República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil - UTEG

Facultad de Posgrado e Investigación

Tesis en opción al título de Magister en:

Sistemas de Información Gerencial

Tema de Tesis:

Modelo de un Sistema de Información basado en la Norma ISO/IEC 27000 para Proyectos de Ampliación de Redes GPON en las PYMES Proveedoras de Servicios de Internet del Norte de la Ciudad de Guayaquil.

Autor:

Ing. Lenin Isaac Montes Acosta

Director de Tesis:

Ing. José Townsend Valencia, Ph.D.

Diciembre 2019

Guayaquil – Ecuador

Declaración expresada

“La responsabilidad del contenido de esta Tesis de Postgrado me corresponde exclusivamente y el patrimonio intelectual de la misma a la Universidad Tecnológica Empresarial de Guayaquil.”

Ing. Lenin Isaac Montes Acosta.

Dedicatoria

Dedico este trabajo de titulación a Dios, a mí amada esposa por su constante apoyo incondicional, a mis padres por su confianza en mí y a mis hermanos.

También lo dedico a mis amigos, profesores y a mi tutor especialmente por su constante ánimo y consejos.

Agradecimiento

Agradezco a Dios por sobre todo, a mi esposa por su amor inmenso, a mis padres, a mis hermanos todos ellos son mi gran inspiración.

Agradezco a mis amigos, compañeros de tesis, a mis profesores y mi tutor por su gran aporte en realizar este trabajo de titulación y recordando la frase de Stan Lee "*La vida nunca está completamente sin sus desafíos*".

Resumen

El presente trabajo de investigación propone un Modelo de un Sistema de Información basado en la Norma ISO/IEC 27000 para proyectos de ampliación de redes GPON en las PYMES proveedoras de servicios de Internet del Norte de la ciudad de Guayaquil, para esto es necesario analizar los problemas no visibles por la falta de un modelo de seguridad de la información para encontrar controles de seguridad de la información basados en la Norma ISO/IEC 27002 y analizar las prácticas de la Seguridad de la Información existentes en las PYMES ISP para los proyectos de ampliación de la red GPON. La investigación se fundamenta en las normas de seguridad de la información, tomando características específicas de la familia de normas de la Norma ISO/IEC 27000 y las buenas prácticas de Gestión de proyectos, la metodología de la investigación es cualitativa y cuantitativa; dando como resultado un modelo con variables, dimensiones, indicadores e ítems, para ser considerados en proyectos de ampliación de redes GPON en las PYMES proveedoras de servicios de Internet. Para los datos obtenidos de los métodos cualitativos, cuantitativos, inductivos e históricos, se utilizó la herramienta SPSS para analizar estadísticamente los resultados de las encuestas y bases de datos y, por último, se realizó entrevistas a colaboradores de las PYMES proveedoras de servicios de Internet. Los resultados finales de las dimensiones, indicadores e ítems del modelo de seguridad de la información basado a los requerimientos de la Norma ISO/IEC 27000 muestran que las PYMES ISP no utilizan procedimientos o procesos dentro de sus proyectos que garanticen la disponibilidad, integridad y confidencialidad.

Palabras Claves: PYMES ISP, Proyecto, Red GPON, Normas ISO/IEC 27000.

Abstract

This research paper proposes an Information System Model based on the ISO / IEC 27000 Standard for GPON network expansion projects in SMEs Internet services provide in the North of the city of Guayaquil, for this it is necessary to analyze the problems that are not visible due to the lack of an information security model to find information security controls based on ISO / IEC 27002 and analyze the Information Security practices in ISP SMEs for projects to expand GPON network.

The research is based on information security standards, taking specific characteristics of the ISO / IEC 27000 family of standards and good Project Management practices, the research process is research is qualitative and quantitative; resulting in a model with variables, dimensions, indicators and items, to be considered in projects to expand GPON networks in SMEs that provide Internet services. For the data obtained from the qualitative, quantitative, inductive and historical methods, the SPSS tool was used to statistically analyze the results of the surveys and databases and, finally, interviews were conducted with collaborators of SMEs that Internet service provider.

The final results of the dimensions, indicators and items of the information security model based on the requirements of the ISO / IEC 27000 standard show that ISP SME companies do not use procedures or processes within their projects that guarantee availability, integrity and confidentiality.

Keywords: ISP SMEs, Project, GPON Network, ISO / IEC 27000 Standards.

Índice General

Índice de Anexos

Índice de Tablas

Índice de Figuras

Índice de Gráficos

INTRODUCCIÓN

La seguridad de la información en las pequeñas y medianas empresas proveedoras de servicio de internet (PYMES ISP) en proyectos de ampliación de red GPON (Gigabit Passive Optical Network, Res óptica pasiva Gigabit); tecnología de acceso de telecomunicaciones que utiliza cable de fibra óptica para llegar hasta el usuario final; presentan poco interés en cómo administrar la seguridad de la información y cómo implementar controles de seguridad, aunque estas empresas enfrentan las mismas amenazas y vulnerabilidades de seguridad que las grandes organizaciones de telecomunicaciones.

El conocimiento sobre la seguridad de la información en proyectos a menudo está incorporado en procedimientos y estándares de la empresa siendo una ventaja competitiva frente a otras organizaciones del mismo sector, debido a que la disponibilidad, confiabilidad e integridad de la información es de vital importancia en el día a día del negocio, ya que genera una reducción de costos de operación e impide filtración y fuga de información.

En este documento nos enfocaremos en la Norma ISO/IEC 27000 y en las buenas prácticas de Gestión de Proyectos basados en la guía del PMBOK para presentar un Modelo de un Sistema de Información para proyectos de ampliación de red GPON en las PYMES ISP del Norte de la ciudad de Guayaquil.

El presente trabajo de investigación presenta una propuesta de Modelo de un Sistema de Información basado en la Norma ISO/IEC 27000 para proyectos de ampliación de red GPON en las PYMES proveedoras de servicios de Internet del Norte de la ciudad de Guayaquil, que se requiere para impulsar el uso de una controles de seguridad en proyectos de telecomunicaciones.

El capítulo I Diseño de la Investigación, contempla los antecedentes, el planteamiento del problema, formulación y sistematización de la investigación definiendo el objetivo general y los específicos, además del marco teórico necesario para la investigación.

El capítulo II Marco metodológico, describe el tipo de diseño de la investigación, alcance, y enfoque a utilizar definiendo los métodos, unidad de análisis, población y muestra seleccionada para la recolección de información.

El capítulo III Análisis, presentación de resultados y diagnóstico, aborda el análisis de la situación actual, el análisis comparativo, evolución, tendencias de proyectos de ampliación de red GPON en las PYMES ISP y los resultados de la investigación.

CAPÍTULO I

1. DISEÑO DE LA INVESTIGACIÓN

1.1. Antecedentes de la investigación

Hace unos pocos años atrás, los proveedores de servicios de Internet solo se dedicaban a vender Internet, enfocándose en el macro entorno únicamente. Con la coexistencia de la digitalización de los procesos internos y la gran generación de información en el micro entorno los proveedores de Internet se han visto en la necesidad de resguardar la información e integrarla hacia el mejoramiento continuo de sus procesos primarios como el de aumentar su infraestructura tecnológica para brindar servicios a más suscriptores.

Las PYMES de telecomunicaciones suelen dedicar poco tiempo a cómo administrar la seguridad de la información y cómo implementar controles de seguridad, aunque enfrentan las mismas amenazas y Vulnerabilidades de seguridad que las grandes organizaciones de telecomunicaciones. (Sector & Itu, 2017)

Las vulnerabilidades han aumentado y son un riesgo en la tecnología de la información concretamente la seguridad de la información se ha convertido en la principal atención en la mayoría de las encuestas de seguridad de la información global realizada por Contador Público. (Said, 2015)

Además la carencia en la documentación de los proyectos no cumple con los principios de la seguridad de la información que son: integridad, confiabilidad y disponibilidad de la información que puede acarrear problemas al replicar los proyectos y ocasionando a su vez no tener una acción de mejora por no poder recurrir a lecciones aprendidas.

En el área de riesgo de seguridad de la información el encuestado coloca que las prioridades del negocio son: la continuidad y recuperación de desastres, riesgos cibernéticos y amenazas cibernéticas, pérdida de datos y prevención de pérdida de datos. (ISACA, 2019)

El propósito de la seguridad de la información es para proteger y preservar la confidencialidad, integridad y disponibilidad de la información. También puede implicar la protección y preservar la autenticidad y confiabilidad de la información y asegurar que las entidades puedan rendir cuentas (ISO 27000, 2013).

De una u otra manera se debe considerar que la confidencialidad, disponibilidad e integridad de la información, a través de sus controles, llevarla a cabo solo a través de una perspectiva tecnológica, tendría un enfoque incompleto, pues los estudios que se han realizado a la fecha, demuestran que es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel primordial. Así menciona un informe de Gartner en el 2014, además se informa que las empresas deben adoptar un enfoque multifacético, apalancando personas, procesos y tecnología juntas, para crear comunidades de confianza respaldadas por la supervisión y el análisis. (Schatz, Wall, & Wall, 2017)

Los factores ambientales, los activos de los procesos organizacionales y la información han hecho que las empresas implementen estándares de gestión de seguridad de tecnología de la información con el objetivo de mejorar sus servicios a sus usuarios y clientes para dar mejor apoyo y cumplimiento a sus objetivos estratégicos de organización. Y al mismo tiempo, el aumento en el uso de la tecnología tiene como ingrediente estar expuesto a un número creciente de amenazas y vulnerabilidades. Por lo tanto, tiene que ser una meta para la organización y una necesidad además que tenga un sistema de gestión de seguridad de la información eficiente. (Ali, 2014)

1.2. Problema de investigación

1.2.1. Planteamiento del problema

Las pequeñas y medianas empresas proveedoras de servicio de internet del Norte de la ciudad de Guayaquil ofrecen servicios de internet ilimitado por fibra óptica y en su mayoría cuentan con los siguientes departamentos: Gerencia, Contabilidad, Ventas, Recursos Humanos y Técnico.

