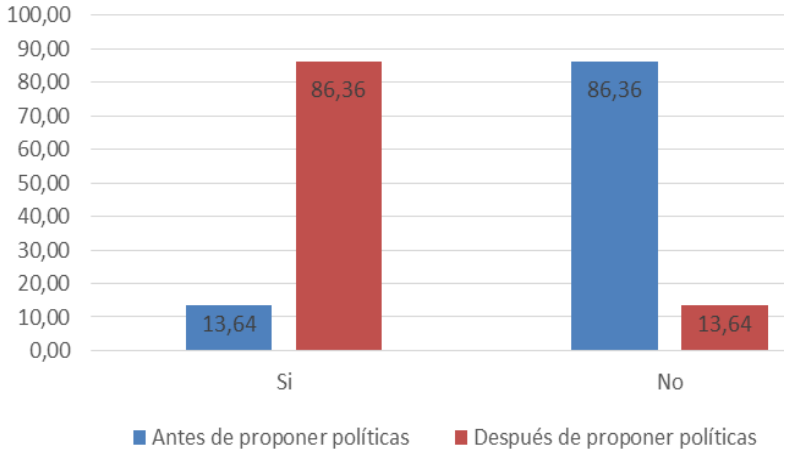

Figura 3: Resultados de encuesta para Integridad

Fuente: Elaboración propia.

De acuerdo con los datos mostrados en el instrumento de evaluación, como se puede apreciar en la figura 3, la variable integridad en la información pasó de 13,64% a 86,36%.

Disponibilidad

11. ¿Elabora un formulario de solicitud de cambios en el dispositivo móvil (modificación de hardware, instalación de software, cambios en la configuración)?

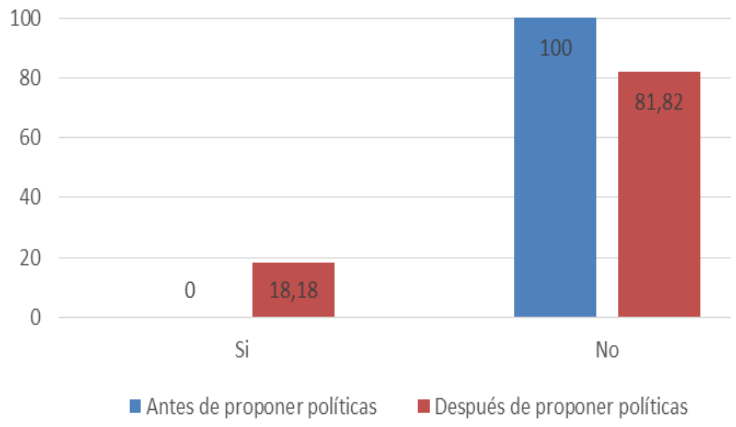

Figura 4: Resultados de encuesta para Disponibilidad

Fuente: Elaboración propia.

Antes de la aplicación de las políticas, no se tenía información disponible desde los

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

dispositivos móviles. Después de la aplicación de las políticas, se manifiesta que para el 18,18% de las personas la información se encuentra disponible a través de dispositivos móviles, tal como se muestra en la figura 4.

Confidencialidad

13. ¿Cifra la información confidencial y la elimina de forma segura (o solicita la eliminación al técnico responsable)?

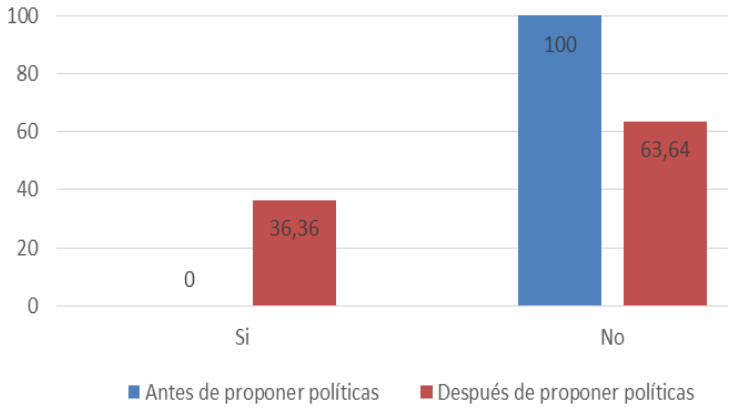

Figura 5: Resultados encuesta para Confidencialidad

Fuente: Elaboración propia.

