FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas

“**APLICACIÓN MOVIL Y LA GESTION DE LA SEGURIDAD DE PYMES DE LA REGION LA LIBERTAD AÑO 2021**”

Tesis para optar el título profesional de:

Ingeniero de Sistemas

Autor:
Luis Eduardo Merino Hidalgo

Asesor:
Mg. Edwin Mendoza Torres

Trujillo - Perú

2021

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi padre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones. A mi madre, a pesar de nuestra distancia física, siento que estás conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para ti como lo es para mí. A mi amada esposa Carmen Aguilar Haro, por su apoyo incondicional, por acompañarme durante todo este arduo camino y compartir conmigo alegrías y fracasos. A mi hijo Luciano Merino Aguilar, él es lo mejor que me ha pasado en la vida, es sin duda mi referencia para el presente y para el futuro.

Luis Eduardo Merino Hidalgo

AGRADECIMIENTO

En primer lugar, doy infinitamente gracias a Dios, por haberme dado fuerza y valor para culminar esta etapa de mi vida.

Agradezco también la confianza y el apoyo brindado por parte de mi Sra. Esposa, que sin duda alguna en el trayecto de mi vida me ha demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

A mis hermanos, que con sus consejos me ha ayudado a afrontar los retos que se me han presentado a lo largo de mi vida.

A mi padre, que siempre lo he sentido presente en mi vida. Y sé que está orgulloso de la persona en la cual me he convertido.

Al Mg. Edwin Mendoza Torres por toda la colaboración brindada, durante la elaboración de este proyecto.

Luis Eduardo Merino Hidalgo

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente trabajo de investigación se realizó con el objetivo de determinar la influencia en la gestión de la seguridad de la información en PYMES de la Región la Libertad durante el año 2018.

El tiempo de estudio fue de un año; con una muestra de una PYME con 15 trabajadores. Para la recolección de datos se aplicó la entrevista, el instrumento es la guía de entrevista la cual fue realizada al gerente de la empresa y a los trabajadores. Para el análisis de datos se utilizó un análisis de correlación de las variables.

Las dimensiones comprendidas en la Variable Gestión de la Seguridad en PYMES son confidencialidad, disponibilidad e integridad, mientras que las dimensiones comprendidas en la Variable Aplicación Móvil es la calidad de la aplicación móvil. Con base a lo mencionado podemos concluir que se logró determinar que la relación entre la gestión de la seguridad de la información y de la aplicación móvil es directamente proporcional y se condicionan directamente.

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad problemática

Actualmente las diferentes organizaciones públicas o privadas, implementan políticas de seguridad informáticas con el afán de proteger su activo más importante que es su información. Marcinkowski y Stanton (2003) señalan que la política de seguridad de la información está en el corazón de los enfoques de muchas organizaciones para reforzar las conductas deseables de seguridad de la información y reforzar las restricciones contra los comportamientos de seguridad indeseables (p.2527). Según Alnatheer (2015), una política de seguridad es una parte esencial de las prácticas de seguridad dentro de las organizaciones y podría tener un impacto sustancial en su seguridad organizacional (p.1). "Sin una política, las prácticas de seguridad se desarrollarán sin una delimitación clara de los objetivos y responsabilidades" (Higgins, 1999, p.1; citado en Alnatheer, 2015, p.1).

Sin embargo, considerar que la protección de la seguridad de la información, a través de sus políticas, se llevaría a cabo solo a través de una perspectiva tecnológica, tendría un enfoque incompleto, pues los estudios que se han realizado a la fecha, demuestran que es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel fundamental. Tal es así, que en un reporte de Gartner (2014), menciona que las empresas deben adoptar un enfoque multifacético, apalancando personas, procesos y tecnología juntas, para crear comunidades de confianza respaldadas por la supervisión y el análisis (Walls, 2014, p.6). La tecnología no puede garantizar únicamente un entorno seguro para la información; deben tenerse en cuenta los aspectos humanos de la seguridad de la información, además de los aspectos tecnológicos (Sohrabi Safa, Solms & Furnell, 2016, p.2). Por lo tanto, las amenazas a la seguridad de la información no pueden prevenirse, evitarse, detectarse o eliminarse

concentrándose únicamente en soluciones tecnológicas (Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014, p.1). Por ejemplo, respecto a la importancia del factor humano dentro de las organizaciones, los datos del 2015 de Forrester, señalan que el 39% de los tomadores de decisiones empresariales y tecnológicas de Norteamérica y Europa en firmas con 20 o más empleados que tuvieron una violación de seguridad en los últimos12 meses dijeron que los incidentes internos dentro de su organización eran una de las maneras más comunes en que las violaciones ocurrieron (citado en Kindervag, Shey & Mak, 2016, p.3). Afirmación que coincide con un reporte de investigación de la empresa de seguridad Imperva (2016), en la que indica que les resulta preocupante que muchas brechas significativas en los datos son en última instancia en el "trabajo interno". Los iniciados, ya sean empleados, contratistas, socios comerciales o socios, representan el mayor riesgo para los datos empresariales, ya que por definición se les otorga acceso confiable a datos confidenciales (Imperva, 2016, p.2).

El incumplimiento total o parcial de las políticas de seguridad informáticas, violaciones a los sistemas de información, conllevan a pérdidas económicas o de imagen de la organización, los cuales son significativas. Por ejemplo, según AT&T Cybersecurity Insights (2017), espera que los daños causados por los delitos cibernéticos lleguen a los 6 trillones de dólares anuales para el año 2021, representando la mayor transferencia de riqueza económica de la historia y los riesgos de incentivos para la innovación y la inversión. Para IBM y Ponemon Institute (2016) el costo total promedio de una violación de datos para las 383 empresas que participaron en su investigación aumentó de $ 3,79 a $ 4 millones y el costo promedio pagado por cada registro perdido o robado que contenía información sensible y confidencial aumentó de $ 154 en 2015 a $ 158 en el estudio de este año. Kaspersky Lab (2017) sostiene que en promedio las empresas pagan US$ 551

000 para recuperarse de una violación de seguridad y que las PYMES gastan 38K. Este es el gasto directo necesario para recuperarse de un ataque.

En Latinoamérica el origen de incidentes de seguridad de la información está representados mayormente por ex empleados, actuales empleados y cibercriminales con un porcentaje de incidentes de 38,85%, 34,53% y 28,22% respectivamente. Además, según el diario El (Comercio 2015).Afirma que "se podría decir que actualmente hay muchas formas relativamente fáciles de acceder a la información de organizaciones que no estén bien protegidas, causando graves perjuicios para la empresa". En la actualidad, muchas empresas han adoptado diversos tipos de desarrollos tecnológicos, logrando así un aumento de su productividad; el desarrollo tecnológico que destaca en las ventas de los trabajadores en muchas empresas, son las aplicaciones móviles; ya que, los trabajadores pueden valerse de esta herramienta móvil para facilitar algunas labores con más eficiencia y rapidez (Fernando Miranda Alonso, 2007).

Es así que las aplicaciones móviles basadas en Android, no solamente se desenvuelven en empresas, también encontramos ejemplos como en la biblioteca de Salamanca. Fernando Miranda (2017). Afirma que "para mejorar su gestión de procesos en cuanto consulta, ubicación y reserva de libros ha optado por este tipo de tecnología móvil que interactúa directamente con sus trabajadores y sus visitantes con el fin de ahorrar tiempo".

También encontramos este tipo de aplicaciones en el medio nacional como es el caso del cine "CinePlanet" que tiene aplicaciones móviles para que sus trabajadores puedan informar y registrar pedidos de manera rápida y eficaz, a través de otra aplicación los usuarios también pueden acceder a consultar la cartelera con información debida, de esta forma logran optimizar su gestión de ventas. De igual forma en la ciudad de Trujillo en el hotel Bracamonte, está usando la tecnología móvil mediante una aplicación interactiva que permite la rápida inducción de los trabajadores para optimizar procesos en la gestión de

ventas.

Es así que las empresas hoy en día desconocen cómo proceder ante un evento de pérdida de información o la existencia de algún delito que comprometa la seguridad de la información, es por ello que con esta aplicación se pretende tener un instrumento que nos indique cómo proceder ante ciertos eventos y también que lineamientos debemos tomar en cuenta para el aseguramiento de la información presentar y describir el problema de investigación.

Un estudio elaborado por la compañía de seguridad Kaspersky denominado "Informe Especial ¿Quién le espía? Ninguna empresa está a salvo del ciberespionaje" señala que ninguna empresa está exenta de sufrir ciberataques o ciberespionaje. No obstante, el mayor riesgo lo tienen las pymes, más vulnerables a esta problemática por su mayor falta de recursos y también por su menor concienciación en este aspecto. El problema no es solo que éstas sean atacadas, aunque sean pequeñas no significa que no tengan datos importantes e información confidencial a proteger, sino que, además, pueden convertirse, sin quererlo, en una puerta de entrada de los atacantes a empresas grandes de las que sean socios de confianza.

El caso no queda ahí, GlobalGate publica el análisis desarrollado por el Laboratorio de Investigación de ESET. Kaspersky ESET Security Report (2014). Especificando que "el 41% de las empresas de América Latina afirma haber sufrido infección por códigos maliciosos, informe que analiza el estado de la seguridad informática en Latinoamérica y que presenta los resultados de encuestas realizadas a más de 3300 profesionales de distintas organizaciones".

Por otro lado; Kaspersky ESET Security Report (2014) . PP 6. Afirma que, "el 70,6% del phishing financiero, unos de los ciberataques más frecuentes, estuvo dirigido a las páginas

de los bancos, 20,7% fue contra las tiendas online y 8,7% contra los sistemas de pago". Según la investigación, en la categoría de 'sistemas de pago', los cibercriminales se han dirigido principalmente a robar los datos de usuarios de tarjetas Visa (31,02% de las detecciones), PayPal (30,03%) y American Express (24,6%)".

Además, Eset Security Report Latinoamérica (2014). Precisa que "las pequeñas y medianas empresas (pymes) durante el 2013 sufrieron en primera medida incidentes de infecciones de malware, puntualmente un 67,10% de las empresas. Los casos de phishing y explotación de vulnerabilidades ocupan los lugares siguientes, habiendo afectado al 48, 43% y 47,35% de las empresas respectivamente. Si bien las empresas grandes también sufrieron incidentes de infección de malware y phishing, el tercer lugar corresponde a la falta de disponibilidad (afectando al 51,35% de las empresas".

Kosutic, (2014), Establece que "la Norma ISO/IEC 27001 es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información, ayudando así a proteger la información de posibles robos o daños. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2".

No obstante, ISO/IEC 27001 (2005). Establece que "la Seguridad de la Información definida como parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, La confidencialidad de la información definida como la propiedad que esa información esté disponible y no se divulgada a personas, entidades o proceso no autorizado".

También, ISO/IEC (2005). Afirma que "los incidentes de seguridad de la información como uno solo o una serie de eventos de seguridad de la información no deseados o

inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. Un evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad".

Según un informe de la firma Digiware (2012). señala que "el Perú es el quinto país de América Latina que más recibe ataques cibernéticos. Según el estudio, el Perú concentra el 11.22% de recepción de ataques cibernéticos, luego aparecen Colombia 21.73%, Brasil con el 19% de recepción de ataques cibernéticos, Argentina con el (13.94%), mientras que Ecuador tiene un porcentaje similar que el Perú (11.25%)"

La tesis de Guachi Aucapiña, T.V., Guevara Aulestia D.O. (2012), en Ambato. Ecuador denominada "Norma De Seguridad Informática ISO 27001 Para Mejorar La Confidencialidad, Integridad Y Disponibilidad De Los Sistemas De Información Y Comunicación En El Departamento De Sistemas De La Cooperativa De Ahorro Y Crédito San Francisco Ltda." – Universidad Técnica de Ambato. Este trabajo reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Montoya Pachas, N. K. (2012), en Lima. Perú, presentó la tesis "Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional", cuyo objetivo fue proteger los activos de la información ante las amenazas a las cuales están expuestas, y de

esta manera dar un tratamiento a los riesgos de información en los procesos de la Municipalidad , este proyecto se realizó siguiendo lo propuesto en la Norma ISO/IEC 27001:2005 para elaborar el diseño de un SGSI donde se establezcan una política, objetivos , procesos y procedimientos.

La presente investigación brindó un apoyo en la consideración del Sistema de Gestión de Seguridad de la Información el cual se basó bajo la misma Norma ISO 27001 de la investigación, por lo que permitió gestionar la seguridad de sus activos con el objetivo de darle un tratamiento adecuado.

Espinoza Aguinaga, H. R. (2013), En Lima. Perú, realizó una tesis titulada: "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo – Pontifica Universidad Católica del Perú", el problema presentado en la empresa es en cuanto al manejo de la seguridad de la información. En el cual se planteó el análisis y diseño de un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo. De las cuales era Inventariar los procesos de negocio, los procesos de Este trabajo es motivado por el aporte y utilidad que puede significar a los empleados de una Pyme de como registrar las incidencias y sobre todo que hacer en caso de que se presente , debido a la necesidad creciente de cerrar brechas de seguridad que se originan en ataques focalizados al usuario, como por ejemplo a través de trampas de ingeniería social y que sumados a que casi todo lo utilizado por el atacante es ahora descartable genera la percepción de que ahora los atacantes avancen a un ritmo que los defensores nunca podrán alcanzar (Arbor Networks, 2017, pp. 3-4), por lo que se hace necesaria contrarestarla a través del establecimiento de políticas de seguridad que impliquen el conocimiento del comportamiento del usuario para su cumplimiento.

La tesis de Justino Salinas, Zully Isabel titulada "Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013" establece que la información, tanto digital como física, cumple un papel muy importante en una organización ya que actúa como activo principal y genera valor económico real para esta. Es por ello que toda información debe de ser protegida para que se encuentre accesible en tiempo y forma adecuados o, desde el punto de vista de seguridad de la información, conserve sus características de confidencialidad, integral y disponibilidad.

