ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES PARA EL MANEJO DE LA INFORMACIÓN EN PYMES

JENNY GABRIELA VIZUETE SALAZAR

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

Agosto 2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** titulado "IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES PARA EL MANEJO DE INFORMACIÓN EN PYMES", de responsabilidad del Srta. Jenny Gabriela Vizuete Salazar ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Mario Vargas Guambo
PRESIDENTE

Firmado electrónicamente por:
JUAN MARIO VARGAS GUAMBO

FIRMA

Ing. Raúl Humberto Cuzco Naranjo, M.Sc.
DIRECTOR

RAUL HUMBERTO CUZCO NARANJO
Firmado digitalmente por RAUL HUMBERTO CUZCO NARANJO
Fecha: 2020.09.23 18:59:43 -05'00'

FIRMA

Ing. Wilian Xavier Sánchez Labre, M.Sc.
MIEMBRO

Firmado electrónicamente por:
WILIAN XAVIER SANCHEZ LABRE

FIRMA

Ing. Paúl Fernando Bernal Barzallo, M.Sc.
MIEMBRO

Firmado electrónicamente por:
BERNAL BARZALLO PAUL FERNANDO

FIRMA

Riobamba, agosto 2020

DERECHOS INTELECTUALES

Yo, Jenny Gabriela Vizuete Salazar, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

JENNY GABRIELA VIZUETE SALAZAR
No. Cédula: 0603622085

DECLARACIÓN DE AUTENTICIDAD

Yo, Jenny Gabriela Vizuete Salazar, declaro que el presente **Trabajo de Titulación modalidad Proyecto de investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de Maestría.

Riobamba, agosto 2020

_____

JENNY GABRIELA VIZUETE SALAZAR
No. de Cédula: 0603622085

DEDICATORIA

Este trabajo está dedicado primero a Dios. A mis padres Rosa e Ignacio por ser el pilar más importante de mi vida y apoyarme en todo momento, por haberme inculcado sus valores, por la motivación constante que me han permitido ser una persona de bien. A mi esposo Frank David quien me ha apoyado incondicionalmente para culminar con éxito un objetivo más en mi vida. A mis hermanos y sobrinos por esta siempre presente y darme palabras de aliento para seguir adelante.

Jenny Gabriela

AGRADECIMIENTO

Quiero agradecer a Dios por permitirme cumplir un objetivo más en mi carrera profesional.

Le doy gracias a mis padres Rosa e Ignacio por ser mi ejemplo de constancia, superación, sin su apoyo y sabios consejos no estaría hoy aquí.

A mi esposo Frank por creer en mí y alentarme a ser mejor cada día, sobre todo por su paciencia, comprensión y demostrarme su amor incondicional.

A mis hermanos Ximena, David y Katherine por ser parte importante en mi vida y apoyarme en todo momento.

A mis sobrinos por todo su cariño que me demuestran y llenar mi vida de grandes y bonitos momentos.

A mis amigos, que me ayudaron de una u otra forma para poder culminar este proyecto, gracias por su apoyo, comprensión y amistad.

Quiero también agradecer a los profesionales que fueron parte fundamental para el desarrollo de este proyecto de investigación, de manera muy especial al tutor y a los miembros del tribunal.

Jenny Gabriela

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

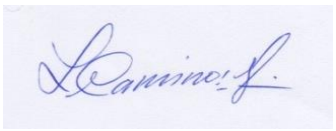
ÍNDICE DE GRÁFICOS

INDICE DE ANEXOS

RESUMEN

El objetivo de este estudio es implementar políticas de seguridad en dispositivos móviles para el manejo de la información en pequeñas y medianas empresas (PYMES), para el desarrollo de este proyecto de investigación se aplicó la metodología que está basada en las normas ISO/IEC 27001:2015, de acuerdo a las necesidades de la empresa TELECOMEXPERT. En primer lugar, se realizó un levantamiento de la situación actual de la empresa referente a la normativa que posee la empresa en cuanto a dispositivos móviles para el manejo de la información. La salida de este proceso proporcionó las bases para poder realizar el análisis de las políticas que se necesitaron desarrollar para la aplicación en la empresa. Se realizó un análisis de riesgos, amenazas y vulnerabilidades a los que están expuestos los datos que se acceden a través de los dispositivos móviles, en donde se obtuvieron puntos claves para la creación de las políticas de seguridad en dispositivos móviles, para lo cual se procedió con la identificación de los activos y se categorizó en base a la importancia que representa cada uno para la empresa**.** De los procesos mencionados anteriormente se obtuvieron los datos necesarios para la implementación de políticas que se adecúen a la realidad de la empresa TELECOMEXPERT, tomando en cuenta los lineamientos de la normativa NTE INEN-ISO/IEC 27001:2015 y NTE INEN-ISO IEC 27002. Luego de la aplicación de las políticas procedió a evaluar las mismas y se pudo apreciar un aumento en el conocimiento de las normativas y políticas que se implementaron en la empresa TELECOMEXPERT, mejorando la integridad de la transmisión de datos por medio de dispositivos móviles pasando de 13.64% a 86.36%, mejorando la confidencialidad de los datos en un 36.36%, así como la disponibilidad de los mismos en un 18,18%. En la actualidad estamos en una era en donde la tecnología juega un papel, por lo que es importante tener las herramientas necesarias para mantener la seguridad de la información por lo que la correcta implementación de las políticas de seguridad para el manejo de la información a través de dispositivos móviles ayuda a mantener la confiabilidad, disponibilidad e integridad de la misma.

Palabras clave: <SEGURIDAD INFORMÁTICA >, <PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES)>, <POLÍTICAS DE SEGURIDAD>, <DISPOSITIVOS MÓVILES>



13-08-2020

0206-DBRAI-UPT-2020

ABSTRACT

The objective of this study is to implement security policies in mobile devices for the management of information in small and medium-sized enterprises (SMEs), for the development of this research project the methodology that is based on the ISO / IEC 27001 standards was applied: 2015, according to the needs of the TELECOMEXPERT company. In the first place, a survey of the current situation of the company was carried out regarding the regulations that the company has in terms of mobile devices for information management. The output of this process provided the basis for conducting the analysis of the policies that needed to be developed for application in the company. An analysis of risks, threats and vulnerabilities to which the data accessed through mobile devices are exposed was carried out, where key points were obtained for the creation of security policies on mobile devices, for which we proceeded with the identification of the assets and it was categorized based on the importance that each one represents for the company. From the aforementioned processes, the necessary data was obtained for the implementation of policies that adapt to the reality of the TELECOMEXPERT company, taking into account the guidelines of the NTE INEN-ISO / IEC 27001: 2015 and NTE INEN-ISO IEC 27002 regulations. After applying the policies, they were evaluated and an increase in knowledge of the regulations and policies that were implemented in the TELECOMEXPERT company could be appreciated, improving the integrity of data transmission through mobile devices. going from 13.64% to 86.36%, improving the confidentiality of the data by 36.36%, as well as the availability of the same by 18.18%. Nowadays it is an era where technology plays a role, so it is important to have the necessary tools to maintain the security of the information, so the correct implementation of security policies for the management of information through Mobile devices help maintain the reliability, availability and integrity of this.

Keywords: <COMPUTER SECURITY>, <SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)>, <SECURITY POLICIES>, <MOBILE DEVICES>

CAPÍTULO I

1. INTRODUCCIÓN

En el mundo de hoy los dispositivos móviles juegan un papel relevante dentro de las empresas debido a que proporciona grandes ventajas como acceder de manera instantánea a información actualizada en el momento oportuno permitiendo tomar decisiones acertadas y no dejando escapar oportunidades.

El correo electrónico empresarial se popularizó con los dispositivos BlackBerry, sin embargo, en la actualidad se puede acceder a información en tiempo real de manera fácil y rápida. Por supuesto el uso de estas herramientas 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.

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 Usano, Silvia, 2015)

En la primera parte de este documento se describe la problemática y la justificación de este trabajo de investigación. Se introduce a la importancia de los dispositivos móviles en las empresas y los problemas que conllevan su uso.

En la segunda parte se habla sobre las PYMES, evolución de los dispositivos móviles junto con sus aplicaciones y tecnología. Además de cómo se maneja la información de las empresas y como ha crecido el uso de los dispositivos móviles en las labores y actividades diarias de las organizaciones. También se hace un análisis comparativo de la normativa vigente en el Ecuador y la norma internacional.

En la tercera parte del trabajo de investigación se centra en la metodología de investigación, tipo de estudio, la población, muestra, métodos y técnicas a utilizar además se realiza el análisis de las

variables y los indicadores de las variables dependientes e independientes de seguridad en dispositivos móviles para el manejo de la información en PYMES.

En el cuarto se realiza el desarrollo de las políticas y se expondrá los resultados obtenidos una vez que las políticas han sido implementadas en una empresa. En el capítulo 5 de evidenciarán las conclusiones que se han podido obtener durante todo el estudio realizado.

1.1 Problema de investigación

1.1.1 Planteamiento del problema

Hoy en día cualquier empresa grande, mediana o pequeña está sujeta al uso de nuevas tecnologías, sin embargo, no ponen atención a los problemas que conlleva no contar con el hardware y software apropiado para sus procesos. Muchas empresas piensan que están exentas de ataques cibernéticos, por lo que no toman las medidas suficientes para prevenir y mitigar estos riesgos.

Dentro de una red contamos con diferentes equipos: servidores, dispositivos Wifi, routers, firewall, portátiles, impresoras, teléfonos inteligentes y otros dispositivos capaces de conectarse con una dirección IP. La gran mayoría de las empresas ofrecen protección a los equipos que se encuentran conectados a la red a través de medios físicos, pero los dispositivos móviles que se encuentran conectados mediante la red inalámbrica no les prestan las mismas medidas de seguridad por lo que quedan expuestos a posibles ataques, comprometiendo toda la información que en ellos se almacena y se maneja para las actividades cotidianas.

Cuando se realiza la instalación de programas en los dispositivos móviles, los usuarios no son conscientes de las acciones que va a realizar el programa que se están descargando sobre el dispositivo móvil, ni de los problemas que puede implicar esta acción. Las empresas más afectadas resultan ser las medianas y pequeñas empresas debido a que no prestan las suficientes medidas de seguridad a la información que se obtiene o se ingresa a través de los dispositivos móviles.

Los estafadores usan aplicaciones falsas o fraudulentas para robar los datos personales a los usuarios, dichas aplicaciones son instaladas de forma normal por el usuario sin saber que existe un delincuente que busca robar su información. Una vez instaladas en los dispositivos móviles la aplicación presenta un formulario en donde le solicita al cliente llenar los datos mediante un formulario al dar clic en enviar estos son enviados en texto plano al servidor del atacante.

Un ejemplo de una aplicación maliciosa es MyEtherWallet falsa, esta aplicación filtra información robada y la publica, exponiendo las claves privadas y cuentas de las víctimas. Así como MyEtherWallet existen un sin número de aplicaciones que buscan robar la información aprovechando la falta de seguridad de los dispositivos móviles. Con la ayuda de políticas de seguridad en dispositivos móviles para el manejo de la información se podrían minimizar este tipo de ataques y mantener segura la información de las empresas. (Stefanko, Lukas, 2018)

Los trabajos realizados hasta el momento se han enfocado en políticas de seguridad en general pero no se han centrado en el problema que se está presentando con la información que se tiene o se maneja a través de los dispositivos móviles dentro de las PYMES.

1.2 Formulación del problema

¿Cómo la implementación de políticas de seguridad en dispositivos móviles para PYMES reducirá los riesgos sobre la información que se maneja a través de los mismos?

1.2.1 Sistematización del problema

- ¿Cuáles son las normas para desarrollar políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES?
- ¿Cuáles son los problemas más comunes de no contar con políticas de seguridad en dispositivos móviles para el manejo de la información para PYMES?
- ¿Cuál es la metodología que se utilizará para desarrollar una propuesta de políticas de seguridad en dispositivos móviles para PYMES para el manejo de la información?
- ¿En qué caso de estudio se aplicarán las políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES?
- ¿Cuáles son los resultados una vez aplicadas las políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES?

1.3 Justificación

Los dispositivos móviles ofrecen varias ventajas dentro de la empresa como portabilidad, disponibilidad, captura de datos en tiempo real. Por ejemplo, a través de la portabilidad se puede tener una comunicación digital desde cualquier parte sin estar dentro de la empresa, lo que genera una participación más activa de los empleados. En cuanto a la disponibilidad los dispositivos móviles ayudan a la visualización de cualquier información sobre productos o servicios en el

momento que se requiera. Mientras a lo que se refiere a la captura de datos en tiempo real, los dispositivos móviles nos permiten capturar la información y enviar los datos recolectados a cualquier sistema que sea necesario. (Siniša Husnjak, 2016)

Otra de las razones que hacen a las redes inalámbricas tan populares, es que se puede tener acceso a la red sin la necesidad de cables, convirtiéndose en una ventaja y desventaja a la vez. En este aspecto no se puede garantizar la seguridad de la información cuando se usa el aire como medio de transmisión de los datos y existen muchos delincuentes que buscan explotar las vulnerabilidades que se presentan en este medio de transmisión.

Existe un estudio del 2016 realizado por Weplan en el cual se notificó que el 93.5 % del consumo de internet móvil se realiza a través de conexiones WIFI. Además, también se indica que, de las 13.839.445 líneas en todo el país, solo el 34.97 % están sujetas a un plan celular con datos para navegar. (Protecseguros Lola, 2016)

Otra desventaja evidente es la pérdida o robo de los dispositivos móviles, en el 2017, tomando en cuenta las bases de datos de las operadoras telefónicas, la Agencia de Regulación y Control de las Telecomunicaciones, registró 305.020 reportes de robo o pérdidas de celulares, laptops y tabletas, un promedio de 852 casos por día en el país; en el 2016 fueron reportados 971 casos cada 24 horas.

La problemática que se tiene actualmente en las empresas es la falta de seguridad cuando se usan los dispositivos móviles para realizar cualquiera de las tareas antes mencionadas debido a que no existe políticas de seguridad para la información que se maneja a través de los dispositivos móviles, y los atacantes pueden usar los dispositivos móviles como medio para vulnerar la seguridad de la información de la empresa.

Tomando como base lo antes mencionado y debido a la definitiva importancia de su estudio, surge la necesidad de desarrollar la presente investigación, tomando como unidad de análisis las PYMES, en las cuales se han identificado diferentes problemas cuando hacen uso de dispositivos móviles para el manejo de la información.

Dentro de las instituciones no se cuenta con políticas de seguridad en dispositivos móviles para el manejo de la información. Toda la información puede llegar a verse comprometida debido al aumento de amenazas que aprovechando cualquiera de las vulnerabilidades existentes, pueden

someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente, otro riesgo es la pérdida de estos dispositivos o el robo de los mismos que son los problemas del día a día en nuestro país.

1.4 Objetivos de la investigación

1.4.1 General

Realizar una propuesta de políticas de seguridad en dispositivos móviles para el manejo seguro de la información en PYMES

1.4.2 Específicos

- Realizar una recopilación de la situación actual de la seguridad de la información de la empresa.
- Seleccionar la metodología para el desarrollo de las políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES.
- Identificar mediante el análisis de riesgo, las amenazas y vulnerabilidades a las que están expuestas los dispositivos móviles de la institución en el caso de estudio planteado.
- Elaborar las políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES.
- Aplicar las políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES en la empresa TELECOMEXPERT.

1.5 Marco hipotético

Al aplicar las políticas de seguridad desarrolladas para el uso de dispositivos móviles sí permitirá manejar la información de las PYMES de forma segura.

CAPÍTULO II

2. MARCO TEÓRICO

En este capítulo se describe sobre los antecedentes del uso de los dispositivos móviles. Se realiza una descripción acerca de las PYMES, conceptos y también se hace un resumen de la participación de las PYMES en Ecuador. También se realizó la investigación de la evolución de los dispositivos móviles, sus aplicaciones y las tecnologías que se han empleado a lo largo de los años. Para entender sobre la relación entre los dispositivos móviles y la información se ha investigado como se maneja la información de forma general dentro de las empresas.

