UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA

TESIS

LA FALSA PERCEPCIÓN EN LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

PRESENTADA POR:

JHON RICHARD HUANCA SUAQUITA

PARA OPTAR EL GRADO ACADÉMICO DE:

DOCTOR EN ESTADÍSTICA E INFORMÁTICA

PUNO, PERÚ

2018

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA

TESIS

LA FALSA PERCEPCIÓN EN LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

PRESENTADA POR:

JHON RICHARD HUANCA SUAQUITA

PARA OPTAR EL GRADO ACADÉMICO DE:

DOCTOR EN ESTADÍSTICA E INFORMÁTICA

APROBADA POR EL JURADO SIGUIENTE:

PRESIDENTE .....

Dr. FELIX OLAGUIVEL LOZA

PRIMER MIEMBRO .....

Dr. IVAN DELGADO HUAYTA

SEGUNDO MIEMBRO .....

Dra. GUINA GUADALUPE SOTOMAYOR ALZAMORA

ASESOR DE TESIS .....

D.Sc. ALEJANDRO APAZA TARQUI

Puno, 26 de Julio del 2018

ÁREA: Estadística.
TEMA: Seguridad de los sistemas informáticos.
LÍNEA: Tecnologías de información.

DEDICATORIA

A mis padres Aurelio Huanca Veliz y Alejandra Suaquita Sucacahua porque creyeron y Depositaron su entera confianza en cada reto Que se me Presentaba sin dudar ni un solo Momento de mí. Gracias por su comprensión y Consejos.

A mi amada esposa Gladys Marleny y mi maravilloso hijo Joao Parker ya que siempre estuvieron impulsándome en los momentos más difíciles con su valioso apoyo, sincero e incondicional, lo cual desencadenó en mi un crecimiento académico permanente.

AGRADECIMIENTOS

- A Dios porque ha estado conmigo en cada paso que doy hoy y siempre, dándome así fortaleza para continuar desarrollándome en este escenario académico social profesional.

- Agradezco en forma especial al Doctor Alejandro Apaza Tarqui, Director de la Maestría en Informática por su valiosa contribución a través de sus orientaciones y su permanente apoyo como asesor del presente trabajo de investigación.

- A mis docentes de la Facultad de Estadística e Informática de la UNA Puno, que en un inicio nos marcaron con sus enseñanzas teniendo a si sólidos conocimientos académicos, los cuales hoy en día se ven claramente acrecentados, gracias a ello actualmente compartimos todos estos frutos académicos con la Sociedad. Gracias por prepararnos para un futuro competitivo no solo como los mejores profesionales sino también como mejores personas.

ÍNDICE GENERAL

Pág.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

RESUMEN

El presente trabajo aborda temas de seguridad e inseguridad en los sistemas informáticos, debido a la incertidumbre sobre la percepción de seguridad existente. Se espera cumplir con la con la confidencialidad, integridad y disponibilidad de la información según ISO 27001, esto se aplica en diversos escenarios de desarrollo de software en forma empírica, estos requerimientos toman mayor valor en la administración de datos de entidades públicas y privadas, debido a que la ausencia de la seguridad en los sistemas desestabiliza el orden social global. El presente trabajo se asocia a un grupo de Mypes muestreadas, en el cual se evidencia la inseguridad, debido al modo de desarrollo de sus procesos para el aseguramiento de la información. En cuanto al método se evaluaron cuatro tratamientos tecnológicos en dos factores fijos midiendo así el grado se seguridad e inseguridad en las Mypes a través del Diseño Factorial Completamente al Azar. Los cuatro tratamientos han sido aplicados al grupo muestral, buscando así identificar diferencias entre los tratamientos. En cuanto a los resultados y según el planteamiento de la hipótesis general, la prueba de Análisis Factorial Univariante resultó no significativo P-valor > nivel se significancia, lo que conlleva a indicar como conclusiones que no es suficiente suministrar tratamientos tecnológicos físicos y lógicos a las Mypes muestreadas, esto si el personal que los dirige no tiene solvencia académica requerida para el desarrollo adecuado de los protocolos de seguridad, planes de gestión tecnológica y sistemas de gestión de seguridad de la información, las cuales contribuyen en el aseguramiento de la información.

Palabras Clave: Confidencialidad de información, falsa percepción de seguridad, inseguridad, seguridad informática y sistema de seguridad.

ABSTRACT

The present work addresses issues of security and insecurity in computer systems, due to the uncertainty about the perception of existing security. It is expected to comply with the confidentiality, integrity and availability of information according to ISO 27001. This is applied in various scenarios of software development in an empirical way, these requirements take greater value in the data management of public and private entities, because the absence of security in the systems destabilizes the global social order. The present work is associated to a group of Mypes sampled, in which the insecurity is evidenced, due to the way of development of its processes for the assurance of the information. Regarding the method, four technological treatments were evaluated in two fixed factors, so measuring the degree of safety and insecurity in the Mypes through the Completely Random Factorial Design. The four treatments have been applied to the sample group, seeking to identify differences between treatments. Regarding the results and according to the general hypothesis, the Univariate Factor Analysis test was not significant P-value> level is significant, which leads to indicate as conclusions that it is not enough to provide physical and logical technological treatments to the Mypes sampled, this if the staff that directs them does not have the academic solvency required for the adequate development of security protocols, technological management plans and information security management systems, which contribute to the assurance of information.

Keywords: Confidentiality of information, false perception of security, insecurity, computer security and security system.

INTRODUCCIÓN

Actualmente el desarrollo de sistemas de información ha optimizado los procesos del sector empresarial y académico en sus diferentes dimensiones, aún más con el avance tecnológico computacional, así toda empresa o entidad gestora de información táctica, trabaja con información que le permiten tener la versatilidad para el éxito empresarial en el ámbito comercial y empresarial así pude ser más competitivo, pues las empresas poseen información importante y esta requiere ser protegida y monitoreada (IEC/ISO 27001, 2005) frente a riesgos y amenazas de usuarios no autorizados y otros. fue necesario evidenciar la inseguridad de la información digital en las Micro y Pequeñas empresas - Mypes de la Región de Puno, aquellas asociadas a la producción textil y de confecciones.

El propósito del presente trabajo es primero: evidenciar la falsa percepción de seguridad en los sistemas de información, segundo: una vez evidenciadas las deficiencias y vulnerabilidades en la gestión de los sistemas de información de las Mypes se propone cuatro tratamientos para garantizar y asegurar el respaldo de la información táctica ubicada en los Sistemas Informáticos de las Mypes. Esta información táctica es imprescindible para toda empresa. Entre los tratamientos se tiene el Sistema de Gestión de Seguridad de la Información (SGSI), que según norma ISO 27001, permite desarrollar un plan de seguridad para proteger la información de entidades, en este caso de las Mypes muestreadas. Su proceso está basado en protocolos de seguridad, sin embargo no resultó significante en la reducción de la inseguridad de la información. Expuesto esto se dio fundamento a este trabajo de investigación asociado a la línea de investigación de seguridad informática, por lo que se expone la estructura de la misma, haciendo mención que la presente se divide en cuatro capítulos disgregados.

En el Capítulo I se contextualiza el marco teórico puntualizando las últimas investigaciones con respecto a la seguridad de la información, los sistemas de gestión de seguridad de la información, conceptos puntuales sobre integridad, confiabilidad y disponibilidad de la información, además en este capítulo se contemplan la descripción por objetivo de los antecedentes asociados al presente trabajo de investigación, en el Capítulo II se hace mención al planteamiento del problema, fundamentación, justificación, objetivos de la investigación e hipótesis de la investigación.

Aquí se describe la problemática en las Mypes, específicamente en la administración de la seguridad de la información digital, por tanto se tiene por objetivo evidenciar la falsa de percepción de la seguridad en los sistemas de gestión de datos de las Mypes muestreadas a partir de un total población de 231 Mypes.

En el Capítulo III se aborda el detalle de la metodología que se utilizó en la investigación, el diseño estadístico para evidenciar la falsa percepción, la definición del tamaño poblacional y la determinación del tamaño de muestra. En el Capítulo IV se expone los resultados del trabajo de investigación, la descripción del programa computacional *SustracFile* y la interacción con el Sistema Operativo; Por otro lado se ejecutaron cuestionarios que permitieron obtener indicadores del estado actual de las Mypes en lo que respecta a la seguridad de la información, gestión de la información y protocolos de seguridad. Finalmente se presenta las discusiones, donde se evidencia que el Sistema Operativo Windows exporta funciones restringidas, los cuales atentan contra la seguridad del mismo Sistema Operativo, en las conclusiones y recomendaciones se hace alcances para futuros trabajos de investigación.

CAPÍTULO I

REVISIÓN DE LITERATURA

1.1 Marco teórico

1.1.1 Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado. (Congreso de la República del Perú, 2013).

1.1.2 Análisis del Modelo con efectos fijos

Los efectos del tratamiento o factor pueden considerarse como desviaciones de la media global. Por consiguiente una forma equivalente de escribir las hipótesis en términos de efectos de los tratamientos t1 es Ho: $t_1 = t_2 = \ldots = ta = 0$) y Ha: $t_i \neq 0$) para al menos una i, donde i es un tratamiento (Montgomery, 2004). Los efectos fijos son factores manipulados por el investigador cada factor es una variable independiente categórica, estos factores contienen los tratamientos aplicados a las unidades experimentales. Los tratamientos mencionados son tecnológicos.

1.1.3 Análisis estadístico

Se investiga cómo puede llevarse a cabo una prueba formal de la hipótesis. La siguiente asociación indica que no hay diferencias en las medidas de los

tratamientos (Ho: $\mu_1 = \mu_2 = \ldots = \mu_a$ o de manera equivalente, Ho: $t_1 = t_2 = \ldots = t_a = 0$). puesto que se ha supuesto que los errores e_{ij} (residuos generados durante el análisis) siguen una distribución normal e independiente con media cero y varianza σ^2, las observaciones y_{ij} tienen una distribución normal e independiente con media $\mu + t_i$ y varianza σ^2 (Montgomery, 2004). El análisis estadístico es una forma de comprobar un resultado a través de la prueba estadística, si la prueba resulta significante (p-valor < α) aceptamos la hipótesis de diferencias (Ha); en caso contrario: (p-valor > α) aceptamos la hipótesis de igualdades (Ho). Estos procedimientos contribuyen a la validación, incluyendo al presente.

1.1.4 Análisis de datos

Luego del levantamiento de los datos se procede al análisis, lo cual consiste en verificar valores atípicos en las variables (*outliers*). Se requiere cumplir con los supuestos de normalidad en los datos si el tratamiento estadístico es paramétrico; en cambio si el tratamiento es no paramétrico no se requiere (Montgomery, 2004).

1.1.5 Análisis de datos cuantitativos

Al analizar los datos cuantitativos se debe recordar dos cuestiones: primero, que los modelos estadísticos son representaciones de la realidad, no la realidad misma; y segundo, los resultados numéricos siempre se interpretan en contexto, por ejemplo, un mismo valor de presión arterial no es igual en un bebé que en una persona de la tercera edad (Hernández, Fernández, 2014).

1.1.6 Aceptación de riesgo

Decisión de aceptar el riesgo (ISO/IEC Guie 73, 2009). La norma cuantifica la aceptación del riesgo al que se está expuesto, esta norma provee definiciones en términos generales del riesgo en la gestión de dirección, tiene el propósito de fomentar una comprensión mutua y coherente de la descripción de las actividades relacionadas con la gestión del riesgo, además del uso adecuado de la definición de la terminología en riesgos.

1.1.7 Alfa de Cronbach

El alfa de Cronbach es una técnica estadística de consistencia interna basado en el promedio de las correlaciones entre los ítems (interrogantes). El Alfa de Cronbach permite evaluar la posibilidad de mejoría o deficiencia de la fiabilidad de un instrumento (George & Mallery, 2012). Sugiere los siguientes parámetros para evaluar los coeficientes del Alfa de Cronbach.

Coeficiente Alfa > 0,9 es excelente
Coeficiente Alfa > 0,8 es bueno
Coeficiente Alfa > 0,7 es aceptable
Coeficiente Alfa > 0,6 es cuestionable
Coeficiente Alfa > 0,5 es pobre
Coeficiente Alfa < 0,5 es inaceptable

1.1.8 Análisis de riesgo

Uso sistemático de la información para identificar fuentes y para estimar el riesgo (ISO/IEC Guía 73, 2002) : *Risk management – vocabulary – guidesline for use in standars, este gestiona la* selección e implementación de medidas para modificar el riesgo, las medidas de tratamiento de riesgo implementadas contemplan acciones como: evitar, optimizar, transferir y retener el riesgo.

1.1.9 Análisis factorial

El análisis factorial es una técnica estadística de análisis de datos usada para explicar la influencia de los factores en la variable dependiente, los factores son variables independientes categóricas, y estás deben de componerse como mínimo de 02 factores (Montgomery, 2004). El análisis factorial se usa en el nivel investigativo explicativo, su propósito es encontrar la causalidad en un experimento, su aplicación también se extiende a las ciencias del comportamiento, ciencias sociales, marketing, gestión de productos, ingeniería de alimentos, investigación operativa, y otras ciencias aplicadas que se desarrollan en nivel investigativo explicativo.

1.1.10 Análisis de Varianza

El análisis de varianza es una técnica estadística que se desarrolla en función a un factor fijo y una variable dependiente, su propósito es evidenciar el efecto del factor en la variable respuesta (Montgomery, 2004). La técnica requiere cumplir con los supuestos de normalidad y homogeneidad de varianzas.

1.1.11 Análisis Multivariado

Es una técnica estadística que permite realizar un análisis multidimensional multivariante, el cual consiste en evidenciar el efecto de los factores en las variables respuestas las cuales se componen de 2 a más variables dependientes (Montgomery, 2004). Los factores requieren cumplir con los supuestos de normalidad y homogeneidad de varianzas.

1.1.12 API

Por sus siglas en Ingles *Application Programming Interface* es un conjunto de reglas (código estructurado) y especificaciones que las aplicaciones computacionales pueden seguir para comunicarse entre ellas: sirviendo de interfaz entre diferentes programas, de la misma manera que la interfaz de usuario facilita la interacción humano-software.

1.1.13 Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa (Congreso de la República del Perú, 2013).

1.1.14 Cobit

Control de Objetivos para la Información y Tecnologías Relacionadas, es una guía de mejores prácticas presentada como un área de trabajo, dirigida al control y supervisión de tecnología de la información (Peña, 2012). El presente trabajo planifica y propone los parámetros de seguridad para una determinada entidad.

También se le puede definir como un conjunto de herramientas de soporte empleadas por los gerentes para reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Así, mediante COBIT se puede desarrollar una política clara que permite el control de las Tecnologías de la información en la organización. La aplicación de este marco incide especialmente en el cumplimiento regulatorio y ayuda a incrementar el valor asociado al área de Tecnologías de información de la organización (Peña, 2012).

1.1.15 Confidencialidad

Confidencialidad es la propiedad que garantiza que la información esté disponible y no sea divulgada a personas no autorizadas, dicha garantía se lleva a cabo a través de reglas que limitan el acceso a esta información (ISO/IEC 13335-1, 2004).

1.1.16 Coeficiente de Correlación

El coeficiente de correlación es técnica estadística paramétrica que permite determinar la relación numérica entre dos variables. Con dispersión en sus variables crecientes, variables decrecientes y variables de sentido nulo. Esta técnica estadística se enmarca entre los límites de [-1 hasta 1]. Dónde: -1: correlación perfecta negativa; **+1**: correlación perfecta positiva (Martinez, 2012). Su interpretación se realiza con el *r* cuadrado. En la prueba de hipótesis de la correlación al aceptar la hipótesis alterna indicamos que existe asociación entre las variables analizadas.

1.1.17 Componentes reutilizables de Software

Los componentes reutilizables de software en el sistema operativo son representados como módulos o sub-sistemas, por ejemplo, en el sistema operativo Windows, se tiene módulos que corresponden al núcleo del Sistema, a continuación, se presenta su gráfica.

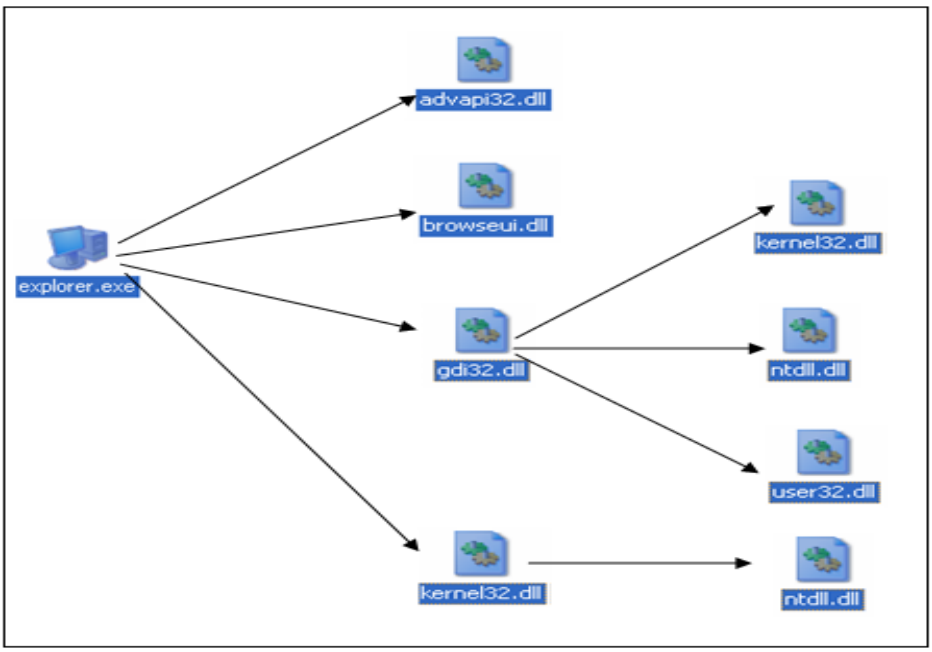

Figura 1. Diagrama de Componentes Reutilizables

En la Figura 1 se ilustra las relaciones de dependencia entre los componentes del Sistema Operativo (S.O.).