Las PYMES tienen de tres a siete años en el mercado, por lo cual no cuentan con un Sistema de Seguridad de la Información que permita establecer un marco de trabajo y con controles que generen valor al cliente y a la organización. (Deloitte, 2018) Según estudio de la consultora Deloitte publicado en el 2016 “Evolución de la Gestión de Ciberriesgos y Seguridad de la Información”, se evidenció que cuatro de cada diez empresas sufrieron una brecha de seguridad entre el 2014 y 2016. Además se confirma que un 30% de estas son PYMES que no cuentan con sistemas de seguridad de la información. (Timesaver, 2018)

El departamento Técnico de las PYMES puede dividirse en tres áreas de trabajo como son: Soporte Técnico, Instalaciones y Sistemas, este departamento es administrado por el Jefe Técnico el cual tiene a cargo a un Técnico Líder que posee un equipo de trabajo formado por profesionales capacitados en el soporte técnico e instalaciones, además este departamento realiza el proceso de manejar proyectos de ampliación de la red GPON que es la inspección en campo y una breve revisión del lugar donde existan posibles clientes, este proceso se realiza sin el uso de procedimientos, estándares de proyectos y seguridad de la información, además que generalmente no se cuenta con el soporte documental necesario.

El ente regulador de Ecuador para el uso del espectro radioeléctrico y los servicios de telecomunicaciones es la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL); esta agencia realiza de forma aleatoria inspecciones a las empresas proveedoras de servicios de internet para regular y asegurar el cumplimiento de la Ley Orgánica de las Telecomunicaciones.

En la Ley Orgánica de las Telecomunicaciones (Registro Oficial Nº 439, 2015) se puede visualizar en el CAPÍTULO II Prestadores de Servicios de Telecomunicaciones Artículo 24.- Obligaciones de los prestadores de servicios de telecomunicaciones, literal 15 “Adoptar las medidas para garantizar la seguridad de las redes.” Además en el CAPÍTULO I Secreto de las comunicaciones Artículo 76 **[…]** “Medidas técnicas de seguridad e invulnerabilidad. Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión

adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes (Registro Oficial Nº 439, 2015).

Estas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. En caso de que exista un riesgo particular de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para atenuar o eliminar ese riesgo no están bajo su control, sobre las posibles soluciones." (No, Hugo, & Pozo, 2015)

Dentro de las resoluciones presentadas por ARCOTEL en la RESOLUCIÓN ARCOTEL-2018-652 señala en al artículo 12.- Confidencialidad y NO Divulgación de información como parte de las actividades de gestión de incidentes o vulnerabilidades; establece que el encargado de la seguridad debe firmar Acuerdos de Confidencialidad y no divulgarlos. (ARCOTEL, 2018).

De los párrafos descritos anteriormente se puede visualizar una serie de requisitos que deben cumplir las PYMES y problemas que estas empresas tienen debido a la estructura organizacional de las mismas, al no tener procedimientos estandarizados para el desarrollo de proyectos de red GPON; la disponibilidad de la información de forma segura y confiable se vuelve un problema futuro para solucionar con cada nueva resolución de ARCOTEL.

1.2.1.1. Síntomas

1. Falta de confidencialidad de la información en los proyectos de ampliación de red GPON; (Rec. UIT-T X.1053 (2017)
2. No disponibilidad de la información en los proyectos de ampliación de la red GPON; y, (Resolución ARCOTEL 584, 2017)
3. Falta de integridad de la información en los proyectos de ampliación de red GPON. (Registro Oficial No. 331, 2018)

1.2.1.2. Causas

1. No existen procesos formalizados y estructurados en el área técnica.

2. Bajo nivel de productividad en el desarrollo de nuevas redes GPON de la empresa; y,
3. Disminución de ventajas competitivas por no existir una integración de las actividades en el Área Técnica.

1.2.1.3. Pronóstico

1. Pérdida de la información;
2. Medidas de seguridad vulnerables;
3. Poca participación en el mercado; y,
4. No disponibilidad del servicio.

1.2.2. Formulación del problema de investigación

¿Cómo incide un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27000 en el proyecto de ampliación de red GPON en los proveedores de Internet del sector de las PYMES del norte de la ciudad de Guayaquil?

1.2.3. Sistematización del problema de investigación

1. ¿La falta de confidencialidad de la información en el proyecto de ampliación de red GPON pueden superarse aplicando la Norma ISO/IEC 2700?;
2. ¿Los proveedores de Internet de las PYMES pueden continuar sin tener disponible la información sobre el proyecto de ampliación de red GPON?; y,
3. ¿Existen procedimientos que eviten la manipulación y alteración de la información en el proyecto de ampliación de red GPON?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar un modelo de un sistema de información de seguridad de la información de basado en la Norma ISO/IEC 27001:2013 para los proyectos de ampliación de la red GPON en las PYMES ISP del norte de Guayaquil.

1.3.2. Objetivos específicos

1. Identificar un modelo de seguridad de la información basado a los requerimientos de la Norma ISO/IEC 27000 para los proyectos de ampliación de la red GPON;
2. Analizar las variables, dimensiones, e ítems prácticos de la Seguridad de la Información existentes en las PYMES ISP para los proyectos de ampliación de la red GPON; y,
3. Correlacionar controles de seguridad de la información basados en la Norma ISO/IEC 27002 para los proyectos de ampliación de la red GPON en Guayaquil.

1.4. Justificación de la investigación

1.4.1. Justificación teórica

El presente trabajo se realiza con el propósito de proponer un modelo de seguridad de la información para las PYMES ISP en el norte de Guayaquil mediante la Norma ISO/IEC 27000 buscando beneficios a las partes interesadas y para el desarrollo del negocio debido a que las PYMES proveedoras de Internet presentan varias brechas donde el capital es limitado, la infraestructura de red de fibra es insuficiente y los procesos no se encuentran optimizados o capitalizados.

Si el responsable de la seguridad de la información no promueve el uso de ésta en los proyectos de aumento de red GPON; en perentoria, causaría a la empresa riesgos de pérdida de información, manipulación de la información y no confidencialidad de la información.

Se busca con este trabajo de investigación determinar un modelo de seguridad de la información para las PYMES ISP de Guayaquil, debido a que la Alta Gerencia tiene la responsabilidad y autoridad para materializar el uso de una norma internacional Norma ISO/IEC 27000 para la seguridad de la información en su proceso de aumento de red GPON.

1.4.2. Justificación práctica

Las herramientas que brinda la Norma ISO/IEC 27000 permite gestionar la seguridad de la información en el proceso de ampliación de la red GPON en proveedores de servicios de internet, esta propuesta se enfoca en que la información debe ser confidencial, integra y estar disponible en cualquier situación de necesidad de la empresa.

Con la revolución industrial 4.0 se ha generado una transformación holística en los procesos de Tecnología de la Información, las PYMES ISP tienen la necesidad de efectuar cambios y mejoras que le permitan la operación de la empresa a largo plazo en un segmento de mercado es muy competitivo y cambiante. Muchos de ellos están enfocados en aumentar su cobertura de red GPON de ahí nace la necesidad de agregar un sistema de seguridad de la información basado en la Norma ISO/IEC 27000 para lograr con éxito sus objetivos estratégicos.

En ese perfil tecnológico se ha visto la ocasión adecuada de aprovechamiento de la Norma ISO/IEC 27000, con el fin, de trazar una hoja de ruta a las PYMES ISP, una oportunidad de aplicar un sistema de seguridad de la información para tener ventajas competitivas.

Es importante destacar los beneficios que se tiene con la implementación de un modelo de seguridad de la información para las PYMES, debido a que la inversión para aumentar la cobertura de fibra óptica es considerablemente alta para una pequeña o mediana empresa y este proceso dentro de cada ISP es fundamental.

1.5. Marco de referencia de la investigación

1.5.1. Normas ISO

Son normas definidas por la red mundial ISO (International Organization for Standardization) una organización no gubernamental independiente en 164 organismos nacionales de normalización. Las normas se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión que especifican requerimientos para garantizar que los productos y

servicios ofrecidos por organizaciones cumplen con su objetivo alcanzando la calidad deseada. (ISOTools, 2014).

Las normas ISO se pueden clasificar en 4 criterios relacionados con: la calidad; la calidad en el Medio Ambiente y Sostenibilidad; la Gestión de la Seguridad; la Calidad en la Investigación y Desarrollo.

Figura 1.1 Criterios de clasificación Normas ISO

Fuente: ISO/IEC 27000:2013
Elaborado por: Autor

Dentro del grupo de normas relacionadas a la Gestión de la seguridad encontramos la norma ISO 18000 OHSAS enfocada en el sector de seguridad y salud de los trabajadores; la Norma ISO/IEC 27000 enfocada en el sector de seguridad de la información y la Norma ISO/IEC 22000 enfocada la seguridad en el sector de la alimentación.

En este documento nos enfocaremos en la norma ISO/IEC 27000 que son una serie de normas y estándares creados por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información orientadas a empresas privadas, públicas, pequeñas y grandes.

1.5.1.1. Cuadro descriptivo familia de Norma ISO/IEC 27000

La familia de normas ISO/IEC 27000 son estándares interrelacionados que contienen una serie de componentes destinados a ayudar a las

organizaciones de todos los tipos proporcionando orientación para diversos aspectos de una implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), así como orientación sectorial específica. En este documento se trabaja con las siguientes normas ISO 27000:

Tabla 1.1 Descriptivo familia de normas ISO/IEC 27000

Enfoque	Norma	Nombre de la norma	Alcance	Propósito
Vocabulario Estándar	ISO/IEC 27000	Sistemas de gestión de seguridad de la información- Descripción general y vocabulario	a) Una visión general de la familia de normas ISMS; b) Una introducción a los sistemas de gestión de seguridad de la información; y c) Términos y definiciones utilizados en toda la familia de normas del SGSI.	Describe los fundamentos de los sistemas de gestión de seguridad de la información, que forman parte del tema de la familia de estándares SGSI y definen los términos relacionados.
Requerimientos Estándar	ISO/IEC 27001	Sistemas de gestión de seguridad de la información Requerimientos	Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de sistemas de gestión (SGSI). Especifica los requisitos para la implementación de controles de seguridad de la información personalizados para las necesidades de organizaciones individuales o partes de las mismas.	Proporciona requisitos normativos para el desarrollo y la operación de un SGSI, incluido un conjunto de controles para el control y la mitigación de los riesgos asociados con los activos de información que la organización busca proteger al operar su SGSI.
Directrices Estándar	ISO/IEC 27002	Código de práctica para controles de seguridad de la información	Proporciona una lista de los objetivos de control comúnmente aceptados y los controles de mejores prácticas que se utilizarán como guía de implementación al seleccionar e implementar controles para lograr la seguridad de la información.	Proporciona orientación sobre la implementación de controles de seguridad de la información. Proporcionan consejos de implementación específicos y orientación sobre las mejores prácticas para respaldar los controles especificados en ISO / IEC 27001.
Directrices Sector Especifico	ISO/IEC 27011	Guía de gestión de seguridad de la información para organizaciones de telecomunicaciones basada en la ISO/IEC 27002	Proporciona pautas que respaldan la implementación de controles de seguridad de la información en organizaciones de telecomunicaciones.	ISO / IEC 27011 permite a las organizaciones de telecomunicaciones cumplir con los requisitos básicos de administración de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.