Para finalizar también describe sobre los conceptos de seguridad informática y su importancia, además de las normas NTE INEN ISO IEC 27001-2011 y NTE INEN-ISO IEC 27002 que son utilizadas por las empresas y las que se encuentran vigentes en el Ecuador. Se presenta un cuadro comparativo de las normas en donde se llegó a evidenciar que no hay políticas dirigidas a los dispositivos móviles específicamente para el manejo de la información para PYMES.

2.1 Antecedentes del problema

Los sistemas de comunicación inalámbricos han evolucionado de forma constante en las últimas décadas. Los avances tecnológicos en este tipo de comunicaciones han sido muy notables y actualmente proporcionan comunicaciones más eficientes rompiendo las conexiones físicas, garantizando la movilidad de los usuarios y la capacidad de conexión de múltiples dispositivos como laptop, Tablet, Smartphone, y cualquier dispositivo que pueda conectarse por una red WIFI.

Los dispositivos móviles tienen una gran cantidad de funcionalidades aparte de llamar y enviar mensajes, actualmente permiten responder correos electrónicos, generar requerimientos en tiempo real, recopilar información, etc., Esto ayuda a que las personas se vuelvan más productivas al momento de resolver problemas en el menor tiempo posible, generando una mayor producción en beneficio de la empresa. Sin embargo, de la misma forma en que los dispositivos móviles pueden beneficiar a la empresa en general, también puede constituirse en un problema.

Según Betancur y Erazo(2015), anteriormente las amenazas se propagaban usando bluetooth, SMS, y muchas veces a través de técnicas de ingeniería social; en la actualidad los Smartphone u

otros dispositivos como las tabletas, son mucho más vulnerables de ser atacados, tal como lo informan compañías de antivirus, donde han aumentado las amenazas contra aplicaciones que tienen los dispositivos móviles. Una de las causas principales es el desconocimiento del usuario para proteger su dispositivo, ya que muchas veces se enfocan a utilizar aplicativos que se encuentran instalados relacionados con correo electrónico, juegos, servicios de mensajería, redes sociales, multimedia, entre otros, pero son muy pocos los que toman conciencia sobre las medidas de seguridad para la protección de la información.

Los usuarios de dispositivos móviles pueden ser en cualquier momento víctimas de un ataque, la mayor parte de los virus troyanos llegan vía mensajes SMS, aplicaciones falsas y malware espía. El trabajo del autor menciona que adicionalmente a los ataques informáticos de virus también se añade la poca precaución que tienen las personas respecto a lo que instalan en sus dispositivos móviles, siendo un problema la instalación de aplicaciones sin tener el conocimiento base de donde proviene y si es seguro para el dispositivo.

Muchas actividades se realizan sin contar con las debidas medidas de seguridad apropiadas para mantener a salvo toda esta información. De hecho, tal como lo menciona Castro, Guantiva, y Zárate (2015) es posible evidenciar la existencia de varios factores de riesgo cuando una empresa utiliza dispositivos móviles.

En base a los datos obtenidos de un estudio de medianas y pequeñas empresas se dice que en el Ecuador el 4.39 % de todas las empresas son PYMES dando un total de 21864 números de establecimientos. A nivel nacional el 86% de pequeñas, 96 % de medianas tienen RUC. En el caso de Riobamba, el total de micro, pequeña, mediana y grande empresa es de 8071 empresas.

Por lo que tomando como base el estudio de diagnóstico de aplicación de las NTIC en las PYMES de Riobamba 2015 se tienen que 3.72 % de las empresas son pequeñas que son 302 pequeñas empresas y el 0.64% son medianas que son 52 empresas medianas, dando un total de PYMES de 354 en la ciudad de Riobamba. (Slusarczyk, María, 2015)

Tabla 1-2: Número de establecimientos Riobamba

TIPO DE EMPRESA	PORCENTAJE	NÚMERO DE ESTABLECIMIENTOS
Micro	95,42	7701
Pequeña	3,75	302
Mediana	0,64	52
Grande	0,2	16 (3)[5]

Fuente: (INEC, Censo Nacional Económico, 2010)

A partir de lo expuesto previamente, se realizará una propuesta de políticas de seguridad en dispositivos móviles para el manejo de la información en PYMES, con el fin de proteger la información ante las amenazas a las cuales están expuestos los dispositivos móviles, y de esta manera dar un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes de la empresa.

2.2 Bases teóricas

2.2.1 Las PYMES

Existen una diversidad de criterios para definir y de este modo clasificar a las empresas como micro, pequeñas, medianas y grandes, estos criterios son diferentes, dependiendo del país o entidad que las define y clasifique. Por ello resulta interesante precisar si las empresas presentan características que puedan ser tomadas como elementos que permitan establecer una diferenciación entre grande, pequeña, micro o mediana empresa. (Saavedra, María; Hernández, Yolanda, 2008)

Según Saavedra & Hernández se ha llegado a una clasificación de las PYMES en donde separan a las empresas grandes de las MIPYME, dada por el crecimiento de la demanda en donde al llegar a cierto nivel es posible que pasen de ser pequeñas a grandes.

2.2.2 Historia de las PYMES en el ecuador

En Ecuador, de acuerdo con el actual régimen legal: la ley de la Comunidad Andina de MIP (micros y pequeñas empresas) y ME (medianas empresas) la Ley de Fomento Artesanal y la Ley de Fomento de la Pequeña Industrias, se estructuró una clasificación en la cual, se destaca los principales conceptos relacionados con las micros, pequeñas, medianas y grandes empresas. De

acuerdo a su tamaño, las empresas tienen las categorías siguientes: (Soriano, Barbara; Pinto, César, 2006)

- **Microempresas:** emplean hasta 9 trabajadores, y sus tramos de ingresos son de hasta 100 mil dólares.
- **Pequeña Industria:** puede tener hasta 49 obreros
- **Mediana Industria:** alberga de 50 a 199 obreros, y el tramo de ingresos no sobrepasa los 5 millones de dólares.
- **Grandes Empresas:** son aquellas que tienen más de 200 trabajadores y más de 5 millones de dólares en tramos de ingresos.

Las PYMES se caracterizan por el uso intensivo de la mano de obra, escaso desarrollo tecnológico, baja división del trabajo, pequeño capital, baja productividad e ingreso, reducida capacidad de ahorro y limitado acceso a los servicios financieros y no financieros existentes.

Sin embargo, en términos de programas de desarrollo, programas de financiamiento, o asesorías para las pequeñas y medianas empresas a nivel internacional, muchos gobiernos dejan en segundo plano a este sector y se concentran en el apoyo a las grandes empresas, claro ejemplo se dio en la última crisis financiera en Estados Unidos, dónde el gobierno intervino en los grandes bancos, pero no en los pequeños debido a que las grandes empresas representan mucho más en PIB (Producto interno bruto) de una economía y resulta más complejo ayudar a varias entidades que una sola. (Enroke, 2019)

Las PYMES juegan un papel de gran importancia dentro del desarrollo de toda economía debido a su relación e incidencia en la generación de empleo, y crecimiento económico. De esta forma las PYMES se relacionan directamente con el desarrollo económico en todas las regiones del país. Si bien al analizar los factores de crecimiento económico se identifican como responsables a las grandes empresas, en realidad los resultados indican que el crecimiento depende en buena medida del desempeño de sus PYMES. (Redacción EKOS, 2012).

El desarrollo de la economía del país se debe a la generación de empleo que ofrecen las pequeñas y medianas empresas. Según el Banco Central en el Ecuador las empresas que registran mayor parte de actividad económica son las provincias de Pichincha y Guayas.

En base a cifras que maneja la Superintendencia de compañías y seguros las PYMES tienen participación más alta en el sector comercial con un 26.80 % las pequeñas empresas y el 36.23% las medianas empresas. (OCDE-CEPAL, 2013)

COMERCIO			INDUSTRIA FACTURERA			TRANSPORTE Y ALMACENAMIENTO		
								
26.80 %	**36.23 %**	**29.54 %**	**8.81 %**	**13.18 %**	**10.08%**	**9.70 %**	**6.82 %**	**8.87 %**
Pequeña	Mediana	Total general	**Pequeña**	Mediana	Total general	**Pequeña**	Mediana	Total general
ACTIVIDADES AGROPECUARIAS			**CONSTRUCCIÓN**			**ACTIVIDADES ADMINISTRATIVAS Y DE APOYO**		
								
6.40 %	**12.36 %**	**8.13 %**	**7.92 %**	**6.16 %**	**7.41 %**	**6.48 %**	**5.10 %**	**6.08 %**
Pequeña	Mediana	Total general	**Pequeña**	Mediana	Total general	**Pequeña**	Mediana	Total general
ACTIVIDADES INMOBILIARIAS			**INFORMACIÓN Y COMUNICACIÓN**			**OTROS (MENOS DE 3 %)**		
								
5.99 %	**2.48 %**	**4.97 %**	**4.17 %**	**2.33 %**	**3.64 %**	**23.73 %**	**15.33 %**	**21.29%**
Pequeña	Mediana	Total general	**Pequeña**	Mediana	Total general	**Pequeña**	Mediana	Total general

Figura 1-2: Participación de las PYMES en el Ecuador
Fuente: (Superintendencia de compañías y seguros, 2013)

2.2.3 Evolución de los dispositivos móviles, aplicaciones y tecnología

Un dispositivo móvil se describe como un aparato tecnológico relativamente pequeño que posee capacidad de procesamiento, conexión a una red de forma inalámbrica y poseen una memoria

limitada. Está diseñado para realizar funciones específicas. A lo largo de los años los dispositivos móviles han tenido una evolución significante. La historia empieza desde los años 1940 con la creación de los primeros equipos de comunicación y hoy en la actualidad existen diversos dispositivos móviles accesibles en el mercado como: PC portables, PocketPC, tabletas, celulares etc. (Baz, Arturo; Ferrerira, Irene; Álvarez, María; García, Rosana, 2013)

Los dispositivos móviles se componen de varios elementos, los tres elementos principales que son: hardware, aplicaciones y tecnologías de acceso y redes. A continuación, se describe la evolución de estos componentes en donde se muestra la evolución en base a la historia: desde antes del año 1970 en donde los aparatos tenían características como gran tamaño, peso y poca duración de la batería. En los años 80 empieza la comercialización de los primeros celulares básicos, además de la primera portátil. Desde los años 90 se cuentan con dispositivos con teclado QWERTY y GPS. Además, los portátiles ya contaban con puertos USB.

Desde el año 2000 los aparatos móviles poseían pantalla a color, internet y bluetooth. La velocidad de los computadores mejoró, se integra WIFI y puertos HDMI. Para los años 2010 – 2012 existe una diversificación masiva de fabricantes, aparecen tabletas con sistemas operativos con grandes mejoras para los usuarios. En el futuro se presume que los dispositivos tendrán un menor tamaño, pero con mucha más capacidad de almacenamiento y procesamiento. **(Ver tabla 2-2)**

Tabla 2-2 Evolución de los dispositivos móviles

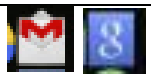
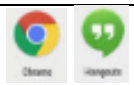
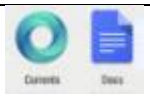
EVOLUCIÓN DE LOS DISPOSITIVOS MÓVILES						
ANTES DE 1970	**70'S**	**80'S**	**90'S**	**00'S**	**2010-2012**	**FUTURO**
Policía y militares usaban dispositivos sin cables para comunicarse. Los aparatos eran muy pesados y con muy poca duración de batería	Se crea el primer auricular portátil y comienza la venta de los buscapersonas. Primeros ensayos públicos de teléfonos celulares (Motorola)	Comercialización de los primeros celulares básicos con pantalla en blanco y negro. Venta del Osborne 1, como primer portátil, aunque requería de energía eléctrica, y del Grid Compas, que era plegable	Se venden los PDA y los dispositivos de mensajería. Se crean los celulares con teclado QWERTY, mp3 y GPS. Computadoras portátiles con puertos USB y mouse táctil	Comienza la revolución de los dispositivos móviles, con aparatos de pantalla a color, internet, bluetooth integrado Computadores rápidos con puertos USB, HDMI, WIFI	Diversificación masiva de fabricantes. Aparecen las tablets y los sistemas operativos pugnan por un lugar en el mercado. Las computadoras tienen una gran potencia	Dispositivos con un menor tamaño, pero mayor capacidad de almacenamiento. La computadora se utiliza sobre muy diversas superficies. Equipos multitareas cada vez más rápidos
						

Fuente: (Macías, María, 2016)

Para que los dispositivos móviles sean tan utilizados por las personas han sido diseñados y desarrollados con programas que permiten realizar diferentes tareas que ayudan a los usuarios a realizar actividades diarias y simplificar el manejo de la información. Estas aplicaciones suelen ser desarrolladas por los operadores celulares o por terceros. Desde los años 90 se comenzó con el uso de aplicaciones móviles. Estas aplicaciones en un principio fueron off-line. En cambio, en el año 2000 aparecieron las primeras aplicaciones on-line con sincronización con la red ej.: aplicaciones bancarias, correo electrónico.

En el 2010 se cuenta con tiendas de aplicaciones móviles de las empresas como Play store, Apple store en donde se pueden encontrar aplicaciones de entretenimiento y ocio (juegos, reproductores, libros, chat), información (correos, noticias, revistas), corporativas (empresariales), herramientas (calendarios, calculadoras, alarmas, conversores), etc. **(ver tabla 3-2)**

Tabla 3-2: Evolución de aplicaciones móviles

EVOLUCIÓN DE APLICACIONES MÓVILES						
ANTES DE 1970	**70'S**	**80'S**	**90'S**	**00'S**	**2010-2012**	**FUTURO**
			Primeras aplicaciones móviles off-line, sincronización por medio físicos. Contactos, calculadora, alarmas, calendarios son las "apps" más comunes	Primeras aplicaciones móviles on-line con sincronización a la red. Se desarrollan sitios para móviles Aparecen aplicaciones bancarias, correo electrónico	Aparecen las tiendas de aplicaciones. Aparecen las versiones móviles de las empresas	Aplicaciones que faciliten las actividades diarias, centros de salud y alertas Personalización de aplicaciones móviles empresariales
						

Fuente: (Macías, María 2016)

La tecnología de acceso y redes es muy importante para los dispositivos móviles. A través de estas es posible la comunicación directa y se pueden comunicar entre sí. En la actualidad las más comunes son: red celular, wifi, bluetooth, RFID. Sin embargo, estas han tenido su evolución desde los años 70 en donde los celulares transmitían mensajes cortos.

Desde l980, 1990, 2000, se cuenta con las tecnologías 1G, 2G, 3G. Estas redes permitían a los dispositivos conectarse a redes móviles. Desde la aparición del 4G se cuenta con redes móviles

de alta velocidad que permiten realizar transacciones complejas por medio de los dispositivos móviles. **(Ver tabla 3-2.)**

Tabla 4-2: Evolución de las tecnologías de acceso y redes

EVOLUCIÓN DE LAS TECNOLOGÍAS DE ACCESO Y REDES						
ANTES DE 1970	**70'S**	**80'S**	**90'S**	**00'S**	**2010-2012**	**ACTUALIDAD**
Celulares con mínima cobertura	Celulares con un alcance medio. Los celulares transmitían mensajes cortos a los buscapersonas y celulares específicos	Aparece la tecnología 1G que utilizan los celulares análogos Cobertura limitada y mucha interferencia	Segunda generación 2G, que funcionan en dispositivos digitales Redes más rápidas que permiten sincronizar correos. Aparece el WIFI para conectar a los dispositivos sin cables	Aparece las redes 3G y 3.5G para dispositivos digitales. Las redes transmiten a grandes velocidades. Surge el RFID, mejora el WIFI Mejora el servicio de internet de las operadoras celulares	Aparecen las redes 4G en los dispositivos digitales. Redes móviles de alta velocidad Conexión continua para transacciones complejas	Tecnologías cada vez más avanzadas y de mayor velocidad, con soporte más avanzado, incluyendo 5G. Menor costo, mayor velocidad y mejor cobertura.
						