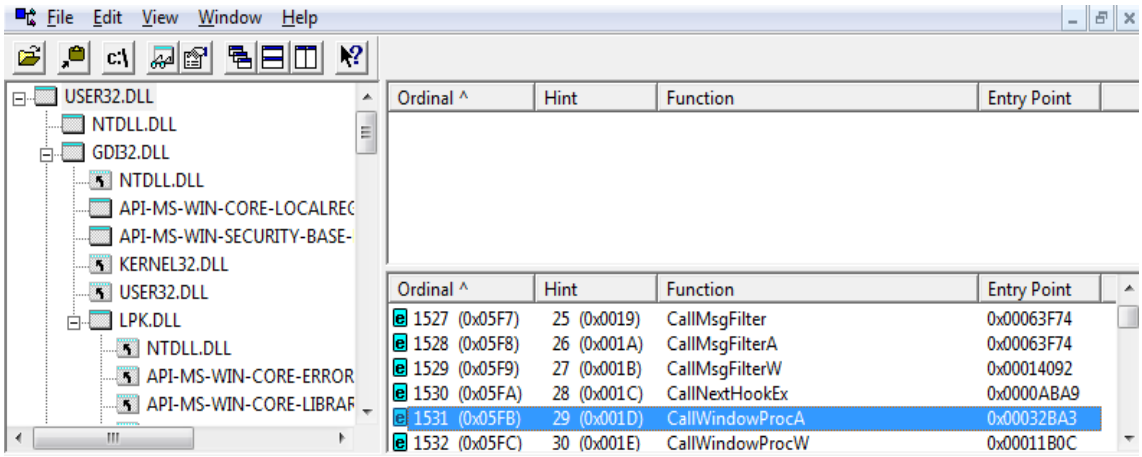

Figura 2. Ilustración de user32.dll

Claramente se puede distinguir la dependencia entre aplicaciones, por tanto para que el sistema operativo sea funcional requiere de múltiples componentes que administren y controles las operaciones que lleva a cabo entre el Sistema Operativo. En la Figura 02 se observa claramente la función (*CallWindowsProc)* del *user32.dll,* función que es reutilizada para entre otras cosas la sustracción de datos con ayuda de un *Hook.*

1.1.18 Diseño Completamente al Azar desbalanceado

Se refiere a que el número de réplicas de cada tratamiento (factor fijo) es diferente y así cada tratamiento tendrá réplicas (i = 1, 2, 3,..., t). donde t: número de tratamientos; estos diseños se pueden representar en el caso que se esté comparando un factor control contra otros tratamientos ya que se quiere obtener buena información acerca del tratamiento suministrado, por ello este tendrá más replicas en un grupo (tratamiento) que en otros grupo (Montgomery, 2004). Otro caso en el que se suele presentarse es cuando las unidades experimentales se pierden, en caso de seres vivos perdidos (Supo, 2016).

1.1.19 Diseños Factoriales

En muchos experimentos se requiere que se intervenga en el estudio de los efectos dos o más factores, debido al contexto fenomenológico o natural del experimento. En general los diseños factoriales o multifactoriales son más eficientes que los unifactoriales (estudios teóricos) en la aplicación de los experimentos. Por diseño multifactorial se entiende que en cada ensayo o replica completa del experimento se investigan todas las combinaciones posibles de los tratamientos de los factores. El efecto de un factor independiente categórico se define como el cambio en la respuesta producida por un cambio en el nivel del factor (causa). Con frecuencia se llama efecto principal (al factor sin interacción) porque se refiere a los factores de primarios en el experimento (Montgomery, 2004). En la vida real la mayoría de los experimentos requieren de incluir a todas las variables o factores fijos que se requiera (tratamientos manipulados por el investigador) los cuales afectan al resultado del experimento, así como también se deben incluir las variables no controladas (covariables e

intervinientes) claro esta previa evidenciación de que afectan al resultado final. Todo esto contribuye en generar un diseño experimental robusto y adecuado.

1.1.20 Disponibilidad

La propiedad de estar disponible y utilizable cuando lo requiera una entidad Autorizada, presenta los conceptos y modelos fundamentales para una comprensión básica de la seguridad de las Tecnologías de Información y comunicaciones (TIC) y aborda los problemas generales de administración que son esenciales para la planificación, implementación y operación exitosa de la seguridad de las TIC. La parte 2 de la norma ISO / IEC 13335 proporciona orientación operativa sobre la seguridad de las TIC. Juntas, estas partes se pueden usar para ayudar a identificar y administrar todos los aspectos de la seguridad de las TIC. (ISO/IEC 13335-1, 2004).

1.1.21 Dispositivo Extraíble

Es un dispositivo de almacenamiento de datos que utiliza una memoria flash para guardar información. Se le conoce también con el nombre de unidad flash Usb, lápiz de memoria, minidisco duro, unidad de memoria, llave de memoria, pendrive, entre otros. Estas memorias son resistentes a daños externos y algunos casos hasta al agua, factores que si afectan a otros tipos de dispositivos de almacenamiento, como los antiguos disquetes. Estas memorias flash se han convertido en el sistema de almacenamiento y transporte personal más utilizado, desplazando en este uso a los tradicionales disquetes.

1.1.22 Librería dvapi32.dll

Es una librería dinámica basada en interfaz de programación de aplicaciones (APIs) soporta numerosas APIs. Incluyendo las llamadas de seguridad y registro del Sistema Operativo Windows.

1.1.23 Escala de Likert

La escala Likert se implementa creando un alto número de afirmaciones objetivas que califiquen al tema de actitud y se proponen a un grupo muestral piloto para obtener las puntuaciones del grupo en cada afirmación. Las

afirmaciones encontradas cuyas puntuaciones se correlacionen significativamente con las puntuaciones de toda la escala, se seleccionan para integrar en la medida. Por lo que, hay que determinar la confianza y validez de la escala. Para esta escala se recogen puntuaciones favorables, desfavorables o de orden ordinal, pero no neutros. Cada afirmación propuesta en el cuestionario va seguida de una escala estimativa que consiste en una graduación que va desde el "totalmente es seguro" hasta el "totalmente es inseguro", en la escala de Likert los encuestados tienen que expresar su libre opinión sobre todos los indicadores propuestos y además de forma gradual categórica (Likert, 1932).

1.1.24 Evento de seguridad de la información

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 (ISO/IEC TR 18044, 2004).

1.1.25 Firewall

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes externas, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa (violación de acceso). Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios adicionales de seguridad como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben usar el mismo método de encriptación-desencriptación para entablar la comunicación robusta, como se muestra en la figura 03.

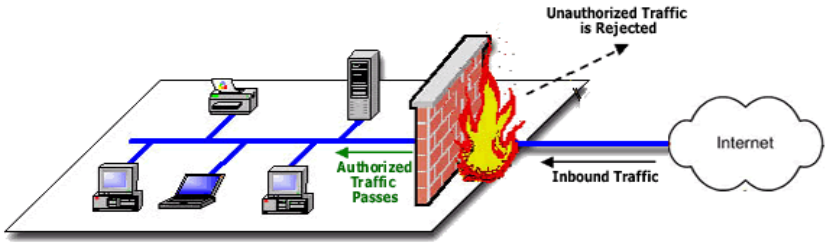

Figura 3. El Firewall y su entorno operacional

1.1.26 Librería Gdi32.dll

Librería Dinámica que se encarga de la interfaz de desarrollo gráfico, la librería en mención exporta múltiples funciones para aplicaciones que representan y generan gráficos. Sin la presencia de esta librería no sería posible graficar siquiera un punto en la pantalla del monitor.

1.1.27 Gestión y Dirección de tecnologías de la Información

Este se encarga de la administración interna como: La planificación, implementación, gestión de sistemas de información, y la infraestructura tecnológica de cómputo con equipos como por ejemplo: los Firewall, gestión de servidores entre otros. En el presente trabajo se incide más en la infraestructura tecnológica de cómputo y comunicaciones. Consiste en tomar decisiones operativas dentro del gobierno de las Tecnologías de la Información. La gestión de la Tecnologías de la Información se refiere a los aspectos operativos para el suministro de productos y servicios de tecnologías de información en la forma más eficaz (EAC, 2018).

1.1.28 Gestión, Dirección y Construcción de Infraestructura adecuada

Aborda la Seguridad desde el enfoque físico material tangible, contempla y propone parámetros adecuados para la construcción de áreas especializadas (MVCS, 2006). La norma está dirigida a la gestión de seguridad en la construcción de instalaciones para el sector público y privado (Mypes).

1.1.29 Incidente de Seguridad de la Información

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 (ISO/IEC TR 18044, 2004).

1.1.30 Integridad

La propiedad de salvaguardar la exactitud e integridad de los activos, presenta los conceptos y modelos fundamentales para una comprensión básica de la

seguridad en las tecnologías de la información (TICs), aborda los problemas generales de administración que son esenciales para la planificación, implementación y operación de la seguridad de las TICs. (ISO/IEC 13335-1, 2004).

1.1.31 Intrusismo

Se define intrusismo como el ejercicio de actividades profesionales por persona no autorizada para ello. Puede constituir delito. En el contexto de las ciencias de la computación se evidencia regularmente el intrusismo (RAE, 2018).

1.1.32 Librerías Estáticas

Archivo con contenido algorítmico, también llamado cabecera de programa, es una librería que al momento de compilarse el código objeto "se copia" en la aplicación generada. Una vez que se tiene el ejecutable del programa este se ve incrementado en su tamaño, puesto que contiene las funciones y procedimientos que usó el programa, en adelante el nuevo programa ya no dependerá de las librerías estáticas compiladas.

1.1.33 Librerías Dinámicas

Aplicación binaria que tiene como característica principal proveer y disponer las funciones y procedimientos implementados en ella así como los programas que requieren acceso a ella. A diferencia de las librerías estáticas estas no se copian en los programas generados. A través de estas librerías dinámicas se puede generar aplicaciones especializadas en base a distintos lenguajes de programación. Todos unificados por una interfaz de intercomunicación entre aplicaciones.

1.1.34 Mype

Se representa como una Micro y Pequeña Empresa (Mype) es una unidad económica constituida por una persona natural o jurídica (empresa), bajo cualquier forma de organización y tiene como objeto desarrollar actividades de

extracción, transformación, producción, comercialización de bienes o prestación de servicios (SUNAT, 2017).

1.1.35 Muestreo Probabilístico

Se le denomina muestreo probabilístico si la selección de las unidades muéstrales se realiza utilizando un esquema muestral equiprobabilístico para cada unidad, basado en las probabilidades que tienen sujetos de la población en formar parte de la muestra, también podemos disgregarlo en el muestreo probabilístico con remplazo y sin remplazo.

1.1.36 Programa malicioso

El software malicioso, es un programa conocido en inglés como "*malware*", es también conocido como un software diseñado específicamente para obtener acceso a un equipo local o remoto con el propósito de dañarlo sin que el usuario tenga conocimiento. Hay distintos tipos de software malicioso, tales como el *spyware*, los registradores de pulsaciones de teclas, los virus que infectan ejecutables, los gusanos o cualquier tipo de código malicioso que se infiltre en un equipo local o remoto. Generalmente, para determinar si el software es malicioso, se considera la intención de su creador, más que sus características de operación. Hoy en día la creación de software malicioso está en aumento, esto se debe a que se crean nuevos tipos todos los días y al atractivo del dinero que puede ganarse mediante el crimen organizado a través de Internet. Inicialmente, el software malicioso se creó como un experimento de laboratorio para realizar bromas, pero las posibilidades de poder crear lo que se imagina dio lugar al vandalismo y a la destrucción de equipos informáticos. Actualmente, la mayoría del software malicioso se crea para ganar dinero a través de publicidad forzada (publicidad no deseada), el robo de información confidencial (*spyware*), la difusión de *spam* o pornografía por correo electrónico o la extorsión (*ransomware*).

Existen factores que pueden hacer que un equipo sea más vulnerable a los ataques de software malicioso, como defectos en el diseño del sistema operativo, que todos los equipos de una red ejecuten el mismo Sistema Operativo, que los

equipos estén conectados al internet (Norton, 2018). Debido a la popularidad de Microsoft, la mayoría del software malicioso se escribe para el sistema Windows.

1.1.37 Prueba Estadística McNemar

La prueba estadística en mención es una prueba no paramétrica, se aplica para estudios observacionales y estudios experimentales. Identifica modificaciones en una variable dicotómica categórica a través del tiempo para lo cual se requiere realizar por lo menos dos mediciones una medida antes y una medida después. Cuando solo se realiza una observación entre el antes y el después dicha prueba se asocia a estudios observacionales, sin embargo, si realizamos modificaciones entre el antes y el después la prueba de McNemar se asocia a estudios experimentales por tanto se ubica en el nivel investigativo explicativo (Supo, 2016). Es importante mencionar que las variables analizadas requieren ser categóricas dicotómicas.

1.1.38 Pruebas no paramétricas

Una prueba no paramétrica es una prueba de hipótesis que no requiere que la distribución de la población sea caracterizada por ciertos parámetros. Por ejemplo, muchas pruebas de hipótesis parten del supuesto de que la población sigue una distribución normal con los parámetros μ y σ. Las pruebas no paramétricas no parten de este supuesto, de modo que son útiles cuando los datos son considerablemente no normales y resistentes a transformaciones (Minitab, 2018).

En la estadística paramétrica, se presupone que las muestras provienen de distribuciones totalmente especificadas y caracterizadas por uno o más parámetros desconocidos sobre los cuales se desea hacer inferencias. En un método no paramétrico, se presupone que la distribución de la que proviene la muestra no está especificada y, con frecuencia, se desea hacer inferencias sobre el centro de la distribución. Por ejemplo, muchas pruebas de la estadística paramétrica, como la "*prueba t de student de una muestra*", se realizan bajo el supuesto de que los datos provienen de una población normal con una media

desconocida. En un estudio no paramétrico, se elimina el supuesto de normalidad. Los métodos no paramétricos son útiles cuando no se cumple el supuesto de normalidad y el tamaño de la muestra es pequeño. Sin embargo, las pruebas no paramétricas no están completamente libres de supuestos acerca de los datos. Por ejemplo, es fundamental presuponer que las observaciones de las muestras son independientes y provienen de la misma distribución. Además, en los diseños de dos muestras, se requiere el supuesto de igualdad de forma y dispersión (Minitab, 2018).

1.1.39 Librería Kernel32.dll

Es un tipo de librería dinámica desarrollado por Microsoft para el Sistema Operativo Windows. Esta librería en forma de archivo contiene funciones implementadas en código máquina, las cuales le permiten interactuar entre los componentes lógicos y físicos del Computador. Las funciones elementales de imprimir caracteres en pantalla, en un dispositivo externo como una impresora, la contiene este archivo de nombre *Kernel32.dll.*

1.1.40 Prueba de Wilcoxon

La prueba de Wilcoxon es una prueba estadística no paramétrica esta es el equivalente de la "*Prueba T de student para muestras relacionadas*", esta prueba se usa cuando a un grupo se hacen dos mediciones, un antes y un después. Se asociado según el propósito del estudio al nivel investigativo descriptivo o al nivel investigativo explicativo (Supo, 2016). Además, la prueba de Wilcoxon no requiere que se cumpla con los supuestos de normalidad y esfericidad.

1.1.41 Riesgo residual

El riesgo remanente después del tratamiento del riesgo, uso sistemático de la información para identificar las fuentes y estimar el riesgo (Riesgos, 2002).

1.1.42 Seguridad

El término seguridad posee múltiples definiciones concordantes, se puede afirmar que este concepto que proviene del latín *securitas* hace foco en

la característica de seguridad es decir realza la propiedad de algo donde no se registran daños ni riesgos.

1.1.43 Seguridad Lógica

Es una parte del amplio espectro que se debe abordar para no vivir con una sensación ficticia de seguridad. Como ya se ha indicado, el activo más importante que se posee en el contexto computacional es la información, y por lo tanto deben existir técnicas y mecanismos, más allá de la seguridad física, que la garanticen el aseguramiento (Basaldúa, 2005).

1.1.44 Seguridad Informática

Parte fundamental de la estabilidad y orden de la información. La Seguridad de la información de las entidades requiere de mecanismos de protección de acuerdo al Sistema de Gestión de la Seguridad de la Información - SGSI (ISO/IEC 27001, 2005)**,** Abordando así la infraestructura computacional y todo lo relacionado con este. De este modo contribuyen a incrementar la seguridad, para ello existen una serie de estándares. La calidad de Software contribuye en el desarrollo de software a través de protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos de la confiabilidad de la información (ISO/IEC 9126, 2005). La definición de seguridad de la información no debe ser confundida con la de seguridad informática ya que esta última sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

1.1.45 Seguridad de información

Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad (ISO/IEC 17799, 2005).

1.1.46 Sistema de gestión de Seguridad de la Información (SGSI)

Hace referencia a un plan de requerimientos planteado por el ISO 27001, sugiere un análisis de requisitos, la planeación y generación de protocolos de seguridad y aplicación de reglas las cuales deben contribuir en la seguridad de la información de las Mypes. El SGSI es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse a través de un proceso sistemático, documentado y conocido por toda las Mypes. Este proceso es el que constituye un SGSI. Su propósito garantizar que los riesgos de la seguridad de la información sean conocidos, gestionados y minimizados por las Mypes de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos y su entorno. Esa 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. El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos (ISO/IEC 27001, 2005), la gestión de la Seguridad de la Información se debe realizarse a través de un proceso sistémico, documentado y conocido por toda la empresa. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información, los tres términos son:

• **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Para garantizar que la seguridad de la

información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

1.1.47 Librería user32.dll

Librería dinámica que contiene funciones exportables para la administración adecuada del Sistema Operativo Windows. Por otro lado esta librería contiene funciones que contribuyen en la inseguridad del Sistema Operativo, debido a que exporta funciones como: *CallWindowProc, CallNextHookEx, SetWindowsHookA* entre otras. *A* través de ellos un desarrollador de sistemas puede programar aplicaciones a medida las cuales permiten sustraer información de los usuarios finales.

1.1.48 Vulnerabilidad

La vulnerabilidad de los sistemas de información afecta la seguridad. Las vulnerabilidades pueden ser causadas por software, diseño de hardware y defectos de programación (ISO/IEC 29147, 2014, pág. 5), es por lo cual que se generan incidentes informáticos.

1.2 Antecedentes

Aguirre & Fabian (2015) plantean un Plan de Seguridad Informática para la *ESPE* sede Latacumga, dicho trabajo de investigación tuvo por objetivo principal: Realizar el Plan de Seguridad Informática aplicable para la Universidad de las Fuerzas Armadas *ESPE* extensión Latacunga, mediante la utilización del Marco de referencia COBIT 5, COBIT para la Seguridad de la Información y la normas técnicas ecuatorianas NTE INEN-ISO/IEC 27000 para la gestión de seguridad de la información, como resultado se indicó: que los activos más relevantes identificados durante la ejecución de las entrevistas y la recepción de la información proporcionado por las partes interesadas fueron: el inventario de activos. El proyecto se desarrolló por cada activo además se realizó el análisis con los respectivos responsables, acerca de las posibles amenazas potenciales.

Estrada (2011) plantea estrategias de seguridad informática en capas, aplicando la concepción de Operaciones Militares por acción retardante, el referido trabajo tuvo como objetivo emplear las estrategias militares en la Seguridad Informática el cual consistió en realizar un análisis de las diferentes estrategias ofensivas que emplean las fuerzas terrestres para plantear una analogía con las técnicas empleadas para la seguridad informática. Llegando así a los siguientes resultados: creó un ciclo permanente cuya característica fundamental es la constancia y la actualización de conocimientos hasta ejecutar un plan de contingencia con el cual detecta una vulnerabilidad que no fue detectada por el *Snort* por tanto genera una regla en *local rules* para que así este sea identificado.