La tesis de Huamán Monzón, Fernando Miguel titulada Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano plantea la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información de la misma. Esta necesidad, a causa del carácter obligatorio de las normas mencionadas, es reconocida como la atención a la falta de procedimientos que permitan realizar auditorías que verifiquen el cumplimiento de la NTP-ISO/IEC 17799 como parte del proceso de cumplimiento integral de la NTP-ISO/IEC 27001 en las empresas del estado peruano.

La tesis de Talavera Álvarez, Vasco Rodrigo titulada Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013 desarrolla el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud.

La tesis de Espinoza Aguinaga, Hans Ryan titulada Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. En el presente proyecto se tomaran en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información para que pueda ser empleado por una empresa dedicada a la producción de alimentos de consumo masivo en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo que respecta a seguridad de información.

La tesis de Barrantes Porras, Carlos Eduardo; Hugo Herrera, Javier Roberto titulada Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos, dicha investigación permitió un gran aumento de la seguridad de los activos de la información de la empresa en la que se aplicó.

Las pequeñas empresas que implementan ISO/IEC 27001 pueden lograr los mismos niveles de éxito que las grandes organizaciones. Es por eso que este trabajo plantea cómo ISO/IEC 27001 mantiene en el cumplimiento con las normas de seguridad de la información de clase mundial, así como con la legislación y por ende la gestión adecuada de la seguridad de la información.

La presente investigación se justifica porque la implementación de esta solución permitirá Reducir los riesgos de seguridad de la información de las PYMES de la Región la Libertad y también Incrementar el nivel de seguridad basados en el ISO 27001 respecto a la eficacia

de los resultados del acceso a los estándares de seguridad de la información a través de la aplicación móvil.

Tecnológicamente la implementación de esta solución permitirá dejar una base de conocimiento en cuanto a la integración de una aplicación móvil y el uso de una norma como la ISO 2700.

Socialmente la aplicación de esta solución permitirá que los miembros de una pyme sin previos conocimientos sobre ISO 27001 sean más conscientes de los riesgos y además podrán instruirse mejora a través del uso de una aplicación móvil sencilla y fácil de usar.

Implementar esta solución permitirá reducir el consumo de papel, ya que la información para registrar incidencias y para saber que hacer frente a una de ellas estará en formato digital, contribuyendo así a la conservación del medio ambiente.

Se encontraron las siguientes limitaciones en el desarrollo del proyecto: falta de experiencia por parte del tesista, en el desarrollo de aplicaciones móviles, falta de tiempo por parte del personal de la pyme para entrevistar y falta de conocimiento metodológico para la aplicación de la norma ISO 27001 por parte del tesista. Sin embargo, estos tres puntos fueron abordados de manera satisfactoria mediante la investigación y asesoramiento externo, se pudieron entrevistar al gerente de la empresa, los gerentes de operaciones y de sistemas, y a los empleados, Conjuntamente, en este trabajo de investigación recogemos conceptos como:

Activos de información de importancia de las PYMES

Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

Los activos se encuentran relacionados, directa o indirectamente, con las demás entidades según el siguiente esquema:

A nivel internacional, la ISO 27002 define activo como "Cualquier cosa que tiene valor para la organización", y recomienda los siguientes tipos de activos de información para las pymes:

- Datos o Información
- Software
- Hardware
- Servicios
- Personas
- Conocimiento

Identificación de amenazas para PYMES

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. El Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 ayuda a controlar las amenazas que pueden desencadenar los incidentes.

La definición de amenaza es la diversidad de consecuencias, lo que hay que tener en cuenta es examinar el impacto (ISO/IEC 27001:2005).

Características

La definición anterior recoge la esencia de las amenazas, es decir, es un potencial evento. La consecuencia de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma, que se trate la amenaza o las agresiones materializadas (ISO/IEC 27002).

La consecuencia de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma, que se trate la amenaza o las agresiones materializadas.

Tipos de Amenazas

Todas las causas de las amenazas permiten ser clasificadas por su naturaleza. Podemos emplear cuatro causas amenazadoras: no humanas, humanas involuntarias, humanas intencionales que necesitan presencia física y humana intencional que proceden de un origen remoto (ISO/IEC 27001:2005).

No Humanas

A1: Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.

A2: Averías que pueden ser de origen físico o lógico, se debe al efecto de origen.

A3: Accidente físico de origen natural, riada, fenómeno sísmico o volcánico.

A4: Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.

A5: Accidentes mecánicos o electromagnéticos.

Humanas

E1: Errores de utilización ocurridos durante la recogida y transmisión de datos.

E2: Errores de diseño existentes desde los procesos de desarrollo del software.

E3: Errores de ruta, secuencia o entrega de la información durante el tránsito.

E4: Errores de monitorización, trazabilidad o registros del tráfico de información.

Políticas de la seguridad de la información en PYMES

Las políticas de seguridad de la información es uno de los puntos más relevantes del proceso de implantación del sistema y, frecuentemente, uno de los peor entendidos en las pequeñas empresas. (ISO/IEC 27001:2005)

La creación de una política eficaz y aplicable a estas organizaciones requiere de la comprensión de los activos, riesgos y recursos disponibles para la gestión de riesgos. Lo que queremos decir es que antes de dirigirse a proteger algo, primero se debe saber qué es lo que hay que proteger y de qué.

Una metodología para desarrollar la política de Seguridad de la Información que propone ISO-27001 puede ser la siguiente:

- Identificar de lo que se está tratando proteger.
- Determinar de qué lo estamos protegiendo.
- Determinar qué amenazas tiene y la frecuencia de que ocurran.
- Poner en marcha medidas que protejan los activos, evaluando costes y efectividad.
- Revisar periódicamente el proceso con objeto de hacer mejoras cuando se encuentren debilidades.

El proceso más difícil para las pequeñas empresas suele ser la determinación de lo que realmente es esencial proteger para poner en marcha la Política de Seguridad de la Información.

Una solución fue entrevistar al propietario de la organización y a los trabajadores que participan en el Sistema de Seguridad de la Información. En pequeñas empresas se dan menos este tipo de entrevistas ya que operan de modo distinto a las grandes.

La identificación de activos de personal puede ser más fácil en el caso de la pequeña empresa, simplemente por el número de empleados.

La persona encargada de iniciar el proceso de esta Política debe tener una base tecnológica razonable y conocer los procesos del Sistema de Seguridad de la Información.

No es esencial el conocimiento detallado de la tecnología, se le da más valor a poseer la capacidad de comunicarse y obtener información.

Para concluir cabe preguntarse, ¿Qué puede hacer la Política de Seguridad de la Información para reducir o eliminar riesgos? ¿Qué medidas hay que tomar para asegurar que el negocio sigue funcionando? ¿A quién va dirigida la Política?

Gestión de Activos

La información que se debe proteger de riesgos y amenazas en las organizaciones y así asegurar el correcto funcionamiento de su negocio. Esto es lo que se denomina activo de seguridad de información el cual es imprescindible en cada empresa y su protección es el objetivo de todo Sistema de Gestión de seguridad de la Información.

Para proteger los activos de información es necesario conocerlos e identificar cuáles son dentro de la organización. Para esta tarea se elaborará un inventario que los identifique y clasifique.

Cada activo del inventario debe incluir toda la información esencial de cada activo, incluyendo el tipo de activo, valor, localización, licencias, formato, etc.

El propietario del activo debe ser quien defina el grado de seguridad que requiere su activo.

El propietario no tiene, necesariamente, que ser quien va a gestionar el activo o ser su usuario, pero si es en quién recae la última responsabilidad de la correcta gestión de su activo (ISO/IEC 27001:2005) .

Por ejemplo, una empresa certificada en ISO 27001 tendrá una base de datos de clientes que puede pertenecer al Director Comercial de una empresa, su gestión puede estar encomendada al área de sistemas y sus usuarios pueden ser los comerciales, pero es el Director Comercial quién debe comprobar que todo se está realizando correctamente.

Una vez identificados todos los activos hay que realizar un análisis de las dependencias existentes entre ellos. Para establecer esas dependencias se pueden hacer preguntas del tipo ¿quién depende de quién? o ¿si hay un fallo en el activo X qué otros activos se van a ver perjudicados o involucrados?

Además, para cada nivel de clasificación deben determinarse los procedimientos de etiquetado y tratamiento durante todo el ciclo de vida del activo, así como los métodos de destrucción seguros (ISO/IEC 27001:2005).

Como resultado de dicho análisis se obtendrá un árbol de dependencias de activos en el que se podrá ver la relación existente entre todos los activos de una organización desde los de más alto nivel hasta llegar a los de nivel más bajo.

No todos los activos tienen la misma importancia para la organización, ni generan los mismos problemas sin son atacados. Por ello es necesario realizar una valoración de los activos en función de la relevancia que tengan para el negocio y del impacto que una incidencia sobre el mismo pueda causar a la organización.

Podemos realizar una valoración cuantitativa, en la que se estima el valor económico del activo, o cualitativa.

La valoración cualitativa se establece de acuerdo a una escala, por ejemplo, del 0 al 10 o con valores del tipo: bajo, medio y alto. En este tipo de

valoración es muy importante que exista un criterio homogéneo de valoración que permita comparar entre activos. El criterio que se suele utilizar está basado en las características principales de la información, es decir, en la integridad, confidencialidad y disponibilidad.

Organización de la seguridad de la información

Organización interna

Roles y responsabilidades para la seguridad de la información

Control

Se deberían definir y asignar todas las responsabilidades de la seguridad de la información

Guía de Implementación

- Se deberían identificar y definir los activos y los procesos de seguridad de la información.
- Se debería asignar la entidad responsable de cada activo o proceso de seguridad de la información, y se deberían documentar los detalles de esta responsabilidad
- Se deberían definir y documentar los niveles de autorización.
- Los individuos nombrados deberían ser competentes en el área y se les debería brindar oportunidades de mantenerse actualizados con los avances en este tema.
- Se deberían identificar y documentar la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores
- Información adicional

Muchas organizaciones nombran un gerente de seguridad de la información que asuma la responsabilidad total por el desarrollo e implementación de la seguridad

de la información y que apoye la identificación de los controles. Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección diaria (ISO/IEC 27001:2005).

Separación de deberes

Control

Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización

Guía de implementación

- Ninguna persona pueda acceder, modificar o usar activos sin autorización ni detección.
- El inicio de un evento debería estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación.
- Para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, pero el principio se debería aplicar en tanto sea posible y viable. Siempre que resulte difícil hacer la separación, se deberían considerar otros controles, tales como el seguimiento de actividades, los rastros de auditoría y la supervisión de la dirección.

Información adicional

La separación de los deberes es un método para reducir el uso indebido, accidental o deliberado, de los activos de una organización.

Contacto con las autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de qué autoridades se debería contactar a las autoridades, y cómo se deberían reportar de una manera oportuna los incidentes de seguridad de la información identificados.

Información adicional

Las organizaciones que son atacadas por Internet pueden necesitar que las autoridades emprendan acciones contra la fuente del ataque.

Contacto con grupos de Interés adicional

Control

Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Guía de implementación

La membresía en grupos o foros de interés especial se debería considerar como un medio para:

a) Mejorar el conocimiento acerca de las mejores prácticas y permanecer al día con la información de seguridad pertinente.
b) Asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.
c) Recibir advertencias tempranas de las alertas, avisos y parches acerca de ataques y vulnerabilidades.
d) Obtener acceso a asesoría especializada en seguridad de la información;
e) Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
f) Brindar puntos de enlace adecuados cuando se trata con incidentes de seguridad de la información.

Información adicional

Se pueden establecer acuerdos acerca de intercambio de información para mejorar la cooperación y coordinación de cuestiones de seguridad. Estos acuerdos deberían identificar los requisitos para la protección de información confidencial.

Seguridad de la información en la gestión de proyectos

Control

La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.

Guía de implementación

Los métodos de gestión de proyectos que se usen deberían requerir que:

a) Los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto.

b) La valoración de los riesgos de seguridad de la información se lleva a cabo en una etapa temprana del proyecto, para identificar los controles necesarios.

c) La seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

Dispositivos Móviles y teletrabajo

Política para dispositivos móviles

Control

Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Guía de implementación

La política de dispositivos móviles debería considerar:

- El registro de los dispositivos móviles.
- Los requisitos de la protección física.

- Las restricciones para la instalación de software.
- Los requisitos para las versiones de software de dispositivos móviles y para aplicar parches.
- La restricción de la conexión a servicios de información.
- Controles de acceso
- Técnicas criptográficas.
- Protección contra software malicioso.
- Deshabilitación remota, borrado o cierre.
- Copias de respaldo.
- Uso de servicios y aplicaciones web.

Teletrabajo

Control

Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo

Guía de implementación

Las organizaciones que permiten actividades de teletrabajo deberán expedir una política que defina las condiciones y restricciones para el uso del teletrabajo. Cuando se considera aplicable y lo permite la ley, se deberían considerar los siguientes asuntos:

- La seguridad física existente en el sitio del teletrabajo, teniendo en cuenta la seguridad física de la edificación y del entorno local.
- El entorno físico de teletrabajo propuesto.
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la

sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno.

- El suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada.
- La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento.
- El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica.
- Las políticas y procedimientos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada.
- Acceso a equipo de propiedad privada, que se puede impedir mediante legislación.
- Acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos
- Requisitos de firewall y de protección contra software malicioso.

Las directrices y acuerdos que se consideren deberían incluir:

- El suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización;
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder;

- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto;
- Seguridad física;
- Las reglas y la orientación sobre el acceso de la familia y los visitantes a los equipos y a la información;
- El suministro de soporte y mantenimiento del hardware y el software;
- El suministro de seguros;
- Los procedimientos para copias de respaldo y continuidad del negocio;
- Auditoría y seguimiento de la seguridad;
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.

Control de acceso

El objetivo dentro de las organizaciones que cuentan con activos de información valiosos, más aún para las PYMES es limitar el acceso a información y a instalaciones de procesamiento de información.

Las PYMES propietarias de los activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a sus activos, con la cantidad de detalle y severidad de los controles, que reflejen los riesgos de seguridad de la información asociados.