Fuente: (Macías, María, 2016)

2.3 Manejo de la información en pymes

Las empresas sean grandes pequeñas o medianas empresas acumulan una gran cantidad de información. Todos estos datos deben ser llevados, almacenados y manejados de una manera adecuada para poder tomar decisiones que ayuden al crecimiento de las mismas. Contar con datos exactos y precisos podría resultar muy valioso para las empresas ya que hoy en día estos se consideran como un activo más. Es desde aquí que se toman decisiones y se proyectan objetivos o metas. (Reporte Digital, 2019).

El objetivo principal del manejo apropiado de la información es apoyar la toma de decisiones de los altos mandos de las empresas para el crecimiento o expansión de estas. En los últimos años ha existido un crecimiento en la computación móvil, los dispositivos móviles son usados para facilitar las labores y actividades diarias a cualquier momento desde cualquier lugar. Todo esto se puede evidenciar en las pequeñas y medianas empresas también.

Se determina que gracias al gran auge de la movilidad y la heterogeneidad de los dispositivos móviles dan lugar a nuevos escenarios que favorecen la cooperación entre los individuos mediante el uso generalizado y ubicuo de dichos dispositivos. (D'Angelo, Gabriele; Ferretti, Stefano; Ghini, Vittorio; Panzieri, Fabio, 2014)

Este escenario representa un "ecosistema digital", que constituye la articulación dinámica y sinérgica de comunidades digitales que consiste en la interconexión, interrelación e interdependencia de los recursos digitales y un ambiente digital que interactúa recíprocamente como una unidad funcional que se une a través de infraestructura tecnológica, acciones, transacciones y flujo de información (Hadzic, M.; Chang, E.; Dillon, T., 2007).

El Ecosistema Digital ofrece un modelo de Oferta y Demanda para el mercado digital. La Oferta está compuesta por la Infraestructura y los Servicios que son ofrecidos por los operadores, mientras que la Demanda se genera por parte de los usuarios que usan las Aplicaciones. La visión de este modelo describe que es necesario estimular tanto la Oferta como la Demanda de servicios digitales para lograr un círculo virtuoso que se retroalimente positivamente como se representa en la figura 2-2. (Guerrero, Carlos, 2014)

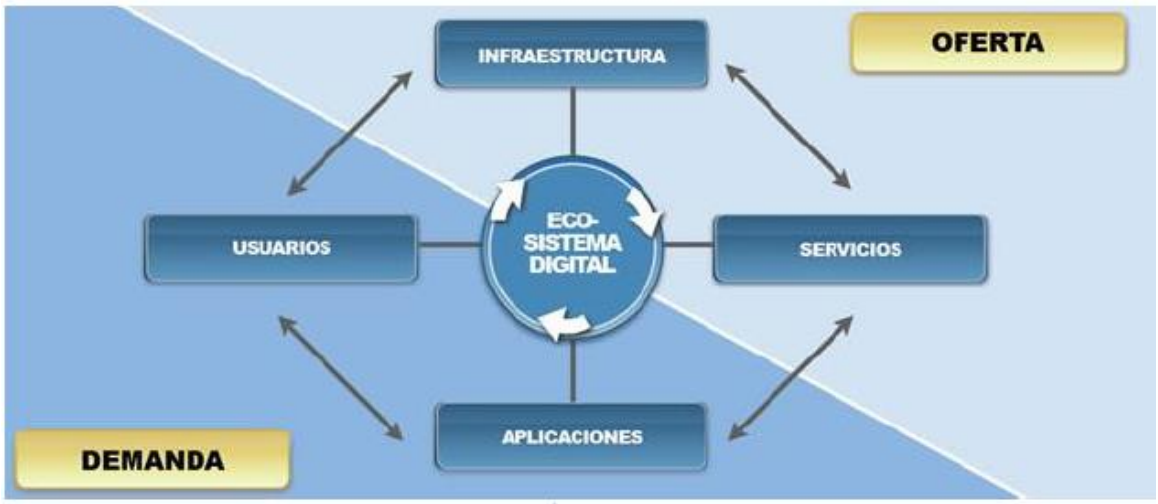


Figura 2-2: Ecosistema Digital
Fuente: (Guerrero, Carlos, 2014)

De esta forma, se puede determinar que los dispositivos móviles y su interacción entre sí puede ser entendida como un "ecosistema digital" donde, a través de las redes de comunicación, los "organismos digitales" se relacionan entre sí utilizando dispositivos móviles que les permiten

intercambiar recursos entre ellos (información) y proveer una serie de servicios que otros "organismos digitales" pueden consumir en forma remota en cualquier momento.

2.4 Seguridad informática, conceptos e importancia

La seguridad informática se basa en mantener protegida la infraestructura computacional y todo lo relacionado. Para esto existen estándares, protocolos, métodos, herramientas y leyes para minimizar las posibles amenazas que pueden afectar su funcionalidad. Ya sea por corrupción, acceso indebido e incluso hurto o robo o eliminación de la información.

La confidencialidad, integridad y disponibilidad son los objetivos de la seguridad informática y se enfocan en proteger los activos de la empresa. Estos activos comprenden desde software, bases de datos, metadatos, archivos y todo lo que la organización valore como activo. (Baca, Gabriel, 2016)

La integridad como propósito garantizar que la información no haya sido modificada o alterada por personas no autorizadas.

La confidencialidad busca que solo la persona o personas autorizadas tengan acceso a cierta información, tanto en su lugar de almacenamiento, sistemas, dispositivos, dentro de la red que reside o durante su procesamiento y manejo o hasta llegar al destino final.

La disponibilidad tiene como propósito que la infraestructura física y tecnológica que permite el acceso a la información estén disponibles al momento que cualquier usuario autorizado la necesite. También hace referencia a la capacidad que deben tener los sistemas para recuperarse frente interrupciones del servicio (Vieites, Alvaro, 2017).

La seguridad informática en dispositivos móviles se ha convertido en un asunto muy importante debido al incremento de ataques recibidos y las consecuencias que estos tienen. Los ataques vienen incentivados por la popularización de los dispositivos móviles, el aumento de información personal confidencial que almacenan y las operaciones realizadas a través de ellos, como por ejemplo operaciones bancarias, por lo tanto, se hace necesario conocer: cuáles son las vulnerabilidades que presentan los dispositivos móviles. (Sheldon, Robert, 2012)

2.4.1 Conceptos de seguridad informática

En primer lugar, es importante señalar que existe cierta diferencia entre preservar documentos y la seguridad informática. El primer término se refiere al conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica, así como la protección del contenido intelectual de documentos de archivo adquiridos, con objeto de lograr en ellos una secuencia de existencia a largo plazo continua, perdurable, estable, duradera, ininterrumpida, inquebrantada, sin un final previsto (Interpares, 2019).

En tanto la seguridad informática se define como el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos (Voutssas, M., 2010).

2.4.2 Políticas de seguridad informática

Una política de seguridad es un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico (Dussan, Ciro, 2006).

Las políticas de seguridad para dispositivos móviles definen la manera en que los empleados pueden usar smartphones y tabletas para actividades relacionadas con la empresa. Las compañías deben dejar claros a sus empleados los riesgos asociados con estos dispositivos y hacerles saber que tienen una responsabilidad a la hora de mitigar esos riesgos. La política de seguridad para móviles para las empresas enmarca el alcance de esa responsabilidad y jugar un rol clave en la estrategia general de protección de información sensible y propiedad intelectual (Sheldon, Robert, 2012).

Las organizaciones van de la mano con la tecnología; y su infraestructura de red es un tema importante que no se debe subestimar dado que las fallas de seguridad provienen del interior de la red, es aquí donde la mitigación de ataques es parte de la seguridad y esta se relaciona con la protección de los recursos y la información a través de la implementación de políticas de seguridad (Vieites, Alvaro, 2017).

El análisis y evaluación de riesgos permite a las compañías tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que deben hacer para mejorar.

En el mundo de las certificaciones de calidad y en el cumplimiento de estándares internacionales que permitan acceder a nuevos mercados o se brinden nuevos valores agregados que marquen una diferenciación o ventaja competitiva, las políticas definen la forma de hacer las cosas, el mejoramiento de los procesos.

Reconocer las limitaciones y restricciones de la tecnología es un buen paso para entender la importancia de las políticas. En este sentido podemos definir la política como un instrumento gerencial que traza una dirección predeterminada describiendo la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los colaboradores de la empresa la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.

Aunque las políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes va dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas. Estas son obligatorias y pueden considerarse a una ley propia dentro de la organización.

Para crear una política de seguridad será necesario basarse en las normas ISO que son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

2.4.3 Objetivos de seguridad informática

El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. Para ello utilizaremos estructuras organizacionales técnicas, administrativas, gerenciales o legales.

El objetivo secundario de la seguridad informática –se subraya que es de especial interés desde el punto de vista de la preservación documental– consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad. Este concepto varía de acuerdo a distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada.

2.4.4 Seguridad en dispositivos móviles

Los dispositivos móviles han experimentado una intensa evolución en los últimos años. Los primeros dispositivos eran de un tamaño grande, en la actualidad son de tamaño muy pequeño con diferentes características. Las características de los dispositivos actuales son similares a las de una computadora portátil.

En la actualidad existen una variedad de amenazas, ataques y/o riesgos para los smartphones: malware, phishing, fraudes y robo o pérdida del dispositivo. Cada uno de estos riesgos pueden perjudicar al usuario de diferentes maneras exponiendo la información o los datos que se almacena en los mismos. Las características con las que cuentan y han evolucionado los dispositivos móviles son:

- Un hardware que poseen grandes características, con muchos sensores y conexión a red inalámbricas.
- Un sistema operativo, los más utilizados son: Android, IOS, Windows 10 Mobile, BlackBerry OS, Symbian, Firefox OS, Ubuntu Touch.
- Aplicaciones completamente integrado en el sistema y muy intuitivo, lo que facilita las transacciones tanto a los usuarios como a los desarrolladores.

Gracias a las nuevas funcionalidades que ofrecen los sistemas operativos para móviles, las aplicaciones y las características físicas que se han creado sobre ellos, los dispositivos móviles acaban almacenando gran cantidad de datos, generalmente confidenciales como información personal, como pueden ser cuentas bancarias, documentos o imágenes, etc.

Este aumento de la información personal almacenada provoca que más personas puedan estar interesadas en obtenerla de cualquier forma. Además, los sistemas operativos para móviles han incrementado los agujeros de seguridad expuestos. Por lo tanto, cuando se utiliza dispositivos móviles, es recomendable seguir unas medidas de seguridad que evite ser víctimas de los ataques mal intencionados de los ladrones de internet llamados hackers.

La seguridad en los móviles personales y/o los de las Pymes sin duda apuesta a una mayor concientización de los usuarios. En lo correspondiente a la toma de conciencia sobre la prevención, la toma de medidas preventivas y acciones tendientes a la seguridad de la información es el primer paso para propender por un camino seguro hacia el mejor uso de las tecnologías. Cuando sean redes, como las de bibliotecas, aviones, autobuses, trenes, aeropuertos, hoteles, entre otras, el peligro está en los otros, puesto que se supone el gestor de la red WiFi es seguro. Sin embargo, depende de cada usuario que las claves y los datos privados estén a salvo de manos ajenas.

2.4.5 Amenazas informáticas

Los primeros virus informáticos surgieron como experimentos en universidades, juegos, o simplemente con el propósito de molestar, pero no directamente con el objetivo de causar daños en los equipos informáticos. En la actualidad la propagación del malware resulta mucho más rápida, sobre todo gracias al uso de internet. Además, ahora los virus no buscan en la mayoría de los casos la notoriedad, sino más bien todo lo contrario: permanecer ocultos en el sistema sin que la persona usuaria sepa que su ordenador está infectado.

Los virus o amenazas consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma. Entre ellas se identifica como las principales de acuerdo a (Granger, Saah, 2001):

El advenimiento y proliferación de "malware" o "malicious software", programas cuyo objetivo es el de infiltrarse en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.

La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.

La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.

El acceso no autorizado a conjuntos de información.

La pérdida, destrucción o sustracción de información debida a vandalismo. Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber–criminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.

Los "phishers", especializados en robo de identidades personales y otros ataques del tipo de "ingeniería social".

Los "spammers" y otros mercadotecnistas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.

La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterramiento, des magnetización, ralladura o descompostura de dispositivos de almacenamiento, etcétera.

La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.

El advenimiento de tecnologías avanzadas tales como el cómputo quantum, mismas que pueden ser utilizadas para desencriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales

2.4.6 Vulnerabilidades informáticas

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Se Puede diferenciar tres tipos de vulnerabilidades según cómo afectan al sistema (Quiroz & Macías, 2017):

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche. Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa. Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Esto ha llevado a que empresas como Microsoft dispongan de departamentos dedicados exclusivamente a la seguridad, como es Microsoft Security Response Center (MSRC). Sus funciones son, entre otras, evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, y preparar y divulgar revisiones y boletines de seguridad que respondan a estos informes. Para ello clasifica las vulnerabilidades en función de su gravedad, lo que nos da una idea de los efectos que pueden tener en los sistemas: críticas, importantes, moderadas y bajas.

2.4.7 Elaboración de la política

Para elaborar una política de seguridad de la información es importante tomar en cuenta las exigencias básicas y las etapas necesarias para su producción.

1. Exigencias de la Política: La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado en seguridad de los profesionales involucrados con su aplicación y comprometimiento. Es importante considerar que para la elaboración de una política de seguridad institucional se debe:

a. Integrar el comité de seguridad responsable de definir la política (equipo multidisciplinario)

b. Elaborar el documento final (preocupaciones de la administración, atribución de las responsabilidades de las personas involucradas, legislación y cláusulas contractuales, prevención contra amenazas, educación y formación en seguridad de la información.)

c. Hacer oficial la política una vez que se tenga definida (aprobación por parte de la administración, mecanismos de comunicación efectiva a socios, empleados, proveedores y clientes de la empresa).

2. Etapas de producción de la política: Elaborar una política es un proceso que exige tiempo e información. Es necesario saber cómo se estructura la organización y cómo son dirigidos en la actualidad sus procesos (Dussan, Ciro, 2006).

2.4.8 Normas para las pymes

Existen normas internacionales sobre seguridad de la información que pueden ser aplicadas a las PYMES. La norma internacional ISO/IEC 27000:2012 es una norma internacional para cualquier tipo de organización ya sea grande o pequeña, privada o pública. En esta norma se recopila las mejores prácticas sobre Gestión de la seguridad de la Información.

Norma ISO 27001 tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información y también promueve la mejora continua a través del modelo PDCA (Plan-Do-Check-Act).

Norma ISO 27002 constituye una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. (López & Ruiz, 2019)

Uno de los objetivos es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información. La ISO/IEC 27002:2015 está organizado en base a 14 dominios, 35 objetivos de control y 114 controles. (ISO 27002, 2019)

Norma 37000-2016 esta normativa está enfocada sobre una serie de medidas que se utilizan para que las empresas implementen para mejorar su capacidad de prevención, detección y tratamiento del riesgo de soborno.

Ahora el definir una política de seguridad significa incluir el marco general y los objetivos de seguridad de la información de la organización, teniendo en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad y es ahí donde los controles de la ISO/IEC 27002:2015 tiene gran relevancia.