Amparo (2015) propone el diseño e implantación de una red privada virtual (VPN) a través de la infraestructura como servicio (IAAS) para el acceso a una entidad bancaria mediante *single sign on (SSO)*, El objetivo principal de este trabajo fue diseñar e implantar una red privada virtual (VPN) a través de la Infraestructura como Servicio (*IaaS*) para el acceso a una entidad bancaria mediante *Single Sign On* (SSO). Con el fin de alcanzar este objetivo se realizaron diversos análisis sobre la plataforma tecnológica. Se llevó a cabo un estudio de la situación actual con la finalidad de conocer el mejor escenario que se adaptara tanto a nivel técnico como al retorno de inversión a mediano plazo. En el levantamiento de información también se consideraron las bases teóricas

sobre los aspectos concernientes a la seguridad de los datos de acceso de los usuarios y todas aquellas actividades necesarias para poder establecer políticas, normas y procedimientos apropiados. El diseño e implantación se logró de forma satisfactoria, solventando así las innumerables llamadas al *Help Desk* por no contar una clave única para el inicio de sesión en las diferentes aplicaciones que se tienen con proveedores de servicio que se encuentran en la nube.

Díaz (2000) aborda el estudio del núcleo de seguridad para un Sistema Operativo orientado a objetos y soportado por una máquina abstracta. Describe un mecanismo de protección basado en capacidades diseñado para un Sistema Integral Orientado a Objetos (*SIOO*), que cumple los requisitos generales de diseño de un mecanismo de seguridad y los específicos para un *SIOO*. Además, aporta propiedades adicionales, como una protección automática de las capacidades y permisos de longitud variable. Todo ello configura un sistema que soluciona de manera más elegante y completa las necesidades de protección de un *SIOO*, con un rendimiento adecuado.

Parra (2014) contempla al ISO 27001 aplicado a las Mypes. El objetivo principal fue proponer una metodología de implementación de la ISO 27001 para que sea aplicada en la implementación de Sistemas de Gestión de Seguridad de la Información en PYMES. Como resultados indica que las grandes compañías pueden tener más desarrollo en infraestructura tecnológica, pero también deben hacer esfuerzos importantes en la capacitación de los usuarios, para concienciarlos de los riesgos potenciales que tienen en sus manos, por el simple hecho de tener acceso a la tecnología; así mismo indica que no es suficiente tener muchas implementaciones de medidas de seguridad, si estas no van acompañadas de políticas y procedimientos, que ayuden a consolidar mecanismos de defensa, en favor de la seguridad informática. Por otro lado, indica que se pueden generalizar los procedimientos y políticas a todos los tipos de empresas, realizando las adecuaciones que las personalicen, ya que complementan las que existan en las empresas, aunque se tengan soluciones costosas y sofisticadas.

Pacheco (2015) plantea una Metodología para la Seguridad de Tecnologías de Información y Comunicaciones en la Clínica Ortega, el cual tuvo por objetivo general: Determinar el nivel de importancia de la metodologías de seguridad de tecnologías de información y comunicaciones que permita la continuidad de procesos de la clínica

Ortega cuyos servicios principales dependen de la tecnología una vez culminado el estudio se arribó a las siguientes conclusiones: dentro del aseguramiento del entorno de tecnologías de información y comunicaciones, se debe considerar un tiempo para realizar el balance respecto de la efectividad y adecuación de los cambios implantados en el entorno y evaluar la necesidad de realizar ajustes. Además, Todo plan sufre cambios continuos a través del tiempo, que deben acompañar la transformación del entorno. Estos cambios deben ser considerados dentro del plan de aseguramiento, en los distintos modelos propuestos para cada etapa.

Heffel & Linares (2016) contemplan a la ciberseguridad industrial en la distribución de energía eléctrica, el trabajo que concluye dando a entender a la ciberseguridad industrial como una disciplina moderna, y a la vez contemporánea, ya que el grado en el cual la sociedad actual depende de la tecnología sigue aumentando en forma exponencial gracias a la investigación, el desarrollo y la innovación.

Macero (2015) implementa de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría y Auditoría, aplicando la Norma ISO/EIC 27001. La investigación se desarrolló en Ambato – Ecuador. El objetivo fue: el de Proponer un Modelo de Gestión de Seguridad Informática para garantizar la continuidad del negocio en la CACPE Pastaza. Así mismo este llego a los siguientes resultados: la Seguridad Informática no puede ser considerada como un producto, sino como un proceso basado en un ciclo iterativo, en el que incluyen actividades como valoración del riesgo, prevención, detección y respuesta ante incidentes de seguridad por otro lado: El Análisis de Riesgos toma parte fundamental dentro de la Gestión de la Seguridad Informática, es en esta etapa en donde se logra identificar de forma proactiva los riesgos a los que están expuestos los procesos, recursos y servicios críticos y que pueden causar interrupción en el negocio. La gestión, a tiempo de los riesgos, permite crear estrategias que nos garantice la continuidad de las operaciones, aunque estos riesgos se llegarán a materializar.

Peña (2016) muestra el diseño e implementación de una red privada virtual cuyas siglas en ingles son *VPN-SSL*, utilizo el método de autenticación *LDAP* en una empresa privada, La investigación tuvo como propósito diseñar e implementar una Red Privada Virtual (*VPN-SSL*) utilizando el método de autenticación *LDAP* en una empresa

privada, con el objetivo de proteger las conexiones de acceso remoto hacia la organización a través del contenido cifrado, garantizando la integridad, confidencialidad y seguridad de los datos. En su desarrollo, se abordaron aspectos teóricos de una *VPN*, seguridad y documentación de los protocolos que se utilizan actualmente para las conexiones seguras de acceso remoto. En relación a la metodología, se desarrolló bajo el esquema de proyecto factible. Para la obtención de los resultados, se empleó la técnica de observación documental y arqueo bibliográfico, en base a ello se llevaron a cabo cada una de las fases planificadas, logrando la implementación de una *VPN-SSL* integrada con el protocolo *LDAP*. Se realizaron una serie de adecuaciones y configuraciones en la empresa privada en el que se definió la política de acceso remoto a la red, se comparó el protocolo *SSL* con respecto al *IPSec*, se estudió el protocolo *LDAP*, se definió la arquitectura de implementación de la *VPN-SSL*, se configuró e integró el firewall con el directorio activo de la empresa, se establecieron las políticas de firewall para la conectividad de los usuarios de la *VPN*, se verificó la redundancia en la conectividad a través de pruebas de conexión a través de la *VPN-SSL*, y por último desarrolló un manual el cual permitió gestionar la conexión a través de la *VPN*. Entre las conclusiones más relevantes se destacan: la arquitectura utilizada permite redundancia en la conexión vía *SSL-VPN*, se garantiza la continuidad del negocio permitiendo establecer conexión desde cualquier ubicación geográfica.

Ramón (2015) aborda los factores críticos en la adopción de medidas de seguridad utilizadas por los estudiantes de los Centros formativos universitarios de tecnologías *TICs* al usar herramientas 2.0. El referido trabajo de investigación tesis doctoral tuvo por objetivo conocer si los estudiantes adoptan suficientes medidas de seguridad cuando navegan por internet haciendo uso de las redes sociales. Así mismo el referido trabajo de investigación tuvo los siguientes resultados: solo el 04% de los encuestados utilizan contraseñas complejas, alrededor del 40% tienen una contraseña única para todos sus accesos, la tercera parte de los participantes no protege el acceso a su propio ordenador, más del 25% abren email desconocidos, y una sexta parte no tienen inquietud por conocer los bugs y vulnerabilidades del sistema, finalmente con respecto a las redes sociales más del 60% de los participantes se dan de alta sin leer las condiciones de registro y casi la mitad (entre 40% y el 45%) manifiestan y publican libremente sus opiniones sobre temas sensibles.

Santiago (2017) el trabajo de investigación doctoral encuentra patrones de seguridad empresarial, desarrolla meta-modelos arquitectónicos que contribuyen a las organizaciones a diseñar e implementar arquitecturas de seguridad empresariales que protejan y respalden sus activos de información, a la hora de desarrollar nuevos sistemas de información. Llegando así a los siguientes resultados: los patrones de seguridad son un método útil para presentar las soluciones comunes, pero los patrones en su conjunto analizados no siguen una guía un común a la hora de documentar las soluciones, por lo tanto, es complicado llegar a obtener una clasificación de patrones de seguridad adecuada, concluye indicando que los patrones de seguridad actuales tienen limitaciones disgregadas en tres puntos específicos.

Tibaquira (2016) plantea una metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma *SIEM(* Correlacionador de Eventos de Seguridad*)* de una entidad financiera basada en la norma ISO/IEC 27035 e ISO/IEC 27005, se basa en la definición de un modelo de gestión de incidentes de seguridad de la información y de gestión de riesgos sobre estos incidentes, que son detectados o derivados de la implementación y operación de una herramienta *SIEM*. La definición de los modelos de gestión se realizó bajo las normas ISO 27035 para incidentes de seguridad y 27005 para la gestión de riesgos.

Tola (2015) realiza la implementación de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría y Auditoría, aplicando la Norma ISO/EIC 27001, el cual tuvo por objetivo general: lograr la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A&C Group S.A, al final del estudio se llegó a los siguientes resultados: en la última fase del Sistema de Gestión de Seguridad de la Información acuña la concientización y formación del personal, con el fin de crear en la empresa una cultura de seguridad mostrando la importancia de sus actividades y como ellos pueden contribuir al logro de los objetivos establecidos en el sistema. La concientización y divulgación consiguen que el personal conozca qué actividades se están llevando a cabo y por qué se están realizando.

Yesid (2015) plantea una metodología de gestión y administración de incidentes de Seguridad de la Información digital y Gestión de riesgos para la plataforma SIEM de una Entidad Financiera basada en los estándares ISO/IEC 27035 e ISO/IEC 27005. El referido trabajo de investigación tuvo por objetivo: Definir e implementar una metodología de gestión de incidentes de seguridad informática y gestión de riesgos asociados a los incidentes identificados por la plataforma SIEM de la Entidad Financiera, teniendo como referencia los estándares ISO/IEC 27035 e ISO/IEC 27005, llegando así a los siguientes resultados: logra construir un modelo completo que aborda la gestión de incidentes y la gestión de riesgos asociada a estos incidentes, los cuales permitieron la identificación y el análisis de los componentes que hacen parte del establecimiento del contexto bajo el cual se implementaron las normas – estándares.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 Identificación del problema

En la actualidad y en adelante la Seguridad de la información pasó a ser parte pilar requerida para garantizar la estabilidad social, debido a que los protocolos de seguridad contribuyen con el orden global en los procesos de transferencia de datos en diferentes escenarios (Tola, 2015). tales como el sector público privado específicamente: el sector financiero-bancario, las políticas gubernamentales, la información tributaria, indicadores nacionales e internacionales teniendo como objeto el aseguramiento de la información (Parra, 2014), para el presente trabajo se contempló el análisis en un grupo de Mypes correspondientes al departamento de Puno a través de un muestreo. El aseguramiento de la información sin estos protocolos de Seguridad en los Sistemas de Información desestabilizaría el orden social global. Por otro lado, la Seguridad informática absoluta es utópica, el presente trabajo de investigación tiene por objetivo evidenciar la falsa percepción de seguridad en las Mypes muestreadas.

2.2 Enunciado del Problema

Hoy en día la inseguridad de la información requiere ser abordada por los desarrolladores de Sistemas informáticos con mayor responsabilidad. Debido a la existencia de errores - *bugs* y de vulnerabilidades que ponen en riesgo a los usuarios del Sistema Operativo Windows (Zero, 2016). y con la exposición del Sistema Operativo a público abierto se puede entrever dichos errores y vulnerabilidades existentes, sin embargo solo se difunden en las redes las descubiertas benignamente, muchas veces con propósitos académicos, dejando de lado las no difundidas como por ejemplo las puertas

traseras - *backdoors* y otros del cual, solo tienen conocimiento los especialistas y en muchos casos especialistas anónimos que hacen uso y abuso de dichos accesos para su uso personal. Actualmente la ciberseguridad en el contexto de *Big Data* es conocido como un problema crítico y presenta un gran reto para la comunidad investigadora (Sabar, Yi, & Song, 2018), por lo que es de importancia su abordaje. La comunidad de investigadores busca reducir estas brechas de riesgo, la seguridad planteada del sistema Operativo Windows no puede garantizar en su totalidad la confidencialidad, integridad y disponibilidad de la información, Aun cuando Microsoft lanza parches de Seguridad cada año para solucionar sus problemas de compatibilidad e inseguridad en sus componentes (Microsoft, 2017). El cual, deja una brecha de riesgo, siendo utópico el aseguramiento de la información total, motivo por el cual se implementan teorías, técnicas y modelos de aseguramiento en los Sistemas de información como SGSI del ISO 27001, COBIT, entre otras. El aseguramiento está dirigido a contribuir en el manejo adecuado de protocolos, reglas y buenas prácticas manufactureras, la no presencia de estos modelos en la gestión pública y privada contribuye en la inseguridad de la información, las empresas de la Región de Puno requieren crecer económicamente y tecnológicamente, sin embargo no todas llegan a tales propósitos, en la mayoría de los casos debido a la informalidad y los argumentos planteados estas resultan en quiebra. Por otro lado en la Región de Puno y el resto del país actualmente los usuarios finales tienen una gran preferencia por el Sistema Windows 7, 8 y 10 siendo el Sistema Operativo de mayor uso por los usuarios, entre ellos las Mypes, debido a su entorno de interacción a través de ventanas, además su facilidad de operación y compatibilidad con múltiples *drivers* - controladores de software y sistemas existentes, es por lo que el Sistema Operativo Windows tiene mayor demanda de uso en la Región y por ende es el más vulnerable. El presente trabajo de investigación tiene por objetivo dar a conocer la falsa percepción de Seguridad en las Mypes de la Región de Puno. Los equipos tecnológicos y procesos de las Mypes requieren ser gestionadas y dirigidas apropiadamente, especialmente en el aseguramiento de la información. Las Mypes por la estructuración planteada por la Sunat son: microempresas de persona natural - jurídica que buscan emerger incrementalmente, sin embargo no todas tienen éxito. Muchas terminan con un cierre definitivo antes de lo previsto debido a lo comentado y otros factores propios de la realidad nacional. La implementación de los modelos

indicados busca contribuir en la Seguridad de la Información de las Mypes, evidenciando así las deficiencias de sus Sistemas, incluido el Sistema Operativo que usan, en el presente trabajo se incluye una aplicación de software que permite evidenciar la inseguridad en el Sistema Operativo, su identificación y detección por parte de los Software antivirus comerciales hacia este es ineficiente, debido a que no registran sus rasgos y atributos en los bancos de datos de dichos software antivirus. Es por lo que existe riesgo de inseguridad, la adición de capas para salvar los problemas de desadaptación que presenta el paradigma de la orientación a objetos provoca una serie de inconvenientes cuando se acrecienta el proyecto (Díaz, 2000). Por otro lado los antivirus informáticos contribuyen en la seguridad de los sistemas, sin embargo estos solo ven el aspecto lógico operacional del software. No controlan protocolos de seguridad física en las Mypes así como las Estrategias de Seguridad Informática por capas (Estrada, 2011). La cual plantea incrementar la seguridad a través de capas. Estos procedimientos reducen los riesgos de inseguridad a través de la implementación de mecanismos especializados no solo a nivel de software si no a niveles físico-lógicos. El presente trabajo de investigación aborda y cuantifica la inseguridad a través del suministro de modelos de aseguramiento en las Mypes, buscando así evidenciar las vulnerabilidades para reducir del riesgo de inseguridad en las Mypes. Por todo lo mencionado me planteo la siguiente interrogante **¿Se evidencia la falsa percepción de seguridad en las Mypes muestreadas?**

2.3 Justificación

El presente trabajo tiene por objetivo contribuir en la línea de investigación de la Seguridad de la Información digital, a través de la identificación de vulnerabilidades del Sistema Operativo. Buscando a si reducir los incidentes de inseguridad, contribuyendo en contrarrestar uno de los principales problemas del país, el cual ya fue legislado bajo el nombre de ”Los delitos Informáticos ”, según base legal Ley Nº 27309 “Ley que incorpora lós Delitos Informáticos de intrusísmo y cracking al código penal nacional”.

2.4 Objetivos

2.4.1 Objetivo general

Evidenciar la falsa percepción de Seguridad en los Sistemas de las Mypes.

2.4.2 Objetivos específicos

1. Analizar e identificar funciones restringidas exportables de uso exclusivo del Sistema Operativo Windows® que afecten la Seguridad.
2. Determinar el grado real de Seguridad Informática con que cuentas las Mypes muestreadas

2.5 Hipótesis

2.5.1 Hipótesis general

Se evidencia la falsa percepción de seguridad en las Mypes, es decir no existe diferencia entre las combinaciones de tratamientos (grupos) por tanto la inseguridad es permanente en cada tratamiento (grupo).

2.5.2 Hipótesis especificas

1. La reutilización de funciones exportables reservadas del sistema operativo afecta en la identificación de nuevos puntos vulnerables del Sistema Operativo.
2. El grado de Seguridad Informática en las Mypes está por debajo de lo adecuado. Por lo que, la inseguridad prevalece.

CAPÍTULO III

MATERIALES Y METODOS

3.1 Lugar de estudio

Geográficamente el lugar de estudio es la ciudad de Puno, perteneciente a la Región Puno del Perú, según las coordenadas, su ubicación es de 15°50'31" de Latitud Sur y 70°01'11" de Longitud Oeste del Meridiano de Greenwich con una altitud sobre el nivel del mar de 3825 msnm.

3.2 Población

En el presente trabajo de investigación, se consideró como población de estudio a las empresas de tipo Mypes en Región de Puno asociados específicamente al rubro Textil Confecciones. Que a la fecha son 231 Mypes según, el reporte de Mypes contratadas por el núcleo ejecutor de compras de chompas escolares DU Nº 058-2011–FONCODES. En cada unidad poblacional se consideraron los Sistemas físico lógicos computacionales que contribuyen en la dirección, sistematización, administración y operación de sus datos.

3.3 Muestra

Para determinar el tamaño muestral se usó la estimación de promedios con población conocida obteniéndose así el tamaño muestral de 39.398, siendo el tamaño apropiado de 40 Mypes ubicadas en la Región de Puno.

$$n = \frac{N * Z^2_{1-\alpha/2} * S^2}{d^2 * (N-1) + Z^2_{1-\alpha/2} * S^2}$$

Dónde:

$Z^2_{1-\alpha/2}$: *Valor tabular Z.*

S^2 : *Varianza*

N : *Tamaño de la población*

d^2 : *Error elevado al cuadrado.*

A través de la formula arriba y con los parámetros N=231; α = 0.05 (Error de tipo I – tolerancia de la prueba); S=2.0 (antigüedad de las Mypes a través de una muestra piloto) y d = 0.57. Con los cuales se determinó el tamaño muestral indicado n = 40.

Para la selección de las unidades muestrales se hizo uso de la técnica de muestreo probabilística al azar: muestreo aleatorio simple a través del cual se identificó a las 40 Mypes.