Se debería dar a los usuarios y a los proveedores de servicios una indicación clara de los requisitos del negocio que deben cumplir los controles de acceso

La política debería tener en cuenta lo siguiente:

- Los requisitos de seguridad para las aplicaciones del negocio

- Las políticas para la divulgación y autorización de la información, por ejemplo, el principio de lo que se necesita conocer, y los niveles de seguridad de la información y de clasificación de la información.
- La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes
- La legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios
- La gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles
- La separación de los roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso, administración del acceso
- Los requisitos para la autorización formal de las solicitudes de acceso
- Los requisitos para la revisión periódica de los derechos de acceso
- El retiro de los derechos de acceso
- El ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente
- Los roles de acceso privilegiado

Cuando se especifican las reglas de control de acceso se debería considerar:

- Establecer las reglas basadas en la premisa "En general, todo está prohibido, a menos que se permita expresamente" y no la menos estricta: "Todo está permitido a menos que se prohíba expresamente"
- Los cambios en las etiquetas de información que son iniciados automáticamente por las instalaciones de procesamiento de información, y los que se inician a discreción del usuario.
- Los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información, y los iniciados por un administrador
- Las reglas que requieren aprobación específica antes de su promulgación, y las que no requieren aprobación

METODOLOGIA XP

Descripción

La metodología XP o Programación Extrema es una metodología ágil y flexible utilizada para la gestión de proyectos.

Extreme Programming se centra en potenciar las relaciones interpersonales del equipo de desarrollo como clave del éxito mediante el trabajo en equipo, el aprendizaje continuo y el buen clima de trabajo (Diego, 2018).

Características

- Se considera al equipo de proyecto como el principal factor de éxito del proyecto
- Software que funciona por encima de una buena documentación.
- Interacción constante entre el cliente y el equipo de desarrollo.
- Planificación flexible y abierta.
- Rápida respuesta a cambios.

Fases

A. Fase: Planificación del proyecto.

En esta primera fase se debe hacer una recopilación de todos los requerimientos del proyecto, también debe haber una interacción con el usuario final del producto software, se debe planificar adecuadamente entre el equipo de desarrolladores del proyecto, acerca de que es lo que se quiere para el proyecto para así lograr los objetivos del proyecto.

B. Fase: Diseño.

Se sugiere que hay que conseguir diseños simples y sencillos. Para procurar hacerlo lo menos complicado posible para el usuario o cliente, para conseguir un diseño fácilmente entendible e implementable que costará menos tiempo y esfuerzo para desarrollarlo. En esta fase se logrará crear parte del proyecto la parte visual, la interfaz

que tendrá el usuario o cliente con el proyecto y modelará la lógica de las funcionalidades del producto software.

C. Fase: Codificación.

Como ya se mencionó en la introducción, el cliente es una parte más del equipo de desarrollo; su presencia es indispensable en las distintas fases de XP. A la hora de codificar una historia de usuario su presencia es aún más necesaria. No olvidemos que los clientes son los que crean las historias de usuario y negocian los tiempos en los que serán implementadas. Antes del desarrollo de cada historia de usuario el cliente debe especificar detalladamente lo que ésta hará y también tendrá que estar presente cuando se realicen los test que verifiquen que la historia implementada cumple la funcionalidad especificada. En esta fase de la codificación los clientes y los desarrolladores del proyecto deben estar en comunicación para que los desarrolladores puedan codificar todo los necesario para el proyecto que se requiere, en esta fase está incluido todo lo de codificación o programación por parte de los desarrolladores del proyecto.

D. Fase: Pruebas.

Uno de los pilares de la metodología XP es el uso de test para comprobar el funcionamiento de los códigos que vayamos implementando.

Para esta fase lo que se implementa es el caso de uso de test que son pruebas que se le hacen al proyecto o como ya se dijo a los códigos que se vayan implementando.

Figura N° 1

. 1 Metodología

PRUEBA DE HIPÓTESIS

Las pruebas de hipótesis es una parte de la inferencia estadística que consiste, básicamente, en decidir cuál de dos posibles conjeturas sobre la población es verdadera, basándose en la información proporcionada por una muestra aleatoria. Una de las conjeturas se supone verdadera ya sea porque la historia o la experiencia así lo ha establecido o porque así lo indica el modelo que genera los datos. La otra conjetura es la que los datos parecen respaldar. La primera conjetura se denota como hipótesis nula y la segunda conjetura se denota como hipótesis alternativa. Generalmente, la hipótesis alternativa es aquella que defiende el investigador. (QUEVEDO & PÉREZ, 2014)

Hipótesis Alternativa

Se llama hipótesis alternativa a la conjetura que se pone a prueba. Es la hipótesis de investigación. La hipótesis alternativa se denota como Ha o H1. (QUEVEDO & PÉREZ, 2014)

Hipótesis Nula

Se llama hipótesis nula a la conjetura que se considera cierta, ya sea porque el modelo así lo indica, porque la historia lo ha probado o porque es lo aceptado. La hipótesis nula se identifica con el símbolo H0. (QUEVEDO & PÉREZ, 2014)

Estadística de Prueba

Se llama estadística de prueba a la función de los datos muestrales que se utiliza para tomar la decisión. (QUEVEDO & PÉREZ, 2014) Un estadístico de prueba es una variable aleatoria que se calcula a partir de datos de muestra y se utiliza en una prueba de hipótesis.

Puede utilizar los estadísticos de prueba para determinar si puede rechazar la hipótesis nula. El estadístico de prueba compara sus datos con lo que se espera bajo la hipótesis nula. El estadístico de prueba se utiliza para calcular el valor p. (MINITAB, 2018)

Tipos de prueba de hipótesis

Las diferentes pruebas de hipótesis utilizan diferentes estadísticos de prueba según el modelo de probabilidad asumido en la hipótesis nula. Las pruebas comunes y sus respectivos estadísticos de prueba incluyen:

Tabla 3. Pruebas comunes y sus respectivos estadísticos de prueba

Prueba de hipótesis	**Estadístico de prueba**
Prueba Z	Estadístico Z
Pruebas t	Estadístico t
ANOVA	Estadístico F
Pruebas de chi-cuadrada	Estadístico de chi-cuadrada

Fuente: MINITAB (2018)

Prueba Chi-cuadrada

Existen varios tipos de pruebas de chi-cuadrada:

Prueba de bondad de ajuste de chi-cuadrada

Utilice este análisis para probar qué tan bien una muestra de datos categóricos se ajusta a una distribución teórica.

Por ejemplo, usted puede comprobar si un dado es justo, lanzando el dado muchas veces y utilizando una prueba de bondad de ajuste de chi-cuadrada para determinar si los resultados siguen una distribución uniforme. En este caso, el estadístico de chi-cuadrada cuantifica qué tanto varía la distribución observada de los conteos con respecto a la distribución hipotética.

Pruebas de chi-cuadrada de asociación e independencia

Los cálculos para estas pruebas son iguales, pero la pregunta que se está tratando de contestar puede ser diferente.

Prueba de asociación: Utilice una prueba de asociación para determinar si una variable está asociada a otra variable. Por ejemplo, determine si las ventas de diferentes colores de automóviles dependen de la ciudad donde se venden.

Prueba de independencia: Utilice una prueba de independencia para determinar si el valor observado de una variable depende del valor observado de otra variable. Por ejemplo, determine si el hecho de que una persona vote por un candidato no depende del sexo del elector.

1.2. Formulación del problema

¿De qué manera el desarrollo de una aplicación móvil se relaciona con la Gestión de la Seguridad de la información en PYMES de la Región La Libertad?

1.3. Objetivos

1.3.1. Objetivo general

Determinar la relación en la gestión de la seguridad de la información en PYMES de la Región la Libertad a través del desarrollo de una aplicación móvil.

1.3.2. Objetivos específicos

- Determinar el nivel de los conocimientos; en el ámbito de seguridad de la información, de las PYMES de la Región la Libertad.
- Desarrollar la aplicación móvil para gestionar la seguridad de la información de las PYMES en la Región la Libertad
- Reducir los riesgos de seguridad de la información de las PYMES de la Región la Libertad.
- Determinar la relación entre el nivel de seguridad basados en el iso 27001 respecto a la eficacia de los resultados del acceso a los estándares de seguridad de la información a través de la aplicación móvil.

- Medir la relación de la aplicación móvil y los resultados de acceder a consultar estándares basados en iso 27001 de la seguridad de la información.
- Medir la relación entre la satisfacción del usuario con respecto a la gestión de la seguridad de la información y de la aplicación móvil.

1.4. Hipótesis

1.4.1. Hipótesis general

El desarrollo de una aplicación móvil se relaciona significativamente con la gestión de la seguridad de la información basado en las normas ISO 27001/27002 en las PYMES de la región La Libertad.

1.4.2. Hipótesis especificas

HE1: El desarrollo de una aplicación móvil se relaciona significativamente con la gestión de la confidencialidad de la información basado en las normas ISO 27001/27002 en las PYMES de la Región la Libertad.

HE2: El desarrollo de una aplicación móvil se relaciona significativamente con la gestión de la integridad de la información basado en las normas ISO 27001/27002 en las PYMES de la Región la Libertad.

HE1: El desarrollo de una aplicación móvil se relaciona significativamente con la gestión de la disponibilidad de la información basado en las normas ISO 27001/27002 en las PYMES de la Región la Libertad.

CAPÍTULO II. METODOLOGÍA

2.1. Tipo de investigación

Investigación correlacional.

2.2. Técnicas e instrumentos de recolección y análisis de datos

Recolección de datos

Técnicas

Para la obtención Porcentaje de archivos clasificados encriptados (PPWP) Porcentaje de postulantes con antecedentes investigados (PPAI) Porcentaje de contrataciones nuevas con acceso permitido (PCAP), se usó la técnica de la observación.

Por otra parte, para la obtención del porcentaje de Colaboradores con acceso permitido a modificación de archivos (PCAM) Porcentaje de Colaboradores con responsabilidad en la información (PCRI) Porcentaje de Colaboradores con funciones segregadas (PCFS), se usó como técnica a la encuesta.

Además, para la obtención del Porcentaje de Activos de Información Inventariados (PAII), Porcentaje de Colaboradores con acceso permitido a información clasificada (PCAIC) y el Porcentaje de la política de planificación y continuidad de negocios implementado (PPCN) se usó como técnica a la entrevista.

Instrumentos

De acuerdo con las técnicas aplicadas, el instrumento utilizado para los indicadores antes mencionados fue la ficha de observación. Este instrumento fue esquematizado para completar datos como la fecha, datos del observador, descripción del proceso observador persona que ejecuta la acción, así como también estructurado para ingresar información de los indicadores anteriormente mencionado, este instrumento

fue aplicado al gerente y personal clave de la pyme. Cabe mencionar que al tratarse de una pyme la información proporcionada por el gerente es muy valiosa.

Por otro lado, el instrumento utilizado para los indicadores sobre integridad y disponibilidad de los datos fue el cuestionario.

Este instrumento fue elaborado en Google Forms, dado que las personas a las que va dirigido son las que manipulan directamente la información para modificarla, el mismo fue estructurado en preguntas relacionadas con los indicadores anteriormente mencionados.

Análisis de datos

Para el análisis de datos se utilizó como herramienta estadística la herramienta XLSTAT, con la cual se realizó la tabulación de datos y posteriormente se aplicó la prueba estadística chi-cuadrada

2.3. Procedimiento

Para elaborar los instrumentos se analizaron los datos brindados por los trabajadores, mediante reuniones de trabajo en campo y virtuales como Zoom Meetings. Con lo cual se identificó elaborar 3 instrumentos, 2 cuestionarios y 1 ficha de observación. El cuestionario consta de preguntas obligatorias y de respuesta corta elaborado en Google Forms, enfocadas a obtener información con respecto a la evaluación de los indicadores. En cuanto a la ficha de observación se elaboró utilizando Microsoft Word, enfocada a obtener datos con respecto a la confidencialidad de la información.

Para la recolección de datos antes de la implementación se tomó contacto con el gerente de la empresa y el administrador de recursos humanos además de los colaboradores quienes brindaron su apoyo en las modalidades anteriormente expuestas. La información recolectada se pasó a Excel para ser tabulada obteniendo:

Tabla 2: Nivel de relación con la confidencialidad de la información en las PYMES, de la Libertad.

Confidencialidad	**Porcentaje de accesos a páginas web peligrosas prevenido**	**(Número de accesos a páginas web peligrosas prevenido/ Número total de accesos a páginas web) *100%**
	Porcentaje de archivos clasificados encriptados	(Número de archivos clasificados encriptados de la empresa/ Número total de archivos clasificados de la empresa)*100%
	Porcentaje de postulantes con antecedentes investigados	(Número de postulantes a trabajar en la empresa con antecedentes investigados / Número total de postulantes a trabajar en la empresa)*100%
	Porcentaje de contrataciones nuevas con acceso permitido	(Número de contrataciones nuevas de personal con acceso permitido a los archivos de la empresa/ Número total de contrataciones nuevas de personal de la empresa)*100%
Integridad	**Porcentaje de Colaboradores con Acceso permitido a modificación de archivos**	**(Número de colaboradores con acceso permitido a modificación de archivos de la empresa/ Número de total de colaboradores con acceso permitido a archivos de la empresa)*100%**
	Porcentaje de colaboradores con responsabilidades en la información definidos	(Número de colaboradores con responsabilidad en la integridad de la información definido/ Número de total de colaboradores)*100%
	Porcentaje de colaboradores con funciones segregadas	(Número de colaboradores con funciones segregadas / Número total de colaboradores)*100%

Tabla N° 3

Nivel	N°	%
PPWP	1	8%
PPAI	2	32%
PCAP	5	60%
Total	8	100%

Fuente: Datos obtenidos sobre seguridad de la Información en MYPES de la Región la Libertad

Leyenda:

Porcentaje de archivos clasificados encriptados	PPWP
Porcentaje de postulantes con antecedentes investigados	PPAI
Porcentaje de contrataciones nuevas con acceso permitido	PCAP

Figura N° 20

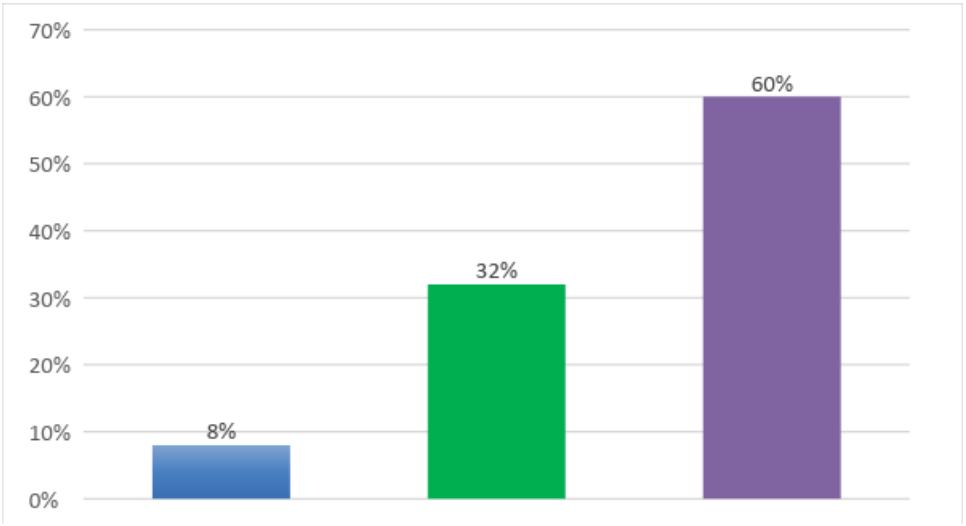


Figura **20***:*
Nivel de relación con la confidencialidad de la información en las PYMES, de la región la Libertad

Tabla 3: Nivel de relación con la Integridad de la información en las PYMES, de la Libertad.