El Estándar Internacional ISO/IEC 27002 contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

2.4.8.1 Organización de la Seguridad de la Información

Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial. (ISO 27002, 2019)

2.4.8.2 Gestión de activos

Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos. (ISO 27002, 2019)

2.4.8.3 Seguridad en recursos humanos

Antes de la contratación de un empleado – o incluso de proveedores – es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones. (ISO 27002, 2019)

2.4.8.4 Seguridad física y del medio ambiente

Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales. (ISO 27002, 2019)

2.4.8.5 Seguridad de las operaciones y comunicaciones

Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones. (ISO 27002, 2019)

2.4.8.6 Control de acceso

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera. (ISO 27002, 2019)

2.4.8.7 Adquisición, desarrollo y mantenimiento de sistemas

Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos. (ISO 27002, 2019)

2.4.8.8 Gestión de incidentes de seguridad de la información

Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil. (ISO 27002, 2019)

2.4.8.9 Gestión de continuidad del negocio

Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas. (ISO 27002, 2019)

2.4.8.10 Conformidad

Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios. (ISO 27002, 2019)

Tabla 5-2: Resumen de los dominios de control de la norma ISO 27002

RESUMEN DE LOS DOMINIOS DE CONTROL DE LA NORMA ISO 27002	
Dominios	Control
Política de seguridad	Proporcionar orientación y apoyo a la alta gerencia para la seguridad de la información, de acuerdo con las leyes actuales
Organización de la seguridad de información	Gestionar la información dentro y fuera de la organización
Gestión de activos	Proteger los activos de la organización
Seguridad relativa a los recursos humanos	Asegurar que empleados, contratistas o terceras personas tengan conocimiento de las políticas que tiene la organización.
Seguridad física y del ambiente	Asegurar las instalaciones de las áreas de procesamiento de información y los recursos tecnológicos de la organización.
Gestión de comunicaciones y operaciones	Asegurar la operación correcta y segura de los medios de procesamiento de Información
Control de acceso	Controlar el acceso a la información
Adquisición, desarrollo y mantenimiento de los sistemas de información	Asegurar los sistemas de información que tiene la organización
Gestión de incidentes en la seguridad de la información	Establecer lineamientos para prevenir incidentes de pérdida de información
Gestión de la continuidad del negocio	Asegurar que existan planes de continuidad del negocio
Cumplimiento	Asegurar el cumplimiento de requisitos legales de seguridad

Fuente: (Caiza & Bolaños, 2014)

2.5 Cuadro comparativo entre ley ecuatoriana y la norma 27002

Como se puede observar en la tabla 6-2 Cuadro comparativo de normas, se realizó una comparación entre las normas NTE INEN-ISO/IEC 27001:2015 y la norma NTE INEN-ISO IEC 27002. Estas normas abarcan las leyes vigentes en el Ecuador en donde se puede evidenciar que en las normativas analizadas no contemplan normas para el manejo de información a través de dispositivos móviles orientado a PYMES.

Tabla 6-2: Cuadro comparativo de entre Ley Ecuatoriana y la norma 27002

Ley o Normativa Ecuatoriana	Articulo	Control de la norma NTE INEN-ISO/IEC 27002:2011
Constitución Política del Ecuador	Artículo 325-333	A.7.1.1 Investigación de antecedentes A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gestión A.7.2.2 Concienciación, educación y capacitación en seguridad de la información A.7.2.3 Proceso disciplinario A.7.3.1 Responsabilidades ante la finalización o cambio
Política de seguridad de información del Ministerio de Transporte y Obras Públicas (MTOP)	Artículo 2	A.5.1 Directrices de gestión de la seguridad de la información A.6.1. Roles y responsabilidades en seguridad de la información A.8.1 Responsabilidad sobre los activos A.8.3 Manipulación de los soportes
Esquema Gubernamental de Seguridad de Información (EGSI). Ley o Normativa Ecuatoriana	1. Política de seguridad de la información	A.5 Políticas de seguridad de la información
	2. Organización de la seguridad de la información	A.6 Organización de la seguridad de la información A.15 Relación con los proveedores
	3. Gestión de los activos	A.8 Gestión de activos
	4. Seguridad de los recursos humanos	A.7 Seguridad relativa a los recursos humanos
	5. Seguridad física y del entorno	A.11 Seguridad física y del entorno
	6. Gestión de comunicaciones y operaciones	A.12 Seguridad de las operaciones A.13 Seguridad de las comunicaciones

	7. Control de acceso	A.9 Control de acceso A.10 Criptografía
	8. Adquisición, desarrollo y mantenimiento de sistemas de información	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información
	9. Gestión de los incidentes de la seguridad de la información	A.16 Gestión de incidentes de seguridad de la información
	10. Gestión de la continuidad del negocio	A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio
	11. Cumplimiento	A.18 Cumplimiento
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos.	Toda la Ley	A.9.1.1 Política de control de acceso A.9.1.2 Acceso a las redes y a los servicios de red A.9.2.1 Registro y baja de usuario A.9.2.2 Provisión de acceso de usuario A.9.2.3 Gestión de privilegios de acceso A.9.2.5 Revisión de los derechos de acceso de usuario A.9.2.6 Retirada o reasignación de los derechos de acceso A.10.1.1 Política de uso de los controles criptográficos A.10.1.2 Gestión de claves A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.2 Derechos de Propiedad Intelectual (DPI) A.18.1.3 Protección de los registros de la organización A.18.1.4 Protección y privacidad de la información de carácter personal A.18.1.5 Regulación de los controles criptográficos

Fuente: (NTE INEN-ISO/IEC 27001:2015, NTE INEN-ISO IEC 27002.)
Realizado por: (Vizuete, Jenny, 2019)

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Introducción

En esta sección se determina los procedimientos y/o técnicas utilizados, para la definir las políticas de seguridad en los dispositivos móviles para el manejo de información en la empresa TELECOMEXPERT, además de la metodología y herramientas que se utilizaron para el desarrollo de este proyecto de tesis.

3.1.1 Diseño de estudio

El presente trabajo investigativo es cuasi experimental, con el cual se da a conocer las políticas de seguridad para dispositivos móviles al momento de manejar la información en la empresa TELECOMEXPERT de la ciudad Riobamba.

Para la investigación se considera como población el personal que trabaja en la empresa. Con lo cual, por medio de la aplicación de una encuesta, se pudo conocer las principales falencias de seguridad de los dispositivos móviles las mismas que requieren de una política para contrarrestar su efecto negativo.

La muestra se tomará con el objetivo de conocer el estado de la situación actual del manejo de la información a través de los dispositivos móviles, para posteriormente realizar una evaluación de los puntos más vulnerables en cuanto a la seguridad de la información al momento de usar dispositivos móviles dentro de las PYMES.

3.1.2 Tipo de estudio

El presente trabajo es principalmente de tipo exploratorio, ya que por medio de la información recopilada se determinó las causas del problema de seguridad en los dispositivos móviles; y explicativa, debido a que por medio de la información recolectada se pudo dar forma a los problemas que padece la empresa TELECOMEXPERT y con ello se implementó políticas de seguridad orientado al uso de los dispositivos móviles.

3.1.3 Población

La población la constituye el personal que labora en la empresa TELECOMEXPERT, entre los cuales se encuentra: el administrador, personal de marketing y personal técnico.

3.1.4 Muestra

En esta investigación la muestra está constituida por toda la población.

- El número de encuestados está representado por N=11

3.1.5 Especificación del estadístico

Se supone la distribución para la población como una distribución de Chi cuadrado en el cual determinamos si la observación o la situación del escenario antes de la propuesta es igual o cambia después de entrega de la propuesta. Con un nivel de significancia del 95%, para ellos se crea una tabla con los resultados obtenidos en las encuestas aplicadas al grupo experimental.

3.1.6 Métodos

En la presente investigación se ha utilizado el método científico – 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.

3.1.7 Técnicas

La técnica que se utilizará para la presente investigación será la experimentación, la observación y la encuesta, aplicada a los diferentes actores de la investigación. Los datos que se obtengan de estas técnicas ayudarán a entender la calidad de seguridad que tienen actualmente los dispositivos en las PYMES.

Para la demostración de hipótesis será imprescindible aplicar análisis estadístico y estadística inferencial.

3.1.8 Instrumentos de evaluación

Para la presente investigación se obtendrá la información de campo a través de las siguientes técnicas como:

- La observación sistemática y no sistemática
- Entrevistas
- Análisis de riesgos
- Ingeniería social

3.1.9 Aplicación del método

Como se ha podido observar en la revisión de la literatura, los dispositivos móviles poseen una serie de propiedades que le vuelven un blanco fácil para los hackers, y por tanto, una fuente poco segura para el manejo de información importante.

Este estudio incluye una serie de políticas de seguridad dirigidas al uso de los dispositivos móviles al momento de acceder a la información que serán de aplicación necesaria a las PYMES de la ciudad de Riobamba.

La propuesta busca ser un apoyo para la empresa TELECOMEXPERT para buscar seguridad en la información que se administra por dispositivos móviles.

3.1.10 Selección de la metodología para el desarrollo de las políticas de seguridad

La metodología que se llevó a cabo está basada en las normas ISO/IEC 27001, de acuerdo a las necesidades de la empresa TELECOMEXPERT. La metodología irá de la mano con los objetivos planteados en el proyecto para su consecución.

En primer lugar, se realizará un levantamiento de la situación actual de la empresa referente a la normativa que posee la empresa en cuanto a dispositivos móviles para el manejo de la información. La salida de este proceso entregará el insumo base para poder realizar el análisis de las políticas que se necesitan desarrollar para la aplicación en la empresa.

Se realizará un análisis de riesgos en donde se obtendrán puntos claves para la creación de las políticas de seguridad en dispositivos móviles, para lo cual se procederá con la identificación de los activos y se categorizará en base a la importancia que representa cada uno para la empresa**.**

Posteriormente, con el trabajo realizado se establecerán los requisitos para la elaboración de las políticas adecuadas que garanticen la seguridad de la información a través del manejo de los dispositivos móviles.

De los procesos mencionados anteriormente se obtendrán los datos necesarios para proponer políticas que se adecúen a la realidad de la empresa TELECOMEXPERT, tomando en cuenta los lineamientos de la normativa NTE INEN-ISO/IEC 27001:2015 y NTE INEN-ISO IEC 27002.

3.1.11 Instrumentos de recolección de información

Como instrumento para la recolección de información para el presente trabajo se realizó un análisis de riesgos para la identificación de activos de la empresa en donde se realizó la categorización en base a la importancia de cada uno dentro de la empresa. A continuación, se muestra el procedimiento que se siguió en este trabajo de investigación para el análisis de riesgo y todo lo que conlleva**.**

3.1.12 Justificación de la selección del caso de estudio

Para el desarrollo del presente proyecto de investigación es necesario desarrollar un estudio en una empresa PYME que permita analizar las principales debilidades en seguridad de la

información que se presentan al momento del manejo de la información a través de dispositivos móviles.

3.1.13 Justificación de la selección de la empresa TELECOMEXPERT

La empresa TELECOMEXPERT se ha dado la oportunidad de conocer la situación actual sobre la forma en que manejan la información de la empresa a través de los dispositivos móviles, como toda empresa en el Ecuador está en la obligación de preservar su información según las normas vigentes.

Se analizó de forma general a TELECOMEXPERT con el objetivo de identificar las debilidades y fortalezas que presentan al momento de manejar la información a través de los dispositivos móviles. Para esto se utilizó la observación y encuestas al personal que labora en sus instalaciones.

El análisis FODA se realizará de acuerdo a las características de los dispositivos móviles en el uso cotidiano de las personas y las empresas al momento del manejo de la información.

Tabla 1-3: Análisis FODA Dispositivos móviles

FORTALEZAS	**DEBILIDADES**
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	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.

OPORTUNIDADES	AMENAZAS
Se presentan actualizaciones continuamente que pueden mejorar las protecciones del dispositivo. A nivel global se puede compartir información rápidamente	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 Los servicios disponibles a ser utilizados 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

Realizado por: Vizuete, Jenny 2019

3.1.14 Conclusión FODA

De los datos que se han podido recopilar en la **tabla 1-3 Análisis FODA Dispositivos móviles**, se ha podido observar que los dispositivos móviles poseen múltiples beneficios, en especial lo referente a ahorro de tiempo y accesibilidad a la información, además de poseer una amplia gama de aplicaciones cada vez más sencillas e intuitivas de utilizar. Por otro lado, el rápido crecimiento de estos dispositivos ha provocado que sean de los más vulnerables dentro de las herramientas informáticas de la actualidad, con aplicaciones muy inseguras en algunos casos y sistemas operativos que podrían ser susceptibles de ataques de hackers y piratas de la información, lo cual no es demasiado diferente de una computadora de escritorio. Sin embargo, los dispositivos ya tienen mucha similitud respecto a las computadoras portátiles y escritorio, pero con seguridades considerablemente más bajas, ya que no es normal que se instale software de seguridad, además de que se conectan a redes inalámbricas desconocidas e inseguras, y se abusa de la cantidad de aplicaciones abiertas que drenan la batería y reducen la disponibilidad del sistema.

La tecnología de los dispositivos móviles avanza a grandes pasos, mejorando cada vez sus características tanto en hardware como en software, lo que a su vez permite una mejor y mayor trasmisión de datos, con lo cual también aumenta la posibilidad de que existan malwares, además de que las personas no utilizan contraseñas para mantener a sus dispositivos protegidos, transmiten datos no encriptados lo que les vuelve susceptibles de robo, hurto, o incluso filtración involuntaria de datos, además de que pueden recibir ataques de fuerza bruta, ataques DoS, ataques de XSS, Inyección SQL, entre otros.

3.1.15 Clasificación de activos de información / análisis y evaluación de riesgos

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

Esta clasificación se basa a los requerimientos estipulados en el ítem relacionado con la Gestión de Activos de los estándares 27001:2011, ISO 27002, e ISO 27005.

Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, se definieron tres (3) niveles alineados con los tipos de información (**ver Tabla 2-3**):

Tabla 2-3: Tabla de valoración de confidencialidad

CONFIDENCIALIDAD	ALTA	Información disponible sólo parte específicas y departamentos de la empresa. En caso de ser conocida sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica
	MEDIA	Información disponible para el personal de la empresa. En caso de ser conocida por terceros sin autorización no causase mucho efecto en las operaciones de la empresa.
	BAJA	Información que puede ser revelada o publicada sin restricciones dentro y fuera de la entidad, sin que esto implique daños.

Fuente: (NTE INEN-ISO/IEC 27001:2015, NTE INEN-ISO IEC 27002.)
Realizado por: (Vizuete, Jenny, 2019)

Clasificación de acuerdo con la integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles (**ver Tabla 3-3**):

Tabla 3-3: Tabla de valoración de integridad

INTEGRIDAD	ALTA	Información cuya pérdida puede causar un efecto fatal en las funciones de la empresa o generar pérdidas de imagen severas de la entidad.
	MEDIA	Información cuya pérdida de exactitud y completitud no afecta gravemente las operaciones de la empresa.
	BAJA	Información utilizada para consultas, cuya pérdida de exactitud y completitud no conlleva un impacto significativo para la empresa.

Fuente: (NTE INEN-ISO/IEC 27001:2015, NTE INEN-ISO IEC 27002.)
Realizado por: (Vizuete, Jenny, 2019)

Clasificación de acuerdo con la disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso (**ver Tabla 4-3)**.

Tabla 4-3: Tabla de valoración de disponibilidad

DISPONIBILIDAD	ALTA	La no disponibilidad de la información puede llegar a tener un efecto fatal y conllevar un impacto negativo que puede tener repercusión económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
	MEDIA	La no disponibilidad de la información puede que afecte a los procesos que la utilizan. Sin embargo, las operaciones podrían esperar hasta que la información se encuentre disponible.
	BAJA	La no disponibilidad de la información no afecta los procesos de operación de la empresa.

Fuente: (NTE INEN-ISO/IEC 27001:2015, NTE INEN-ISO IEC 27002.)
Realizado por: (Vizuete, Jenny, 2019)

Listado y clasificación de los activos de la empresa

Para la correcta identificación de los activos se realizaron entrevistas con el personal administrativos de la empresa, una vez realizado esto los activos se clasificaron de la siguiente manera (ver **Tabla 5-3)**:

- Software (SW): tales como aplicaciones móviles, sistemas operativos de los dispositivos móviles.
- Hardware (HW): tales como celulares, Tablets.
- Almacenamiento de información (AI): tales como almacenamiento en la nube o en servidor.
- Comunicación (COM): son los que permiten el intercambio dentro y fuera de la empresa.
- Datos (DAT): la información con la que cuenta la empresa NAS y correo electrónico
- Equipamiento auxiliar (AUX): equipos de respaldo como celulares, Tablets, laptops.
- Local e instalaciones (INS): lugar donde se encuentran los equipos informáticos de la empresa.
- Personal/RRHH (PER): los empleados que utilizan los elementos listados anteriormente.
- Servicios Generales (SRV): involucran todos los servicios de comunicación, eléctricos y otros servicios que necesite la empresa para poder operar.