3.4 Método de Investigación

El presente trabajo de investigación por su naturaleza corresponde al nivel investigativo Correlacional - Explicativo.

3.4.1 Método Cuantitativo

La intención de este método es describir, cuantificar, exponer y encontrar el conocimiento ampliado de un caso mediante datos, se requiere evidenciar la frecuencia, realizar un análisis cuantificable. En este método el objeto de estudio parte desde el nivel investigativo exploratorio nivel en el que se postula parte fundamental de la investigación científica, la investigación es normativa, apuntando a leyes generales relacionadas a las variables según su naturaleza. La recolección, tabulación de datos consta de pruebas objetivas como: instrumentos de medición, el análisis estadístico, *tests*, entre otros.

3.4.2 Validez de la confiabilidad del Instrumento

La validación del instrumento - cuestionario se realizó disgregada mente, puesto que para cada tratamiento se plantean interrogantes específicas en un escenario tecnológico diferente, las cuales contribuyen al levantamiento de la información en cada tratamiento planteado. Por tanto se obtiene el Alfa de Cronbach en cada grupo de interrogantes, las cuales se muestra en la siguiente tabla.

Tabla 1
Estadísticas de fiabilidad

N	Grupo Tratamiento	N de elementos	Alfa de Cronbach
1	01	04	90,5
2	02	04	94,4
3	03	04	94,2
4	04	04	93,3

Indicadores obtenidos sobre la fiabilidad de los instrumentos

El análisis de fiabilidad del instrumento por cada tratamiento, da como resultado que el instrumento es fiable, con coeficientes de Alfa de Cronbach superiores a 0,90 lo que se representa porcentualmente superiores al 90% y según los criterios de fiabilidad del Alfa de Cronbach, podemos concluir que el instrumente es altamente fiable (George & Mallery, 2012).

Además se validó el instrumento aplicando: La validación por juicio de expertos, el cual involucro a 04 profesionales en el área de estadística e informática con relación a los tratamientos indicados. La que consistió en asociar la pertinencia y adecuación de las interrogantes en el cuestionario bajo el siguiente esquema:

Pertinencia	¿Las interrogantes contribuyen a los objetivos del estudio?
Adecuación	¿El instrumento está adaptado a las personas a las se les va a solicitar información? (Destinatario - Mypes).

VALIDACIÓN DE CUESTIONARIO POR PREGUNTA E INSTRUMENTO GLOBAL

==========

	Pertinencia	Adecuación
Pregunta (i donde i =1..20)	1 2 3 4 5	1 2 3 4 5

==========

Dónde: 1: Muy malo; 2: Malo; 3: Regular; 4: Bueno; 5: Muy bueno

Resultando adecuado el instrumento planteado (puntuación 3 a más en promedio).

3.5. Descripción detallada de métodos por objetivos específicos

Para desarrollar el primer específico se aplicó la técnica observacional, analítica, a través de Depends.exe de Microsoft Visual Studio 6.0 el cual permitió identificar las funciones que exportan las librerías dinámicas de los sistemas informáticos, incluidos los del Sistema Operativo.

Referente al Segundo objetivo específico se hizo uso del método estadístico en varios tramos del estudio así como el diseño factorial completo al azar (Montgomery, 2004), a continuación, la descripción elemental de las pruebas estadísticas involucradas en el estudio:

3.5.1 McNemar

Debido a que el estudio corresponde a un análisis longitudinal se pudo usar esta prueba para identificar diferencias entre las medidas antes y después, sin embargo las variables de respuesta deberían ser categóricas - dicotómicas (Seguridad e InSeguridad). Sin la necesidad de que se cumplan con los supuestos de normalidad y esfericidad de los datos (Supo, 2016).

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

El presente trabajo de investigación llegó a los siguientes resultados: inicialmente se plantea el siguiente modelo teórico denominado: Análisis factorial univariante con un diseño factorial completamente al azar (Montgomery, 2004).

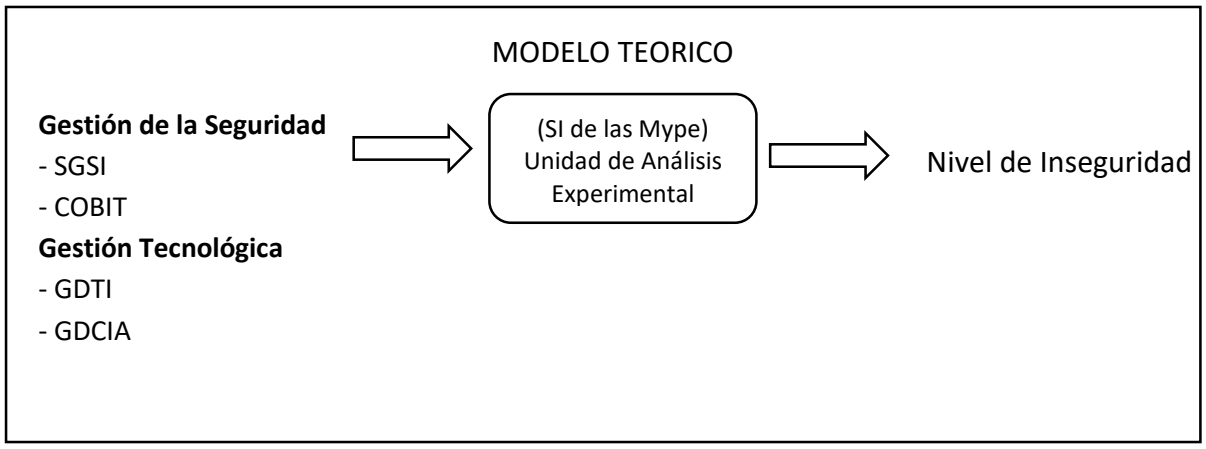

Figura 4. Diseño Factorial Completo al Azar (DFCA)

En el presente modelo se indica los factores de: Gestión de la seguridad y Gestión Tecnológica los cuales cumplen el rol de variable independiente categórica, las categorías de cada factor en adelante las denominaremos como tratamientos: es así que en cada factor tenemos 02 tratamientos. De esta manera se busca generar todas las combinaciones de tratamientos e identificar si hay diferencias entre las combinaciones de tratamientos.

Tabla 2

Combinación de tratamientos del Diseño factorial completo al azar

GRUPO / TRATAMIENTO	Gestión de Seguridad	Gestión Tecnológica	Nivel de Inseguridad
1	SGSI	GDTI	73
	SGSI	GDTI	72
	SGSI	GDTI	68
	SGSI	GDTI	73
	SGSI	GDTI	73
	SGSI	GDTI	76
	SGSI	GDTI	73
	SGSI	GDTI	70
	SGSI	GDTI	76
	SGSI	GDTI	70
2	SGSI	GDCIA	76
	SGSI	GDCIA	70
	SGSI	GDCIA	65
	SGSI	GDCIA	70
	SGSI	GDCIA	74
	SGSI	GDCIA	72
	SGSI	GDCIA	71
	SGSI	GDCIA	75
	SGSI	GDCIA	67
	SGSI	GDCIA	72
3	COBIT	GDTI	70
	COBIT	GDTI	74
	COBIT	GDTI	72
	COBIT	GDTI	75
	COBIT	GDTI	75
	COBIT	GDTI	73
	COBIT	GDTI	70
	COBIT	GDTI	68
	COBIT	GDTI	75
	COBIT	GDTI	68
4	COBIT	GDCIA	70
	COBIT	GDCIA	73
	COBIT	GDCIA	66
	COBIT	GDCIA	73
	COBIT	GDCIA	71
	COBIT	GDCIA	77
	COBIT	GDCIA	73
	COBIT	GDCIA	69
	COBIT	GDCIA	70
	COBIT	GDCIA	70

La información presentada en los 4 grupos cumple con los supuestos de normalidad y homogeneidad entre los grupos, a continuación presentamos los resultados usando las pruebas no paramétricas *Kolmogorov-Smirnov*, *Shapiro Wilk* y Prueba de homogeneidad de varianzas de *Levene*. Las cuales nos permiten saber si los grupos tienen distribución normal y si están homogeneizadas:

Tabla 3

Estadísticas de normalidad de datos

Pruebas de normalidad							
Grupo		***Kolmogorov-Smirnov[a]***			***Shapiro-Wilk***		
		Estadístico	**Gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Nivel de Inseguridad	1	.207	10	,200*	.920	10	.356
	2	.163	10	,200*	.963	10	.822
	3	.160	10	,200*	.872	10	.104
	4	.173	10	,200*	.946	10	.623

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Para este trabajo de investigación se tomó en cuenta la prueba de normalidad de *Shapiro Wilk* debido a que esta es aplicable en grupos pequeños < o iguales a 50 datos, en este caso cada grupo se conforma por 10 mediadas. Resultando: Grupo 1: no significante (P-valor = 0.356 > α); Grupo 2: no significante (P-valor = 0.822 > α); Grupo 3: no Significante (P-valor = 0.104 > α); Grupo 4: no significante (P-valor = 0.623 > α). Por lo que podemos decir que los resultados contemplan la normalidad en sus datos.

A continuación se verifica la homogeneidad de varianzas entre los grupos obteniéndose los siguientes resultados:

Tabla 4

Estadísticas de homogeneidad de varianzas

Prueba de igualdad de Levene de varianzas de error			
F	df1	df2	Sig.
.287	3	36	.834

Del cual podemos indicar que existe homogeneidad entre los 4 grupos, lo cual significa que la variabilidad interna de cada grupo es equivalente a la variabilidad de los demás puesto que según el planteamiento de la hipótesis de homogeneidad se acepta la hipótesis nula puesto que P-valor = 0.834 =83.4% el cual se encuentra por encima del

nivel de significancia. Concluyendo así que los grupos si tienen homogeneidad de varianzas. Cumpliendo los supuestos de normalidad y homogeneidad es razonable desarrollar el análisis factorial univariante, debido a que se demostró analíticamente que los resultados presentados son basales y estructuralmente comparables.

HIPÓTESIS DE INVESTIGACIÓN (Ha)

(Ho): Se evidencia la falsa percepción de seguridad en las Mypes, es decir no existe diferencia entre las combinaciones de tratamientos (grupos) por tanto la inseguridad es permanente en cada tratamiento (grupo).

(Ha): Existe diferencia entre las combinaciones de tratamientos (grupos) por tanto la inseguridad es menor en algún tratamiento (grupo) debido a la eficiencia de algún tratamiento lo que conlleva a no tener la falsa percepción de Seguridad.

Establecer un nivel de significancia

Nivel de Significancia (alfa) α = **0,05=5%**

Prueba Estadística

Para este tipo de datos representados en más de un factor, además de estructurarse sus factores en categorías, es pertinente contrastar la hipótesis planteada con una prueba multifactorial univariante debido a que en el modelo teórico se contempla solo una variable dependiente numérica aleatoria (efecto en el diseño).

Análisis Multifactorial Univariante

Tabla 5

Estadísticas análisis de factores inter-sujetos

Factores		Etiqueta de valor	N
Gestión Seguridad	1	SGSI	20
	2	COBIT	20
Gestión Tecnológica	1	GDTI	20
	2	GDCIA	20

Tabla 6

Pruebas de efectos inter-sujetos variable dependiente: Nivel de inseguridad

Origen	Tipo III de suma de cuadrados	gl	Media cuadrática	F	Sig.
Modelo corregido	10,800[a]	3	3,600	,411	,746
Gestion_Seguridad	,400	1	,400	,046	,832
Gestion_Tecnologica	10,000	1	10,000	1,141	,293
Gestion_Seguridad* Gestion_Tecnologica	,400	1	,400	,046	,832
Error	315,600	36	8,767		
Total	205962,000	40			
Total corregido	326,400	39			

a. R al cuadrado = ,033 (R al cuadrado ajustada = -,047)

A partir de los siguientes resultados obtenemos **Valor de P = 0.746 = 74,6**%(error obtenido en la prueba estadística). El cual indica que la prueba resulto no Significante entre grupos.

Toma de decisiones (Según el nivel de significancia alfa planteado) tenemos:

P = (0.746 = 74,6 > 0.05 = 5%)

Aceptamos la Hipótesis Nula y rechazamos la Ha.

Interpretación General

Se evidencia la falsa percepción de seguridad, es decir no existe diferencia entre las combinaciones de tratamientos (grupos) por tanto la inseguridad es permanente en cada tratamiento (grupo).

Interpretación específica para el primer factor (Gestión de Seguridad)

Del mismo modo obtenemos resultados para el factor Gestión de Seguridad, en el cual resulta el **P-valor**: 0.832 = 83.2% siendo no significante: con lo cual concluimos que no hay diferencia entre los tratamientos COBIT y SGSI(los resultados obtenidos en ambos casos son equivalentes).

Interpretación específica para el segundo factor (Gestión Tecnológica)

Por otro lado obtenemos resultados para el factor Gestión Tecnológica, en el cual resulta el **P-valor**: 0.293 = 29.3% siendo no significante: con lo cual concluimos que no hay diferencia entre los tratamientos GDTI y GDCIA(los resultados obtenidos en ambos casos son equivalentes).

Interpretación de interacción

La interacción de factores conduce a identificar el efecto simultáneo de los dos factores en el resultado según resulte significante o no significante la prueba de Análisis Factorial Univariante. En el presente trabajo de investigación tenemos como resultado **P-valor: = 0.832 = 83.2%** siendo este valor no significante. Por lo que concluimos que los factores no tienen un efecto simultaneo entre sí.

A continuación presentamos el cuadro comparativo entre tratamientos de los factores basados en la estructura de las pruebas estadísticas Post Hoc.

Tabla 7

*Gestión Seguridad * Gestión Tecnológica.*

Gestión Seguridad	Gestión Tecnológica	Media	Error estándar	Intervalo de confianza al 95%	
				Límite inferior	Límite superior
SGSI	GDTI	72,400	,936	70,501	74,299
	GDCIA	71,200	,936	69,301	73,099
COBIT	GDTI	72,000	,936	70,101	73,899
	GDCIA	71,200	,936	69,301	73,099

Donde podemos evidenciar que la peor combinación entre tratamientos resulto ser SGSI y GDTI debido a que en los descriptivos de la interacción de factores nos dio como resultado: **Media = 72,400** siendo este valor el de mayor inseguridad después de haber aplicado los tratamientos multifactoriales.

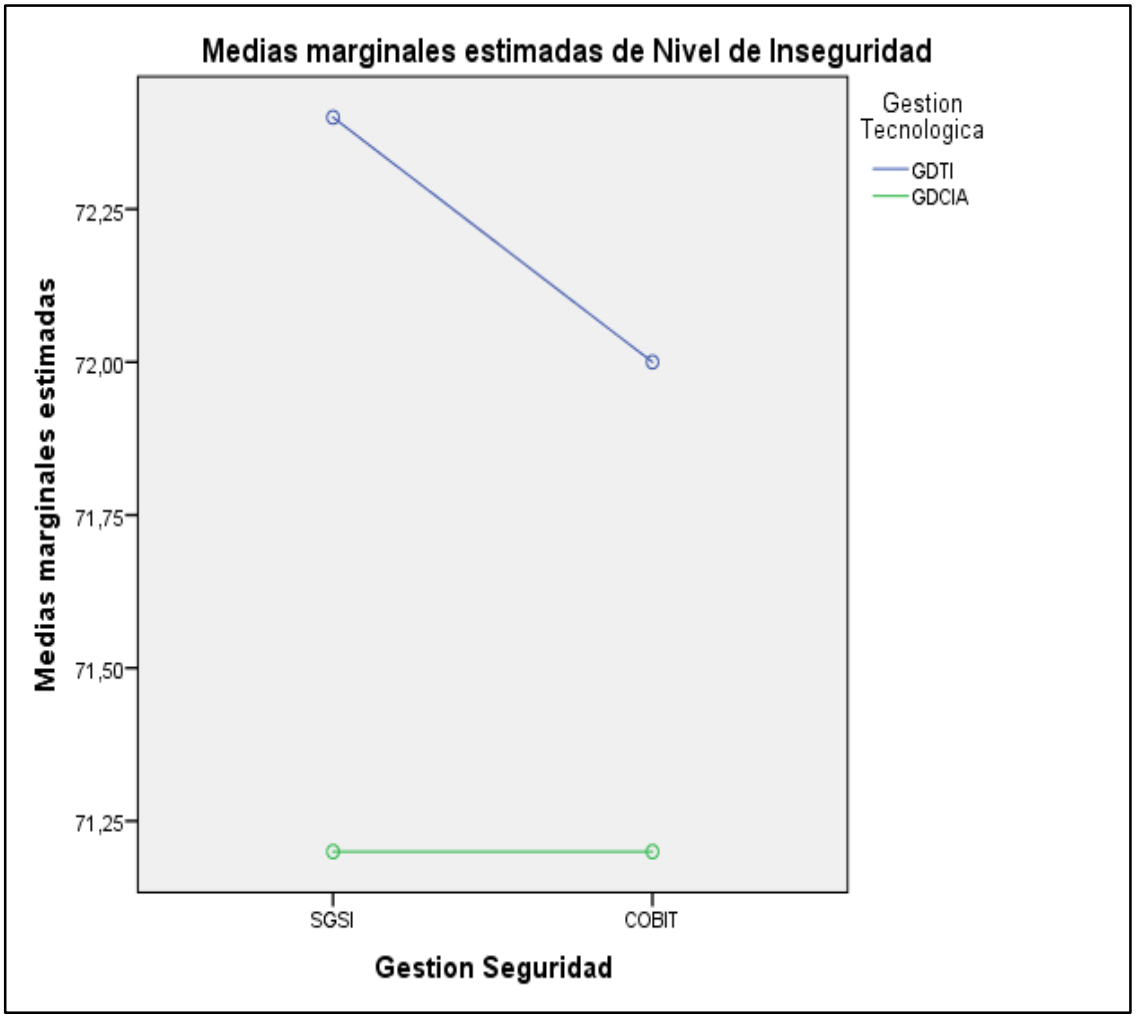

Figura 5. Medidas marginales estimadas de nivel de inseguridad

La siguiente grafica muestra y confirma los resultados obtenidos en la prueba de hipótesis multifactorial univariante. Es de importancia indicar que las variaciones obtenidas en los descriptivos y mostrado en la gráfica corresponden meramente solo a variaciones aleatorias en las variables (factores fijos).

Por tanto confirmamos la conclusión: Se evidencia la falsa percepción de Seguridad, es decir no existe diferencia entre las combinaciones de tratamientos (grupos) por tanto la Inseguridad es Permanente en cada Tratamiento (grupo) después de aplicado los factores fijos en el nivel de Inseguridad.