Fuente: NORMA ISO/IEC 27000, 27001, 27002, 27011
Elaborado por: Autor

1.5.1.2. Beneficios de la Norma ISO/IEC 27001:2013

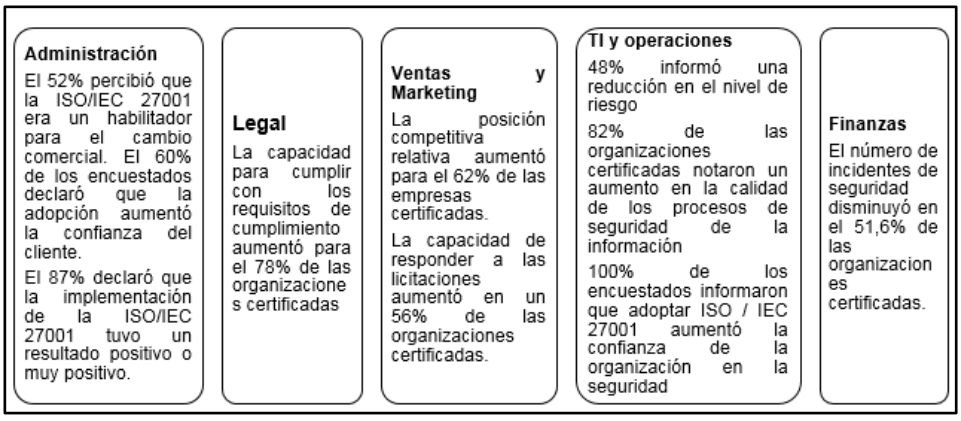
La Norma ISO/IEC 27001:2013 permite que a las organizaciones puedan gestionar la seguridad de sus activos entre esos la información sin

embargo, la Norma ISO/IEC 27001:2013 es el estándar más conocido por organizaciones y profesionales, esta norma mundial lo que hace es proporcionar requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). (Al-dhahri, 2017).

Se enlista los beneficios de la Norma ISO/IEC 27001:

1. Mayor eficiencia empresarial;
2. Riesgo operacional reducido;
3. Asegurar que la seguridad de la información sea racional aplicado;
4. Garantía a los socios comerciales y clientes a través de certificación que se utilizó como iniciativa de marketing; y,
5. Conciencia de seguridad entre los empleados y gerentes.

Figura 1.2 Beneficios de la Norma ISO/IEC 27001:2013



Fuente: Al-dhahri, 2017
Elaborado por: Autor

1.5.2. Seguridad de la información

De acuerdo la familia de Normas ISO/IEC 27000 la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas de información implicados en su tratamiento, dentro de una organización. El objetivo es que las organizaciones puedan garantizar la optimización de riesgo menor que el soportado por la organización, para preservar la confidencialidad, integridad y disponibilidad de la información (ISO 27001, 2013) La series de normas ISO/IEC 27000 contiene

las mejores prácticas para desarrollar, implementar y mantener especificaciones para los Sistemas de Seguridad de la Información.

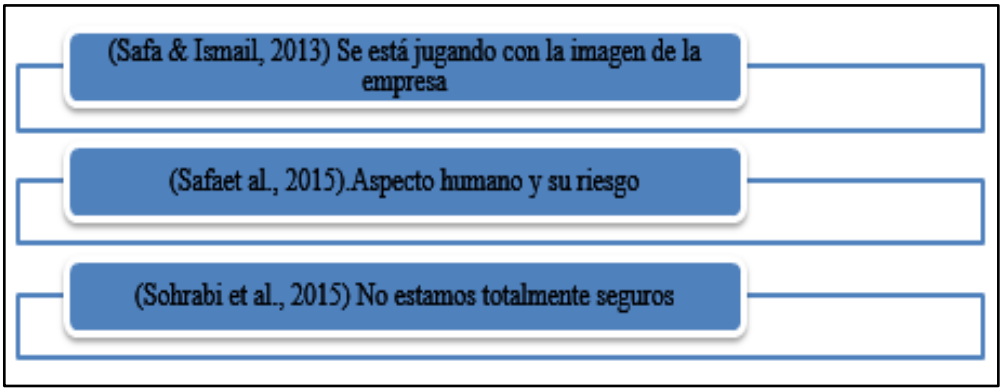
Esta norma internacional puede ser utilizada e implementada por partes internas y externas para ponderar la capacidad de la organización para poder cumplir con sus propios requisitos de seguridad de la información. (ISO 27001:2013, 2013)

El conocimiento sobre la seguridad de la información en proyectos a menudo está incorporado en procesos y rutinas. En proyectos se debe incluir: políticas, procesos y procedimientos estándares de la organización. Y a su vez estos pueden incluir: confidencialidad y acceso a la información; seguridad y protección de datos; políticas de conservación de registros; uso de información protegida por derechos de autor; destrucción de información clasificada; formato y tamaño máximo de los archivos; datos de registro y metadatos; tecnología y medios sociales autorizados. (PMBOK V.6)

1.5.2.1. Aspectos a considerar en la seguridad de la información

Algunos artículos académicos y libros refieren diferentes aspectos a considerar en relación con la seguridad de la información:

Figura 1.3 Aspectos a considerar en la seguridad de la información



Fuente: Sohrabi, Solms, Furnell, Elizabeth, & Africa, 2016
Elaborado por: Autor.

- **No estamos totalmente seguros.**

  Las nuevas tecnologías han generado mucho protagonismo en el área de seguridad para las organizaciones y a sus usuarios, pero

los ataques a la seguridad de la información siguen siendo una preocupación controvertida. Los sistemas anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall, autenticación y detección de intrusos son aristas que abordan la seguridad de la información, pero no pueden garantizar un entorno totalmente seguro para la información (Safaet al., 2015).

- **Se está jugando con la imagen de la empresa.**
  Las brechas en la seguridad de la información no solo traen como consecuencia costos adicionales para las empresas proveedoras de servicios de Internet sino que afectan de forma significativa a su reputación. (Safa & Ismail, 2013)
- **Aspecto humano y su riesgo**
  Los agentes que amenazan a la seguridad de la información de una organización se enfocan en las personas y ya no en la tecnología como tal, por ejemplo los errores de los usuarios al tomar como clave de acceso sus números de identificación, escribir sus contraseñas en un portapapeles en el escritorio de sus computadoras, compartir los usuarios y contraseñas con sus compañeros, abrir correos electrónicos de desconocidos incluso descargar software desde Internet. (Sohrabi et al., 2016)
  Estudios previos han revelado que la conciencia de seguridad de la información de los empleados desempeña un papel vital en la mitigación del riesgo asociado con su comportamiento en las organizaciones. (Asanka, Arachchilage, & Love, 2014)

1.5.3. NORMA ISO/IEC 27011:2016 Guía de gestión de seguridad de la información para organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002:2013

Esta norma internacional provee directrices de interpretación para la implementación y el manejo de seguridad de la información en las organizaciones de telecomunicaciones basadas en la Norma ISO/IEC 27002:2013 (Código de práctica para controles de la seguridad de la información).Para la aplicación de los objetivos y controles de seguridad

descritos en las Normas ISO/IEC 27002, se tomará en cuenta los siguientes dominios:

Tabla 1.2 Dominios de control de la Norma ISO/IEC 27002

ID	Dominio
5	Políticas de seguridad
6	Aspectos organizativos de la seguridad de la información
7	Seguridad ligada a los recursos humanos
8	Gestión de activos
9	Control de acceso
10	Cifrado
11	Seguridad física y ambiental
12	Seguridad de las operaciones
13	Seguridad de las telecomunicaciones
14	Adquisición, desarrollo y mantenimiento de sistemas información
15	Relaciones con los proveedores
16	Gestión e incidentes de seguridad de la información
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio
18	Cumplimiento

Fuente: NORMA ISO/IEC 27002:2013
Elaborado por: Autor

Adicional a esos controles se consideran las características de seguridad: Confidencialidad, Integridad y Disponibilidad y cualquier otra propiedad de seguridad de las telecomunicaciones con el fin de administrar el riesgo de seguridad de manera adecuada. (ISO/IEC 27002:2013, 2013)

Las organizaciones de telecomunicaciones están llamadas a prestar servicios de telecomunicaciones mediante la intermediación de las comunicaciones de otras organizaciones mediante facilidades para el uso de comunicaciones de otras. Por ello, debería tomarse en cuenta que el acceso y el uso de los servicios de procesamiento de la información dentro de la organización de telecomunicación no solamente se da por los propios empleados y contratistas, sino también por varios usuarios fuera de la organización. (ISO/IEC 27011:2016, 2016)

Para proveer servicios de telecomunicaciones, las organizaciones de telecomunicaciones necesitan interconectar o compartir sus servicios e instalaciones de telecomunicaciones, o usar los servicios e instalaciones de telecomunicaciones de otras organizaciones de telecomunicaciones. Por lo tanto, la gestión de seguridad de la información en las organizaciones de telecomunicaciones es mutuamente dependiente y pueden incluir cualquiera y

todas las áreas de la infraestructura de red, aplicaciones de servicios y otras instalaciones.

Si al menos una vez la seguridad de la información fuera violada, por ejemplo un acceso sin autorización al sistema de procesamiento de la información de una organización, la organización podría sufrir daño.

Las organizaciones y sus sistemas de información con su red se enfrentan a amenazas de seguridad de una amplia gama de fuentes, que incluyen fraude asistido por computadora, sabotaje, vandalismo, fuga de información, terremotos, incendios o inundaciones.

Estas amenazas de seguridad pueden originarse desde dentro o fuera de la organización de telecomunicaciones y causar daños a la organización.