Tabla 5-3: Tabla de clasificación de activos

Categorías de los activos de información			**Criterio de clasificación de los activos**			
Identificador	Categoría	Activo	Confidencialidad	Integridad	Disponibilidad	
SW	Software/ Aplicaciones	Aplicaciones móviles	ALTA	ALTA	ALTA	ALTA
		Sistemas operativos para DM	MEDIA	MEDIA	MEDIA	MEDIA
		Antivirus	MEDIA	ALTA	ALTA	ALTA
HW	Hardware/ Equipos	Celulares	ALTA	ALTA	ALTA	ALTA
		Tablets	ALTA	ALTA	ALTA	ALTA
AI	Almacenamiento de información	Almacenamiento en la nube	MEDIA	ALTA	ALTA	ALTA
		Servidor	ALTA	ALTA	ALTA	ALTA
COM	Redes de comunicaciones	Firewall	ALTA	ALTA	ALTA	ALTA
		Routers	MEDIA	ALTA	ALTA	ALTA
		Switch	MEDIA	ALTA	ALTA	ALTA
		Mikrotik	MEDIA	ALTA	ALTA	ALTA
DAT	Datos/información	NAS	ALTA	ALTA	ALTA	ALTA
		Cuentas de correo electrónico	MEDIA	MEDIA	MEDIA	MEDIA
AUX	Equipamiento auxiliar	Celulares de respaldo	MEDIA	ALTA	ALTA	ALTA
		Tablets de respaldo	MEDIA	ALTA	ALTA	ALTA
INS	Local/Instalaciones	Oficina	BAJA	BAJA	BAJA	BAJA
PER	Personal/RR.HH	Gerente	ALTA	ALTA	ALTA	ALTA
		Área de marketing	ALTA	ALTA	ALTA	ALTA
		Personal técnico	ALTA	MEDIA	MEDIA	MEDIA
SRV	Servicios generales	Internet	ALTA	ALTA	ALTA	ALTA
		Electricidad	BAJA	MEDIA	MEDIA	MEDIA
		Agua	BAJA	BAJA	BAJA	BAJA

Realizado por: (Vizuete, Jenny, 2019)

Criterio de evaluación del riesgo

La tabla a continuación muestra el producto de la probabilidad de ocurrencia de una amenaza y el impacto que esta pudiese ocasionar, el resultado de este producto es el nivel de riesgo de cada activo. Los valores para esta evaluación se pueden observar en la **tabla 6-3**.

Tabla 6-3: Tabla de criterio de evaluación del riesgo

	IMPACTO				
PROBABILIDAD	**MUY BAJA (1)**	**BAJA (2)**	**MEDIA (3)**	**ALTA (4)**	**MUY ALTA (5)**
RARO (1)	1	2	3	4	5
IMPROBABLE (2)	2	4	6	8	10
POSIBLE (3)	3	6	9	12	15
PROBABLE (4)	4	8	12	16	20
MUY PROBABLE (5)	5	10	15	20	25

Fuente: (Amutio, Miguel, Candau, Javier, 2012)
Realizado por: (Vizuete, Jenny, 2019)

Identificación de vulnerabilidad, amenazas y riesgos

La identificación de vulnerabilidades a consecuencia de las amenazas naturales físicas o ambientales, humanas o accidentales y organizacionales se realizó en base a visitas y entrevistas en la empresa TELECOMEXPERT. La tabla a continuación muestra las vulnerabilidades encontradas en estos estos grupos y de acuerdo a las amenazas existentes dentro de la organización.

También se realizó la evaluación de acuerdo a los criterios de evaluación del riesgo, definidos en el la Tabla 7-3: Tabla de criterio de evaluación del riesgo.

Tabla 7-3: Vulnerabilidades, amenazas y riesgos inicialmente identificados

TIPO	VULNERABILIDADES	AMENAZAS	RIESGOS	PROBABILIDAD	IMPACTO	ESTIMACIÓN DEL RIESGO
Software/aplicaciones	Fallas en el software de los equipos	Corrupción de Software de los DM	Pérdida de información	3	5	15
	bloqueo del equipo al momento de terminar el trabajo cuando se haga uso del DM	Error en el uso de los DM de trabajo	Pérdida o modificación de información, robo de claves de usuario, modificación de datos	3	5	15
	Software no licenciado	Virus informáticos, malware, utilizar exploit en DM	Mal funcionamiento de sistemas, destrucción de SO, destrucción o modificación de aplicativos e información	4	5	20
	No cambiar las contraseñas de los DM	Ataques de intrusión	Pérdida de la información, robo de claves de usuario, modificación de datos	3	3	9
	Falta de actualización de las aplicaciones, antivirus y S.O de los DM	Mal funcionamiento de SW por falta de actualización de los DM	Mal funcionamiento de sistemas, destrucción de SO, destrucción o modificación de aplicativos e información en los DM	3	5	15
Hardware/equipos	Mantenimiento insuficiente de los DM	Incumplimiento en el mantenimiento de los DM	Pérdida de información	3	5	15
	Susceptibles a polvo, suciedad, caídas	Mala manipulación de los DM	Pérdida de información	4	5	20
	Fallas de hardware en los DM	Hardware en mal estado del DM	Pérdida de información	3	5	15
	Robo de equipos	Hurto de los DM	Pérdida de información	4	5	20
Almacenamiento de información	Ausencia de copias de respaldo de la información almacenada en los DM	Incumplimiento de realizar copias de respaldo de los DM	Pérdida de información	3	5	15
	Información sin ningún tipo de seguridad o cifrado en los DM	Robo o secuestro de la información que se encuentra en los DM	Pérdida de información	5	5	25

Redes de comunicaciones	Gestión inadecuada de red	Cambios en la configuración de la red	Alteración en el funcionamiento de la red	2	5	10
	Dejar activa la conexión a la VPN desde el DM	Error en el uso de la VPN	Intrusión de hackers o personas no autorizadas	3	5	15
	Conexión de datos deficiente de los DM	Fallas de comunicación entre los DM y la red de la oficina	Pérdida del servicio y comunicación entre equipos de red	2	5	10
	No guardar backups de la configuración de los DM	Incumplimiento de realizar copias de respaldo de los DM	No poder restablecer la configuración de backups	3	5	15
Datos/información	No esté protegida la información confidencial almacenada en los DM	Error en la manipulación de la información confidencial almacenada en los DM	Acceso de personas no autorizadas a la información, robo, modificación de la información	2	5	10
Equipamiento auxiliar	Fallas de la batería de los DM	Daño de las baterías del DM	Pérdida de la información	5	5	25
		Sobrecalentamiento de los equipos	Pérdida de la información	5	5	25
	Falla del display	Daño del DM	En caso de falla de energía, pérdida del servicio	4	5	20
Personal/RR.HH	Ausencia del personal que tiene a cargo los DM	Enfermedades, calamidades domésticas	No exista el personal suficiente para realizar las operaciones diarias de la empresa	1	5	5
	Mala manipulación de la información almacenada en los DM	Error en la manipulación de la información confidencial	Modificación de la información, pérdida de la información	3	5	15
	Uso incorrecto de HW y SW de los DM	Error en el uso de los DM de trabajo	Pérdida del servicio	3	5	15
Servicios generales	Falla del servicio de internet planes de datos de los DM	Cortes del servicio de internet por parte del proveedor	Pérdida del servicio a los usuarios	2	4	8

Realizado por: (Vizuete, Jenny, 2019)

3.1.16 Variables e indicadores

Variable independiente: Políticas de seguridad en dispositivos móviles

Variable dependiente: Manejo de información

Tabla 8-3: Variables e indicadores

VARIABLE	TIPO	CONCEPTO
Políticas de seguridad en dispositivos móviles	Variable independiente	Es un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional (Dussan, Ciro, 2006).
Manejo de información	Variable dependiente	Datos que deben ser llevados, almacenados y manejados de una manera adecuada para poder tomar decisiones que ayuden al crecimiento de las mismas. (Reporte Digital, 2019)

Realizado por: (Vizuete, Jenny, 2019)

Tabla 9-3: Operacionalización metodológica

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO / FUENTE
Políticas de seguridad en dispositivos móviles	• Normativa • Políticas	• Análisis documental • Encuesta • Observaciones	NTE INEN-ISO/IEC 27001:2011 Cuestionario escrito
Manejo de información	• Integridad • Confidencialidad • Disponibilidad	• Encuesta • Observación • Ingeniería social • Búsqueda de información	Cuestionario escrito

Realizado por: (Vizuete, Jenny, 2019)

Tabla 10-3: Indicadores e índices

VARIABLE	INDICADOR	ÍNDICES
Políticas de seguridad en dispositivos móviles	Normativas	Grado de relación de las políticas implementadas frente a las normativas vigentes
	Políticas	Número de políticas implementadas referidas a la seguridad de información
Manejo de información	Integridad	La información que se maneja a través de los dispositivos móviles no sea alterada Proceso de verificación de la información
	Confidencialidad	Solo las personas autorizadas puedan acceder a la información
	Disponibilidad	Que la información esté disponible cuando se necesite

Realizado por: (Vizuete, Jenny, 2019)

3.1.17 Análisis de variables

El trabajo busca proponer políticas basadas en la NTE INEN-ISO/IEC 27001:2015 y NTE INEN-ISO IEC 27002, que podrán ser aplicados a la mayor parte de empresas de la ciudad de Riobamba.

Para realizar el análisis será importante buscar si en primer lugar se han establecido normas o políticas que estén normando los procesos de la seguridad de información, o si se han establecido cuales podrían ser los cambios a darse para mejorar las normas con base a la NTE INEN-ISO/IEC 27001 y NTE INEN-ISO IEC 27002.

3.1.18 Indicadores de la variable independiente

Para la comprobación de la hipótesis en primer lugar determinaremos si la empresa TELECOMEXPERT posee políticas de seguridad para el manejo de la información a través de los dispositivos móviles en base a una comparación de controles que sean equivalentes a las leyes y normas vigentes en la NTE INEN-ISO/IEC 27001:2015 y NTE INEN-ISO IEC 27002.

3.1.19 Indicadores de la variable dependiente

Para determinar si se mantiene la confidencialidad, integridad y disponibilidad de la información a través de las políticas que se propongan en base a una comparación de controles que sean equivalentes a las leyes y normas vigentes en la NTE INEN-ISO/IEC 27001:2015 y NTE INEN-ISO IEC 27002.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Presentación de resultados

En la siguiente sección se presenta el análisis de los resultados obtenidos en la investigación aplicando los métodos y técnicas definidos, así como su relación con los objetivos y la hipótesis plateada.

En base a dichos resultados se puede observar la diferencia que existe en la empresa antes y después de la aplicación de políticas de seguridad para dispositivos móviles al momento de manejar la información, y se obtiene la conclusión de que a través de la implementación de las políticas de seguridad se puede manejar la información de la empresa a través de los dispositivos móviles de manera segura.

4.2 Validación y análisis de resultados

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

1. ¿Está conectado con su dispositivo móvil personal a una red de la empresa?

Tabla 1-4: Pregunta 1

Respuestas	Frecuencia	Porcentaje
Si	11	100%
No	0	0%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

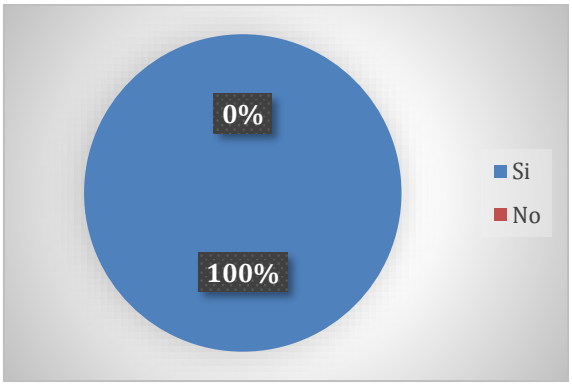


Gráfico 1-4: Pregunta 1
Realizado por: (Vizuete, Jenny, 2019)

La empresa posee una red abierta y todos los miembros de ella pueden acceder sin ninguna clase de obstáculo. Por su facilidad todas las personas se conectan a ella para su uso personal

2. ¿Existen dispositivos móviles de uso personal que son conectados a los sistemas de la empresa?

Tabla 2-4: Pregunta 2

Respuestas	Frecuencia	Porcentaje
Si	11	100%
No	0	0%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

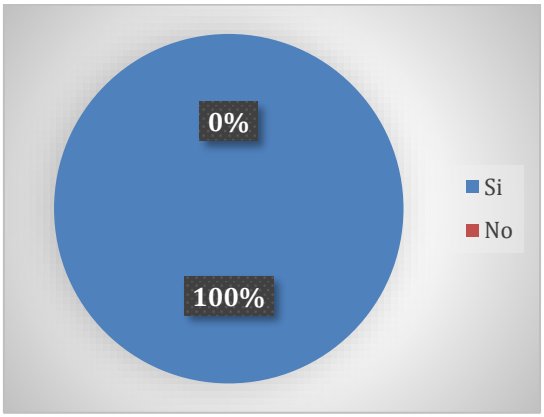


Gráfico 2-4: Pregunta 2
Realizado por: (Vizuete, Jenny, 2019)

Existen dispositivos móviles que se encuentran conectados a los sistemas de la empresa, lo cual constituye una fuente de riesgo bastante importante para la seguridad de la información de la empresa.

3. ¿Existen zonas de la empresa en donde no se permite el uso de dispositivos móviles?

Tabla 3-4: Pregunta 3

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

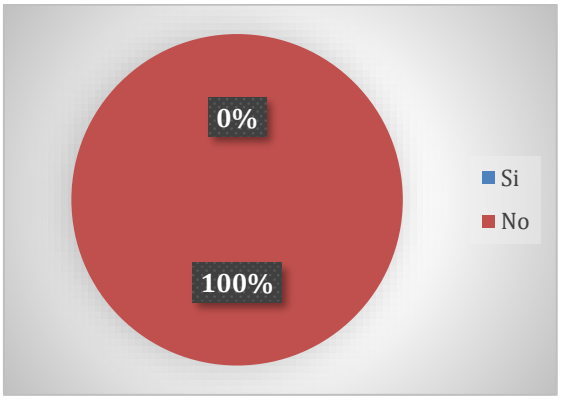


Gráfico 3-4: Pregunta 3
Realizado por: (Vizuete, Jenny, 2019)

No existen restricciones en ninguna zona de la empresa, ni en las vulnerables que podría resultar en pérdida de información de los sistemas de la misma.

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

Tabla 4-4: Pregunta 4

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

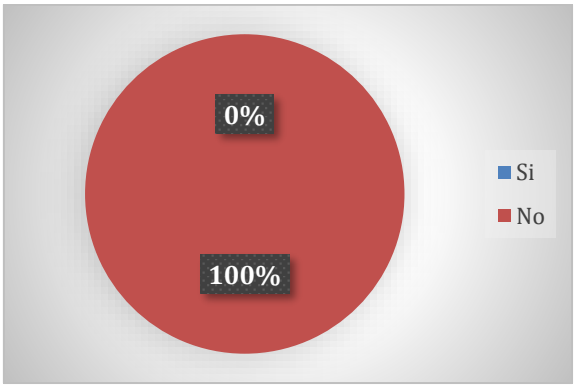


Gráfico 4-4: Pregunta 4
Realizado por: (Vizuete, Jenny, 2019)

No se conoce por parte de ningún elemento de la empresa regulaciones que limite la conexión o uso de dispositivos móviles en le empresa. No se han establecido parámetros o reglas de uso de dispositivos móviles, los cuales, a más de posibles robos de información al estar conectados al sistema de la empresa, también podría provocar distracciones en la labor diaria.