En referencia al primer objetivo específico se tiene:

Evidencia de inseguridad a través de la reutilización de funciones api y funciones exportable del kernel del sistema operativo

El Sistema Operativo Windows tiene estructurado sus componentes, estos le permiten interactuar internamente en el sistema(los componentes físicos con los componentes lógicos). Como parte de ello podemos hacer mención al caso de identificar componentes de almacenamiento interno y externo (identificación de hardware conectado al equipo). El Sistema Operativo cuenta con funciones exportables tales como *CopyFile, OpenFile, ReadFile, CloseFile, Arrived_Device, Remove_Device*, entre otros. Cada función es reutilizada por los programas informáticos para cumplir con sus propósitos, tal es el caso de los programas para el procesamiento de texto. Sin embargo en este escenario es casi imperceptible el nivel de inseguridad alcanzado debido a que solo se reutilizaron funciones de apertura, escritura y lectura de datos. Sin embargo si exportamos las funciones de *DBT_DEVICEARRIVAL, WM_DEVICECHANGE, DBT_DEVICEREMOVECOMPLETE, GetDriveType, GetLogicalDrives* y *DBT_DEVTYP_VOLUME* del *KERNEL* en una aplicación especializada personalizada. Es posible poner al usuario final como víctima de sustracción de información. A través de la implementación de la aplicación Denominada ***SustracFile*** Podemos demostrar que comentado anteriormente si es posible de efectuar. Describimos lo indicado a través de la secuencia de los siguientes cuadros (modelos teóricos).

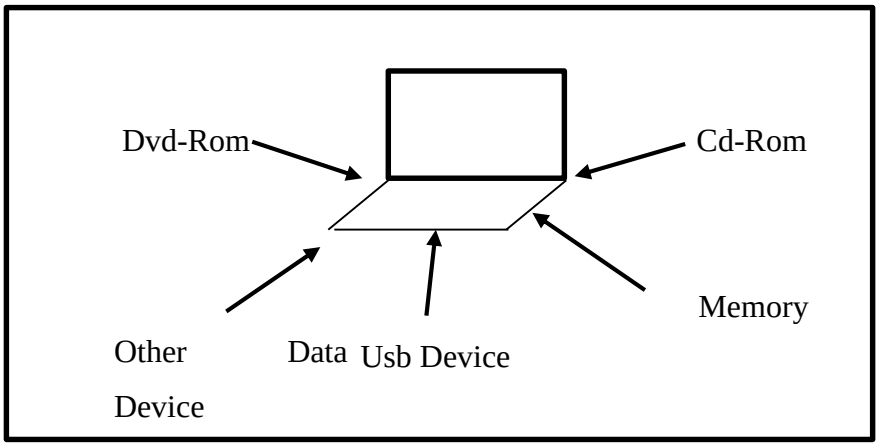

*Figura 6***.** Reconocimiento de Hardware.

PROCESO DE SUSTRACCIÓN DE DATOS

- Una vez reconocido el dispositivo físico, inmediatamente se realiza la sustracción de información almacenada en dicho componente físico a un directorio especificado por el desarrollador del programa sustractor.
- El proceso de sustracción (copia de información) no muestra ningún indicador de progreso de copia, tal como muestra el S.O.

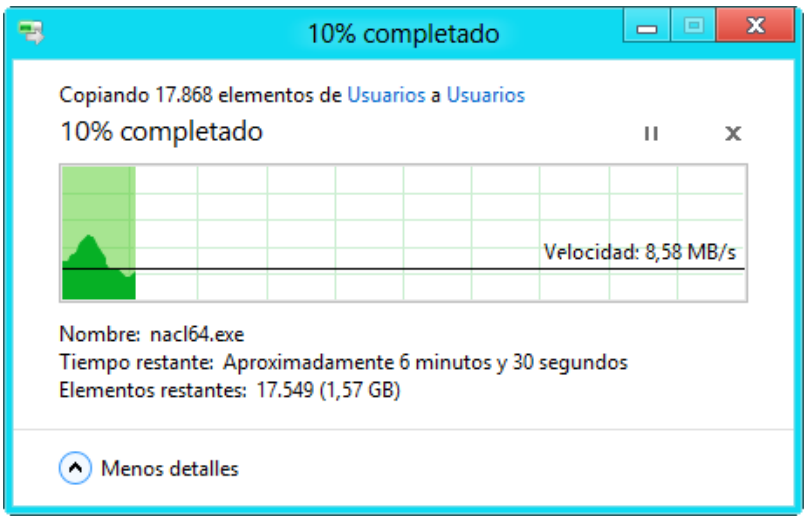

*Figura 7***.** Indicador de Avance

- Culminado el proceso de sustracción el programa sustractor no deja señal, indicio ni bitácora el dispositivo de almacenamiento. Completándose así la sustracción de información sin el consentimiento del usuario final.
- Referente a que si este programa sustractor de datos es detectado por los programas antivirus como un programa malicioso o peligroso podemos indicar que primero tendría que ser identificado como tal, en segundo lugar es importante indicar que la detección de programas víricos por parte de los antivirus depende mucho de los métodos heurísticos implementados en ellos, técnicas de cifrado, detección de rutinas maliciosas en función al banco de datos incremental con patrones de los programas maliciosos identificados.

Figura 8. Visualización de conexión del ordenador con el dispositivo usb

Figura 9. Componente físico BRAIN(H) materia de sustracción de datos

Datos sustraídos en directorio destino

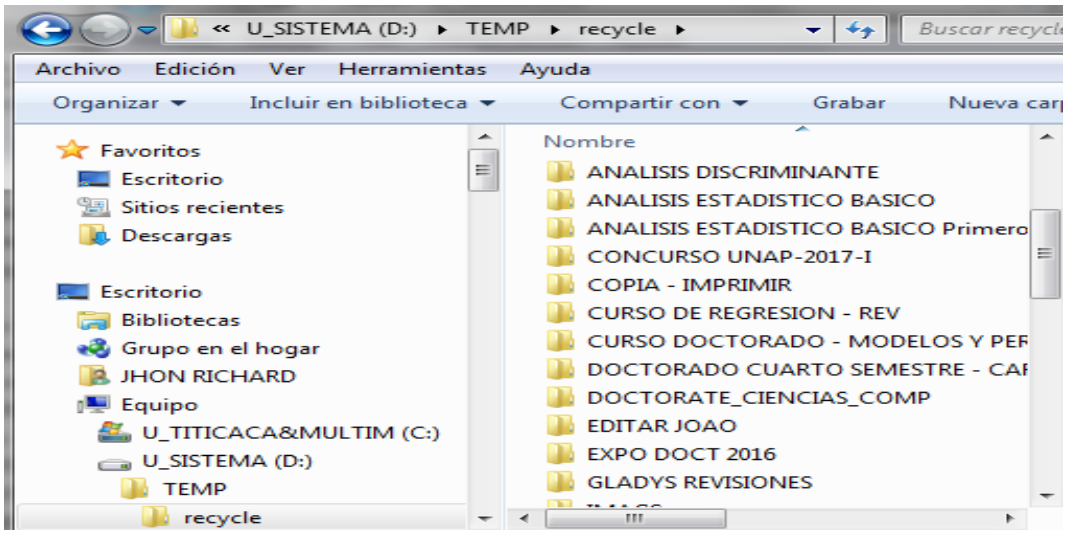

Figura 10. Datos sustraídos a la carpeta d:\temp\recycle

La presente es solo una ilustración de implementación con propósitos académicos donde evidenciamos que el reutilizar algunas las funciones exportables del mismo Sistema Operativo lo pone en contra de sí mismo. Con el cual vulneramos la confidencialidad, disponibilidad de la información administrada por los usuarios debido a que el programa sustractor detecta cualquier unidad extraíble de datos ya sean memoria *stick* de cámaras digitales, dispositivos usb, discos compactos cd rom y dvds.

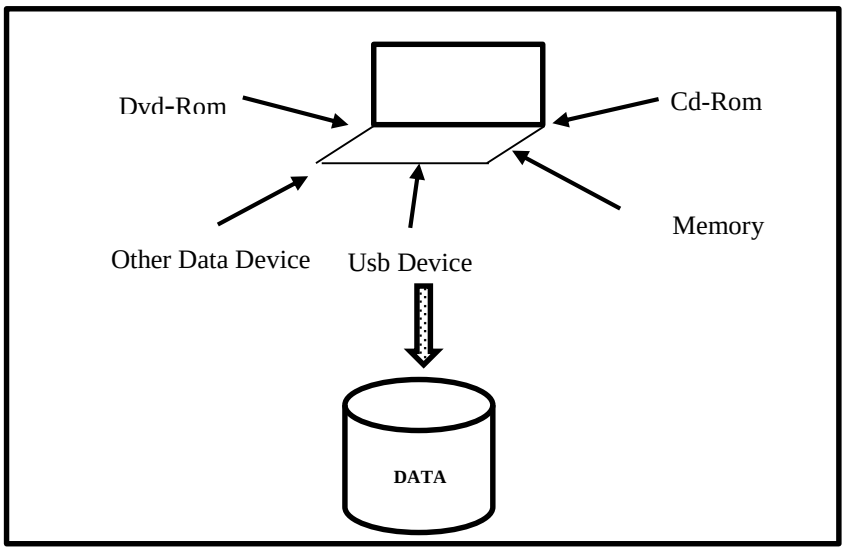

Figura 11. Proceso de sustracción de información

En referencia al Segundo objetivo específico se tiene:

En función a los resultados obtenidos en el análisis multifactorial univariante, tomamos la tabla 8, que corresponde al cuadro comparativo de los descriptivos.

Tabla 8

*Gestión Seguridad * Gestión Tecnológica, comparaciones post-hoc.*

Gestión Seguridad	Gestión Tecnológica	Media	Error estándar	Intervalo de confianza al 95%	
				Límite inferior	Límite superior
SGSI	GDTI	72,400	,936	70,501	74,299
	GDCIA	71,200	,936	69,301	73,099
COBIT	GDTI	72,000	,936	70,101	73,899
	GDCIA	71,200	,936	69,301	73,099

Donde podemos evidenciar el grado de inseguridad de los 04 grupos. En el siguiente cuadro se presenta el resumen:

Tabla 9

Grado de Inseguridad

GRUPO 1		**Media**	**Nivel de Inseguridad**	**Nivel de Seguridad**	**Total**
SGSI	GDTI	72,400	72,4%	27.6%	100%
GRUPO 2		**Media**	**Nivel de Inseguridad**	**Nivel de Seguridad**	**Total**
SGSI	GDCIA	71,200	71,2%	28,8%	100%
GRUPO 3		**Media**	**Nivel de Inseguridad**	**Nivel de Seguridad**	**Total**
COBIT	GDTI	72,00	72%	28%	100%
GRUPO 4		**Media**	**Nivel de Inseguridad**	**Nivel de Seguridad**	**Total**
COBIT	GDCIA	71,20	71,2%	28.8%	100%

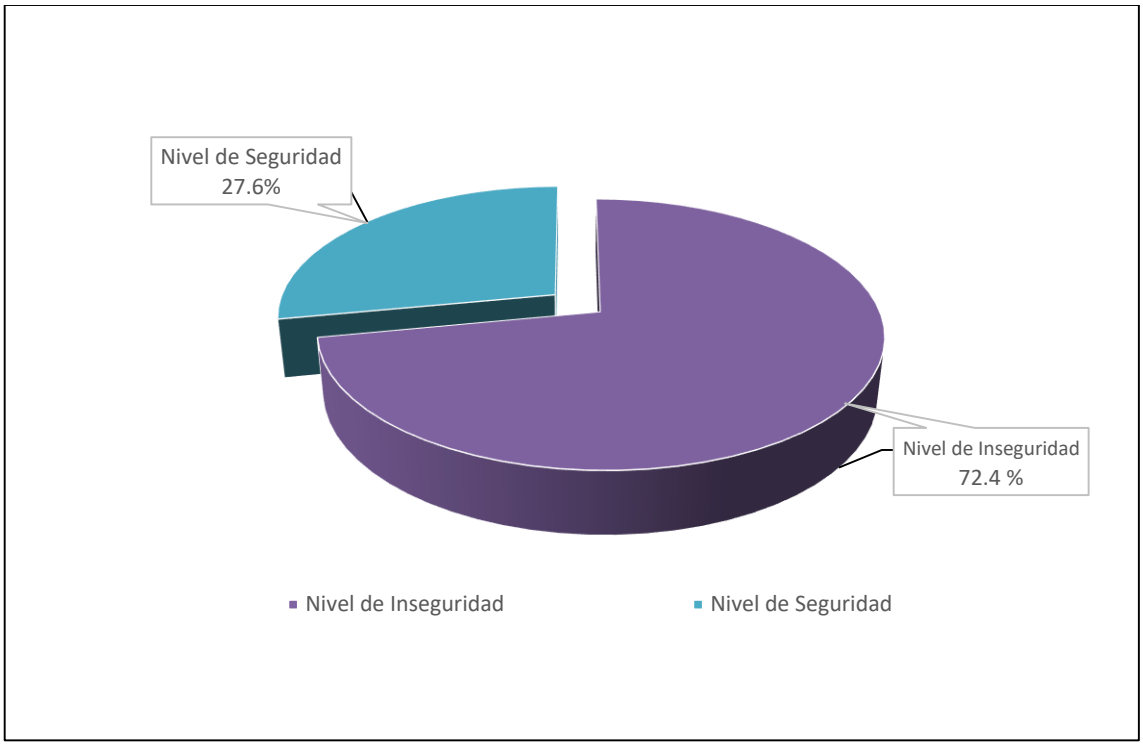

Figura 12. Nivel de Inseguridad de Grupo1 (SGSI y GDTI)

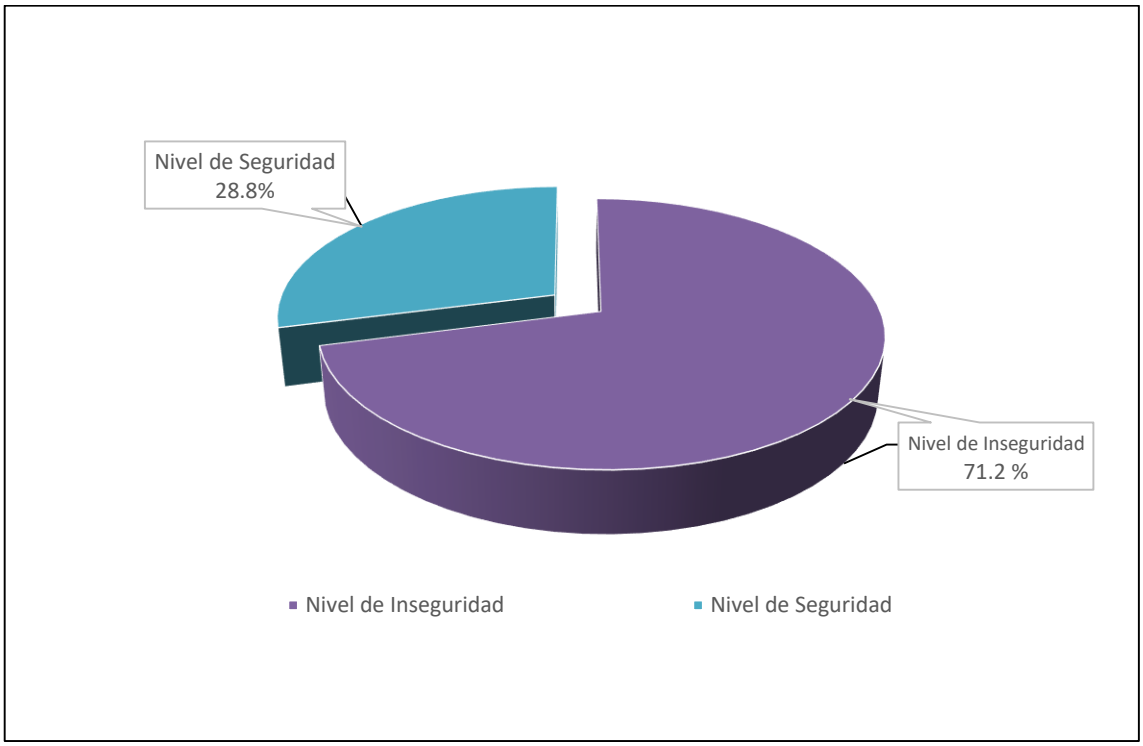

Figura 13. Nivel de Inseguridad de Grupo2 (SGSI y DGCIA)

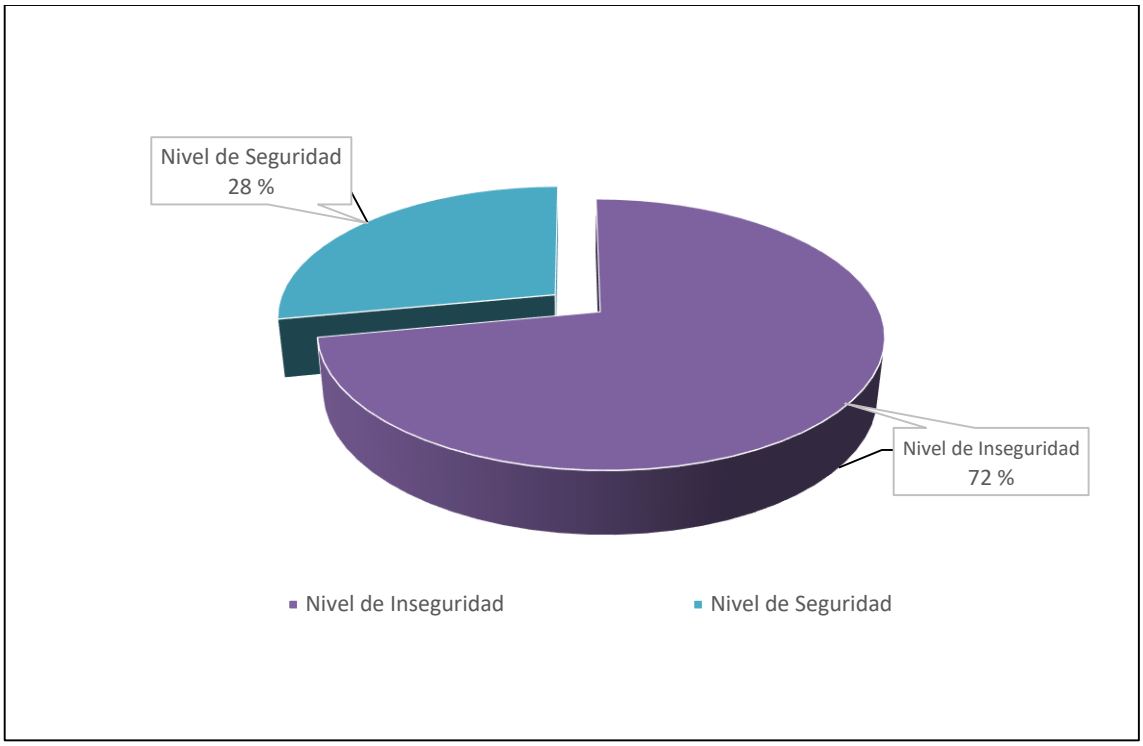

*Figura 14***.** Nivel de Inseguridad de Grupo3 (COBIT y GDTI)