Nivel	N°	%
PCAM	1	80%
PCRI	2	15%
PCFS	5	5%
Total	8	100%

Fuente: datos obtenidos MYPES del Sector Empresarial

Leyenda:

Porcentaje de Colaboradores con acceso permitido a modificación de archivos	PCAM
Porcentaje de Colaboradores con responsabilidad en la información	PCRI
Porcentaje de Colaboradores con funciones segregadas	PCFS

Figura N° 21

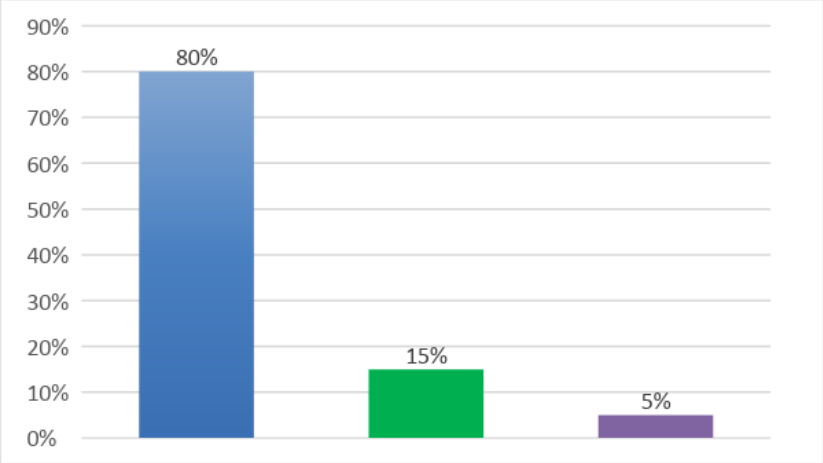


Figura 21:
Nivel de relación con la Integridad de la información en las PYMES, de la región la Libertad.

Tabla 4: Nivel de relación con la Disponibilidad de la Información en las PYMES, de la Libertad.

Disponibilidad	**Porcentaje de activos de información inventariados**	**(Número de activos de información inventariados/ Número total de activos de información)*100%**
	Porcentaje de colaboradores con acceso permitido a la información clasificada	(Número de colaboradores con acceso permitido a información clasificada de la empresa/ Número total de colaboradores de la empresa)*100%
	Porcentaje de la Política de Planificación y Continuidad de Negocios Implementado	(Número de elementos de la Política de Planificación y Continuidad de Negocios implementados/ Número total de elementos de la Política de Planificación y Continuidad de negocios determinado por el equipo de estudio)*100%

Tabla N° 5

Nivel	N°	%
PCAM	1	16%
PCRI	2	72%
PCFS	5	12%
Total	8	100%

Fuente: datos obtenidos MYPES del Sector Empresarial

Leyenda:
Porcentaje de Activos de Información Inventariados PAII

Porcentaje de Colaboradores con acceso permitido a información clasificada PCAIC

Porcentaje de la política de planificación y continuidad de negocios implementado PPCN

Figura N° 22

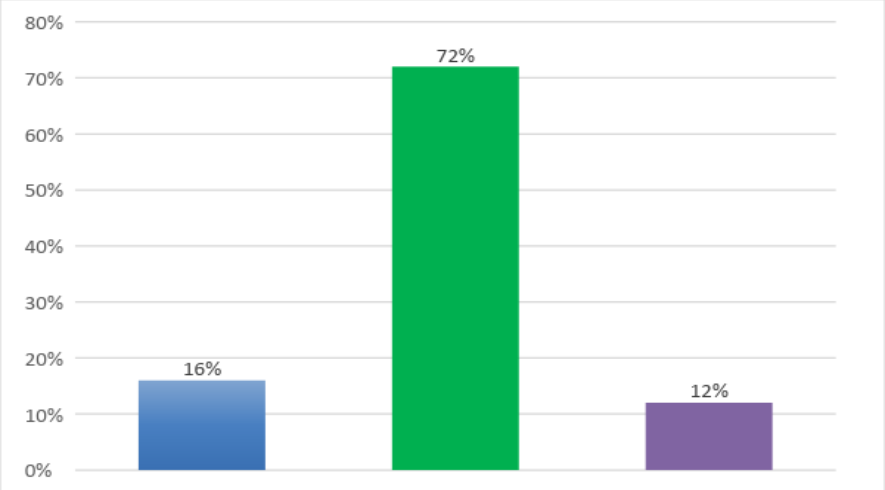


Figura 22:
Nivel de relación con la Disponibilidad de la información en las PYMES, de la región la Libertad.

CAPÍTULO III. RESULTADOS

A continuación, se muestran e interpretan los resultados de la relación entre ***la gestión de la seguridad de información y la aplicación móvil***

Tabla 5: Relación con la gestión de la seguridad de información del uso de la aplicación móvil.

			Uso de la aplicación			Total	Chi tabla	Chi Calculada	gl	P Sig. Asintótica
			C	D	I					
Proceso de llegada	**C**	**Recuento**	4	0	0	4	9.49	17.2	4	0.026
		% del total	53.0%	0.0%	0.0%	53.0%				
	D	**Recuento**	0	1	1	2				
		% del total	0.0%	11.5%	12.5%	24.0%				
	I	**Recuento**	1	0	1	2				
		% del total	10.5%	0.0%	12.5%	23.0%				
Total		**Recuento**	5	1	2	8				
		% del total	62.5%	11.5%	25.0%	100%				

Fuente: Datos obtenidos de la simulación de la aplicación móviledd

LEYENDA

C Confidencialidad
D Disponibilidad
I Integridad

Figura N° 23

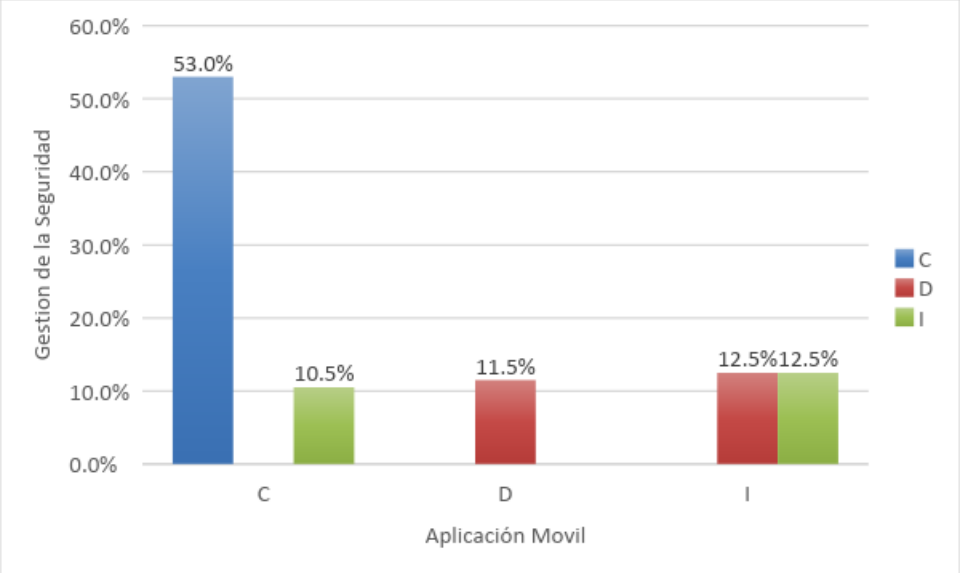
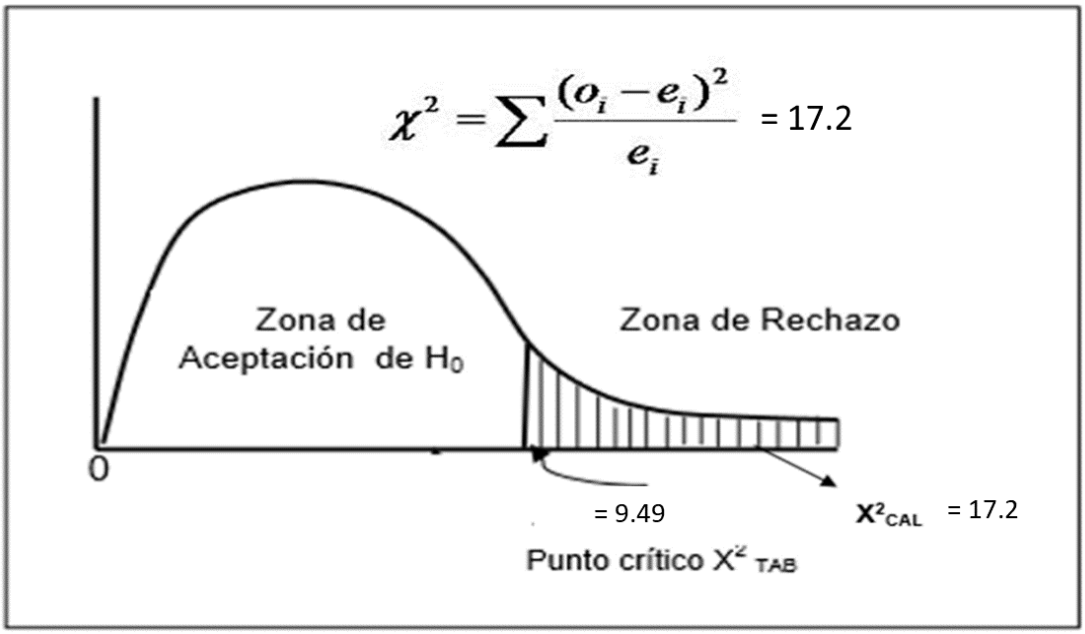


Figura 23:
Relación sobre la gestión de la seguridad de información del uso de la aplicación móvil.

Ecuación 1: Contrastación de hipótesis entre la gestión de la información y la aplicación móvil.



Interpretación: En cuanto los datos obtenidos sobre la relación entre la gestión de la seguridad del uso de una aplicación en las MYPES, se obtiene un valor de Chi cuadrado de 17.2 y valor de p=0.026, el cual hace referencia que hay una relación significativa positiva.

Tabla 6: Relación sobre la disponibilidad de la información del uso de la aplicación móvil.

			Uso de la aplicación			Total	Chi tabla	Chi Calculada	gl	P Sig. Asintótica
			Bueno	Malo	Regular					
Proceso de preparación	**Alto**	**Recuento**	4	0	0	4	9.49	13.267	4	0.035
		% del total	49.0%	0.0%	0.0%	49.0 %				
	Bajo	**Recuento**	0	1	2	3				
		% del total	0.0%	12.5 %	25.0%	37.5 %				
	Regular	**Recuento**	1	0	0	1				
		% del total	13.5%	0.0%	0.0%	12.5 %				
Total		**Recuento**	5	1	2	8				