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

Tabla 5-4: Pregunta 5

Respuestas	Frecuencia	Porcentaje
Si	11	100%
No	0	0%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

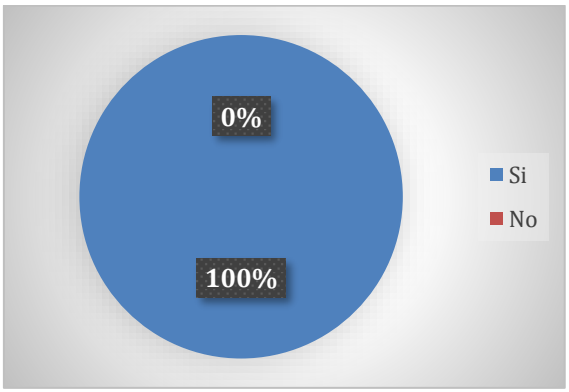


Gráfico 5-4: Pregunta 5
Realizado por: (Vizuete, Jenny, 2019)

Las claves son las únicas seguridades que se han establecido para proteger la red de la empresa, lo cual sin embargo resulta insuficiente si todas las personas tienen acceso ilimitado a ella.

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

Tabla 6-4: Pregunta 6

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

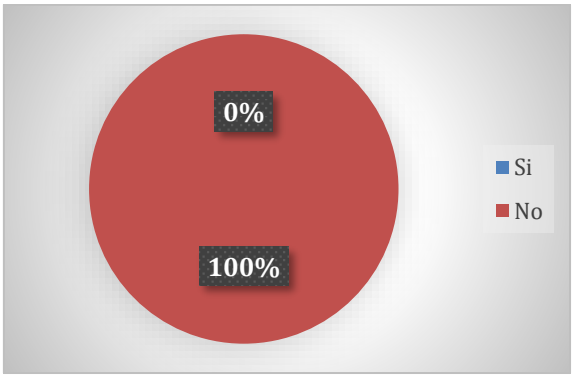


Gráfico 6-4: Pregunta 6
Realizado por: (Vizuete, Jenny, 2019)

No se han establecido políticas de la empresa específicas para el uso de móviles, un problema bastante común en muchas empresas de la localidad.

7. ¿Puede acceder a información interna de la empresa a través de su dispositivo móvil?

Tabla 7-4: Pregunta 7

Respuestas	Frecuencia	Porcentaje
Si	11	100%
No	0	0%
Total	**10**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

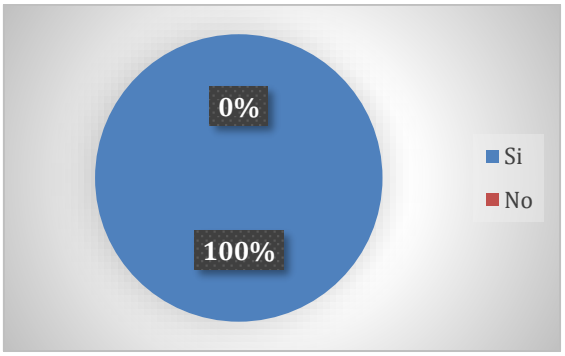


Gráfico 7-4: Pregunta 7
Realizado por: (Vizuete, Jenny, 2019)

Se manifiesta que es posible acceder a información interna de la empresa por medio de los dispositivos móviles. A más de la vulnerabilidad del sistema también es posible acceder a datos que la empresa puede acabar perdiendo o ser víctima de hackers o ladrones de información valiosa de la empresa.

8. ¿Existe algún listado de aplicaciones prohibidas para los dispositivos móviles para el manejo de la información de la empresa?

Tabla 8-4: Pregunta 8

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

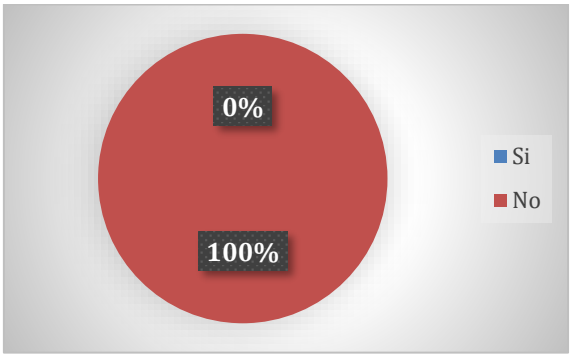


Gráfico 8-4: Pregunta 8
Realizado por: (Vizuete, Jenny, 2019)

No se ha elaborado o tenido en cuenta alguna lista de posibles aplicaciones que puedan tener riesgo de vulnerabilidades para la empresa. No se han realizado estudios que puedan determinar

posibles aplicaciones que puedan ser virtualmente peligrosas, o siquiera que puedan distraer a las personas en su trabajo.

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

Tabla 9-4: Pregunta 9

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

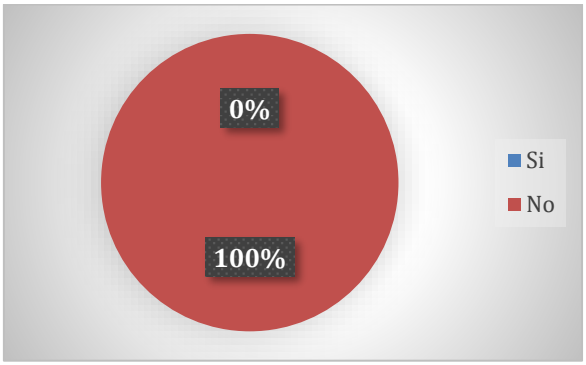


Gráfico 9-4: Pregunta 9
Realizado por: (Vizuete, Jenny, 2019)

No se tiene procesos para asignar dispositivos móviles corporativos. En este caso resulta porque no se utilizan móviles corporativos, ni tampoco se han planteado hacerlo.

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)?

Tabla 10-4: Pregunta 10

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

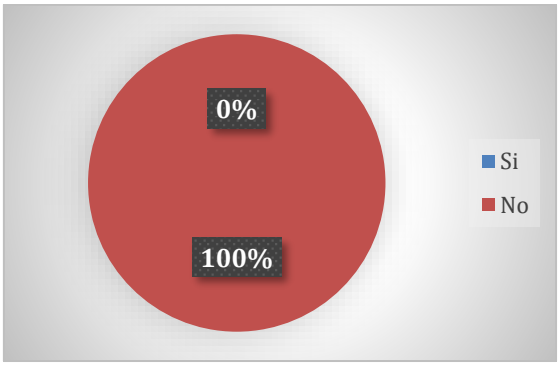


Gráfico 10-4: Pregunta 10
Realizado por: (Vizuete, Jenny, 2019)

No se tiene un registro de los ingresos de los dispositivos móviles a la red, esto se debe a que se tiene acceso ilimitado a la red de la empresa y no se establece un control de quienes se conectan a esta red.

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

Tabla 11-4: Pregunta 11

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

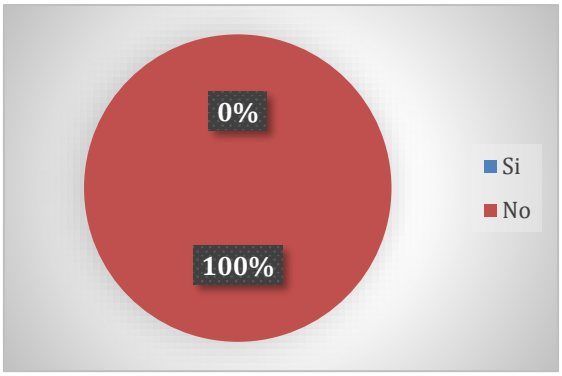


Gráfico 11-4: Pregunta 11
Realizado por: (Vizuete, Jenny, 2019)

No se realizan solicitudes para cambios en dispositivos móviles. Afirma lo revisado en preguntas anteriores acerca de la falta de políticas o procedimientos aplicados a los dispositivos móviles.

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

Tabla 12-4: Pregunta 12

Respuestas	Frecuencia	Porcentaje
Si	3	27%
No	8	73%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

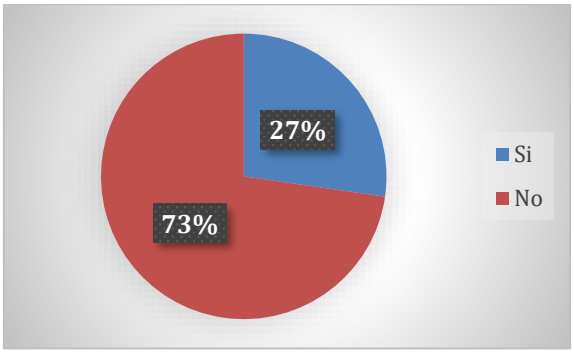


Gráfico 12-4: Pregunta 12
Realizado por: (Vizuete, Jenny, 2019)

El 27% de las personas consultadas guarda información estrictamente necesaria para la empresa en tanto que el 73% no lo hace. Existe cierto grado de responsabilidad por algunas personas al momento de guardar la información de su trabajo.

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

Tabla 13-4: Pregunta 13

Respuestas	Frecuencia	Porcentaje
Si	0	0%
No	11	100%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

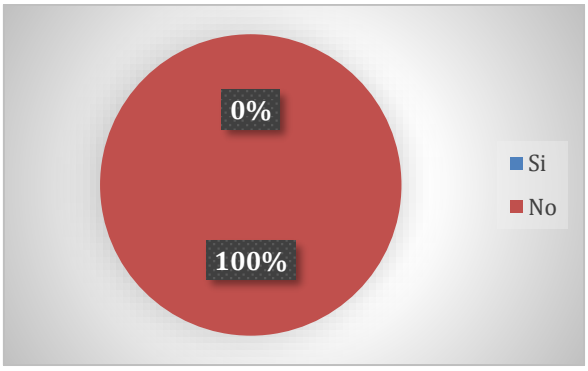


Gráfico 13-4: Pregunta 13
Realizado por: (Vizuete, Jenny, 2019)

No se realiza la eliminación de información innecesaria o que resulte riesgosa para la empresa, ni se han establecido procedimientos para eliminar información innecesaria de los dispositivos.

14. Cuando transporta el dispositivo móvil fuera de la empresa, ¿lo realiza de forma segura?

Tabla 14-4: Pregunta 14

Respuestas	Frecuencia	Porcentaje
Si	7	64%
No	4	36%
Total	**11**	**100%**

Realizado por: (Vizuete, Jenny, 2019)

De qué forma asegura el teléfono móvil (Solo quienes respondan si en la pregunta 14).

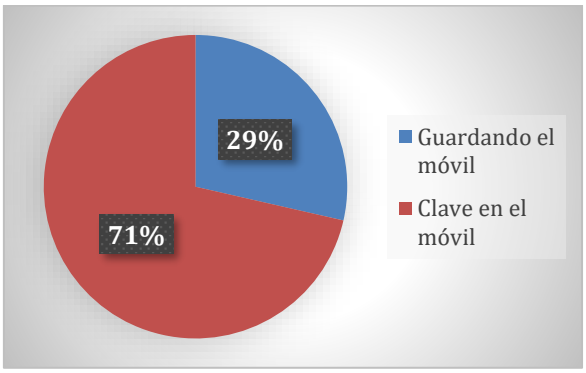


Gráfico 14-4: Seguridad para el móvil
Realizado por: (Vizuete, Jenny, 2019)

El 64% de las personas manifiesta que, si trasportan sus móviles fuera de la empresa de forma segura, en tanto que el 36% manifiestan que no. De quienes dicen llevar sus móviles de forma segura, el 71% lo tiene con clave, en tanto que el 29% lo realiza guardándolo. Las formas de

protección de los móviles, de las cuales se tiene acceso a información de la empresa según lo manifestado, resultan escasas al presenciar que solo un poco de ellos mantiene una clave de seguridad mínima.

4.3 Comprobación de variables

4.3.1 Preguntas correspondientes a los indicadores de variable independiente

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?

Políticas

6. ¿Existen políticas específicas en el uso de dispositivos móviles?
9. ¿Existen algún proceso de solicitud para la asignación de dispositivos móviles corporativos?

4.3.2 Preguntas correspondientes indicadores de variable dependiente

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

Disponibilidad

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

Confidencialidad

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

Valores porcentuales de las encuestas aplicadas

A continuación, se presenta los resultados que se obtuvieron de las preguntas referentes con las variables independiente y dependiente de las encuestas aplicadas a la empresa TELECOMEXPERT antes y después de la aplicación de las políticas. Ver tabla 15-4.

Tabla 15-4: Valores porcentuales de las encuestas aplicadas

Indicador		Antes			Después		
	Pregunta	Si	No	Total	Si	No	Total
Variable independiente	4	0	100	100	100	0	100
	5	100	0	100	100	0	100
	6	0	100	100	90,91	9,09	100
	9	0	100	100	81,82	18,18	100
Variable dependiente	10	0	100	100	81,82	18,18	100
	11	0	100	100	18,18	81,82	100
	12	27,27	72,73	100	90,91	9,09	100
	13	0	100	100	36,36	63,64	100

Realizado por: (Vizuete, Jenny, 2019)

4.3.3 Indicadores de variable independiente

Para su valoración se procedió a realizar una encuesta para validar el cumplimiento del uso de las políticas de seguridad en dispositivos móviles para el manejo de información en la empresa TELECOMEXPERT.

Normativas

Tabla 16-4: Indicadores de variable independiente (Normativa)

Pregunta	Antes de proponer políticas			Después de proponer políticas		
	Si	No	Total	Si	No	Total
4	0	100	100	100	0	100
5	100	0	100	100	0	100
TOTAL	**50**	**50**	**100**	**100,00**	**0,00**	**100**

Realizado por: (Vizuete, Jenny, 2019)

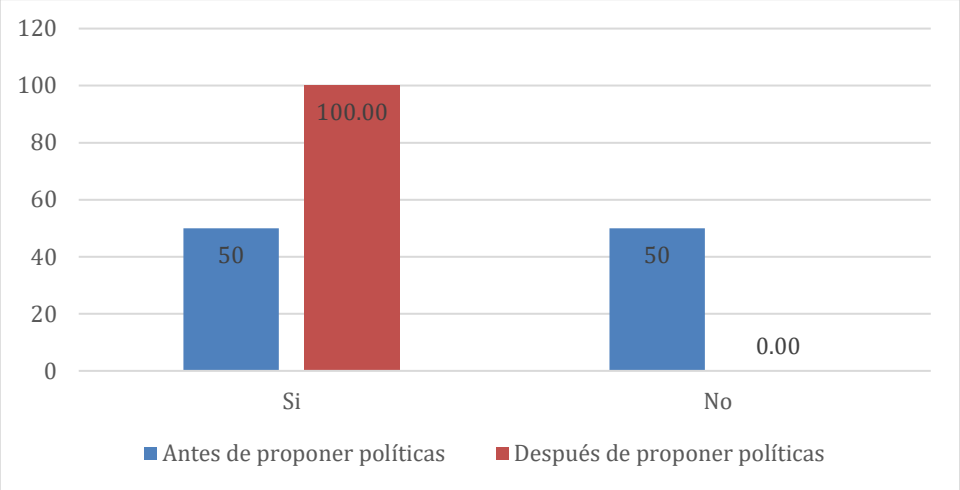


Gráfico 15-4: Indicadores de variable independiente (Normativa)
Realizado por: (Vizuete, Jenny, 2019)

Interpretación del indicador Normativas:

Según los datos recolectados, se puede observar en el gráfico 15-4, 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

Tabla 17-4: Indicadores de variable independiente (Políticas)

Pregunta	Antes de proponer políticas			Después de proponer políticas		
	Si	No	Total	Si	No	Total
6	0	100	100	90,91	9,09	100
9	0	100	100	81,82	18,18	100
TOTAL	**0**	**100**	**100**	**86,36**	**13,64**	**100**

Realizado por: (Vizuete, Jenny, 2019)

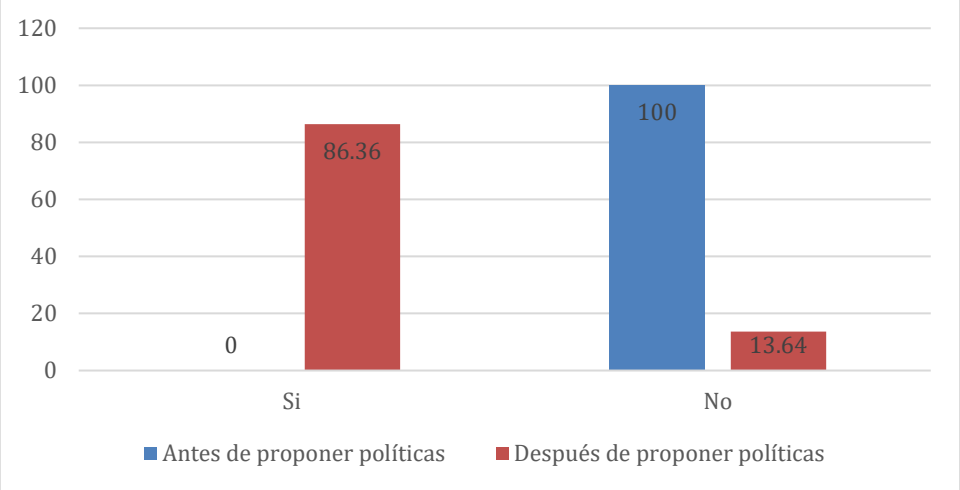


Gráfico 16-4: Indicadores de variable independiente (Políticas)

Realizado por: (Vizuete, Jenny, 2019)

Interpretación del indicador Políticas

Como se puede observar en el gráfico 16-4, 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.