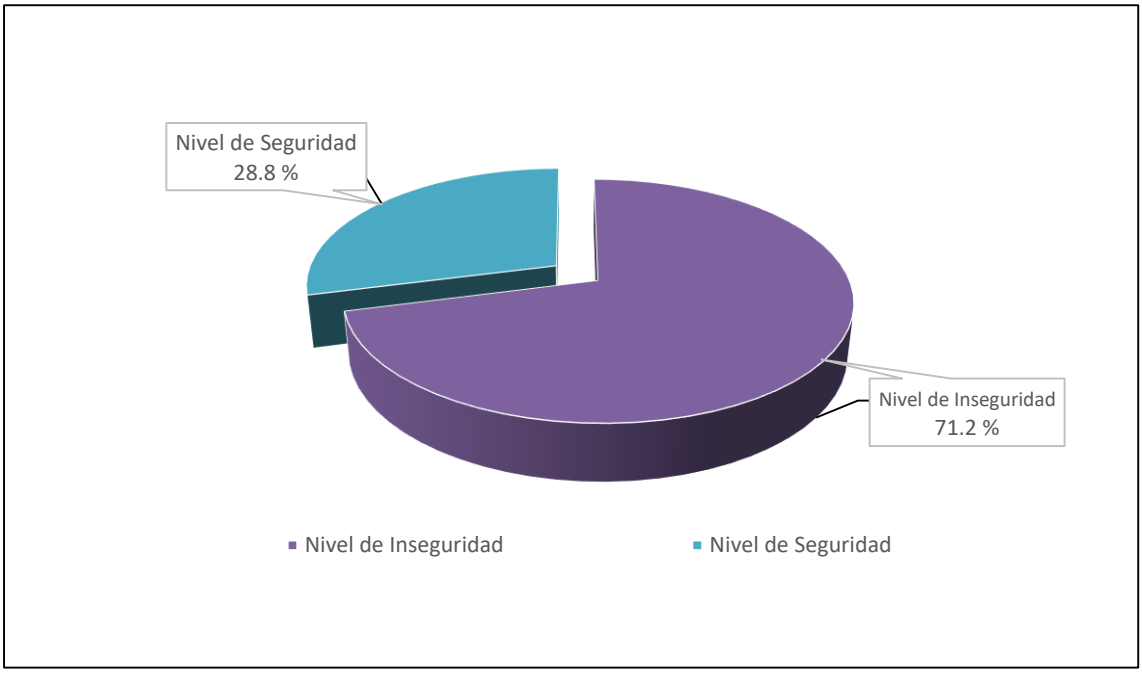

Figura 15. Nivel de Inseguridad de Grupo4 (COBIT y GDCIA)

En función a los resultados obtenidos determinamos el grado Real se Seguridad encontrado en las pymes Muestreadas = **28,3%.**

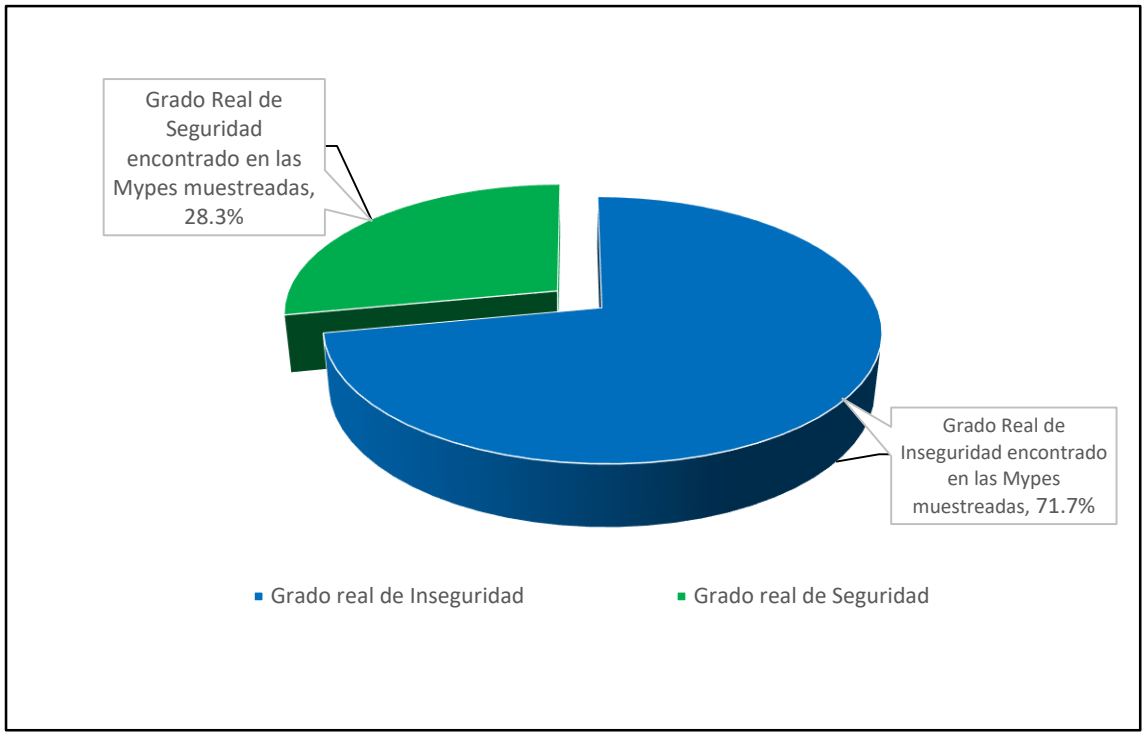

Figura 16. Grado de Seguridad encontrado en las Mypes

En muchos trabajos de investigación se identifica la inseguridad informática, esto debido a incredulidad y falsa percepción de seguridad de los usuarios.

Con respecto a las contraseñas solo el 4,5% de los usuarios muestreados establecen contraseñas complejas. El 33% del grupo de estudio declara no proteger el acceso a su ordenador, un 16% reconoce no preocuparse por vulnerabilidades de seguridad, un 45% sube habitualmente información personal de viajes, fotos, fiestas y composiciones propias, casi dos terceras partes (61%) de los usuarios coinciden en que se dan de alta sin leer las condiciones de registro aceptándolas al asumir que son estándar (Ramón, 2015).

Así mismo se derivó como conclusión que es factible hacer uso de la técnica de "Acción Retardarte" como propuesta para diseñar una estrategia de seguridad informática y seguir su metodología (Alejandro, 2011) ; por otro lado la automatización de los procesos con la implementación de una herramienta tecnológica íntegra que sea conector entre los modelos trabajados, y que permita la alineación con otros procesos. En definitiva, es la implementación de un sistema GRC (*Governance Risk* and *Compliance* – Gobierno, Riesgos y Cumplimiento de TI). Además según indica:

teniendo en cuenta los riesgos identificados de la herramienta SIEM, se debe definir un modelo de estimación cuantitativo para la valoración de los riesgos(Yesid, 2015).

Es importante resaltar que si no se cuenta con el apoyo de la alta gerencia de la institución no se contara con el soporte necesario para lograr los objetivos del SGSI. Así mismo, si el personal de la organización no sigue las políticas y lineamientos propuestos por la alta gerencia siguiendo dicho SGSI / EGSI, no se obtendrá el nivel adecuado de seguridad en los flujos de información de los distintos procesos de la Espe extensión Latacunga (Aguirre & Martinez, 2015).

Los argumentos antes señalados corroboran el propósito del presente trabajo de investigación: evidenciar la ausencia de la Seguridad Informática.

CONCLUSIONES

- No es suficiente tener muchas implementaciones de mecanismos de seguridad, si estas no van asistidas y acompañadas de políticas, protocolos y procedimientos que contribuyan en consolidar mecanismos de defensa en favor de la Seguridad de la información.
- Se implementó el código fuente para el software ***SustracFile,*** haciendo uso de las funciones exportables del Sistema Operativo Windows, con lo cual se evidenció también parte de la falsa percepción de Seguridad en los Sistemas de Información que usan las Mypes muestreadas. Conclusión a la que se llegó debido a que dio a conocer que se puede sustraer información de componentes extraíbles de distintos usuarios haciendo uso de algoritmos que reutilizan funciones del Sistema operativo aplicación que puede sustraer información de distintos tipos de dispositivos extraíbles (*hardware*) así como *usbs*, *Memorias Sticks, Cd-Roms* entre otras.
- Se aplicó métodos estadísticos determinar el tamaño muestral asociado al estudio, se hizo uso de la Prueba: Diseño Factorial Completamente al Azar con lo cual se evidenció que no existe diferencia entre los modelos planteados, sucede esto si estos modelos no son asistidos permanente e incisivamente desde el inicio hasta el final de aplicación del tratamiento tecnológico.
- Si bien se ha tratado de desarrollar e investigar en profundidad puntos estratégicos de este trabajo, se debe destacar que dentro del mismo existen elementos que han aportado significativamente en conceptos y líneas de pensamiento a la comunidad de la Seguridad Informática, teniendo como actor responsable y principal al hombre en el campo de las ciencias del comportamiento y su interacción con las Tecnologías de información (TI). Según los resultados expuestos se requiere cambiar el paradigma

de la Seguridad de la Información a una más tecnológica basado en la Inteligencia Artificial (IA) aplicado a comportamiento humano y su interacción con los ordenadores, debido a que con la IA cuando a una maquina se le da nueva información esta aprende, ajusta sus respuestas y comportamiento, lo que la hace más precisa y eficiente. Con lo cual se permitirá disminuir significativamente la inseguridad en los sistemas de información porque la IA creará nuevas realidades informáticas que permitirán predecir las intrusiones antes de que ocurran.

RECOMENDACIONES

Al margen de todo lo concluido anteriormente se sugiere las siguientes recomendaciones:

- Para garantizar la reducción de la inseguridad y optimizar la eficiencia en la seguridad de los Sistemas de Información de las Mypes se recomienda proponer modelos de Gestión de Sistemas de Información y Tecnologías de Información con un plan simultaneo para el uso, desarrollo, implementación y aplicación adecuada en las Mypes muestreadas.
- Promover en la comunicad de investigadores el desarrollo de nuevos modelos de gestión y administración de Sistemas de Información siendo estos más específicos y especializados considerando en contexto de su aplicación y naturaleza empresarial. La aplicación cíclica asistida de los nuevos modelos documentales contribuirá en la inseguridad de la información.
- se recomienda incidir incisivamente las investigaciones en la Seguridad e inseguridad de la Información Digital, puesto que en plena era del conocimiento y con los cambios tecnológicos se requerirán especialistas que afronten la problemática del hacking así como sus derivados: ataques cibernéticos, interceptación de datos, colapso de servidores, acceso a cuentas bancarias, sustracción de información de tarjetas magnéticas bancarias, clonación de cuentas en redes sociales, sustracción, negociación y difusión de información restringida personal y gubernamental. Que de ser expuesto y evidenciado lo comentado le restaría credibilidad y confidencialidad al orden económico-social.

BIBLIOGRAFIA

Aguirre Martinez, C., Fabian, & Castellanos Campoverde, Y. P. (2015). *Plan de Seguridad Informatica para la espe Sede Latacumga*. Universidad de las Fuerzas armadas de Ecuador.

Alejandro, E. C. (2011). *Estrategia de seguridad informática por capas , aplicando el concepto de Operación Militar por acción retardante*.(Tesis de Doctorado). Universidad Nacional de educación a Distancia. España.

Alvarez Basaldúa, L. D. (2005). *Seguridad en Informática(Auditoría de Sistemas).* Universidad Iberoamericana. Retrieved from http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Congreso de la República del Perú. Ley Nº 30096 – Ley de delitos informáticos, Pub. L. No. Capitulo II, Articulo 2 (2013). Perú: Congreso de La Republica del Perú. Retrieved from http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf

Eac. (2018). Gestión de Tecnologías de Información. España: Asociación Española para la calidad.

George, & Mallery. (2012). Spss for Windows step by step: A Simple Guide and Reference. 11.0. *Revista De Educacion*, *2*(359), 260–273. https://doi.org/10.4438/1988-592X-RE-2011-359-094

Giraldo Parra, Á. M. (2014). *ISO 27001 Para Pymes*. Universidad Internacional de La Rioja.

Guzmán Pacheco, G. F. (2015). *Metodología para la Seguridad de Tecnologías de*

Información y Comunicaciones en la Clínica Ortega. Universidad Nacional del Centro del Perú.

Hernández, S. R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación*. (S. A. McGRAW-HILL / Interamericana Editores, Ed.), *Journal of Chemical Information and Modeling* (Sexta Edic, Vol. 53). Mexico. https://doi.org/10.1017/CBO9781107415324.004

ISO/IEC 13335-1. (2004). *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management* (Vol. 2004). Geneva, Switzerland. Retrieved from www.iso.org

ISO/IEC 17799. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Control*. Geneva, Switzerland. Retrieved from www.iso.org

ISO/IEC 27001. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestion de seguridad de la información - Requerimientos* (Vol. 2005). Geneva, Switzerland. Retrieved from www.iso.org

ISO/IEC TR 18044. (2004). *Information technology — Security techniques — Information security incident management*. *ISO/IEC TR 18044:2004(E)* © (Vol. 2004). Geneva, Switzerland. Retrieved from www.iso.org

ISO 27000, I. (2016). I*nformation tecnology - Security techniques - Information security management systems - Overview and vocabulary*. Vernier, Geneva, Switzerland.

ISO/IEC 13335-1, I. (2004). *Information Technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management.*

ISO/IEC 29147, I. (2014). *Information technology — Security techniques — Vulnerability disclosure*. Switzerland: ISO copyright office.

ISO/IEC 9126, I. (2005). *Estandar de calidad de Software.*

Likert, R. (1932). Método de evaluaciones sumarias, 1–5.

Macancela Macero, D. P. (2015). *Modelo de Gestión de la Seguridad Informática para Garantizar la Continuidad del Negocio en la Cacpe Pastaza*. Universidad Regional Autónoma de los Andes Uniandes.

Martinez Bencardino, C. (2012). *Estadística y Muestreo* (13th ed.). Bogotá: Ecoe ediciones Ltda.

Ministerio de Vivienda Construcción y Saneamiento. Reglamento Nacional de Edificaciones (2006). Perú. Retrieved from http://www3.vivienda.gob.pe/pnc/docs/normatividad/varios/Reglamento Nacional de Edificaciones.pdf

Montgomery, D. C. (2004). *Diseño y Análisis de experimentos*. (E. L. S.A., Ed.), *Limusa Wiley* (2nd ed.). Balderas-Mexico.

Peña, J. Á. (2012). *Cobit 5*. Illinois. Retrieved from http://www.isaca.org/chapters7/Monterrey/Events/Documents/20120305 CobiT 5.pdf

Ramón, J. D. S. (2015). *Factores críticos en la adopción de las medidas de seguridad utilizadas por los alumnos de los Centros formativos universitarios de tecnologías TIC al usar herramientas 2.0*. Tesis de Doctorado. Universitat Politecnica de Valencia.

Real Academia Española. (2018). *Intrusismo*. *2018*. Madrid, España. Retrieved from http://www.rae.es/

Riesgos, A. (2002). Risk management, (57). Retrieved from www.iso.org

Santiago, M. G. (2017). *Enterprise Security Patterns*. Universidad Rey Juan Carlos, Madrid España.

Sunat. (2017). *La Micro y Pequeña Empresa*. Lima, Perú. Retrieved from www.sunat.gob.pe

Supo, J. (2016). Análisis de la Causalidad con Diseños Experimentales, 127. Retrieved from http://dexperimentales.com/

Sabar, N. R., Yi, X., & Song, A. (2018). A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security. *Journal IEEE Access*, *6*, 10421-10431.

Salcedo, B. R. (2014). P*lan de Implementacion de Seguridad basado en la norma ISO 27001:2013.*

Sukumara, Sudarsan, Starck, J., & Vittor, T. R. (2017). Cyber security – security strategy for distribution management system and security architecture considerations. *CIRED, IET Journal*, 2653–2656

Tola Franco, D. E. (2015). *Implementación de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría y Auditoría, aplicando la Norma ISO/EIC 27001*. Escuela Superior Politécnica del Litoral.

Yesid, A. T. C. (2015). *Metodología de Gestión de Incidentes de Seguridad de la Información y Gestión de riesgos para la plataforma SIEM de una Entidad Financiera basada en la norma ISO/IEC 27035 e ISO/IEC 27005*. Universidad Nacional Abierta y a Distancia.

Voutssas, J. M. (2010). *Preservación documental digital y seguridad informática.* México D.F.: Centro Universitario de Investigaciones Bibliotecológicas de la UNAM.

Zero, G. P. (2016). V*ulnerabilidades de OS x y Windows.* Silicon Valley

ANEXOS

Anexo 1. Cuestonario

1.- Indique los tipos de incidentes en seguridad informática que ha ocurrido en la empresa la Mype (marque una o más alternativas) – ***X1****

a) Infecciones víricas

b) Sustracción de información

c) Pérdida de Información accidental

d) No sabe

d) Otro

2.- Indique quien es notificado en caso de incidentes de seguridad informática (Marque solo una alternativa) – ***X2*****

a) No ve la necesidad

b) No hay a quien reportar

c) Si piensa en implementar la asignación de un responsable

d) Se está implementando la asignación de un responsable

e) Jefe de área o de departamento u otro.