% del total	62.5%	12.5 %	25.0%	100%

Fuente: Datos obtenidos de la simulación de la aplicación móvil

LEYENDA

C Confidencialidad
D Disponibilidad
I Integridad

Figura N° 24

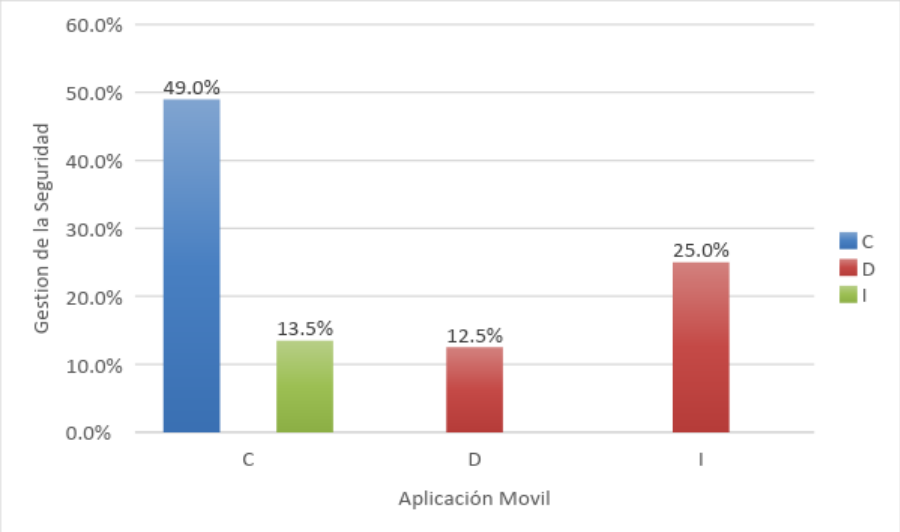
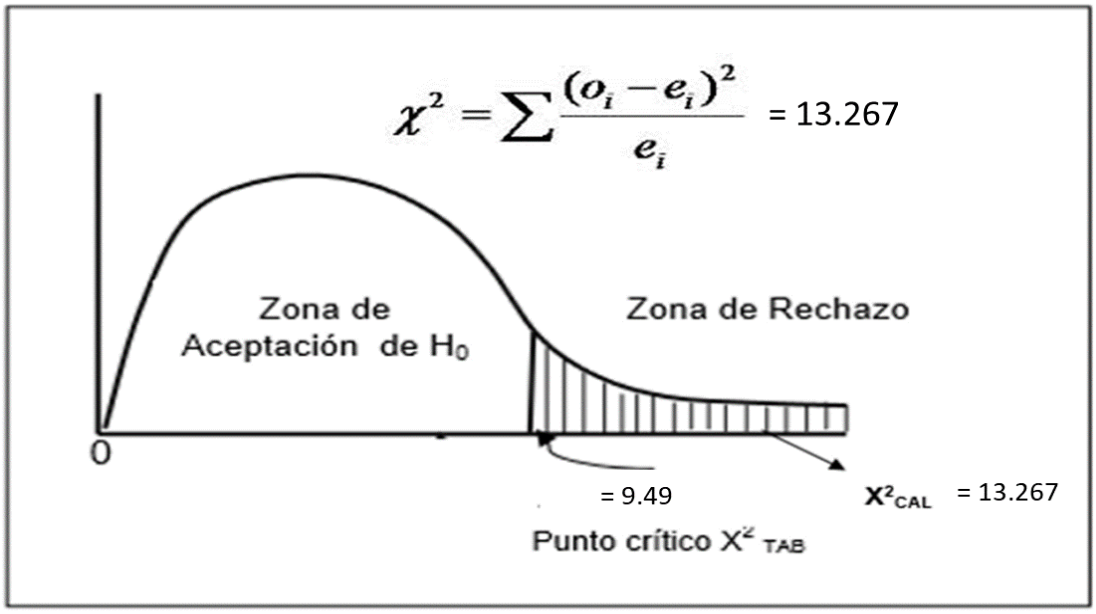


Figura 24:
Relación entre la disponibilidad de la información y el uso de la aplicación móvil.

Ecuación 2: Contrastación de hipótesis entre la disponibilidad de la información y el uso de la aplicación móvil.



Interpretación: En cuanto los datos obtenidos sobre la relación entre la disponibilidad de la información del uso de la aplicación móvil se obtiene un valor de Chi cuadrado de 13.267 y valor de p=0.035, el cual hace referencia que si existe una relación significativa positiva.

Tabla 7: Relación sobre la disponibilidad de la información del uso de la aplicación móvil.

			Uso de la aplicación			Total	Chi tabla	Chi Calculada	gl	P Sig. Asintótica
			C	D	I					
Proceso de entrega y pago	**C**	**Recuento**	4	0	0	4	9.49	12.267	4	0.015
		% del total	50.0%	0.0%	0.0%	50.0%				
	D	**Recuento**	0	1	0	1				
		% del total	0.0%	12.5%	0.0%	12.5%				
	I	**Recuento**	1	0	2	3				
		% del total	12.5%	0.0%	25.0%	37.5%				
Total		**Recuento**	5	1	2	8				
		% del total	62.5%	12.5%	25.0%	100.0%				

Fuente: Datos obtenidos de la simulación de la aplicación móvil

LEYENDA

C Confidencialidad
D Disponibilidad
I Integridad

Figura N° 25

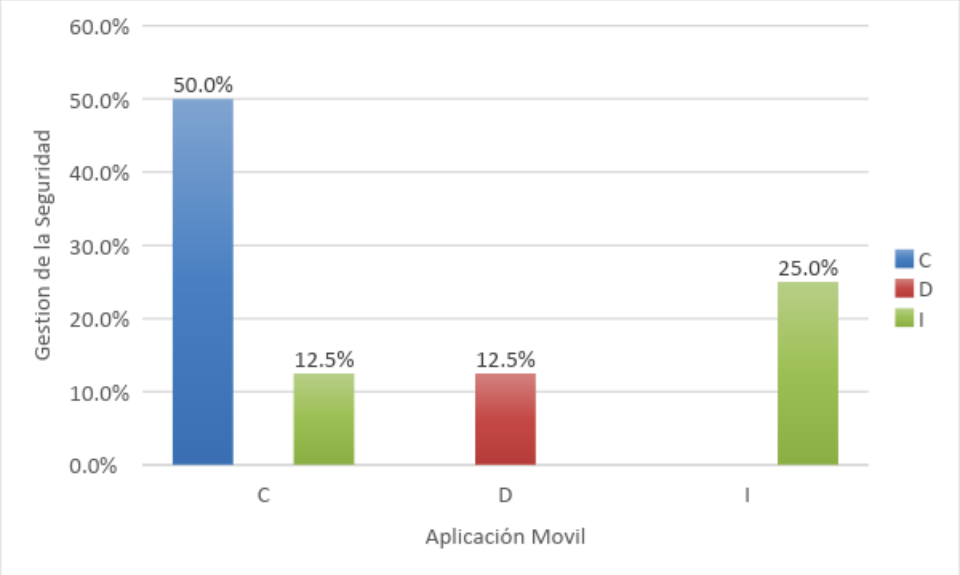
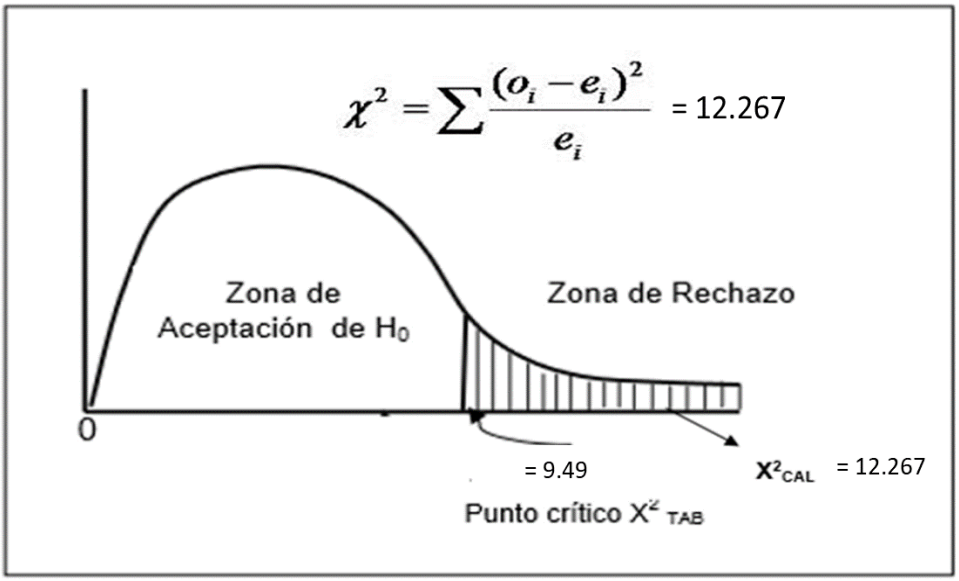


Figura 25:
Relación sobre la disponibilidad de la información del uso de la aplicación móvil.

Ecuación 3: Contrastación de hipótesis Relación entre la disponibilidad de la información y la aplicación móvil.



Interpretación: En cuanto los datos obtenidos sobre la influencia sobre la disponibilidad de la información del uso de la aplicación móvil se obtiene un valor de Chi cuadrado de 12.267 y valor de p=0.015, el cual hace referencia que si existe una relación significativa positiva.

Tabla 8: Relación sobre la integridad de la información del uso de la aplicación móvil.

			Uso de la aplicación			Total	Chi tabla	Chi Calculada	gl	P Sig. Asintótica
			C	D	I					
Proceso de atención	C	Recuento	5	0	0	5	9.49	16	4	0.003
		% del total	62.5%	0.0%	0.0%	62.5%				
	D	Recuento	0	1	0	1				
		% del total	0.0%	12.5%	0.0%	12.5%				
	I	Recuento	0	0	2	2				
		% del total	0.0%	0.0%	25.0%	25.0%				
Total		Recuento	5	1	2	8				
		% del total	62.5%	12.5%	25.0%	100.0%				

Fuente: Datos obtenidos de la simulación de la aplicación móvil

LEYENDA

C Confidencialidad
D Disponibilidad
I Integridad

Figura N° 26

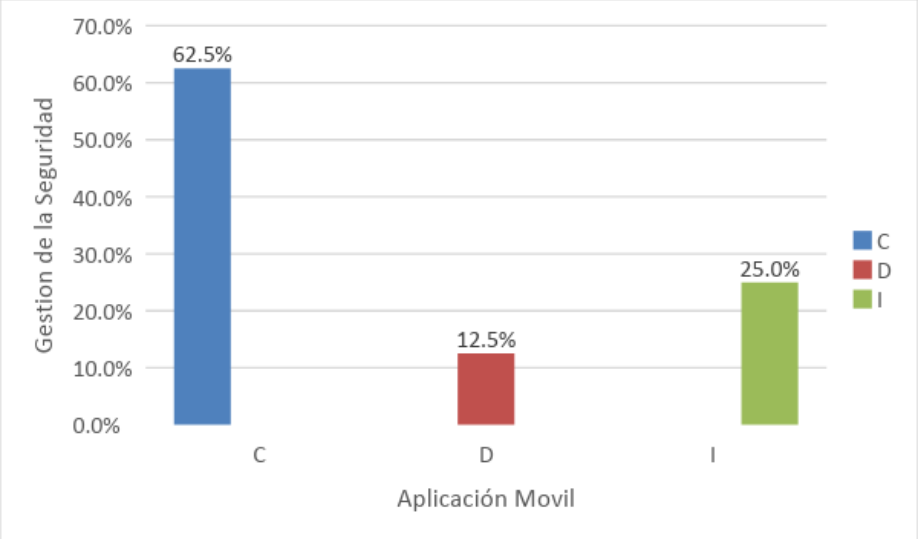
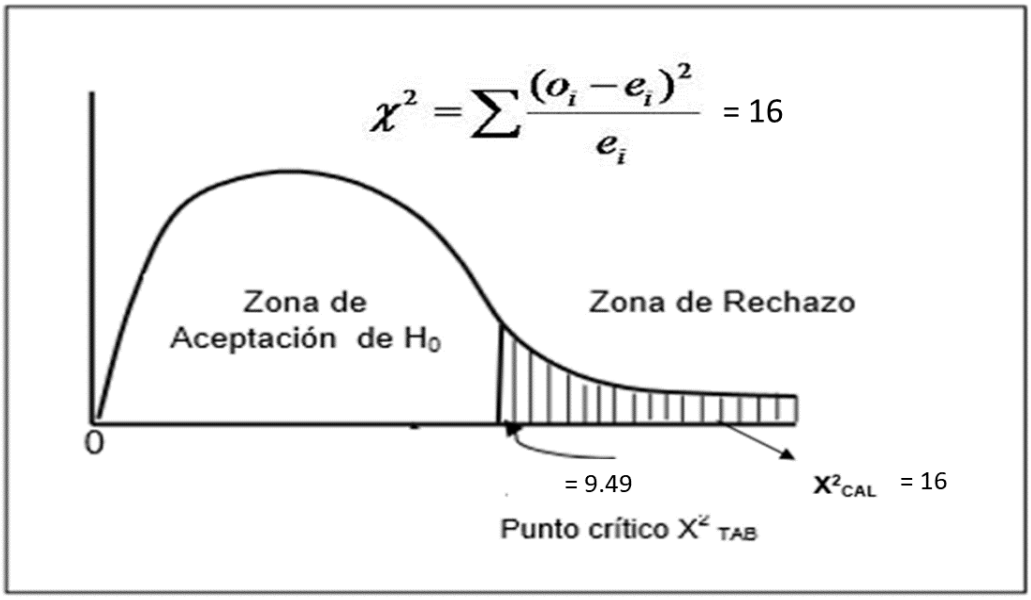


Figura 26:
Relación sobre la integridad de la información del uso de la aplicación móvil.

Ecuación 4: Contrastación de hipótesis entre la integridad de la información y la aplicación móvil.



Interpretación: En cuanto los datos obtenidos sobre la relación entre la integridad de la información del uso de la aplicación móvil se obtiene un valor de Chi cuadrado de 16 y valor de p=0.003, el cual hace referencia que si existe una relación significativa positiva.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1 Discusión

En la investigación se obtuvo en la tabla 1, los valores para los indicadores de la Confidencialidad, en 60%, 32% y 8% lo que nos alerta de los grandes riesgos a los que está expuesta la información. Del mismo modo en la tabla 2, los valores para los indicadores de la integridad de la información eran de 80% 15% y 5% lo que describe el nivel de vulnerabilidad y posible modificación de la información. No obstante respecto a la disponibilidad de la información los valores de los indicadores son, 16% 72% y 12% los mismos que evidencian los riesgos del acceso a la información. Por lo contrario que Espinosa & León (2015), que el desarrollo de una aplicación de escritorio y una aplicación móvil, las empresas ya sea mediana o pequeñas, no cuentan con el suficiente capital para la inversión, además al optimizar los procesos y con una reducción de costos de papel pre impresos, de tal manera que contribuyen al proyecto CERO PAPEL. Respecto a la influencia sobre los indicadores de la variable gestión de la información y el uso de la aplicación móvil, se puede mencionar que tabla 5, en la relación significativa sobre la gestión de la seguridad de la información del uso de la aplicación móvil es positiva la misma que se logra validar a través de los valores de contrastación de la hipótesis que son Chi cuadrado de 17.2 y con un P=0.026. También en la tabla 6, la relación significativa sobre la confidencialidad del uso de la aplicación móvil valida la hipótesis con un valor de Chi Cuadrado de 13.267 y un P=0.035. Finalmente, en la tabla 7, la relación significativa sobre la integridad de los datos del uso de la aplicación móvil valida la hipótesis con un valor de Chi Cuadrado de 12.267 y un P=0.015. Asimismo, Fuentes (2013), menciona que se ha conseguido satisfactoriamente, el principio fundamental que se ha querido realizar para la presentación del prototipo ha sido, por un lado, el establecimiento de comunicación a través del despliegue de la aplicación en la nube. Esto también coincide con Ortega

(2014), que, al utilizar un producto multimedia, brinda varios beneficios en la interacción con el usuario.