Después del establecimiento de políticas, el 86,36% de los encuestados conocían de existencia de políticas acerca de los dispositivos móviles.

4.3.4 Indicadores de variable dependiente

Integridad

Tabla 18-4: Indicadores de variable dependiente (Integridad)

Pregunta	Antes de proponer políticas			Después de proponer políticas		
	Si	No	Total	Si	No	Total
10	0	100	100	81,82	18,18	100
12	27,27	72,73	100	90,91	9,09	100
TOTAL	**13,64**	**86,36**	**100**	**86,36**	**13,64**	**100**

Realizado por: (Vizuete, Jenny, 2019)

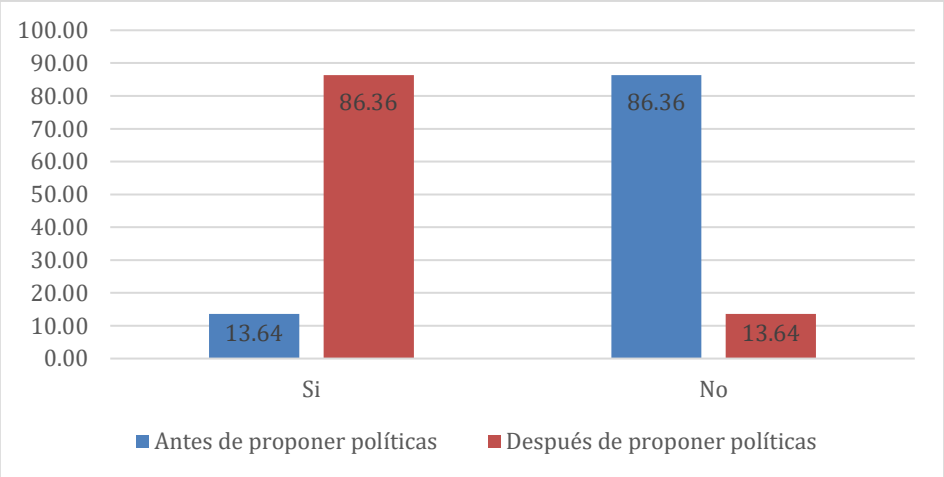


Gráfico 17-4: Indicadores de variable dependiente (Integridad)
Realizado por: (Vizuete, Jenny, 2019)

Interpretación del indicador Integridad

De acuerdo a los datos mostrados en el instrumento de evaluación, como se puede apreciar en el gráfico 17-4, la variable integridad en la información aumentó en un 72,72% (de 13,64% a 86,36%).

Antes del establecimiento de políticas, el 13,64% mencionaba que los datos se transmitían íntegros a las bases, con registros de los dispositivos que se han asignado y almacenamiento de información necesaria para el trabajo.

Después del establecimiento de políticas, el 86,36% mencionaba que los datos se transmitían íntegros a las bases, con registros de los dispositivos que se han asignado y almacenamiento de información necesaria para el trabajo.

Confidencialidad

Tabla 19-4: Indicadores de variable dependiente (Confidencialidad)

Pregunta	Antes de proponer políticas			Después de proponer políticas		
	Si	No	Total	Si	No	Total
13	0	100	100	36,36	63,64	100
TOTAL	**0**	**100**	**100**	**36,36**	**63,64**	**100**

Realizado por: (Vizuete, Jenny, 2019)

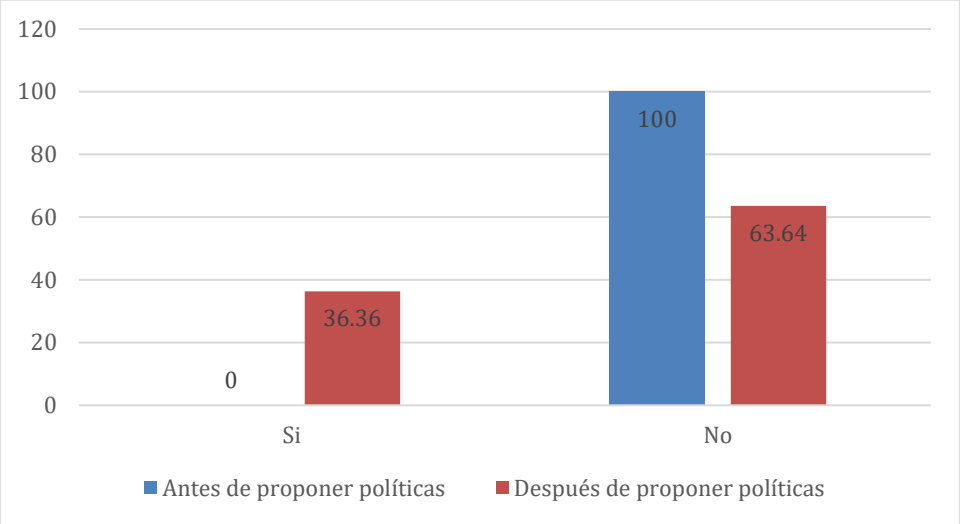


Gráfico 18-4: Indicadores de variable dependiente (Confidencialidad)
Realizado por: (Vizuete, Jenny, 2019)

Interpretación del indicador Confidencialidad

De acuerdo a los datos mostrados en el gráfico 18-4 del instrumento de evaluación, la variable integridad en la información aumentó en un 36,36%.

Antes del establecimiento de políticas se mencionaba que no existía un buen nivel de confidencialidad en la información de la empresa detallada a través de redes móviles.
Después del establecimiento de políticas se menciona que existe un 36,36% de nivel de confidencialidad en la información de la empresa detallada a través de redes móviles.

Disponibilidad

Tabla 20-4: Indicadores de variable dependiente (Disponibilidad)

Pregunta	Antes de implementar políticas			Después de implementar políticas		
	Si	No	Total	Si	No	Total
11	0	100	100	18,18	81,82	100
TOTAL	**0**	**100**	**100**	**18,18**	**81,82**	**100**

Realizado por: (Vizuete, Jenny, 2019)

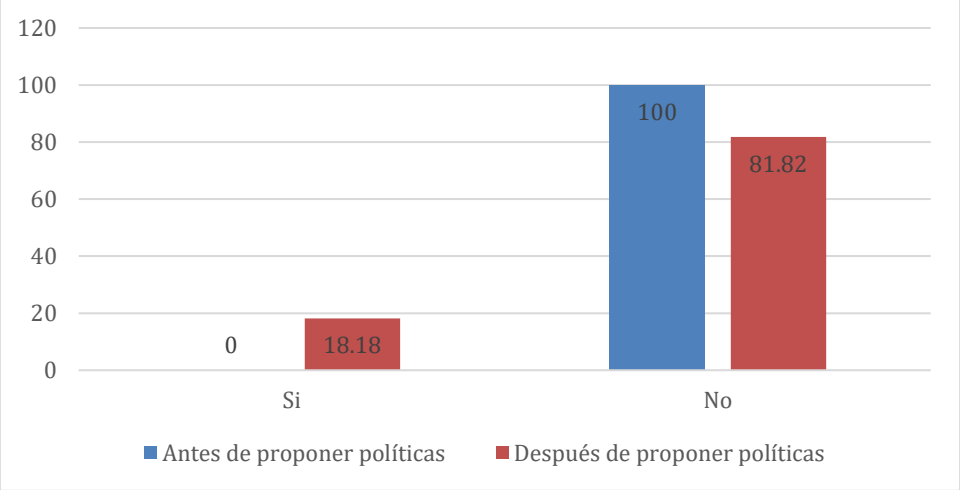


Gráfico 19-4: Indicadores de variable dependiente (Disponibilidad)
Realizado por: (Vizuete, Jenny, 2019)

Interpretación del indicador Disponibilidad

La disponibilidad de información se elevó en un 18,18% una vez que se aplicaron políticas de seguridad para los dispositivos móviles, tal como se muestra en el gráfico 19-4.

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

Resumen de valores porcentuales de las encuestas aplicadas

Tabla 21-4 Resumen de los porcentajes (%) de las variables Independiente y dependiente

		ANTES POLÍTICAS		DESPUÉS POLÍTICAS	
		SI	**NO**	**SI**	**NO**
VARIABLE INDEPENDIENTE	NORMATIVA (%)	50	50	100	0
	POLITICAS (%)	0	100	100	0
VARIABLE DEPENDIENTE	INTEGRIDAD (%)	13,64	86,36	86.36	13,64
	CONFIDENCIALIDAD (%)	0	100	36.36	63,64
	DISPONIBILIDAD (%)	0	100	18.18	81,82

Realizado por: (Vizuete, Jenny, 2019)

4.3.5 Comprobación de hipótesis

Para la comprobación de la hipótesis general "La implementación de políticas de seguridad desarrolladas para el uso de dispositivos móviles permite manejar la información de las PYMES de forma segura", se utilizó estadística referencial aplicando la prueba de Chi-Cuadrado (x^2).

Posterior a la realización de los diferentes análisis, y con los datos obtenidos se procede a definir la hipótesis de investigación Hi y la hipótesis Ho a ser consideradas:

H1: La implementación de las políticas de seguridad desarrolladas para el uso de dispositivos móviles si permite manejar la información de las PYMES de forma segura.

H1: u1>u2

Ho: La implementación de las políticas de seguridad desarrolladas para el uso de dispositivos móviles no permite manejar la información de las PYMES de forma segura.

Ho: u1<u2

Para la demostración de la hipótesis, se considerará las preguntas que representan un cambio en las políticas dentro de la empresa, para lo cual se realizó nuevamente la encuesta y se obtuvieron los resultados presentados en la Tabla 22-4:

Tabla 22-4: Resumen de la encuesta aplicada con políticas de seguridad

Pregunta	Si	No	Si	No
4	0	11	11	0
5	11	0	11	0
6	0	11	10	1
9	0	11	9	2
10	0	11	9	2
11	0	11	2	9
12	3	8	10	1
13	0	11	4	7

Realizado por: (Vizuete, Jenny, 2019)

Para la obtención de la tabla de frecuencias esperadas se toma en cuenta las respuestas positivas de la tabla 22-4, aplicando la siguiente formula en cada valor de la tabla.

$$Fd = \frac{total\ columna * total\ fila}{suma\ total}$$

Tras la aplicación de la fórmula en cada valor de la tabla anterior obtendremos la siguiente **tabla 23-4** de frecuencias esperadas.

Tabla 23-4 Frecuencias Esperadas

Pregunta	fa antes	fd después	Total
4	1,93	9,08	11
5	3,85	18,15	22
6	1,75	8,25	10
9	1,58	7,43	9
10	1,58	7,43	9
11	0,35	1,65	2
12	2,28	10,73	13
13	0,70	3,30	4
Total	**14**	**66**	**80**

Realizado por: (Vizuete, Jenny, 2019)

A continuación, se calcula el valor de chi cuadrado x^2, mediante la siguiente fórmula:

$$x^2 = \sum \frac{(fa - fd)^2}{fd}$$

Fa=frecuencia antes de la aplicación

Fd=frecuencia después de la aplicación

$$x^2 = \frac{(0-1.93)^2}{1.93} + \frac{(11-3.85)^2}{3.85} + \frac{(0-1.75)^2}{1.75} + \frac{(0-1.58)^2}{1.58} + \frac{(0-1.58)^2}{1.58} + \frac{(0-0.35)^2}{0.35} + \frac{(3-2.28)^2}{2.28} + \frac{(0-0.70)^2}{0.70} + \frac{(11-9.08)^2}{9.08} + \frac{(11-18.15)^2}{18.15} + \frac{(10-8.25)^2}{8.25} + \frac{(9-7.43)^2}{7.43} + \frac{(9-7.43)^2}{7.43} + \frac{(2-1.65)^2}{1.65} + \frac{(10-10.73)^2}{10.73} + \frac{(4-3.30)^2}{3.30}$$

$$x^2 = 1.93 + 13.28 + 1.75 + 1.58 + 1.58 + 0.35 + 0.23 + 0.70 + 0.41 + 2.82 + 0.37 + 0.33 + 0.33 + 0.07 + 0.05 + 0.15$$

$$x^2 = 25.92$$

El siguiente paso a seguir es el cálculo de los grados de liberad

Grado de libertad = (n-1) x (m-1)

Donde:

n: número de filas

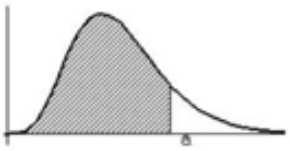
m: número de columnas

gl = (8-1) x (2-1) = 7

En base a la tabla de la distribución de Chi-cuadrado (Figura 1-4), y determinando el nivel de confianza de 95% y nivel de significancia del 5% obtendremos el punto crítico con 7 como valor de grados de libertad.

PERCENTILES DE LA DISTRIBUCIÓN χ^2

F(a) = P (X ≤ a)



	p										
g	**0.001**	**0.025**	**0.05**	**0.1**	**0.25**	**0.5**	**0.75**	**0.9**	**0.95**	**0.975**	**0.999**
1	10.827	5.024	3.841	2.706	1.323	0.455	0.102	0.016	0.004	0.001	0
2	13.815	7.378	5.991	4.605	2.773	1.386	0.575	0.211	0.103	0.051	0.002
3	16.266	9.348	7.815	6.251	4.108	2.366	1.213	0.584	0.352	0.216	0.024
4	18.466	11.143	9.488	7.779	5.385	3.357	1.923	1.064	0.711	0.484	0.091
5	20.515	12.832	11.07	9.236	6.626	4.351	2.675	1.61	1.145	0.831	0.21
6	22.457	14.449	12.592	10.645	7.841	5.348	3.455	2.204	1.635	1.237	0.381
7	24.321	16.013	14.067	12.017	9.037	6.346	4.255	2.833	2.167	1.69	0.599
8	26.124	17.535	15.507	13.362	10.219	7.344	5.071	3.49	2.733	2.18	0.857
9	27.877	19.023	16.919	14.684	11.389	8.343	5.899	4.168	3.325	2.7	1.152
10	29.588	20.483	18.307	15.987	12.549	9.342	6.737	4.865	3.94	3.247	1.479
11	31.264	21.92	19.675	17.275	13.701	10.341	7.584	5.578	4.575	3.816	1.834
12	32.909	23.337	21.026	18.549	14.845	11.34	8.438	6.304	5.226	4.404	2.214

Figura 1-4: Resultados percentiles de la distribución x2

Fuente: (Universidad Militar Nueva Granada, Distribución de Chi cuadrado, 2019)

$$x^2 \text{ crítico} = 14{,}067$$

Con los datos obtenidos anteriormente donde $x^2 = 25.92$ y x^2 crítico = 14.067 se puede aplicar el criterio de decisión y obtenemos la gráfica de la campana de Gauss Figura 2-4:

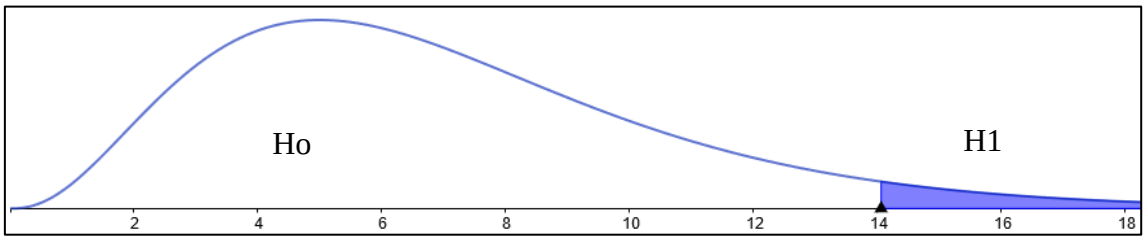


Figura 2-4: Resultado de los valores de la campana de Gauss

Interpretación y análisis

El valor de chi cuadrado calculado es superior al de la tabla (25.92>14,067), como se aprecia en la gráfica se concluye que se rechaza Ho y se acepta H1 con un nivel de confianza del 95% y un nivel de significancia del 5%. La implementación de las políticas de seguridad desarrolladas para el uso de dispositivos móviles si permite manejar la información de las PYMES de forma segura.