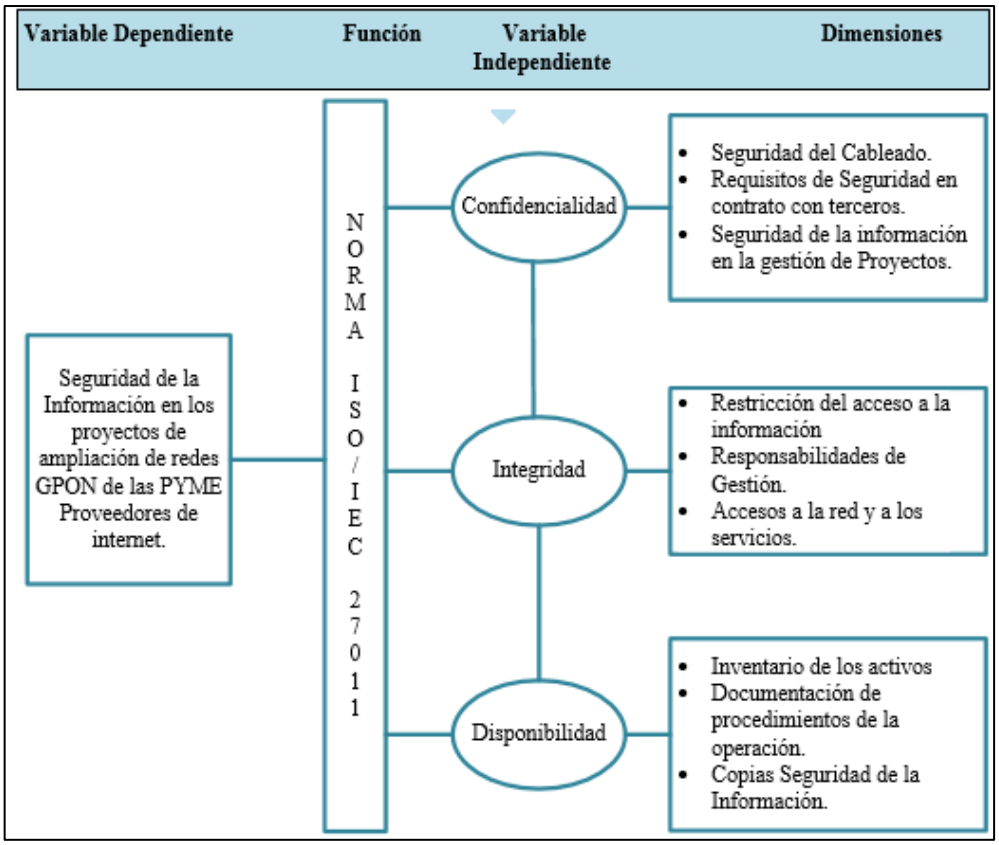
Una seguridad de la información efectiva se logra mediante la implementación de un conjunto adecuado de controles basados en los descritos en la recomendación de la Norma ISO/IEC 27002:2013. Estos controles deben establecerse, implementarse, monitorearse, revisarse y mejorarse en las instalaciones, servicios y aplicaciones de telecomunicaciones. El despliegue exitoso de los controles de seguridad permitirá cumplir mejor los objetivos de seguridad y de negocios de la organización. (Sector & Itu, 2017)

1.5.3.1. Diagrama del modelo de sistema de seguridad aplicado a la investigación

En este modelo conceptual se define una variable dependiente en función de variables independientes; por cada variable independiente se definen las dimensiones con las cuales se interactúa.

En la Figura 1.4 se presenta el modelo conceptual de seguridad de la información basado en la Norma ISO/IEC 27011:2016 junto a los controles que establece la Norma ISO/IEC 27002:2013.

Figura 1.4 Modelo de la seguridad de la información basado en la Norma ISO/IEC 27011:2016



Fuente: Datos recopilados de la investigación - Norma ISO/IEC 27011:2016
Elaborador por: Autor

1.5.3.2. Confidencialidad

Según (ISO/IEC 27011, 2016) la información relacionada con las organizaciones de telecomunicaciones debería estar protegida de divulgación no autorizada.

Esto implica la no divulgación de las comunicaciones en términos de la existencia, el contenido, la fuente, el destino, los datos y tiempos de la información comunicada.

Es fundamental que las organizaciones de telecomunicaciones aseguren que la confidencialidad de las comunicaciones que sean manejadas por ellos no se vulnere. Las personas contratadas por el organismo de telecomunicaciones deberían mantener la confidencialidad de cualquier información relacionada con otras personas, que pueda haber llegado a ser conocida, durante sus tareas de trabajo. (ISO/IEC 27011, 2016).

- **Seguridad del Cableado.-**
  El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño. (ISO/IEC 27002, 2013)
- **Gestión de la provisión de servicio por terceros.-**
  La organización debiera chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona. (ISO/IEC 27002, 2013)
- **Organización Interna.-**
  Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debiera aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización. (ISO/IEC 27002, 2013)

1.5.3.3. Integridad

La instalación y el uso de los servicios de telecomunicaciones deberían ser controlados, asegurando la autenticidad, precisión e integridad de la información transmitida, retransmitida o recibida por cable, radio o cualquier otro método (ISO/IEC 27011, 2016).

- **Restricción del acceso a la información.-**
  Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. (ISO/IEC 27002, 2013)
- **Responsabilidades de gestión.-**
  La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. (ISO/IEC 27002, 2013)

- **Acceso a las redes y a los servicios de red.-**
  Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados. (ISO/IEC 27002, 2013)

1.5.3.4. Disponibilidad

Se debería proveer acceso autorizado a la información de telecomunicaciones, a las instalaciones y a los medios usados para la provisión de los servicios de comunicaciones, solo cuando sea necesario, ya sea que estos sean provistos por cable, radio o cualquier otro método. Como una extensión de la disponibilidad, las organizaciones de telecomunicaciones deberían dar prioridad a las comunicaciones esenciales en caso de emergencia y cumplir con los requerimientos regulatorios. (ISO/IEC 27011, 2016)

- **Inventario de los activos.-**
  Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes. (ISO/IEC 27002, 2013)
- **Documentación de los procedimientos de la operación.-**
  Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten. (ISO/IEC 27002, 2013)
- **Copias de seguridad de la información.-**
  Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente, de acuerdo a la política de copias de seguridad acordada. (ISO/IEC 27002, 2013)

1.5.4. Beneficios de la implementación de Modelo de un Sistema de Información basado en la Norma ISO/IEC 27000:2018

- **Norma ISO/IEC 27001:2013 sirve para a reducir las amenazas de la seguridad de la información y los riesgos de protección de datos para su organización.-**

  Ya sea propia información valiosa de la organización o la de clientes, una seguridad de la información deficiente puede ser costosa. La implementación de la Norma ISO 27001 demuestra a las autoridades reguladoras que su organización se toma en serio la seguridad de la información que posee y, una vez identificados los riesgos, hace todo lo posible para solucionarlos.
- **Norma ISO/IEC 27001:2013 ayudará a ganar nuevos clientes y retener el negocio existente.-**

  Debido a que este es el estándar de las mejores prácticas reconocido internacionalmente, hace que las personas con las que desea trabajar se sientan seguras y protegidas y que la organización (que posee la certificación de la Norma ISO/IEC 27001:2013) cuide sus valiosos activos y la seguridad de la información.
- **Norma ISO/IEC 27001:2013 significa ahorrar tiempo y dinero.-**

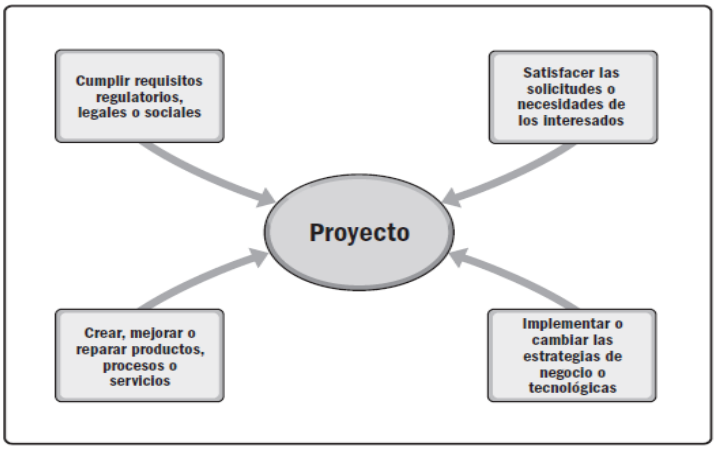
  Los clientes buscan cada vez más la seguridad de su gestión de seguridad de la información y las capacidades de protección de datos. Precautelar la información tiene como consecuencia un ahorro de recursos.
- **Norma ISO/IEC 27001:2013 aumenta su reputación y genera confianza en la organización.-**

  Con un sistema de gestión de seguridad de la información ISO/IEC 27001:2013 estará en una mejor posición para identificar los riesgos de incumplimiento y prevenirlos antes de que ocurran. Como muchas cosas en los negocios, la confianza es importante.

1.5.5. Gestión de proyectos

Los líderes de las organizaciones inician proyectos en respuesta a factores que actúan sobre sus organizaciones. Existen cuatro categorías fundamentales de estos factores, que ilustran el contexto de un proyecto:

Figura 1.5 Contexto de iniciación de proyectos



Fuente: PMBOK Sexta edición
Elaborador por: PMBOK Sexta edición, 2016.

Un proyecto de una organización es creada para realizar un trabajo específico, durante un periodo de tiempo determinado y a la cual se le entrega un conjunto de recursos con el propósito de generar transformación, cambios, crear valor y beneficios para las diferentes partes interesadas, (Adaptación a partir de Turner, 2008). El PMBOK 6d define a un proyecto como un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. Y continua indicando el PMBOK que los proyectos se llevan a cabo para cumplir objetivos mediante la producción de entregables.

Un objetivo se define como una meta hacia la cual se debe dirigir el trabajo, una posición estratégica que se quiere lograr, un fin que se desea alcanzar, un resultado a obtener, un producto a producir o un servicio a prestar. Un entregable se define como cualquier producto, resultado o capacidad única y verificable para ejecutar un servicio que se produce para completar un proceso, una fase o un proyecto. Los entregables pueden ser tangibles o intangibles.

De acuerdo con ello, los proyectos, surgen como una o más de las siguientes consideraciones estratégicas: demanda del mercado, oportunidad estratégica, necesidad comercial, solicitud de un cliente, adelantos tecnológicos, y/o requisitos legales.

1.5.5.1. Ciclo de vida de un proyecto

El ciclo de vida de un proyecto es el conjunto de fases de un proyecto; las fases son actividades del proyecto relacionadas entre sí y que tienen como entregable un producto o servicio parcial o completo, además cada fase puede ser secuencial, interactiva o superpuesta, estas son acotadas en el tiempo es decir con un inicio y fin. Dependiendo del tamaño o complejidad del proyecto se puede dividir en una o más fases y a su vez en sub-fases.