4.2 Conclusiones

- Se logró determinar el nivel de los conocimientos en seguridad de información de los integrantes de las MYPES; lo mismo que estadísticamente se dispuso en las tablas de Confidencialidad, Disponibilidad e Integridad en el ámbito de seguridad de la información, de las PYMES de la región la Libertad lo mismo que reflejo el alto riesgo al que está expuesta la información.
- A través del uso de la aplicación móvil se evidencio como se reducen los riesgos de seguridad en los activos de información de las PYMES.
- A través del uso de la aplicación móvil se demostró cómo se puede Incrementar el nivel de seguridad respecto a la eficacia de los resultados del acceso a los estándares de seguridad de la información.
- Se logró medir la relación entre la aplicación móvil y los resultados de acceder a consultar estándares de la seguridad de la información, a través de los indicadores de confidencialidad, disponibilidad e integridad de los datos.
- Se logró determinar que hay una relación significativa positiva sobre la gestión de la seguridad de la información por parte del uso de la aplicación móvil.

REFERENCIAS

InnovaAge. (2016). Apps Híbridas vs Nativas vs Generadas. Enero 2020, de InnovaAge Recuperado el 15 de Junio en https://www.innovaportal.com/innovaportal/v/696/1/innova.front/apps-hibridas-vs-nativas-vs-generadas-que-decision-tomar

IsoTools. (2017). La norma ISO 27001. Enero 2020, de IsoTools Recuperado el 17 de Junio en https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISO 27000 (2017). SO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES. Recuperado el 20 de Mayo en: http://iso27000.es/download/ControlesISO27002-2013.pdf

SCProgress (2018). Normas ISO 27001-ISO 27002. Recuperado el 13 de abril en: http://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf

ISO 27002 Español (2018). Proyecto de Norma Técnica Colombiana. Recuperado el 15 de Junio en: https://es.scribd.com/doc/313565857/ISO-27002-Espanol-pdf

ISO 27001 (2016) Seguridad de la Información. Recuperado el 14 de Abril en: https://www.normas-iso.com/iso-27001/

Gálvez, E.; Riascos, S. & Contreras, F. (2014). Influencia de las tecnologías de la información y comunicación en el rendimiento de las micro, pequeñas y medianas empresas colombianas. Recuperado el 12 de Agosto en:

http://www.sciencedirect.com/science/article/pii/S0123592314001557

Cineplanet, Aplicaciones y Análisis Android (2015]. Recuperado el 14 de Abril en: http://www.androidpit.es/aplicacion/com.beyond.cineplanet

Tello, E. (2008). Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de México. Recuperado el 12 de Junio en http://www.uoc.edu/rusc/4/2/dt/esp/tello.pdf

TGC (2017). ¿Qué son las Tics o Tecnologías de la información y la comunicación? Recuperado el 15 de Mayo en: http://tugimnasiacerebral.com/herramientas-de-estudio/que-son-las-tics-tic-o-tecnologias-de-la-informacion-y-la-comunicac

ESSET. (2014). El 41 por ciento de las empresas de América Latina sufrió ataques de malware en el último año. Junio 2014, de Globalgate: Recuperado el 12 de Mayo en: https://www.globalgate.com.ar/novedades-el-41-por-ciento-de-las-empresas-de-america-latina-sufrio-ataques-de-malware-en-el-ultimo-ano.html

"Financial cyberthreats in 2014", KASPERSKY LAB REPORT [Online], Recuperado el 20 de Mayo en: http://cdn.securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf, Febrero 2015.

"Eset Security Report Latinoamérica 2014" [Online], Recuperado el 23 de Agosto en: http://www.welivesecurity.com/wpcontent/uploads/2014/06/informe_esr14.pdf, 2014. PP 6.

Yagual Del Valle, C,; Chilán, L. Repositorio Digital Universidad Politécnica Salesiana. [Tesis para obtener el título de Ingeniero de sistemas].; 2014 Recuperado en 12 de

diciembre en: http://www.dspace.ups.edu.ec/bitstream/123456789/7401/1/UPS-GT000773.pdf.

Montoya Pachas, K. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 Recuperado en 15 de diciembre en http://tesis.pucp.edu.pe/repositorio/handle/123456789/5005

Espinoza Aguinaga, R. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 [Consulta 2016 Diciembre 01]. Disponible desde: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957 .

Justino Salinas, Zully Isabel, Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas]. Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013. Recuperado el 16 de noviembre en: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6045

Huamán Monzón, Fernando Migue Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano. Recuperado el 15 de noviembre en: http://hdl.handle.net/20.500.12404/5582

Talavera Álvarez, VascoRodrigo, Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. Recuperado el 15 de noviembre en: http://hdl.handle.net/20.500.12404/6092

Espinoza Aguinaga, Hans Ryan, Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de

producción y comercialización de productos de consumo masivo. Recuperado el 15 de noviembre en: http://hdl.handle.net/20.500.12404/4957

Barrantes Porras, Carlos Eduardo; Hugo Herrera, Javier Roberto, Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos. Recuperado el 12 de mayo en: http://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/609/barrantes_ce.pdf?sequence=3&isAllowed=y

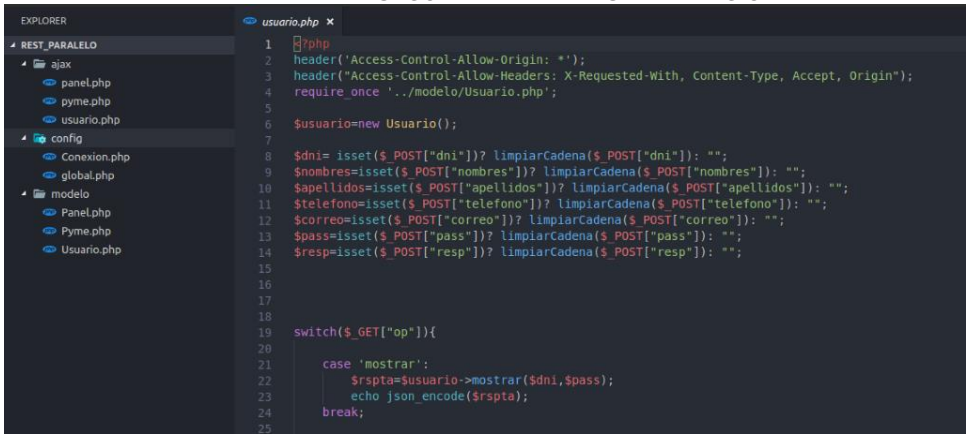
ANEXOS

Anexo 01 MATRIZ DE OPERACIONALIZACION DE VARIABLES

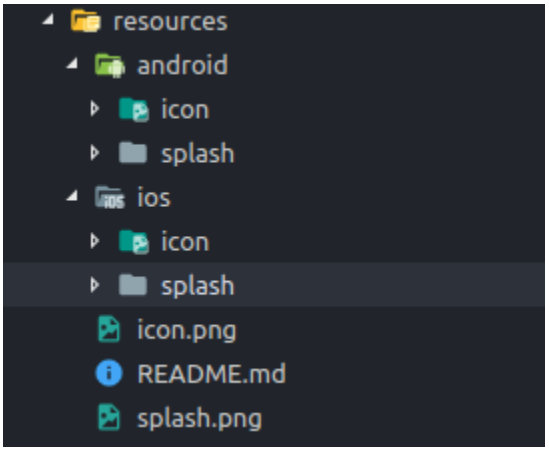
VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	FÓRMULAS
Gestión de la Seguridad de la Información basado en el iso 27002 (Variable dependiente)	Es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013	Confidencialidad	Porcentaje de accesos a páginas web peligrosas prevenido	(Número de accesos a páginas web peligrosas prevenido/ Número total de accesos a páginas web) *100%
			Porcentaje de archivos clasificados encriptados	(Número de archivos clasificados encriptados de la empresa/ Número total de archivos clasificados de la empresa)*100%
			Porcentaje de postulantes con antecedentes investigados	(Número de postulantes a trabajar en la empresa con antecedentes investigados / Número total de postulantes a trabajar en la empresa)*100%
			Porcentaje de contrataciones nuevas con acceso permitido	(Número de contrataciones nuevas de personal con acceso permitido a los archivos de la empresa/ Número total de contrataciones nuevas de personal de la empresa)*100%
		Integridad	Porcentaje de Colaboradores con Acceso permitido a modificación de archivos	(Número de colaboradores con acceso permitido a modificación de archivos de la empresa/ Número de total de colaboradores con acceso permitido a archivos de la empresa)*100%
			Porcentaje de colaboradores con responsabilidades en la información definidos	(Número de colaboradores con responsabilidad en la integridad de la información definido/ Número de total de colaboradores)*100%
			Porcentaje de colaboradores con funciones segregadas	(Número de colaboradores con funciones segregadas / Número total de colaboradores)*100%
		Disponibilidad	Porcentaje de activos de información inventariados	(Número de activos de información inventariados/ Número total de activos de información)*100%
			Porcentaje de colaboradores con acceso permitido a la información clasificada	(Número de colaboradores con acceso permitido a información clasificada de la empresa/ Número total de colaboradores de la empresa)*100%
			Porcentaje de la Política de	(Número de elementos de la Política de Planificación y Continuidad de Negocios

			Planificación y Continuidad de Negocios Implementado	implementados/ Número total de elementos de la Política de Planificación y Continuidad de negocios determinado por el equipo de estudio)*100%
Aplicación Móvil (Variable Independiente)	es una aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles y que permite al usuario efectuar una tarea concreta de cualquier tipo	Calidad de la Aplicación	Pruebas Funcionales	De Razón
			Usabilidad	De Razón
			Pruebas Unitarias	De Razón

Anexo 02 Código BACKEND



Anexo 03 (Creación de código interpretable para Xcode y Android Studio)



ANEXO nro. 4. Ficha de observación – Análisis de la Confidencialidad

Ficha de Observación

Evaluado:

Cargo del evaluado:

Evaluador:

Consideraciones:

En la presente ficha de observación se tomará como actividad a observar el proceso de cómo cada colaborador trata la información

Análisis de la Confidencialidad					
Fecha	Indicador	Variable	Unidad de Medida	Valor	
	Porcentaje de accesos a páginas web peligrosas prevenido	(Número de accesos a páginas web peligrosas prevenido/ Número total de accesos a páginas web) *100%	Numero de Accesos		
	Porcentaje de archivos clasificados encriptados	(Número de archivos clasificados encriptados de la empresa/ Número total de archivos clasificados de la empresa)*100%	Numero de Archivos		
	Porcentaje de postulantes con antecedentes investigados	(Número de postulantes a trabajar en la empresa con antecedentes investigados / Número total de postulantes a trabajar en la empresa)*100%	Numero de postulantes		
	Porcentaje de contrataciones nuevas con acceso permitido	(Número de contrataciones nuevas de personal con acceso permitido a los	Número de contrataciones		

		archivos de la empresa/ Número total de contrataciones nuevas de personal de la empresa)*100%			

ANEXO nro. 5. Cuestionario – Integridad y disponibilidad de los datos

INSTRUCCIONES

- ✓ El cuestionario contiene 10 preguntas las cuales medirán la efectividad del manejo de la integridad y disponibilidad de los datos.
- ✓ Lea atentamente cada una de las preguntas, y de ser necesario, haga uso de los apuntes necesarios.

A continuación, completar:

Apellidos y Nombres

1. ¿Qué es Seguridad de Información?

a) Son una serie de reglas y prácticas que definen como se protegen los recursos informáticos.

b) Es el documento donde se registra cualquier incidencia con la seguridad de información.

c) Son las medias que se emplean para la seguridad del personal

d) Son los medios que empleamos para proteger nuestras Capacidades tecnológicas y activos de información contra cualquier modo de ataque.

2. ¿Qué son las políticas de seguridad?

a) Son una serie de reglas y prácticas que definen como se protegen los recursos informáticos.

b) Es el documento donde se registra cualquier incidencia con la seguridad de información.
c) Son las medidas que se emplean para la seguridad del personal.
d) Son los medios que empleamos para proteger nuestras Capacidades tecnológicas y Activos de información contra cualquier modo de ataque.

3. Tiene acceso a modificar archivos una vez que hayan terminado de ser editados.

4. Qué responsabilidad tiene sobre el repositorio de información generado por su unidad

5. Qué responsabilidad tiene sobre el repositorio de información generado por la empresa

6. Tiene usted funciones segregadas, comente

7. ¿Realizas periódicamente una copia de seguridad de tus datos?

8. ¿Cómo se integran los smartphones de tus empleados en la red de tu empresa?

9. ¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura IT de tu empresa?

10. ¿Están tus sitios web protegidos?

11. Están inventariados los activos de información generados en la empresa

12. Especifique el número de elementos de la Política de Planificación y Continuidad de Negocios que conoce

13. Cuántos elementos de la Política de Planificación y Continuidad de Negocios están implementados ya sea como procesos o con alguna herramienta de TI

ANEXO nro. 6. Aplicación de la Metodología de Desarrollo

A continuación, se presenta cada etapa de la metodología de desarrollo y las tareas aplicadas a estas para lograr el objetivo de desarrollo del aplicativo móvil. [4]

Análisis

Establecer objetivos de desarrollo

A continuación, establecemos los objetivos a lograr durante el desarrollo del presente proyecto.

- Desarrollar un Aplicativo móvil capaz de adaptarse a los distintos entornos empresariales de las PYMES.
- Desarrollar un Aplicativo móvil nativo con las funcionalidades necesarias para el cumplimiento del ISO 27001/27002.

Elección de Herramientas

Con el fin de desarrollar una aplicación híbrida de calidad, es necesario la elección de herramientas que darán soporte para su diseño y programación durante todas las fases de desarrollo.