Antes del establecimiento de políticas no existía un buen nivel de confidencialidad en la información de la empresa a través de redes móviles. De acuerdo con los datos mostrados en la figura 5 del instrumento de evaluación, la variable confidencialidad en la información detalla un 36,36%.

Conclusiones.

- El análisis FODA determinó la situación real de la empresa como punto clave para la creación de las políticas de seguridad en dispositivos móviles para el manejo de la información.
- La situación actual de la seguridad de la información de la empresa determinó que no se habían establecido normas o procedimientos de seguridad de la información para el manejo de la información a través de dispositivos móviles.
- Las políticas implementadas sociabilizadas a los miembros de la empresa mejoraron el nivel de seguridad de la información de la empresa, en integridad de la transmisión de datos por medio de dispositivos móviles aumentó en un 72,72%, la confidencialidad de los datos a un 36.36% ya que antes de aplicación de las

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

políticas no existía, se obtuvo una disponibilidad de un 18,18% en dispositivos móviles, pues antes se obtenía información desde estos.

Referencias bibliográficas.

Antosz, M. (2015). Diagnóstico de aplicación de las NTIC en las PYMES de Riobamba-Ecuador. *3C TIC, 146-168.*

Baz, A., Ferrerira, I., Álvarez, M., & García, R. (2013). Dispositivos móviles. E.P.S.I.G : Ingeniería de Telecomunicación - *Universidad de Oviedo, 1-12.*

Betancur, O., & Eraso, S. (2015). Seguridad en Dispositivos Móviles Android. Perú: UNAD.

Carrasco, S. (2015). Análisis de la aplicación de la tecnología móvil en las empresas.

Castro, A., Guantiva, G., & Zárate, R. (2015). Guía de Políticas de Seguridad para dispoisitivos móviles en Pequeñas y Medianas Empresas. Bogotá: Universidad Católica de Colombia-Facultad de Ingeniería.

D'Angelo, G., Ferretti, S., Ghini, V., & Panzieri, F. (2014). Mobile Computing in Digital Ecosystems: Design Issues and Challenges. Cornell University.

INEN, (2016). Servicio Ecuatoriano de Normalización. Obtenido de buzon/normas/nte_inen_iso_iec_27000.pdf

ISO. (2019). ISO 27002. Obtenido de http://iso27000.es/iso27002.html

Macías, M. A. (2016). Marco conceptual de la computación móvil.

Ramos, P. (2011). Seguridad móvil: consejos y vulnerabilidades. Obtenido de WELIVESECURITY.

Siniša Husnjak, I. F. (2016). Preferences of Smartphone Users in Mobile to WI-FI Data Traffic Offload. Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom.

Slusarczyk, M. (2015). Diagnóstico de aplicación de las NTIC en lsa PYMES de Riobamba-Ecuador. *3C TIC, 145-168.*

Solarte, F. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL.

Vieites, A. (2017). Enciclopedia de la seguridad informática. Madrid: RA-MA, S.A. Editorial y Publicaciones.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

Vizuete, J. (2020). «Implementación de políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES». ESPOCH, Riobamba.

ISSN: 2600-5859
Vol. 4, N°2, p. 261-276, abril-junio, 2021

PARA CITAR EL ARTÍCULO INDEXADO.

Vizuete Salazar, J. G., Cuzco Naranjo, R. H., Vaca Barahona, B. E., & Mantilla Cabrera, C. E. (2021). Políticas de seguridad para dispositivos móviles en el manejo de información en PYMES. ConcienciaDigital, 4(2), 261-276. https://doi.org/10.33262/concienciadigital.v4i2.1676