Los proyectos se pueden configurar dentro del ciclo de vida genérico: inicio del proyecto; organización y preparación; ejecución del trabajo; y finalización del proyecto.

El éxito en la ejecución, es la principal misión del director del proyecto (Too & Weaver, 2014). En este objetivo, es requerido que el líder del proyecto cuente con habilidades, destrezas, capacidades y competencias que le permitan, entre otros, maniobrar entre los requisitos y recomendaciones de las mejores prácticas, así como entre las restricciones y la incertidumbre específicas del proyecto y su entorno.

Los ciclos de vida de los proyectos pueden ser predictivos o adaptativos, además si el dentro del ciclo de vida del proyecto se tiene fases relacionadas con al desarrollo de producto o servicio se habla de ciclo de vida de desarrollo, estos pueden ser: predictivos o también llamados cascada, iterativos, incrementales y agiles o también llamados adaptativos.

En la Figura 1.6 se puede observar las diferencias entre los tipos de ciclos de desarrollo de los proyectos, las formas que se manejan los requisitos, tiempo y costo del proyecto. El proyecto de ampliación de la red GPON tiene un ciclo de vida predictivo ya que en las fases tempranas del proyecto se conoce el alcance, tiempo y costo.

Figura 1.6 Tipos de ciclos de vida de desarrollo.

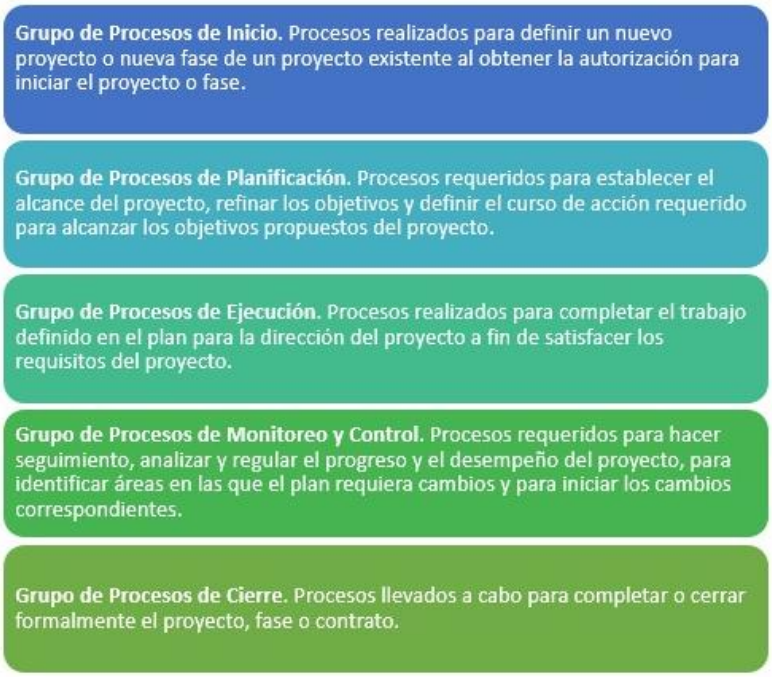
Predictivos	Iterativos	Incrementales	Ágiles
Los requisitos son definidos por adelantado antes de que comience el desarrollo	Los requisitos pueden ser elaborados a intervalos periódicos durante la entrega	Los requisitos se elaboran con frecuencia durante la entrega	
Entregar planes para el eventual entregable. Posteriormente, entregar solo un único producto final al final de la línea de tiempo del proyecto	La entrega puede ser dividida en subconjuntos del producto global	La entrega ocurre frecuentemente con subconjuntos del producto global valorados por el cliente	
El cambio es restringido tanto como sea posible	El cambio es incorporado a intervalos periódicos	El cambio es incorporado en tiempo real durante la entrega	
Los interesados clave son involucrados en hitos específicos	Los interesados clave son involucrados periódicamente	Los interesados clave son involucrados continuamente	
El riesgo y los costos son controlados mediante una planificación detallada de las consideraciones que mayormente se conocen	El riesgo y los costos son controlados mediante la elaboración progresiva de los planes con nueva información	El riesgo y los costos son controlados a medida que surgen los requisitos y limitaciones	

Fuente: PMBOK Sexta edición
Elaborador por: PMBOK Sexta edición, 2016.

1.5.5.2. Procesos de la gestión de proyectos

Dentro de los procesos que forman parte de la gestión de proyectos para alcanzar objetivos específicos del mismo se describen los siguientes:

Figura 1.7 Grupos de Procesos de la Gestión de Proyectos



Fuente: PMBOK Sexta edición, 2016.
Elaborador por: Autor

Se debe diferenciar entre los procesos de la gestión de proyectos y las fases del proyecto. Las fases del proyecto son conjuntos de actividades del proyecto relacionadas que culminan con la finalización de un entregable; el conjunto de fases del proyecto se conoce como el ciclo de vida del proyecto que abarca desde el inicio hasta su conclusión.

Estos procesos no son fases del proyecto; cuando el proyecto está dividido en fases los grupos de procesos interactúan con cada fase del proyecto.

1.5.6. Red GPON

GPON es una tecnología de acceso de telecomunicaciones que utiliza cable de fibra óptica para llegar hasta el usuario final. En la recomendación UIT-T G.984.1 (Unión Internacional de Telecomunicaciones, UIT) (Systems, 2012) describe una red de acceso de fibra óptica con capacidad para soportar las necesidades de ancho de banda de los servicios para empresas y particulares y abarca sistemas con velocidades de línea nominales de 1,2 Gbit/s y 2,4 Gbit/s en sentido descendente (hacia el destino) y de 155 Mbit/s, 622 Mbit/s; 1,2 Gbit/s y 2,4 Gbit/s en sentido ascendente (hacia el origen). Se refieren a sistemas de redes ópticas pasivas con capacidad de Gigabits (GPON, gigabit capable passive optical network) simétricos y asimétricos (ascendentes/descendentes). (UIT-T G.984.1, 2014).

1.5.6.1. Arquitectura de una red GPON

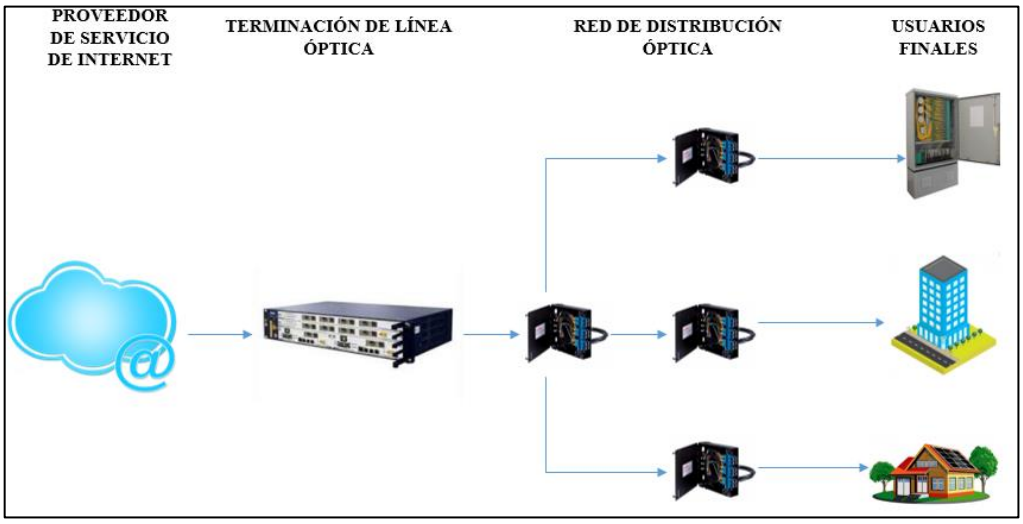
Las redes ópticas pasivas con capacidad gigabit, están definidas por la ITU bajo el estándar G.984 series [1-5], su objetivo principal es llevar un mayor ancho de banda que permite ofrecer cualquier tipo de servicio: voz, datos y video sobre la misma infraestructura IP. (Jaramillo, 2018)

Los sistemas GPON se caracterizan en general por un sistema de terminación de línea óptica (OLT, optical line termination) con una red de distribución óptica (ODN, optical distribution network) pasiva que los interconecta a los usuarios finales mediante una unidad de red óptica (ONU, optical network unit) o una terminación de red óptica (ONT, optical network termination). (UIT-T G.984.1, 2014).

La terminación de línea óptica (OLT) es el elemento principal que está en la central donde se distribuye todos los hilos de fibra óptica.

En la Figura 1.8 se muestra la arquitectura de una red GPON donde muestra la llegada de Fibra Óptica a los usuarios finales. optical network unit)

Figura 1.8 Arquitectura de una red GPON



Fuente: UIT-T G.984.1, 2014.
Elaborador por: Autor

En la arquitectura de red GPON presenta una arquitectura de un solo nodo que tiene una capacidad de 20 km de distancia máxima; si se interconecta a más de una terminación de línea óptica (OLT) se trata de una red troncal.

En la red de distribución óptica encontramos a los elementos distribuidores de fibra conocidos por el nombre de “splitter” que recibe una sola señal de fibra óptica y permite dividirla en múltiples señales que serán distribuidas a los usuarios finales; los usuarios reciben la fibra óptica hasta la unidad óptica de red (ONU) que permitirá conexión a internet de forma alámbrica o inalámbrica, esta conexión se la conoce como red de acceso. (UIT-T G.984.1, 2014).

Figura 1.9 Red de acceso

Fuente: UIT-T G.984.1, 2014.
Elaborador por: Autor

1.5.6.2. Ventajas de una red GPON

Dentro de las ventajas de la utilización de una red GPON se tiene:

- **Velocidad de bits**

  Básicamente, GPON apunta a velocidades de transmisión mayores o iguales a 1.2 Gbit / s. En consecuencia, GPON identifica dos combinaciones de velocidad de transmisión de la siguiente manera: 1.2 Gbit / s arriba, 2.4 Gbit / s abajo y 2.4 Gbit / s arriba, 2.4 Gbit / s abajo.

  La velocidad de bits más importante es de 1.2 Gbit / s arriba, 2.4 Gbit / s baja, constituyendo casi todos los implementados y planeado despliegue de los sistemas GPON. (UIT-T G.984.1, 2014).