3.- Cual es el contexto donde se generan los riesgos informáticos de la Mype (Marque una o más alternativas) – ***X3****

a) Física Interna

b) Física externa

c) Lógica Interna

d) Lógica externa

e) No conoce

4.- Identifique cuales son los principales obstáculos para el desarrollo e implementación de mecanismos de seguridad Informática en la Mype que dirige. (Marque una o más alternativas) – ***X4****

a) La falta de apoyo del gobierno

b) La falta de capacitación especializada

c) Falta de Recursos Humanos y financieros

d) Desconocimiento de la Seguridad Informática

e) Otros

05.- Usted conoce ¿Que es Sistema de Gestión de Sistemas de Información (SGSI)?, **(Marque solo una alternativa)** – ***X5*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

06.- Indique si conoce el propósito del SGSI **(Marque solo una alternativa)** – ***X6*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

07.- Indique si conoce las etapas del SGSI (Plan, Do, Act, Check) **(Marque solo una alternativa)** – ***X7*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

08.- Indique si le conoce los requerimientos mínimos para trabajar con un SGSI **(Marque solo una alternativa)** – ***X8*****

a) Nada

b) Poco

b) Regular

c) Bien

d) Muy bien

09.- ¿Conoce qué es Cobit?, **(Marque solo una alternativa)** – ***X9*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

10.- Indique si conoce el propósito de Cobit **(Marque solo una alternativa)** – ***X10*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

11.- Indique si conoce el proceso de buenas prácticas del control de la información con Cobit **(Marque solo una alternativa)** – ***X11*****

a) No conozco

b) Si conozco aspectos básicos

b) Si conozco regular

c) Si conozco bien

d) Si conozco muy bien

12.- Indique si le conoce los requerimientos mínimos para trabajar con Cobit **(Marque solo una alternativa)** – ***X12*****

a) Nada

b) Poco

b) Regular

c) Bien

d) Muy bien

13.- Conoce el tema de Gestión y Dirección de tecnologías de Información **(Marque solo una alternativa)** – ***X13****

a) Si

b) No / No conoce

14.- Conoce los requerimientos para realizar la Gestión y Dirección de tecnologías de Información **(Marque solo una alternativa)** – ***X14****

a) Si

b) No / No conoce

15.- Indique usted si ve correcto el hecho de implementar tecnologías se Seguridad física –hardware (Firewalls) en la entidad que dirige. **(Marque solo una alternativa)** – ***X15*** ***

a) Si

b) No / No conoce

16.- Indique usted si ve correcto el hecho de implementar tecnologías se Seguridad lógica –Software en la entidad que dirige. **(Marque solo una alternativa)** – ***X16****

a) Si

b) No / No conoce

17.- Conoce el tema de Gestión y Dirección de construcción de infraestructura apropiada para el desarrollo de TI **(Marque solo una alternativa)** – ***X17****

a) Si

b) No / No conoce

18.- Conoce los requerimientos para realizar la Gestión y Dirección de construcción de infraestructura apropiada para el desarrollo de TI **(Marque solo una alternativa)** – ***X18****

a) Si

b) No / No conoce

19.- Indique usted si ve correcto el hecho de contemplar en sus futuras construcciones empresariales la incorporación de planos arquitectónicos especializados sobre el flujo de las redes físicas de datos **(Marque solo una alternativa)** – ***X19****

a) Si

b) No / No conoce

20.- Indique usted si ve correcto el hecho de contemplar en sus futuras construcciones la compra e inclusión de materiales adecuados para una adecuada instalación de las redes físicas de datos (cableados). **(Marque solo una alternativa)** – ***X20****

a) Si

b) No / No conoce

Donde:
* Cada alternativa marcada tiene un peso de 01(inseguridad).
** Peso de las alternativas a = 05 ; b=04; c=03 ; d=02 ; e=01 (inseguridad)
*** Peso de las alternativas a = 01 ; b = 05 (inseguridad)

Anexo 2. Registro de datos del escrutinio del cuestionario

	E.R - Mype				SGSI				COBIT				GDTI				GDIA				Nivel de
ID	X1	X2	X3	X4	x5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X16	X17	X18	X19	X20	Inseguridad
1	4	4	3	3	3	3	2	3	4	5	5	4	3	3	2	3	5	5	4	5	73
2	5	4	4	2	3	3	2	2	5	4	5	4	2	3	2	3	4	5	5	5	72
3	4	5	4	4	2	2	2	2	5	4	4	4	1	3	2	2	4	5	5	4	68
4	4	5	5	5	3	2	1	2	4	4	4	5	2	3	2	3	5	4	5	5	73
5	5	5	3	3	2	3	3	2	4	5	5	5	3	3	2	2	4	5	4	5	73
6	4	5	5	5	2	2	2	3	5	5	4	5	2	2	2	3	5	5	5	5	76
7	4	4	4	4	3	2	2	2	5	5	5	5	3	3	2	2	5	4	4	5	73
8	5	4	4	2	2	3	3	3	4	4	5	4	2	2	2	3	4	5	4	5	70
9	4	5	4	5	3	3	3	1	5	4	5	5	3	3	2	3	5	4	5	4	76
10	5	4	3	3	3	2	2	3	4	5	4	5	2	3	1	3	5	5	4	4	70
11	5	4	4	4	3	2	2	3	5	5	5	5	5	5	5	4	3	3	2	2	76
12	4	4	4	5	2	2	3	2	4	5	5	4	4	4	4	4	2	3	2	3	70
13	4	4	5	2	2	1	2	2	4	4	4	4	4	5	4	4	3	2	2	3	65
14	5	4	4	3	3	3	3	1	5	5	4	5	5	5	4	4	1	2	1	3	70
15	5	5	3	5	2	2	2	3	4	4	5	5	4	5	5	4	3	3	3	2	74
16	4	4	4	4	2	2	3	2	5	5	5	5	5	5	4	5	2	2	2	2	72
17	4	4	5	2	3	3	2	3	5	4	5	5	5	4	4	5	3	2	2	1	71
18	5	4	4	4	3	3	3	2	5	5	4	4	4	5	4	5	3	3	3	2	75
19	4	5	4	3	1	2	3	1	4	5	4	5	5	4	4	5	1	3	3	1	67
20	5	4	5	4	2	3	3	3	4	4	5	4	5	5	4	4	1	2	3	2	72
21	4	4	3	2	5	5	4	4	3	3	2	2	3	2	3	3	5	4	5	4	70
22	5	5	4	4	5	4	5	5	3	2	3	3	3	3	2	2	4	4	4	4	74
23	4	4	5	4	4	5	5	4	2	3	3	2	2	2	2	3	5	4	4	5	72
24	5	4	5	5	5	5	5	5	3	3	2	3	2	2	1	2	5	4	4	5	75
25	4	5	4	3	4	5	5	5	3	2	2	3	3	3	2	3	5	4	5	5	75
26	5	4	5	4	4	4	4	4	3	2	3	2	3	2	3	3	4	5	5	4	73
27	5	4	3	2	4	5	4	4	2	2	2	2	3	3	3	2	5	5	5	5	70
28	5	4	4	3	4	5	4	4	2	1	3	2	2	2	2	2	4	5	5	5	68
29	5	5	5	5	4	4	5	5	3	3	2	3	3	2	2	1	5	4	5	4	75
30	4	5	3	2	4	5	4	4	2	2	3	2	3	3	3	2	4	4	4	5	68
31	4	4	4	3	4	4	5	4	3	2	3	3	4	4	4	4	3	2	3	3	70
32	4	4	5	4	4	4	5	4	2	3	3	3	4	4	5	5	3	3	2	2	73
33	5	5	3	3	4	4	4	1	2	2	3	3	4	4	5	4	3	2	3	2	66
34	4	4	5	5	4	4	5	4	3	2	2	2	5	5	4	5	2	2	3	3	73
35	4	4	4	2	5	4	4	5	2	3	3	2	5	5	4	5	2	3	2	3	71
36	4	5	3	5	5	5	5	5	3	2	3	3	5	5	5	5	2	3	2	2	77
37	4	5	5	4	4	4	4	5	3	2	2	3	5	4	4	4	3	2	3	3	73
38	5	5	3	2	5	4	4	4	2	2	3	2	4	4	4	5	3	2	3	3	69
39	5	4	4	3	3	2	5	5	3	2	2	3	4	5	5	4	3	2	3	3	70
40	5	4	3	2	4	3	4	5	3	2	3	3	5	4	5	5	3	3	2	2	70

Anexo 3. Librerías exportables del Sistema Operativo

Librería Advapi32.dll	
I_ScGetCurrentGroupStateW	CloseCodeAuthzLevel
A_SHAFinal	CloseEncryptedFileRaw
A_SHAInit	CloseEventLog
A_SHAUpdate	CloseServiceHandle
AbortSystemShutdownA	CloseTrace
AbortSystemShutdownW	CommandLineFromMsiDescriptor
AccessCheck	ComputeAccessTokenFromCodeAuth
AccessCheckAndAuditAlarmA	ControlService
AccessCheckAndAuditAlarmW	ControlTraceA
AccessCheckByType	ControlTraceW
AccessCheckByTypeAndAuditAlarmA	ConvertAccessToSecurityDescriptorA
AccessCheckByTypeAndAuditAlarmW	ConvertAccessToSecurityDescriptorW
AccessCheckByTypeResultList	ConvertSDToStringSDRootDomainA
AccessCheckByTypeResultListAndAuditAlarm	ConvertSDToStringSDRootDomainW
AccessCheckByTypeResultListAndAuditAlarm	ConvertSecurityDescriptorToAccessA
AccessCheckByTypeResultListAndAuditAlarm	ConvertSecurityDescriptorToAccessN
AccessCheckByTypeResultListAndAuditAlarm	ConvertSecurityDescriptorToAccessN
AddAccessAllowedAce	ConvertSecurityDescriptorToAccessW
AddAccessAllowedAceEx	ConvertSecurityDescriptorToStringSe
AddAccessAllowedObjectAce	ConvertSecurityDescriptorToStringSe
AddAccessDeniedAce	ConvertSidToStringSidA
AddAccessDeniedAceEx	ConvertSidToStringSidW
AddAccessDeniedObjectAce	ConvertStringSDToSDDomainA
Hadase	ConvertStringSDToSDDomainW

AddAuditAccessAce	ConvertStringSDToSDRootDomainA
AddAuditAccessAceEx	ConvertStringSDToSDRootDomainW
AddAuditAccessObjectAce	ConvertStringSecurityDescriptorToSe
AddUsersToEncryptedFile	ConvertStringSecurityDescriptorToSe
AdjustTokenGroups	ConvertStringSidToSidA
AdjustTokenPrivileges	ConvertStringSidToSidW
AllocateAndInitializeSid	ConvertToAutoInheritPrivateObjectSe
AllocateLocallyUniqueId	CopySid
AreAllAccessesGranted	CreateCodeAuthzLevel
AreAnyAccessesGranted	CreatePrivateObjectSecurity
BackupEventLogA	CreatePrivateObjectSecurityEx
BackupEventLogW	CreatePrivateObjectSecurityWithMulti
BuildExplicitAccessWithNameA	CreateProcessAsUserA
BuildExplicitAccessWithNameW	CreateProcessAsUserSecure
BuildImpersonateExplicitAccessWithNameA	CreateProcessAsUserW
BuildImpersonateExplicitAccessWithNameW	CreateProcessWithLogonW
BuildImpersonateTrusteeA	CreateRestrictedToken
BuildImpersonateTrusteeW	CreateServiceA
BuildSecurityDescriptorA	CreateServiceW
BuildSecurityDescriptorW	CreateTraceInstanceId
BuildTrusteeWithNameA	CreateWellKnownSid
BuildTrusteeWithNameW	CredDeleteA
BuildTrusteeWithObjectsAndNameA	CredDeleteW
BuildTrusteeWithObjectsAndNameW	CredEnumerateA
BuildTrusteeWithObjectsAndSidA	CredEnumerateW
BuildTrusteeWithObjectsAndSidW	CredFree
BuildTrusteeWithSidA	CredGetSessionTypes
BuildTrusteeWithSidW	CredGetTargetInfoA

CancelOverlappedAccess	CredGetTargetInfoW
ChangeServiceConfig2A	CredIsMarshaledCredentialA
ChangeServiceConfig2W	CredIsMarshaledCredentialW
ChangeServiceConfigA	CredMarshalCredentialA
ChangeServiceConfigW	CredMarshalCredentialW
CheckTokenMembership	CredProfileLoaded
ClearEventLogA	CredReadA

Librería Urlmon.dll

ShowTrustAlertDialog	PrivateCoInstall
URLDownloadA	QueryAssociations
URLDownloadToCacheFileA	QueryClsidAssociation
URLDownloadToCacheFileW	RegisterBindStatusCallback
URLDownloadToFileA	RegisterFormatEnumerator
URLDownloadToFileW	RegisterMediaTypeClass
URLDownloadW	RegisterMediaTypes
URLOpenBlockingStreamA	RegisterWebPlatformPermanentSecurityManager
URLOpenBlockingStreamW	ReleaseBindInfo
URLOpenPullStreamA	RevokeBindStatusCallback
URLOpenPullStreamW	RevokeFormatEnumerator
URLOpenStreamA	SetAccessForIEAppContainer
UrlMkBuildVersion	SetSoftwareUpdateAdvertisementState
UrlMkGetSessionOption	ShouldDisplayPunycodeForUri

Librería Kernel32.dll	
AddVectoredExceptionHandler	ConvertFiberToThread
AllocConsole	ConvertThreadToFiber
AllocateUserPhysicalPages	CopyFileA
AreFileApisANSI	CopyFileExA
AssignProcessToJobObject	CopyFileExW
AttachConsole	CopyFileW
BackupRead	CopyLZFile
BackupSeek	CreateActCtxA
BackupWrite	CreateActCtxW
BaseCheckAppcompatCache	CreateConsoleScreenBuffer
BaseCleanupAppcompatCache	CreateDirectoryA
BaseCleanupAppcompatCacheSupport	CreateDirectoryExA
BaseDumpAppcompatCache	CreateDirectoryExW
BaseFlushAppcompatCache	CreateDirectoryW
BaseInitAppcompatCache	CreateEventA
BaseInitAppcompatCacheSupport	CreateEventW
BaseProcessInitPostImport	CreateFiber
BaseQueryModuleData	CreateFiberEx
BaseUpdateAppcompatCache	CreateFileA
BasepCheckWinSaferRestrictions	CreateFileMappingA
Beep	CreateFileMappingW
BeginUpdateResourceA	CreateFileW

Anexo 4. Diagrama de Actividades basado en UML de la Aplicación SustractFile

```
/**********************************************************************************************************
COPYRIGHT(C) : Jhon Richard Huanca Suaquita
PROYECTO: Aplicación de sustracción de datos
ARCHIVO: SustarctFile.exe
PLATAFORMA: Windows 7 y 8.
REQUERIMIENTOS: en Windows Service pack 2 o Superior,
DESCRIPCIÓN: SustracFile.exe es una aplicación de 32 bits compatible con 64 bits, esta
             Aplicación permite sustraer información de dispositivos extraíbles sin solicitar la
             Autorización del usuario final que interactúa con el ordenador. Copia toda la
             Información del dispositivo en un directorio previamente personalizado.
Nota: La aplicación se implementó solo con propósitos académicos y demostrativos, no
buscando comercializar ni buscar beneficio alguno a través de la aplicación SustractFile.exe

**********************************************************************************************************/
```

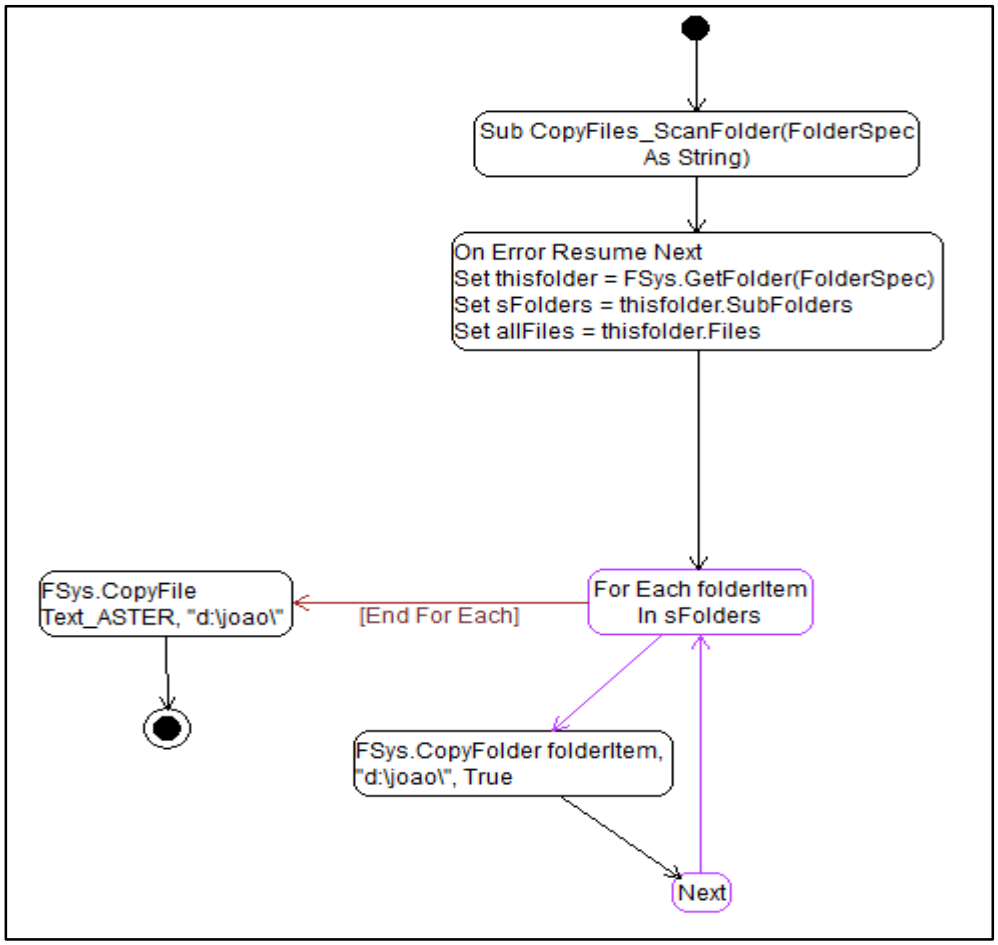

Figura 17. Diagrama de actividad de copia de datos a directorio destino

En la Figura 17 se ilustra el proceso *CopyFile_Scanfolder*, el cual toma como argumento el directorio origen de los datos a ser copiados, información que es depositada en el directorio d:\joao\, copia que realiza con remplazo, es decir si existe archivos con el mismo nombre entonces se reemplaza.

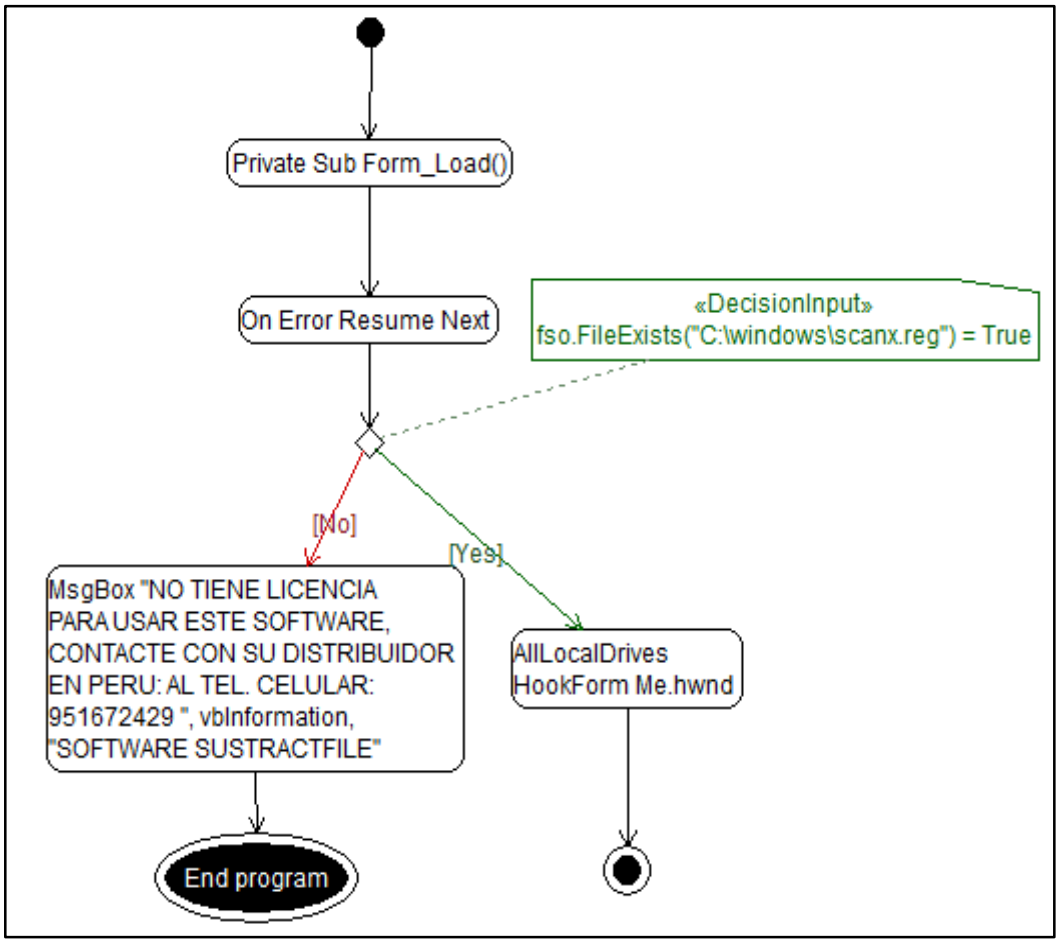

Figura 18. Diagrama de actividad verificación de llave.