A continuación, mostramos las herramientas y tecnologías usadas en función a las fases en las que intervienen.

Tabla N° 1

Fases	Herramientas / Tecnologías
Planificación	Microsoft Office 2013
Diseño	Rational Rose 2007, Mysql Workbench
Codificación	Mysql server, Ionic 3, Visual Code, Postman
Pruebas	Postman, Node JS 8 (servidor de prueba), Ionic View App.

Fuente: Elaboración Propia

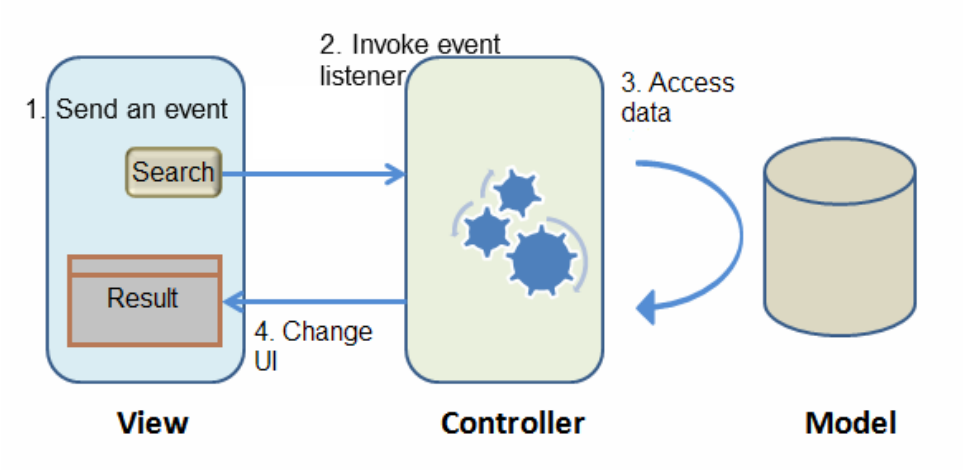
Consideraciones de Arquitectura

Para este proyecto se debe proveer el uso una arquitectura que dé soporte al desarrollo y despliegue del App.

Si bien a continuación se modelará el software como producto, también depende de un modelo de infraestructura el cual es "El modelo vista controlador".

Básicamente consiste en definir una lógica establecida para realizar consultas a un servidor y así obtener datos para ser mostrados en las vistas (interfaces de la App), el modelo debe ser implementado en la arquitectura.

Figura N° 2



Fuente: **https://www.ibm.com/developerworks/ssa/webservices/ws-multitenantpart4/index.html**

Diseño

Descripción de Funcionalidades

El desarrollo del Aplicativo móvil requiere de funcionalidades trascendentales, en las que se hará alto procesamiento de información, por ende, se modelará cada proceso que realizan los actores del sistema.

Desde la información tomada de las directrices de las ISO (27001/27002) se tomado la participación del gerente, el responsable de área de seguridad y el mismo sistema como un agente que realizará operaciones y procesos.

El gerente debe encargarse de registrar a su empresa, luego de ello el sistema deberá pedir la creación de un nuevo usuario, además, debe administrar tanto las áreas como a los usuarios.

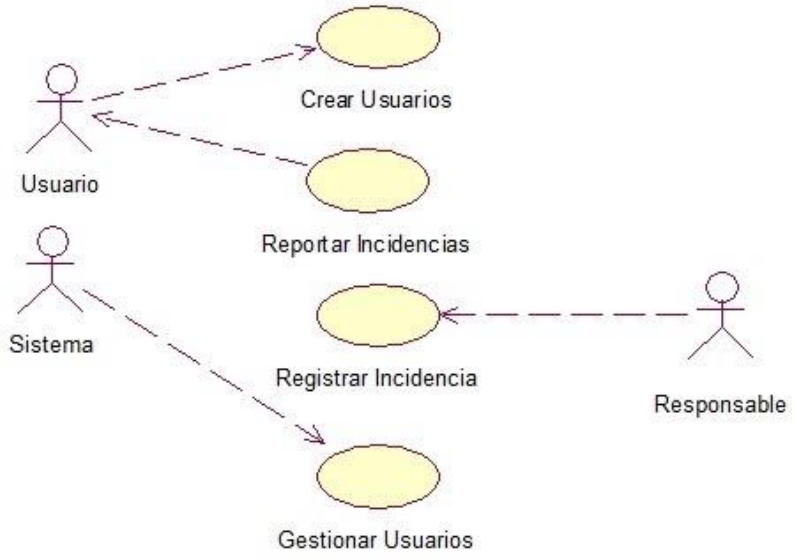
Los incidentes, son reportados por el sistema, esto quiere decir que este, debe controlar las sesiones y las actividades que los usuarios realizan dentro del sistema que ellos poseen; el gerente, responsable de área pueden dar el seguimiento respectivo con estos reportes. Esta abstracción se representa en el siguiente modelado de desarrollo de software basado en UML.

Modelado UML

Modelo de Caso de Uso

Basado en la descripción anterior, nos centramos en la interacción de los tres actores principales del sistema con los casos de uso que el sistema debe ostentar.

Figura N° 3



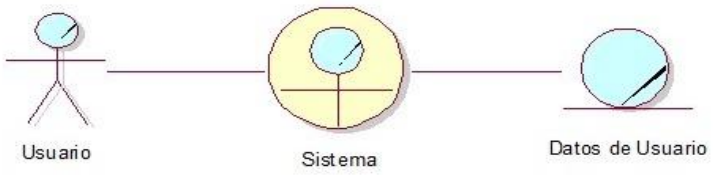
Modelo de Objetos

A. Crear Usuarios

La creación de nuevos usuarios está sujeta a la participación de un usuario exclusivo que ostente la calidad de Gerente dentro del sistema.

Los datos ingresados por medio del sistema deben ser alojados para el control de accesos y participaciones dentro de las funcionalidades del aplicativo móvil.

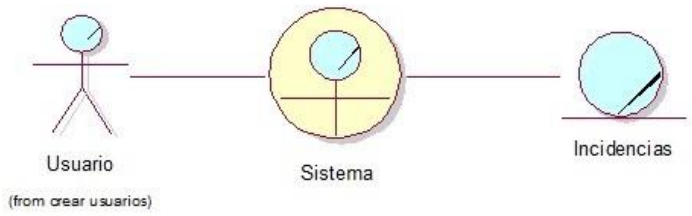
Figura N° 4



B. Reportar Incidencias

El usuario autorizado a visualizar las incidencias viene a ser el gerente, que al interactuar con el Aplicativo móvil deben visualizar todas las incidencias y sus orígenes que derivaron en estas las cuales fueron registradas por los responsables de seguridad.

Figura N° 5

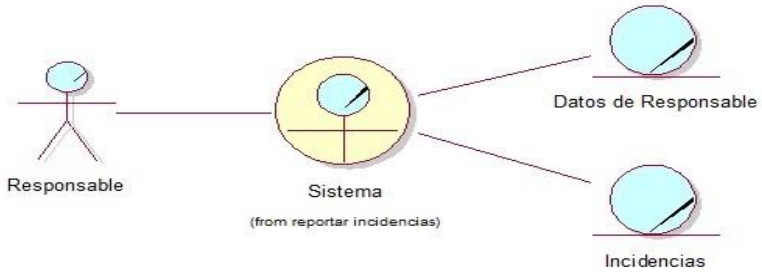


C. Registrar Incidencias

El responsable debe acceder en calidad de usuario con restricciones funcionales, eso validado por el sistema.

Básicamente este proceso consiste en hacer registro de incidencias cuando se presente alguna vulnerabilidad o inconveniente dentro del sistema PYME, estas vulnerabilidades están descritas en identificación de amenazas (7.1.1.2) y políticas de seguridad para PYMES (7.1.1.3).

Figura N° 6



D. Gestionar Usuarios

La funcionalidad de gestión de usuarios debe estar centrada en el control de los datos de usuarios, así como las actividades relacionadas a estos, por ejemplo, podemos gestionar que responsable a registrado más incidencias en el sistema de la organización PYME, o en caso contrario el responsable que ha registrado menos.

El encargado de acceder a esta funcionalidad es el Gerente o alto funcionario de la PYME encargado de monitorear el recurso humano de seguridad del sistema.

Figura N° 7

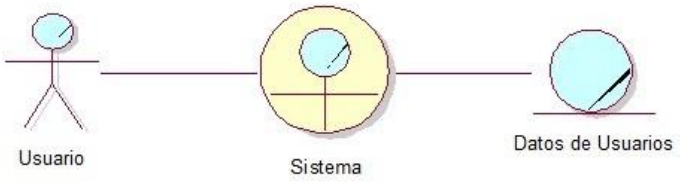
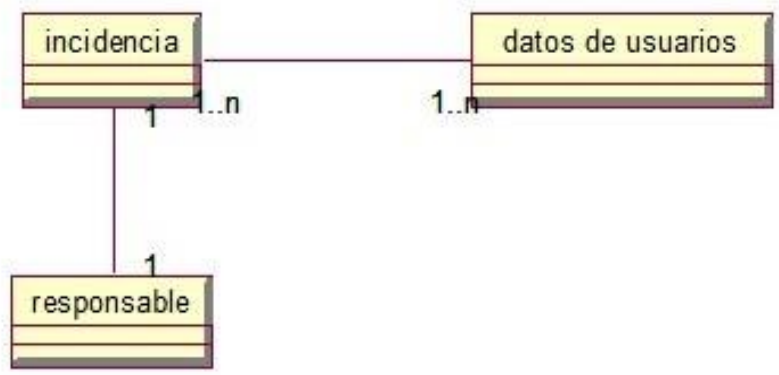


Diagrama de Clases

El siguiente diagrama es resultado de la relación entre objetos junto a sus respectivas cardinalidades que muestran la vinculación de datos de diferentes objetos dentro de los procesos establecidos por los casos de uso.

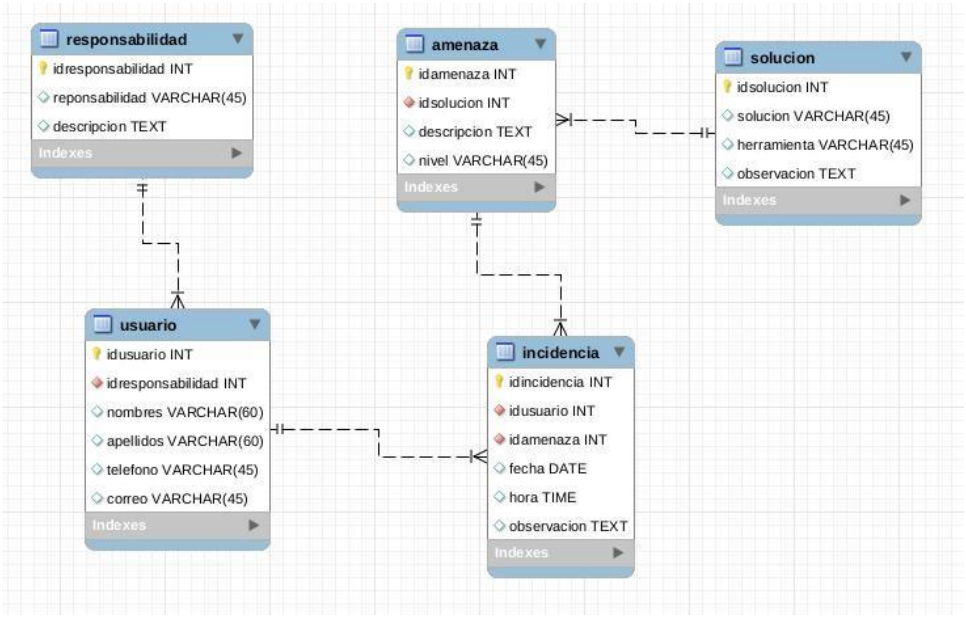
Figura N° 8



Mapeo Objeto – Relacional

Una vez establecido el diagrama de clases en el cual se instancian los objetos y sus relaciones, se procedió a elaborar el mapeo que consiste en convertir una clase en una entidad, la cual al igual que las clases se relacionan entre si mediante el uso de claves (primarias y foráneas), obteniendo el diagrama relacional usado por la herramienta workbench para establecer la estructura de tablas y relaciones de la base de datos en MySQL.

Figura N° 9



Codificación

Generalidades

En el desarrollo de la aplicación móvil se tuvo en cuenta dos aspectos fundamentales en seguridad para PYMES, que son la seguridad en vulneración de datos en los servidores de las PYMES, y el reporte de incidentes a los usuarios responsables según el área y el cargo asignado dentro de la organización.

El trabajo en la programación de este módulo no representa un trabajo completo del sistema según el modelado, sino el objetivo es el cumplimiento de directrices anteriormente descritas. También deja abierta la posibilidad de pasar el código fuente a las plataformas Xcode o Android studio para obtener la aplicación nativa.