- **Alcance lógico**

  El alcance lógico es la distancia máxima entre ONU / ONT y OLT, excepto por la limitación de la capa física. En GPON, el alcance lógico máximo se define como 60 km. (UIT-T G.984.1, 2014).

- **Alcance físico**

  El alcance físico es la distancia física máxima entre la ONU / ONT y la OLT. En GPON, se definen dos opciones para el alcance físico: 10 km y 20 km. (UIT-T G.984.1, 2014).

- **Retardo máximo de transferencia de señal media**

  En GPON debe acomodar servicios que requieren un retardo de transferencia de señal medio máximo de 1.5 ms.

Específicamente, el sistema GPON debe tener un tiempo de retardo de transferencia de señal medio máximo menor a 1,5 ms.

- **Relación de división**

  Básicamente, cuanto mayor es la relación de división para el sistema GPON, más atractivo es para los operadores. Sin embargo, una mayor proporción de división implica una mayor división óptica, lo que crea la necesidad de una mayor potencia Presupuesto para apoyar el alcance físico.

  Las relaciones de división de hasta 1:64 son realistas para la capa física, dada la tecnología actual. Sin embargo, anticipando la evolución continua de los módulos ópticos, la capa TC debe considerar las relaciones divididas hacia arriba a 1: 128. (Al-quzwini, 2017)

1.5.6.3. Desventajas de una red GPON

Dentro de las principales desventajas de la red GPON se tienen:

- Los implementos y materiales para el mantenimiento de la fibra óptica es relativamente costoso;
- Para solventar alguna rotura en el núcleo de la fibra óptica, este debe ser reparado por personal capacitado y especializado, debido a que manipular la fibra se debe tener mucho cuidado y ser minucioso; y,
- En ocasiones se debe conectarse con equipos electrónicos que necesitan energía eléctrica, por lo cual no puede ser enviado a través de la fibra óptica, por lo que se necesitan cables extra para la alimentación para esos dispositivos. (Obtenci, Maestr, Red, & Fibra, 2015).

1.5.7. Definición de proyectos de ampliación de red GPON

Un proyecto de ampliación de red GPON se define cuando una empresa proveedora de servicio de internet implementa nueva cobertura mediante fibra óptica para así extender sus servicios de internet en un sector geográfico determinado previamente. (RODRÍGUEZ & VÁSQUEZ, 2016).

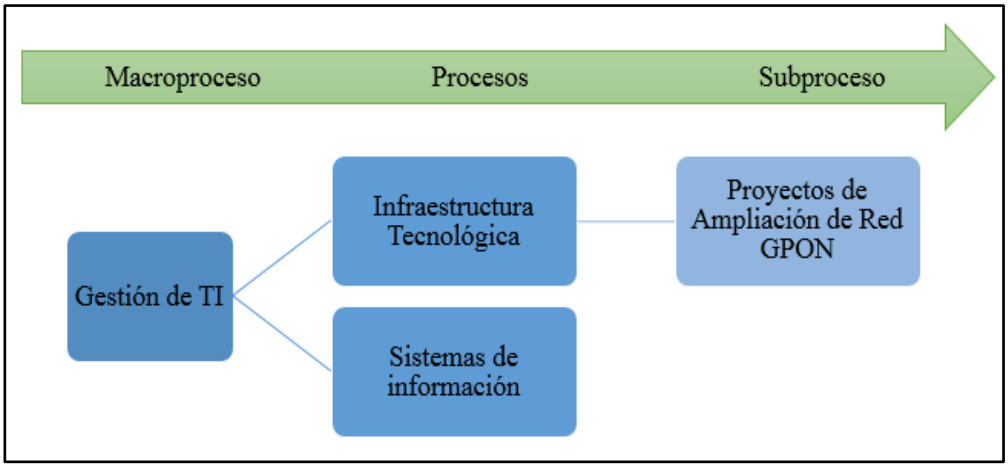
Este tipo de proyectos se realiza cuando las empresas encuentran un nicho de mercado con potencial y mediante proyecciones financieras se define si se realizará o no el proyecto de ampliación.

ETAPA EP empresa pública con matriz en Cuenca implementa red GPON para ser más competitivos en el sector de servicios de internet, brindar más servicios al usuario como por ejemplo televisión por internet, o telefonía utilizando la red de fibra óptica, a pesar que esta implementación tiene el costo de 9 millones de dólares no hacerlo implicaría dejar de percibir 12 millones de dólares. (León, 2014)

TELCONET mantiene como propuesta realizar una ampliación de red GPON en el sector Progreso comunidad Juan Gómez Rendón donde actualmente solo hay dos proveedores de servicios de internet, con esta ampliación se espera dar internet a 7000 usuarios aproximadamente con un costo de 300,000 dólares. (Alcívar, 2015)

Además se debe tener en cuenta que los proyectos de ampliación de red GPON forman parte del proceso de infraestructura tecnológica, pertenecientes al macro proceso de Gestión de tecnología de la información (TI) y comparten las mismas necesidades de información y los métodos de distribución pueden variar ampliamente dependiendo del sector. Procesos COBIT5. (ISACA, 2012)

Figura 1.10 Proceso de infraestructura tecnológica



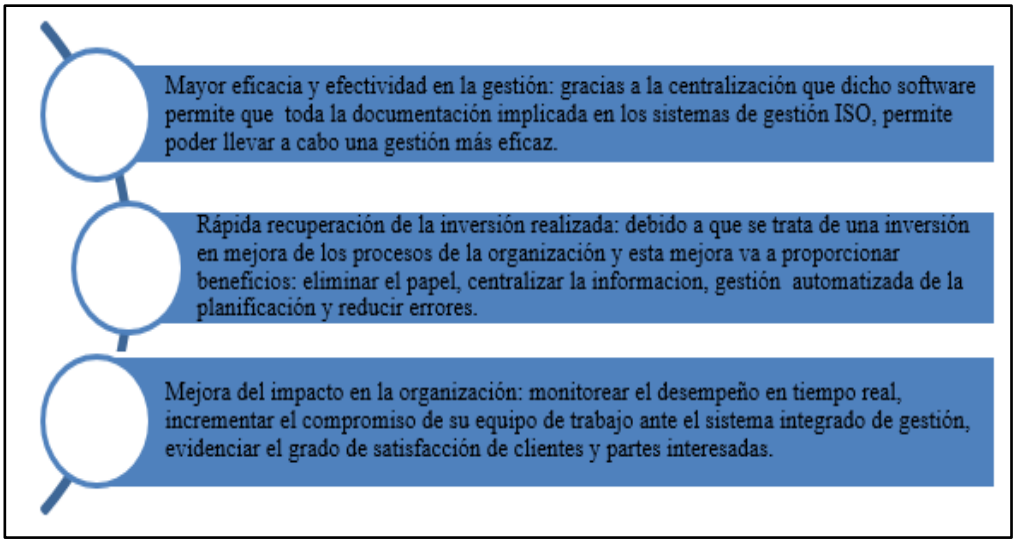
Fuente: Procesos COBIT5. (ISACA, 2012)
Elaborador por: Autor

Dependiendo de la organización de cada PYME los nombres de los procesos pueden variar, además dentro del macro proceso de Gestión de TI puede la empresa tener más de un proceso y subprocesos. En la figura 1.10 se representa una estructura de proceso básica para enlazar desde donde proviene el subproceso de proyectos de ampliación de red GPON en PYMES proveedoras de servicio de internet.

1.5.8. Sistemas de información aplicable a seguridad de la información.

La plataforma tecnológica ISOTools Excellent desarrollada en entorno Web presenta un sistema de información con la Norma ISO/IEC 27001:2013 que ayuda a las organizaciones a administrar, agilizar y automatizar sus sistemas de seguridad de la información. Como ventajas y beneficios se presentan:

Figura1.11Ventajas del software de seguridad de la información ISOTools.



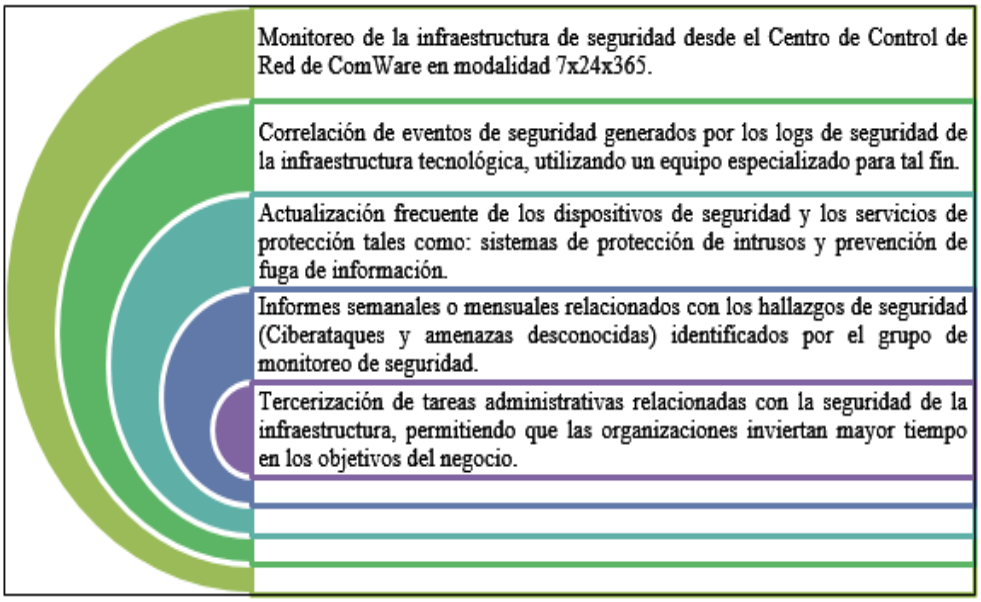
Fuente: ISOTools. (29 de Junio del 2019).
Elaborado por: Autor.

Este software de seguridad de la información ISOTools permite una centralización de toda la documentación implicada en el sistema de gestión de seguridad de la información esto responde a la necesidad de tener un entorno más controlado y así se tenga una gestión eficaz.

En materia económica este software da como beneficio un ahorro de recursos porque permite eliminar el papel, automatiza la planificación y por lo tanto reduce los errores que provocan re planificación.

Además se tiene información de un software de origen colombiano ComWare que se encarga de hacer reportes, planificaciones con respecto a la Norma ISO/IEC 27001:2013 entre sus ventajas destacan:

Figura1.12 Ventajas del software de seguridad de la información ComWare.



Fuente: COMWARE S.A. (15 de Mayo del 2015).
Elaborado por: Autor.