CAPITULO V

5. PROPUESTA POLÍTICAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES PARA EL MANEJO DE LA INFORMACIÓN EN PYMES

En el presente capítulo se presenta las políticas de seguridad en dispositivos móviles para el manejo de información para la empresa TELECOMEXPERT. Las políticas abarcan puntos clave para solventar las vulnerabilidades presentadas en este tipo de empresas.

También se consideraron los lineamientos revisados en el marco teórico de este documento, tomando en cuenta las normas NTE INEN-ISO/IEC 27001:2015 y la norma NTE INEN-ISO IEC 27002.

Cabe recalcar que las políticas creadas en este documento se han definido como obligatorias para que sean cumplidas por el personal de la empresa. Además, dichas políticas pueden ser aplicadas a otras empresas que usen dispositivos móviles para el manejo de la información y en base a las necesidades pueden ser modificadas y adaptadas.

5.1 Políticas de seguridad en dispositivos móviles para el manejo de la información desarrolladas para la empresa TELECOMEXPERT

Generalidades

La seguridad informática ha tomado mucha importancia en los últimos años gracias a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes a través de diferentes dispositivos ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar en una diversidad de mercados; pero a la vez ha traído consigo la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos se enfrentan por medio de una serie de directrices que orientan en el uso adecuado de los elementos tecnológicos y recomendaciones para obtener el mayor provecho de sus ventajas, evitando el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de las empresas.

Las políticas de seguridad informática que se definirán están relacionadas con los dispositivos móviles, y surgen como una herramienta organizacional para mantener la información de la empresa en buen recaudo, lo cual le permitirá mantenerse competitiva.

Ante esta situación, el proponer las políticas de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a la organización.

Alcance

Estas políticas de seguridad son elaboradas basadas en el análisis previo de la empresa TELECOMEXPERT, aunque su uso podría extenderse a otras organizaciones que presenten características similares a la empresa mencionada.

Objetivos

- Propinar un esquema de seguridad adecuado, claro y transparente que se encuentre a cargo de la administración de la organización
- Comprometer al personal a usar sus dispositivos móviles y las redes de la empresa de forma responsable y segura

Responsabilidades

La responsabilidad recae sobre el encargado de la seguridad informática en la tarea de desarrollo, revisión y divulgación, por cualquier medio que disponga la empresa, de los procesos que se mencionen a continuación. Es responsabilidad de los supervisores que se capacite o se tenga al tanto de los procedimientos que se presenten a continuación, además de realizar las correcciones necesarias de acuerdo a la complejidad del sistema informático que se maneje.

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 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.

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 dispositivo móvil de la empresa exclusivo para el efecto.

Responsabilidad

Artículo 10: La persona responsable que tiene a cargo la red de internet de la empresa es la única que puede otorgar claves de 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.

Seguridad

Artículo 13: El acceso a los sistemas de información, deberá contar niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por el personal encargado.

Artículo 14: Se deberá establecer claves de accesos a las redes WIFI de la empresa, además es necesario registrar la MAC e IMEI del dispositivo móvil, el personal encargado 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 así también se debe conocer a quién fue asignado el dispositivo móvil.

Artículo 16: 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 17: 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 seguros (L2TP/IPSec), siempre se debe cerrar la sesión de VPN una vez terminado cualquier actividad.

Artículo 18: 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 19: Establecer un método y período de bloqueo para acceso al dispositivo y su memoria (contraseña o PIN) para los dispositivos móviles institucionales que serán entregados a los usuarios. Además, las contraseñas deben ser cambiadas cada tres meses.

Artículo 20: El personal encargado deberá cifrar el dispositivo móvil antes de ser entregado para el uso dentro de la empresa, en caso de que el dispositivo móvil posea una tarjeta de memoria, esta también debe ser cifrada.

Artículo 21: Se procederá a realizar cambios de claves de las redes en un período máximo de 6 meses por parte del personal responsable.

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 del mismo.

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, todo esto debe constar en el registro que posee la empresa de los dispositivos móviles.

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.

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.

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 las mismas.

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.

Disposiciones finales

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su difusión. Las normas y políticas objeto de este documento, podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando.

Las disposiciones aquí descritas constarán de forma detallada en los manuales de políticas y procedimientos específicos.

La falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

CONCLUSIONES

- Mediante el análisis de la situación inicial de la seguridad de la información de la empresa TELECOMEXPERT, fue posible determinar que la empresa no tenía establecido normas o procedimientos de seguridad de la información para el manejo de la misma a través de dispositivos móviles.

- A través de la demostración de la hipótesis se pudo comprobar que al aplicar las políticas de seguridad en dispositivos móviles en la empresa TELECOMEXPERT se puede manejar la información de las PYMES de forma segura En general se pasó de 4.55% a 46.96% (42.41%).

- Se realizó un análisis para identificar los riesgos, vulnerabilidades, amenazas como complemento para la creación de las políticas de seguridad, además se visualizó como los usuarios interactuaban con los DM y los peligros a los que se exponían.

- Aplicando las políticas en la empresa se pudo mejorar considerablemente el nivel de seguridad de la información de la empresa, existiendo actualmente normativas conocidas por todos los miembros de la empresa, mejorando la integridad de la transmisión de datos por medio de dispositivos móviles pasando de 13.64% a 86.36%, mejorando la confidencialidad de los datos en un 36.36%, así como la disponibilidad de los mismos en un 18,18%.

- En base a los datos expuestos en el punto anterior se puede evidenciar una disminución en el riesgo de uso de los dispositivos móviles en la empresa, aunque desde luego deberá transcurrir más tiempo para tener una conclusión definitiva acerca del impacto de las reglas propuestas y como podrían ser mejoradas en beneficio de la empresa.

RECOMENDACIONES

- En la actualidad estamos en una era en donde la tecnología juega un papel fundamental en las actividades cotidianas de las PYMES, por lo que se debe contar con políticas de seguridad para el manejo de la información a través de dispositivos móviles para mantener la confiabilidad, disponibilidad e integridad de la misma.

- Antes de realizar una implementación de políticas de seguridad en dispositivos móviles para el manejo de información es necesario identificar los recursos con los que cada empresa cuenta, así se podrá aplicar de mejor manera cada política a fin de mejorar el nivel de seguridad de la información.

- Incentivar a las empresas a mejorar las políticas propuestas de acuerdo a su impacto en la empresa, de tal forma que pueda asegurarse que la información se encuentre protegida y que sea utilizada solo para fines que la gerencia decida.

- El tema de investigación propuesto permite que se siga con la investigación ya que las políticas creadas en este documento pueden ser estudiadas más a fondo no solo para PYMES sino para cualquier empresa o institución que posea dispositivos móviles para el manejo de la información por lo que deja oportunidad a fututos maestrante su continuidad.

BIBLIOGRAFÍA

Amutio, Miguel, Candau, Javier. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En *MAGERIT – versión 3.0, Metodología de Análisis y Gestión* (págs. 22-46). Madrid: © Ministerio de Hacienda y Administraciones Públicas.

Baca, Gabriel. (2016). *Introducción a la seguridad informática.* Mexico: Grupo editorial Patria.

Baz, Arturo; Ferrerira, Irene; Álvarez, María; García, Rosana. (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 Usano, Silvia. (2015). Análisis de la aplicación de la tecnología móvil en las empresas. 39-52.

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, Gabriele; Ferretti, Stefano; Ghini, Vittorio; Panzieri, Fabio. (2014). Mobile Computing in Digital Ecosystems: Design Issues and Challenges. *Cornell University*.

Dussan, Ciro. (2006). Políticas de seguridad informática. *Entramado*, 86-92.

Enroke. (15 de Mayo de 2019). *¿Qué son PYMES?* Obtenido de http://www.grupoenroke.com/index.php/proyecto-pymes/46-que-son-las-%20pymes

Granger, Saah. (18 de Diciembre de 2001). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Obtenido de Symantec Connect: https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Guerrero, Carlos. (2014). *Ecosistema digital académico caso aplicado: Unidades tecnológicas de santander.* Santander: Unidad tecnológica de Santander.

Hadzic, M.; Chang, E.; Dillon, T. (2007). Methodology framework for the design of digital ecosystems. *IEEE Int. Conf. Syst. Man Cybern*, 7-12.

Interpares. (2 de Junio de 2019). *International Research for permanent authentic record in electronic system*. Obtenido de Glosario Interpares: http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary

ISO 27002. (17 de Mayo de 2019). *ISO 27002*. Obtenido de http://iso27000.es/iso27002.html

López, A., & Ruiz, J. (10 de Mayo de 2019). *Historia ISO 27001*. Obtenido de www.iso27000.es/download/HistoriaISO27001.pps

OCDE-CEPAL. (2013). Financiamiento de Pequeñas y Medianas Empresas en América Latina Perspectivas Económicas de América Latina. *OCDE/CEPAL*.

Protecseguros Lola. (06 de 05 de 2016). *Protecseguros*. Obtenido de http://www.protecseguros.com/single-post/2016/05/06/El-935-del-consumo-de-datos-celulares-en-Ecuador-se-realiza-a-trav%C3%A9s-de-redes-WiFi

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Ciencias informáticas*, 676-688.

Redacción EKOS. (2012). PYMES: Contribución clave en la economía. *EKOS*.

Reporte Digital. (8 de Abril de 2019). *El análisis en la base de datos es la clave para la toma de decisiones en las empresas*. Obtenido de https://reportedigital.com/cloud/analisis-de-datos/

Saavedra, María; Hernández, Yolanda. (2008). Caracterización e importancia de las MIPYMES en Latinoamérica. *Actualidad Contable FACES 11(17)*, 122-134.

Sheldon, Robert. (2012). *TechTarget.* Obtenido de TechTarget,: https://searchdatacenter.techtarget.com/es/consejo/Como-crear-una-politica-de-seguridad-para-dispositivos-moviles

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

Soriano, Barbara; Pinto, César. (2006). *Finanzas para no financieros.* Fundación Confemetal.

Stefanko, Lukas. (2018). *Fake banking apps on Google Play leak stolen credit card data.*

Universidad Militar Nueva Granada, Distribución de Chi cuadrado. (2019). *Facultad de estudios a Distancia*. Obtenido de

http://virtual.umng.edu.co/distancia/ecosistema/ovas/esp_alt_ger/teoria_de_las_decisiones_gerenciales/unidad_2/medios/documentacion/p7h3.php

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

Voutssas, M. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*,.

ANEXOS

ANEXO A. ENCUESTA DIRIGIDA AL PERSONAL DE LA EMPRESA (ADMINISTRADOR, ÁREA DE VENTAS Y TÉCNICOS) QUE MANEJA DISPOSITIVOS MÓVILES

ENCUESTA APLICADA A LA EMPRESA TELECOMEXPERT

OBJETIVO: Realizar una recopilación de la situación actual de la seguridad de la información de la empresa.

Por favor, anote la respuesta que corresponde a la realidad de su empresa. Sea sincero en su contestación a fin de entender la realidad problemática de la empresa para proponer políticas que mejoren la situación de la empresa

1. ¿Está conectado con su dispositivo móvil personal a una red de la empresa?

Si __ No__

2. ¿Existen dispositivos móviles de uso personal que son conectados a los sistemas de la empresa?

Si __ No__

3. ¿Existen zonas de la empresa en donde no se permite el uso de dispositivos móviles?

Si __ (Lugar)_____ No__

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

Si ___ (¿Cuál?) _____ No__

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

Si __ No__

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

Si __ No__

7. ¿Puede acceder a información interna de la empresa a través de su dispositivo móvil?

Si __ No__

8. ¿Existe algún listado de aplicaciones prohibidas para los dispositivos móviles para el manejo de la información de la empresa?

Si ___ ¿Cuáles? _____

No__

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

Si __ No__

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)?

Si __ No__

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

Si __ No__

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

Si __ No__

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

Si __ No__

14. ¿Cuándo transporta el dispositivo móvil fuera de la empresa lo realiza de forma segura?

Si __ ¿De qué forma? _____

No__

ANEXO B. POLÍTICAS APLICADAS PARA SOLVENTAR LAS VULNERABILIDADES DE LA EMPRESA TELECOMEXPERT

Vulnerabilidades	Tipo Activo	Políticas
Fallas en el software de los equipos	SW	Artículo 24 Artículo 25
Bloqueo del equipo al momento de terminar el trabajo cuando se haga uso del DM	SW	Artículo 19
Software no licenciado, aplicaciones instaladas de fuentes desconocidas	SW	Artículo 24 Artículo 25
No cambiar las contraseñas de los DM	SW	Artículo 20 Artículo 21
Falta de actualización de las aplicaciones, antivirus y S.O de los DM	SW	Artículo 24 Artículo 25|
Mantenimiento insuficiente de los DM	HW	Artículo 22
Susceptibles a polvo, suciedad, caídas	HW	Artículo 22 Artículo 40
Fallas de hardware en los DM	HW	Artículo 22
Robo de equipos	HW	Artículo 40 Artículo 41 Artículo 42
Ausencia de copias de respaldo de la información almacenada en los DM	AI	Artículo 30
Información sin ningún tipo de seguridad o cifrado en los DM	AI	Artículo 18 Artículo 20
Gestión inadecuada de red	COM	Artículo 23 Artículo 38
Dejar activa la conexión a la VPN desde el DM	COM	Artículo 17
Conexión de datos deficiente de los DM	COM	Artículo 39
No guardar backups de la configuración de los DM	COM	Artículo 30
Fallas de la batería de los DM	AUX	Artículo 22
Falla del display	AUX	Artículo 22
Ausencia del personal que tiene a cargo los DM	PER	Artículo 12
Mala manipulación de la información almacenada en los DM	PER	Artículo 20 Artículo 30
Falla del servicio de internet	SRV	Artículo 39

ANEXO C. OFICIO DE COLABORACIÓN OTORGADO POR LA EMPRESA TELECOMEXPERT.

Riobamba, 4 de mayo del 2020

Ingeniero
Oswaldo Martinez Ph.D.;
COORDINADOR DE LA MAESTRÍA DE SEGURIDAD TELEMÁTICA DE LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
Presente. -

Tengo el agrado de dirigirme a Usted, con la finalidad de hacer de su conocimiento que la Srta. Jenny Gabriela Vizuete Salazar; con cédula de identidad N°.0603622085, estudiante de la maestría en Seguridad Telemática, colaboró con el desarrollo de las políticas de seguridad en dispositivos móviles para el manejo de información para la empresa TELECOMEXPERT.

Atentamente,

Ing. Cristian López
Gerente General TELCOMEXPERT
Expertos en Telecomunicaciones

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 17 / 08 /2020

INFORMACIÓN DEL AUTOR/A (S)
N Nombres – Apellidos: Jenny Gabriela Vizuete Salazar
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: Magíster en Seguridad Telemática
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

17-08-2020

0206-DBRAI-UPT-2020