En la Figura 18 se ilustra el proceso de iniciación del programa, se verifica la existencia de un archivo llave, si este no existe en el computador donde se ejecuta este programa entonces termina el programa indicando que se tiene que contactar con el administrador.

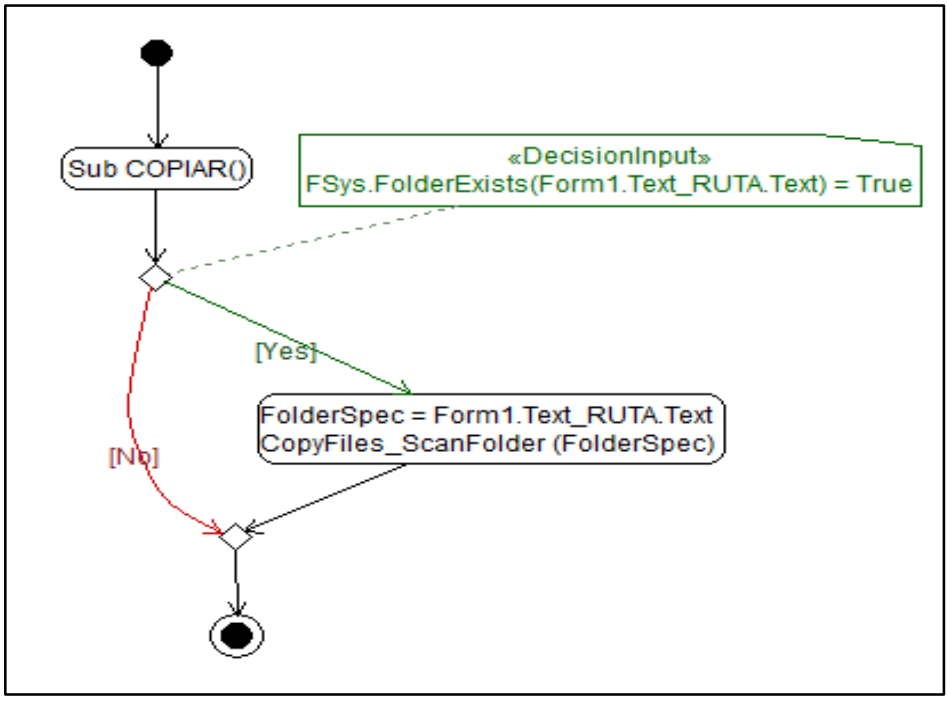

Figura 19. Diagrama de actividad de verificación de ruta de destino

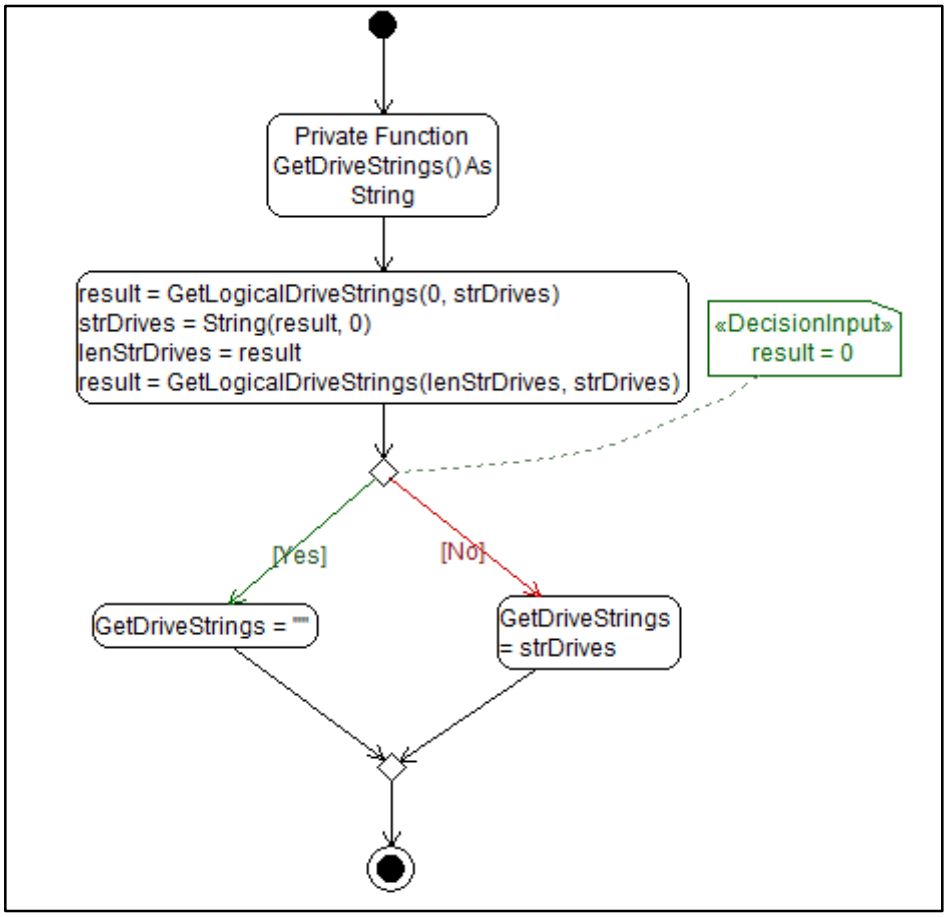

Figura 20. Diagrama de actividad que verifica todas las unidades.

En la Figura 19 se verifica si existe el directorio destino y Figura 20 la Función *GetDriveStrings* se verifica la existencia de unidades lógicas instaladas en el sistema operativo

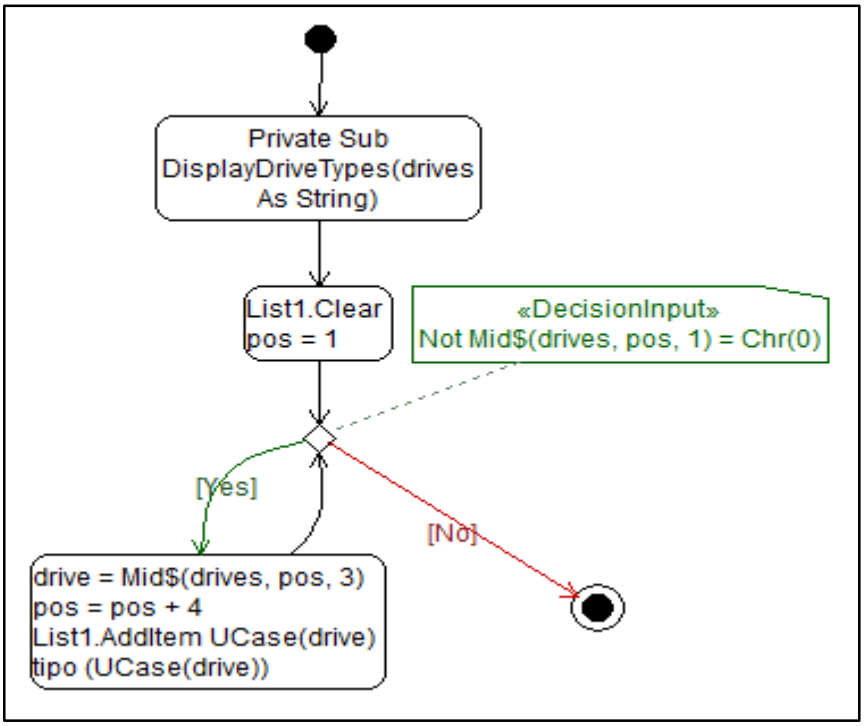

Figura 21. Proceso que genera el listado de unidades reconocidas

En la Figura 21 se ilustra el proceso de agregar en un control *List1* a las unidades detectadas, las cuales se usaran para verificar el tipo de unidad, de ser extraíble se procederá a ejecutar el bucle de copia de información al directorio destino d:\joao\, esta dirección puede ser personalizada.

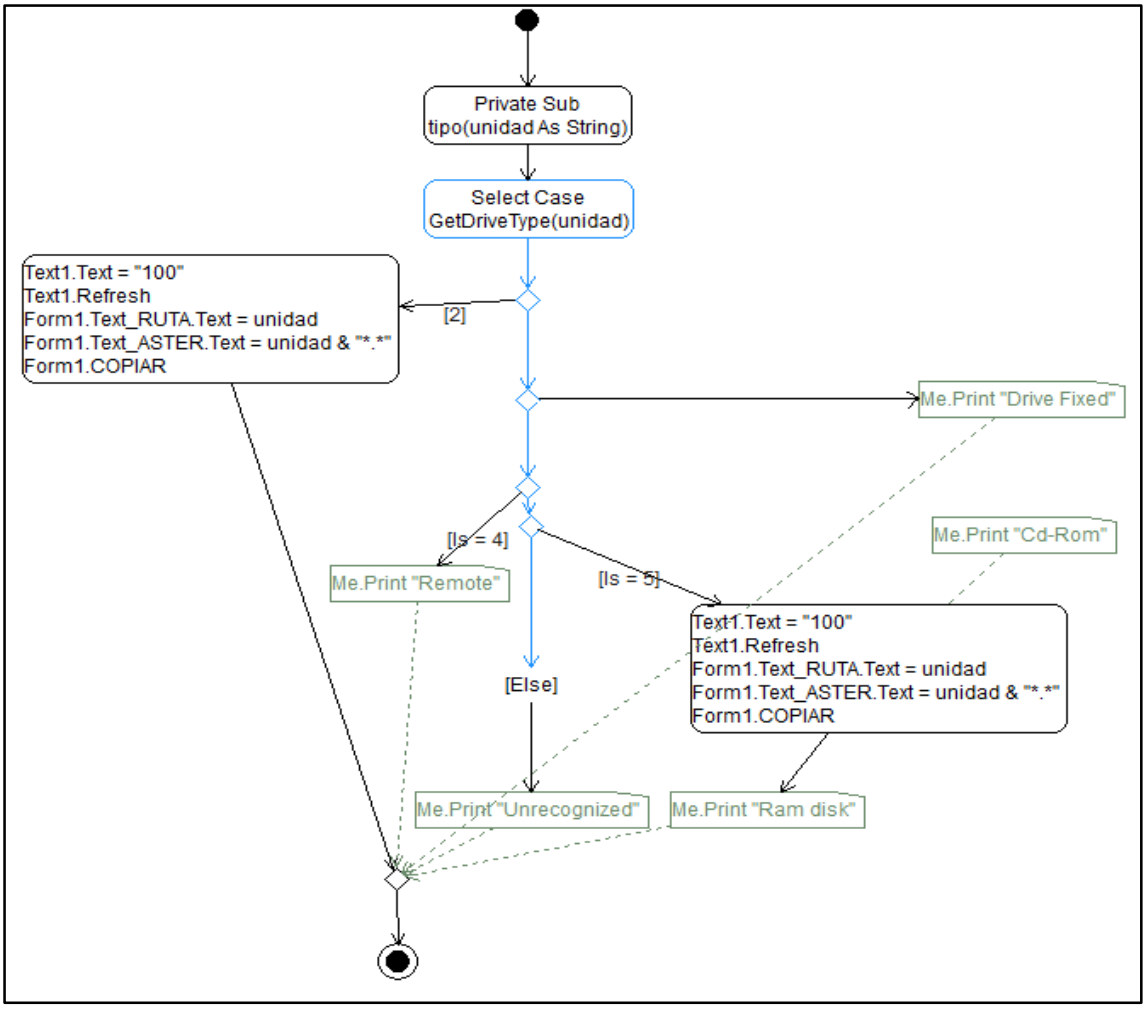

Figura 22. Diagrama de actividad del proceso de reconocer dispositivos extraíbles.

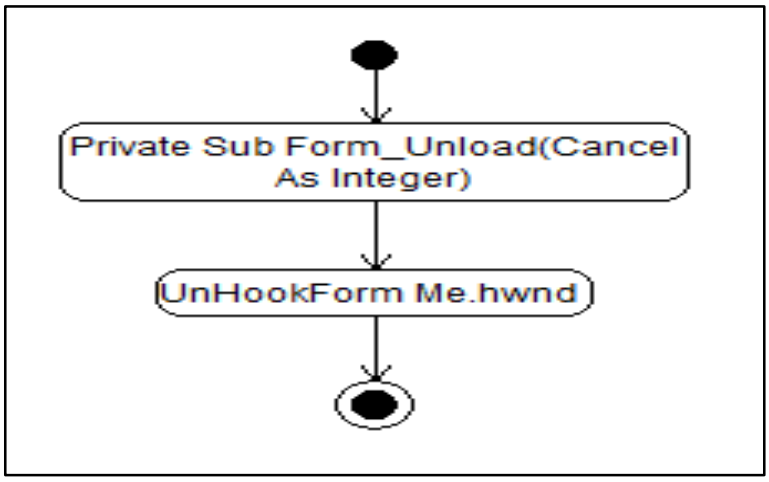

Figura 23. Diagrama de actividad del proceso de descarga del Hook

En la Figura 22 se ilustra el proceso de reconocer los dispositivos extraíbles, realizando la verificación previa del tipo de unidad, ruta de origen y destino. Por otro lado en la Figura 23 se

muestra el proceso de descarga del Hook que intercepta a la conexión de los dispositivos extraíbles.

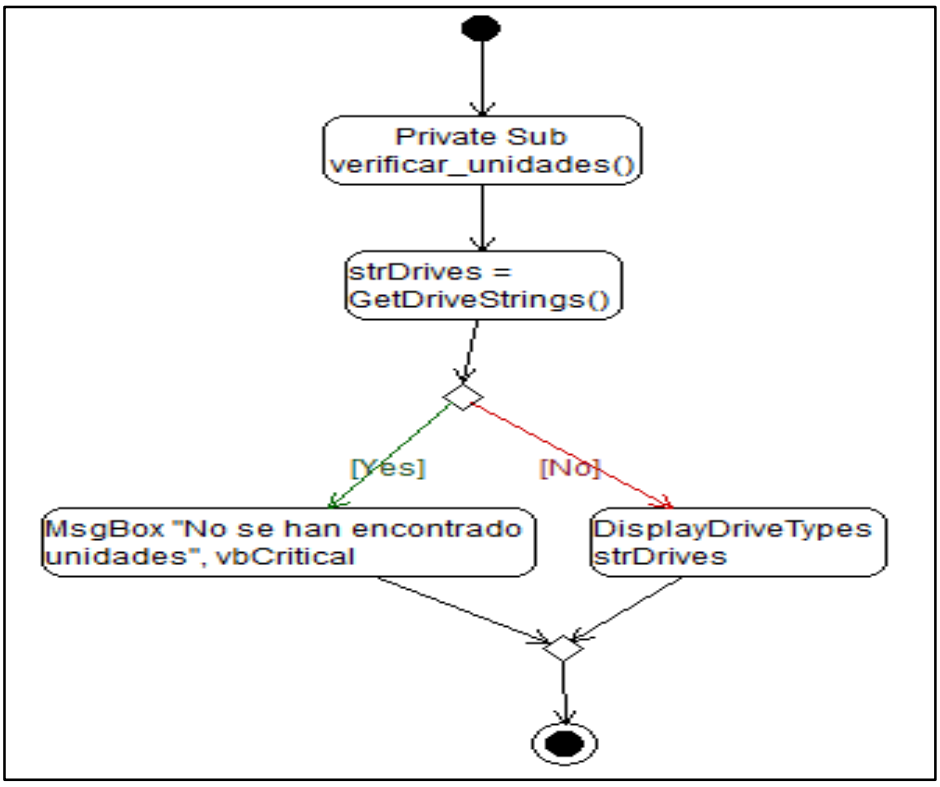

Figura 24. Diagrama de actividad que verifica las unidades conectadas

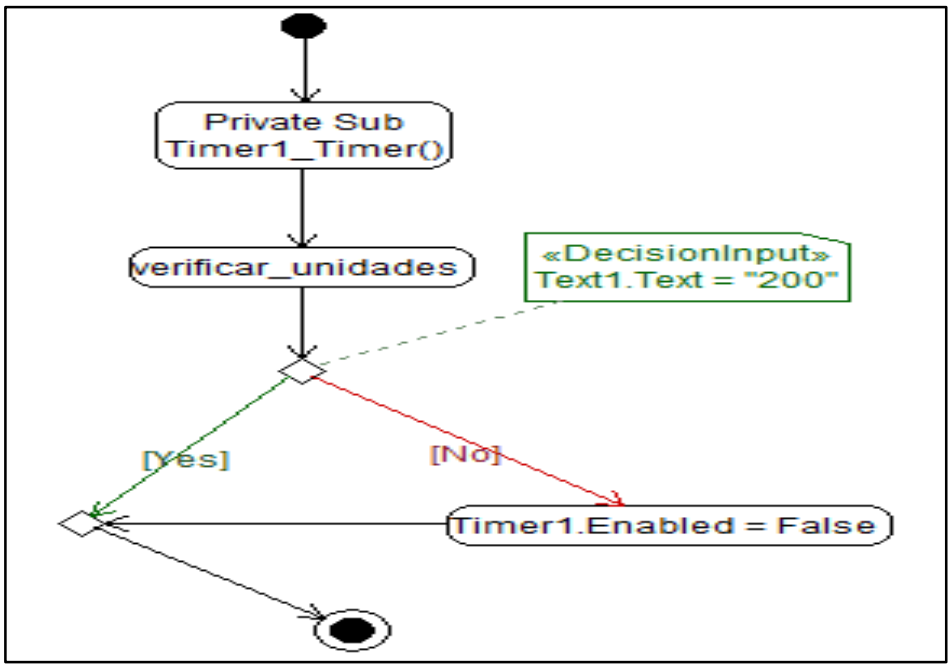

Figura 25. Diagrama de actividad del proceso actualización cada 2 segundos

En la Figura 24 se ilustra el proceso de verificación de los dispositivos extraíbles que estén conectados al computador, por otro lado, en la Figura 25 se muestra el proceso de actualización cada 02 segundos, es decir el programa busca componentes extraíbles cada 02 segundos.