Dentro de las ventajas que destacan en el software de seguridad de la información ComWare son: da un monitoreo los 365 días al año facilitando el control de los eventos y además de correlacionar los eventos de seguridad de la información de forma automática según los log de seguridad que da el sistema de información. Este software también da informes semanales o mensuales relacionados con los hallazgos de seguridad de la información como ciber ataques y amenazas desconocidas.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de la investigación

2.1.1. Tipo de diseño

El proceso de la investigación es cualitativo y cuantitativo por motivo que se orienta a los siguientes tipos de estudios:

2.1.1.1. Estudio descriptivo

Se aplicó este tipo de estudio para poder describir las características de las variables que son parte de la investigación. Este trabajo tiene información que permite evidenciar con un ambiente situacional donde se miden sus conceptos y variables.

2.1.1.2. Estudio correlacional

Permite conocer la relación o grado de asociación entre dos o más ítems, dimensiones, categorías o variables en un contexto en particular; si no hay correlación entre las variables, ello indica que estas varían sin seguir un patrón sistemático entre sí.

2.1.2. Alcance de la investigación

El alcance de la presente documentación está en analizar los problemas no visibles por la falta de un modelo de seguridad de la información basado en la Norma ISO/IEC 27000 para los proyectos de ampliación de red GPON en las PYMES proveedoras de servicios de Internet del norte de la ciudad de Guayaquil.

A este modelo de seguridad de la información para las PYMES se la ha considerado variables, dimensiones, indicadores e ítems.

Este trabajo no tiene como alcance el análisis de otros sectores de mercado del Guayaquil, ni espera hacer un estudio de caso de alguna empresa proveedora de servicios de internet en particular.

2.1.3. Enfoque

Este trabajo de investigación tiene un enfoque de tipo cuantitativo; donde se pretende tener una perspectiva de la realidad de los proveedores de internet de las PYMES en Guayaquil, y en la ausencia de procedimientos de seguridad de la información en los proyectos de ampliación de red GPON.

2.2. Metodología de la investigación

2.2.1. Método Cualitativo

Este método recoge las opiniones de los entrevistados de las PYMES proveedoras de servicio de internet que se realizan en esta investigación a partir de lo que dicen y hacen las personas en el escenario social y cultural; suministra y provee datos descriptivos para proceder a su interpretación.

2.2.2. Método Cuantitativo

Este método ayuda a analizar la evidencia empírica recopilada, se utilizará para analizar los datos recolectados de forma numérica de las PYMES proveedoras de servicio de Internet con el propósito de estudiar con métodos estadísticos posibles relaciones entre las variables que permita conocer su comportamiento.

2.2.3. Método Inductivo

Este método consiste en la recolección de datos sobre casos específicos y su análisis para crear teorías o hipótesis. La investigación pretende obtener conclusiones a partir de los resultados obtenidos por el levantamiento de información en las PYMES ISP de Guayaquil de esta muestra se lo obtendrá en los proyectos de expansión de la red GPON.

2.2.4. Método Histórico.

La investigación utiliza sucesión de hechos y fenómenos que se presentaron en el año 2015 a 2019 en los proyectos de expansión de la red GPON y la seguridad de la información aplicada al área técnica de cada organización, este método identifica los patrones históricos que sean regulares y las causas generales.

2.3. Unidad de análisis, población y muestra.

2.3.1. Unidad de análisis

Para efectos de investigación se tomó como unidad de análisis solo a empresas proveedoras de servicio de internet de las PYMES y que se encuentren en el sector norte de la ciudad de Guayaquil según lo expresado por las entidades de control de Servicio de Rentas Internas y la Agencia de Regulación y Control de las Telecomunicaciones.

2.3.2. Población de estudio

Según la base de datos “Reporte ISP” en la ciudad de Guayaquil en el sector Norte existen 23 empresas proveedoras de servicios de Internet, las cuales son legalmente constituidas y poseen el título habilitante de ARCOTEL.

2.3.3. Tamaño de la muestra

Para el cálculo probabilístico de la muestra se utilizará la fórmula de la población finita que se detalla a continuación:

$$\boldsymbol{n = \frac{z^2 N p q}{(N-1)e^2 + z^2 p q}}$$

Donde:

N: Población total: 23

z: nivel de confianza= 95% coeficiente tabla estadística: 1,96

p: Probabilidad de ocurrencia= 0,5

q: Probabilidad de no ocurrencia (1-p)= (1-0,5)= 0,5

e: Error de muestreo= 5% (0,05)

n: Tamaño de la muestra= 13,57

De acuerdo a la fórmula se debe tomar la cantidad de 13 muestras, pero como la población es pequeña se considera utilizar el total de la población para asegurar un margen de error bajo y una alta confiabilidad.

2.4. Variables de investigación, operacionalización

Variable Dependiente (VD)

- VD01 - Seguridad de la información._ Es la variable del trabajo de investigación que permite determinar el nivel de incidencia.

Variables Independientes (VI)

- VI01-Confidencialidad._ Variable identificada para garantizar que la información este accesible únicamente a personal autorizado;
- VI02-Integridad._ Variable identificada para valorar que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado; y,
- VI03-Disponibilidad._ Variable identificada para asegurar que la información se encontrará a disposición de quienes deben acceder a ella.

2.5. Fuentes, técnicas e instrumentos para la recolección de información

2.5.1. Fuentes de información

En la revisión de la literatura se dividió la fuente de información en primarias y secundarias de organismos gubernamentales y no gubernamentales afines a la información:

2.5.1.1. Fuentes primarias

Se identificó como fuente primaria toda la información proveniente de:

1. ARCOTEL en sus bases de datos de la página oficial;
2. Ministerio de Telecomunicaciones en sus estadísticas e indicadores publicados de la página oficial; y,
3. Información del Registro Oficial desde su página oficial.

2.5.1.2. Fuentes secundarias

Se identificó como fuente secundaria toda la información proveniente de:

1. Información documental estadística de otras fuentes de divulgación diferente de las primarias;
2. Información de artículos científicos en revistas especializadas;
3. Libros de especialidad en administración de empresas orientados en gestión de proyectos; y,
4. Libros de especialidad en el desarrollo de la Norma ISO/IEC 27000.

2.5.2. Técnicas para la recolección de información

2.5.2.1. Técnica documental.

Se consideró esta técnica de investigación para poder recopilar información relacionada al tema de investigación y de todas las fuentes disponibles, tesis, revistas, páginas web, libros, informes técnicos, artículos científicos y toda aquella fuente válida, de las variables confidencialidad, integridad y disponibilidad.

2.5.2.2. Técnica de investigación de campo.

Esta investigación recolectó información del objetivo de estudio mediante el instrumento de encuesta sobre un modelo de un sistema de seguridad de la información Norma ISO/IEC 27001:2013 en las PYMES proveedoras de internet en el proceso de ampliación de red GPON. En el anexo 4 constan las columnas “técnica”, “instrumento” y “fuente de información”.

2.5.3. Instrumentos

2.5.3.1. Investigación documental.

En este trabajo de investigación se utilizó la investigación documental para recopilar datos de documentación que tenga relación con la problemática expuesta en el capítulo anterior.

2.5.3.2. Entrevistas.

Se desarrolló entrevistas ya con un formato previamente elaborado y aprobado por el Autor con diferentes preguntas semiestructuradas a cada uno de los entrevistados.

2.5.3.3. Encuestas.

En las encuestas desarrolló un formulario a través de Google desde la cuenta personal del Autor, donde se registraron los ítems y se envió el enlace respectivo a personal involucrado que consta en la base de datos de los proveedores de Internet descargado desde la página web de la ARCOTEL.

En las respuestas se utilizó escala de Likert, donde “5” indica estar totalmente de acuerdo, “4” es estar de acuerdo, “3” es ni estar de acuerdo ni desacuerdo, “2” en desacuerdo y “1” totalmente en desacuerdo con la pregunta o ítem.

2.6. Tratamiento de la Información

Para el tratamiento de la información que se pudo extraer para esta investigación, se utilizaron las siguientes herramientas:

- **SPSS**

  Se utilizó el software SPSS (Statistical Package for the Social Sciences) con la versión 24 con la finalidad de obtener una estadística descriptiva, tablas de frecuencias y tablas cruzadas que permiten conocer a las PYMES proveedoras de servicio de internet en Guayaquil. Además se utilizó SPSS para realizar el análisis de los datos de las encuestas y representación en tablas de resultados.

- **Microsoft Excel**

  Se utiliza Microsoft Excel para tabular y organizar la información, el registro detallado de datos, cálculos y representación de datos mediante tablas y gráficos que facilitan la comprensión de los resultados.

- **Escala de Likert**

  La escala aplicada para la evaluación de las variables es la escala Likert que permite realizar mediciones y conocer sobre el grado de conformidad del encuestado hacia determinada oración afirmativa o negativa, a continuación se detallada la escala en la Tabla 2.1.

Tabla 2.1 Escala de Likert

Escala	Valoración	Descripción
1	Muy bajo	En total acuerdo con el criterio
2	Bajo	En desacuerdo con el criterio
3	Medio	Ni en acuerdo ni en desacuerdo con el criterio
4	Alto	En acuerdo con el criterio
5	Muy alto	En total acuerdo con el criterio

Fuente: Nequest, 2014
Elaborador por: Autor

Esta escala posee un conjunto de ítem de respuestas que van de lo más favorable a lo menos favorable y permite determinar el nivel de acuerdo o desacuerdo de los encuestados.

CAPÍTULO III

3. ANÁLISIS, PRESENTACIÓN DE RESULTADOS Y DIAGNÓSTICO

3.1. Análisis de la situación actual

3.1.1. Análisis de variable dependiente Seguridad de la Información para proyectos de ampliación de red GPON en las PYMES ISP del Norte de la ciudad de Guayaquil

3.1.1.1. PYMES ISP en el Ecuador

Las PYMES son aquellas empresas que generan ingresos o ventas anuales de entre $ 100.000 y $ 1’000.000. (INEN, 2016)

Según el Catastro del RUC del Servicio de Rentas (SRI, 2016) existen 32.899 PYMES de las cuales el 33% pertenecen al sector del comercio, el 17% a servicios diversos, el 10% al sector de industrias manufactureras, el 9% al sector de construcción, el sector transporte abarca el 6% y el resto de actividades ocupan el 25%. Las PYMES ISP se encuentran dentro del 17%.