Arquitectura

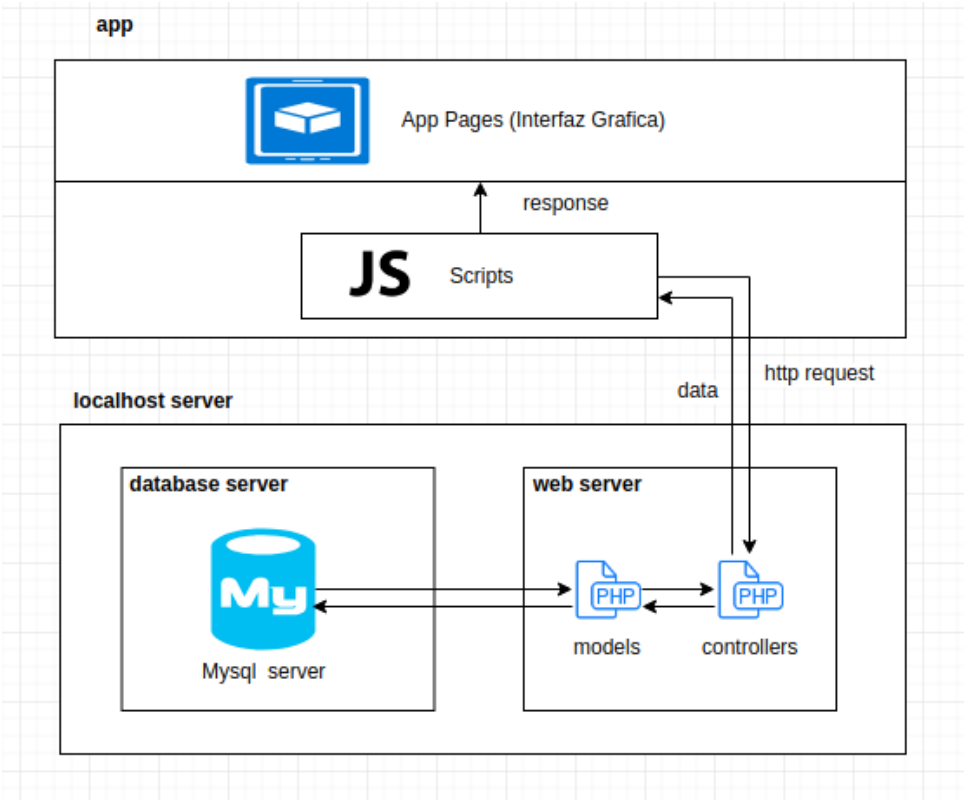
Para el buen funcionamiento de la app se elaboró una infraestructura de servicios basado en el pack para servidor local (XAMPP) el cual provee de servicios web (para el API REST) y servicios de base de datos encargada de gestionar la data para alimentar el aplicativo móvil.

Como se puede ver existen dos capas, la capa APP (cliente) y la capa SERVER LOCALHOST (servidor) estructuradas de tal forma que cumpla con los principios del modelo vista controlador para el despliegue del sistema.

El código del web server está programado en PHP encargado de controlar las consultas que se realizan desde el cliente remoto, en este caso la app que obtiene como respuesta data

codificada para ser interpretada por el cliente (app) y por medio de los scripts de código (JavaScript en el desarrollo y test) se obtiene una respuesta codificada en el formato JSON.

Figura N° 10



IONIC 3 Framework

Primeramente, estableceremos que la app reporta incidencias del monitoreo que realiza el servidor con lo cual, no estamos utilizando la arquitectura del dispositivo móvil, o la del SO, entonces por ello, consideramos realizar esta app de manera híbrida en desarrollo y testeo.

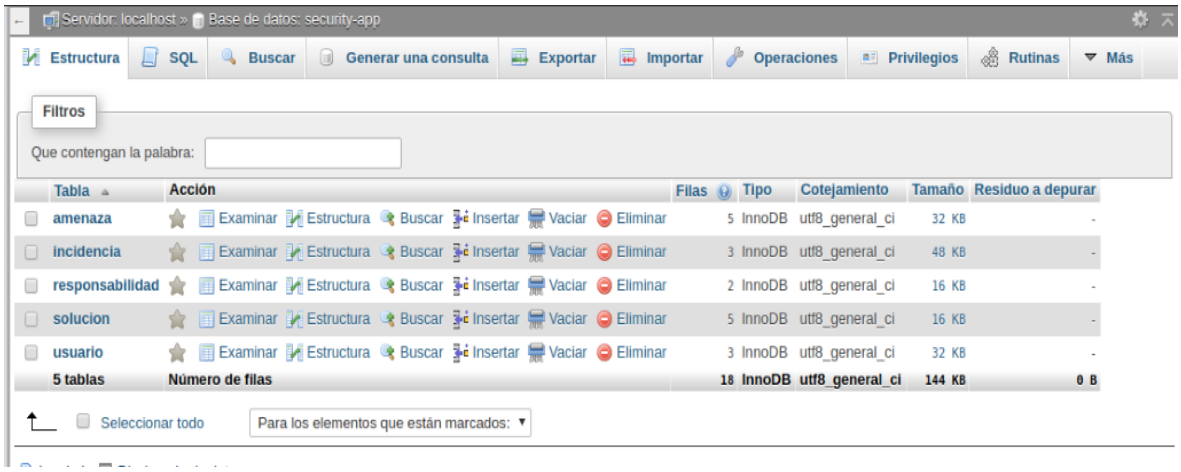
Para el desarrollo de la aplicación móvil se utilizó el framework IONIC en su tercera versión, con el fin de lograr el desarrollo de una aplicación híbrida, ya que por medio de la herramienta IONIC CORDOVA se facilitará la incorporación de cualquier funcionalidad nativa en las plataformas ANDROID y IOS.

Ionic 3 Framework es un SDK de código abierto que permite a los desarrolladores crear aplicaciones móviles de alta calidad utilizando tecnologías web familiares (HTML, CSS y JavaScript).

Implementación de la Base de Datos

En la implementación de la base de datos, se extrajo el código exportado de workbench en la opción “forward engeniering” que consiste en convertir el diagrama relacional a código SQL. Luego de obtener el código SQL, en las últimas líneas se agregó los comandos de inserción de datos en las tablas (usuario, responsabilidad, amenaza y solución) de modo que el sistema parta con los datos necesarios para funcionar, por ejemplo, se necesitará de un usuario administrador que registre a los demás (administrador, responsable de seguridad).

Figura N° 11



También es necesario llenar las tablas de amenaza y solución para facilitar al usuario responsable de seguridad de seleccionar el tipo de amenaza y tan solo añadir la observación pertinente.

Figura N° 12

Desarrollo BackEnd

Se programó un API, en código PHP para implementar servicios basado en REST, para proveer de datos y procesos que vinculen a la aplicación con la base de datos.

En la programación del Back se encuentran los controladores, que se encargarán de gestionar las consultas y retorno de datos a la app; mientras los modelos ejecutarán las consultas provenientes de los controladores a la base de datos y retornan un valor de acuerdo a tipo de consulta (VER ANEXO 1).

Desarrollo FrontEnd

A continuación, se mostrará las interfaces de aplicativo móvil desarrolladas en HTML, CSS y JAVASCRIPT dentro del ámbito de desarrollo híbrido (Programación y test). Las interfaces diseñadas son:

B. **Página Principal**

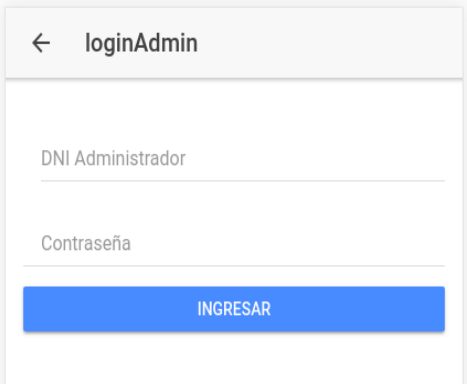
Aquí se encuentra las opciones del login para los dos tipos de usuario (Administrador, Responsable de Seguridad).

Figura N° 13

Login

Esta interfaz consta de un formulario de dos inputs en los que el usuario escribirá sus datos para autenticarse y acceder a las funcionalidades.

Figura N° 14



Panel de Control

En esta interfaz los usuarios accederán a las funcionalidades que están habilitadas para cada tipo de usuario.

Figura N° 15

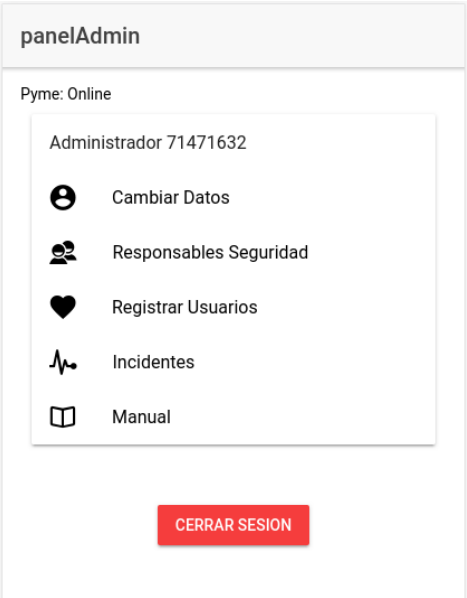
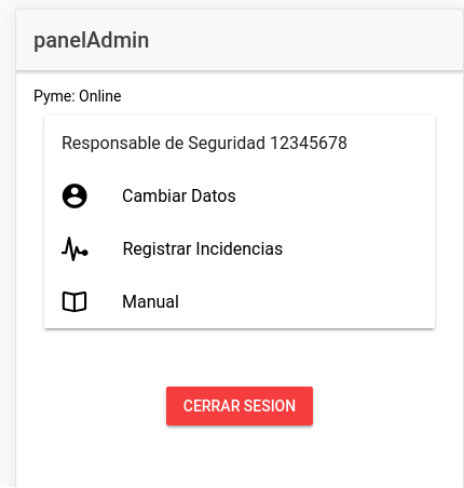


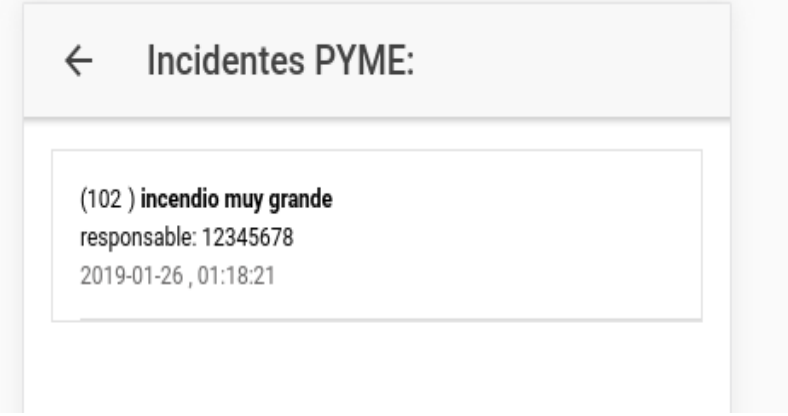
Figura N° 16



Listar Incidentes

Dentro del panel de control de los usuarios Administradores se puede visualizar la relación de incidentes con su respectivo código, responsable y en la fecha y hora exacta en la cual fueron registrados al sistema.

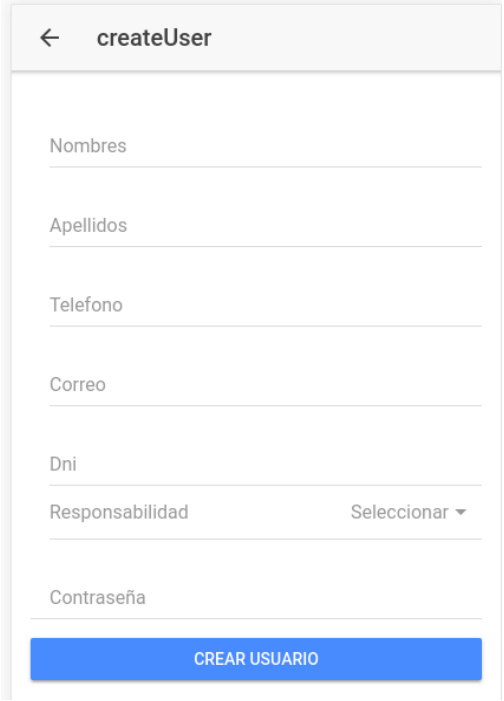
Figura N° 17



Registrar Usuarios

Dentro del panel de control de los usuarios Administradores se encuentra la funcionalidad de registrar usuarios los cuales pueden ser Administradores y Responsables de Seguridad, la vista consta de un formulario en el cual se llenará los datos del usuario a registrar.

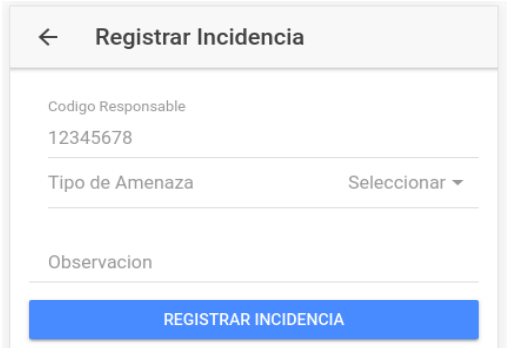
Figura N° 18



Registrar Incidente

Una vez que el usuario Responsable ha accedido mediante la autenticación de sus datos, en su panel de control se muestra la opción de Registrar incidente en el cual registra el tipo y la observación sobre el problema que ha acontecido en torno a los activos de información de la PYME.

Figura N° 19

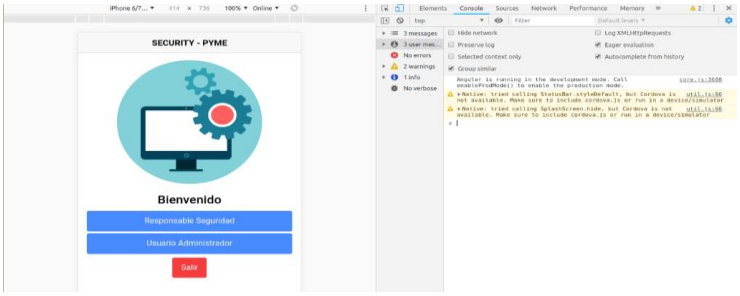


Pruebas

En esta última fase del desarrollo del Aplicativo móvil conjuntamente con los servicios provistos por el API REST programado, se procedió a realizar las pruebas funcionales que cumplan con los requerimientos establecidos en la planificación.

Para realizar el test de la app, se necesitó la ejecución de un servidor de pruebas de IONIC basado en NODE js. Con el comando “ionic serve” escrito en la terminal, se desplegó la aplicación corriendo en el servidor local en el puerto 8100. Para interactuar con la aplicación se procedió a acceder mediante el navegador y modificando las dimensiones de pantalla se logró acceder a la interfaz similar de similar despliegue a un equipo móvil.

Figura N° 20



Por último, se procedió a ejecutar el comando “ionic cordova run android” y “ionic cordova run ios” para obtener el código que las herramientas Android Studio y Xcode interpretaran para obtener la aplicación nativa que podrá desplegarse tanto en Android como IOS. (VER ANEXO 2)