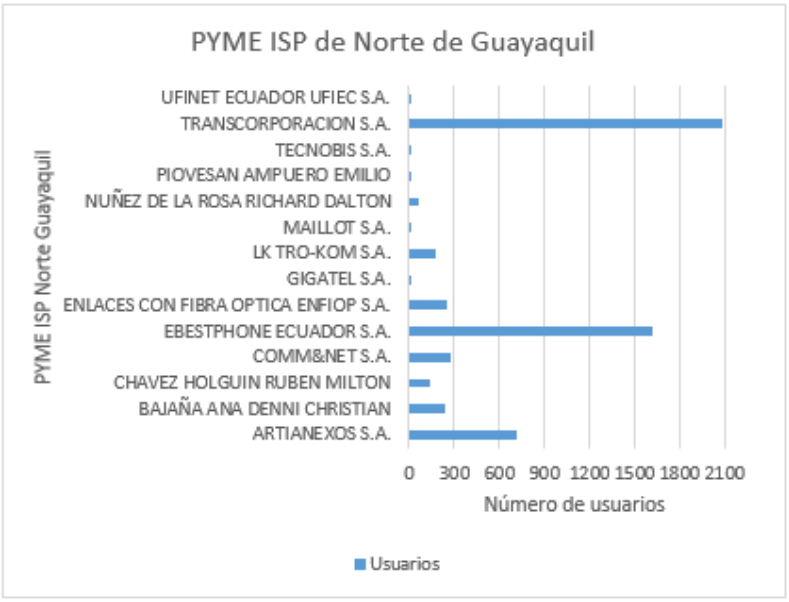
Además, según datos del 2016 del Instituto Nacional de Estadísticas y Censos (INEC, 2016) las PYMES representan aproximadamente el 99,5% del total de empresas registradas. En Guayas están constituidas el 43% del total de las empresas pequeñas y el 40% de empresas medianas, mientras que en Pichincha el 39% son pequeñas empresas y un 40,8% empresas medianas (Catastro del RUC del Servicio de Rentas Internas SRI-2016).

Dentro del Ecuador hay 578 empresas proveedoras de servicio de internet entre las cuales se puede indicar que la participación en el mercado es de 93,11% empresas grandes y 6,89% PYMES. Las empresas grandes son solamente 9, es decir que el 6,89% de la participación está representado por 569 PYMES ISP a nivel nacional. De acuerdo a datos del último boletín de la ARCOTEL en mayo del 2019 la participación del mercado a nivel de la ciudad de Guayaquil de las PYMES ISP es de 7185 cuentas de internet fijo aproximadamente que representa el 12,8%. (SIETEL, ARCOTEL, 2019).

3.1.1.2. PYMES proveedoras de servicios de Internet del Norte de Guayaquil

Según datos de la ARCOTEL 2016 en Guayaquil, especialmente en el sector Norte de la Ciudad existen 23 empresas legalmente constituidas las cuales tiene contrato habilitante para brindar servicios de internet mediante fibra óptica. Estas empresas cubren un total de 5609 cuentas de servicio de internet fijo en el sector norte de la ciudad.

Figura 3.1 PYMES ISP de norte de Guayaquil



Fuente: ARCOTEL 2018
Elaborador por: Autor

En la Figura 3.1 se puede apreciar que las empresas TRANSCORPORACION S.A. y la empresa EBESPHONE ECUADOR S.A. son las que mayor participación tienen en el norte de Guayaquil en lo que respecta a las PYMES. La mayoría de estas empresas están enfocadas en un servicio de internet fijo a través de fibra óptica.

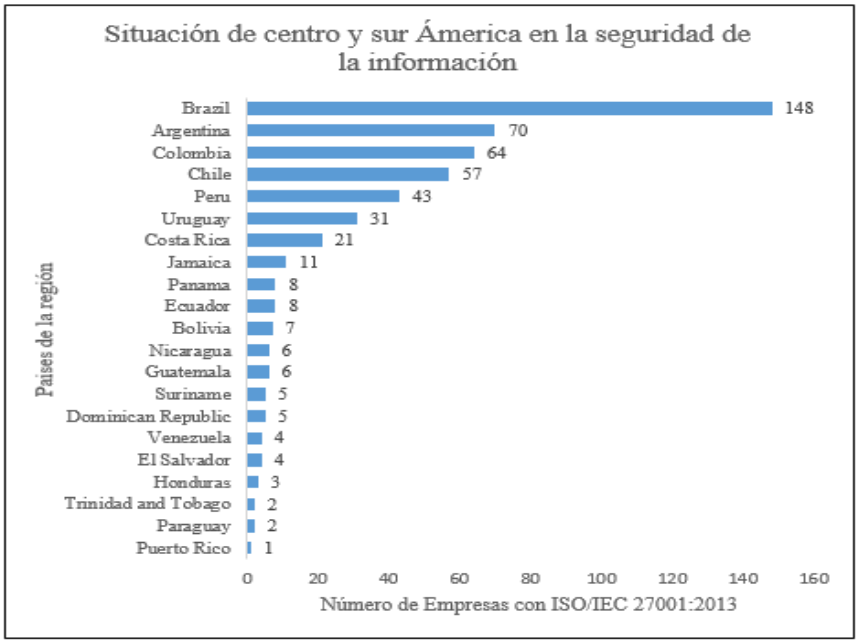
3.1.1.3. PYMES proveedoras del servicio de internet con la Norma ISO/IEC 27001:2013

Lamentablemente no se conoce de las PYMES del sector de telecomunicaciones que cuenten con una certificación de la Norma ISO/IEC 27001:2013 o que se encuentren en proceso de certificación de la misma.

En Ecuador no se registran datos estadísticos del número de las PYMES que son ISP y que poseen un sistema de seguridad de la información además que se utilicen ciertos procedimientos que recomienda la Norma ISO/IEC 27001:2013 en los proyectos de ampliación de red GPON, tales como el registro de incidentes, políticas de confidencialidad, control de accesos etc., lo que si se ha evidenciado es un desconocimiento de los controles de esta norma en el uso de los proyectos para la ampliación de cobertura de la red GPON de acuerdo a resultados de las entrevistas y encuestas.

Los controles que ofrece la Norma ISO/IEC 27011:2016 son herramientas especializadas en empresas de telecomunicaciones que permiten mejorar procesos y ahorrar recursos a diversas empresas en el sector de TI del país, la tecnología con influencia de un marco de referencia como el PMBOK sexta edición aportan valor a los interesados en cada proyecto que se implemente. En la Figura 3.2 se puede visualizar la situación en Centro y Sur América, siendo Brasil el país que cuenta con mayor número de empresas con la Norma ISO/IEC 27001:2013, teniendo una diferencia de 140 empresas con Ecuador.

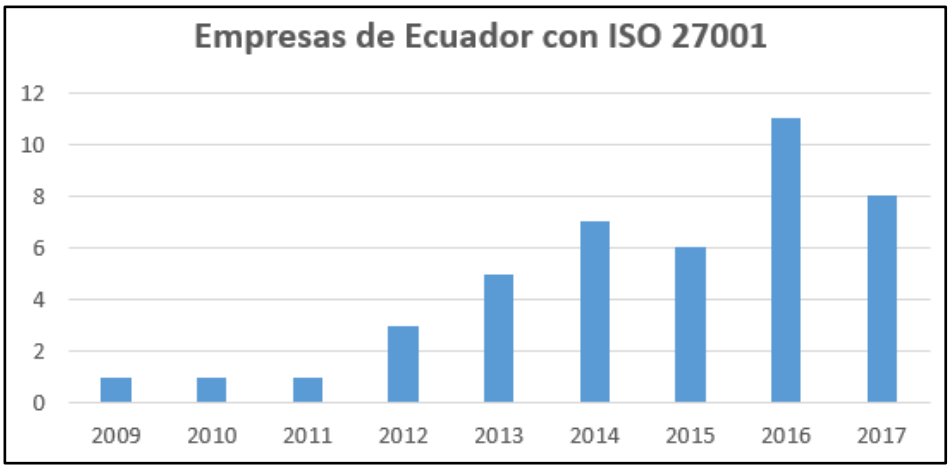
Figura 3.2 Situación de la región en Seguridad de la Información



Fuente: Committee ISO, 2018.
Elaborado por: Autor

Sin embargo, al conocer las estadísticas desde el 2009 hasta el 2017 en Ecuador se puede notar que hay una tendencia a crecimiento, pero que algunas empresas no renovaron posiblemente su certificación en el último año.

Figura 3.3 Empresas del Ecuador con la Norma ISO/IEC 27001



Fuente: Committee ISO, 2018.
Elaborador por: Autor

Actualmente solo 8 empresas ecuatorianas cuentan con la certificación ISO/IEC 27001 de las cuales solo 3 son empresas proveedoras de servicio de Internet, dos de internet móvil y una como internet corporativo. Fuente: (Committee ISO, 2018). El sitio oficial de la organización ISO no proporciona información sobre cuáles son las 8 empresas que en Ecuador están certificadas actualmente, sin embargo algunas de las que han dejado saber de su logro con este estándar son: CNT E.P., TELCONET S.A, (La Republica, 2018). Banco De Guayaquil, (GF Sistemas, 2014). MOVISTAR, ASTINAVE E.P., y QUITO TURISMO. (MAHECHA & COELLO, 2016).

3.1.2. Análisis del marco y micro entorno de la seguridad de la información en las PYMES proveedoras de servicio de Internet en Guayaquil.

Se realizaron tres entrevistas para abordar el tema de un Modelo de un Sistema de Información basado en la Norma ISO/IEC 27001:2013 en las PYMES proveedoras de servicios de Internet del Norte de la ciudad de Guayaquil relacionado con el subproceso de proyectos de ampliación de red GPON.

Las personas entrevistadas fueron Miguel Izquierdo, el Gerente General de EBESTPHONE ECUADOR S.A. empresa que cuenta con 6 años de experiencia, Geovanny Narea Jefe Técnico de ENFIOP S.A. Empresa que cuenta con 3 años de experiencia; Pablo Tinoco Gerente Técnico de INTERCON empresa que cuenta con 8 años de experiencia.

De acuerdo a las entrevistas y encuestas (ver anexo X) realizadas se presenta la información relevante a un análisis PESTEL (Político, Económico, Social, Tecnológico, Ecológico y Legal) y PORTER donde se identifica los factores del entorno general que afectan a las PYME ISP que se relacionan con los proyectos de ampliación de red GPON.

3.1.2.1. Análisis Pestel

- **Político.-** Las políticas arancelarias son un principal problema al momento de importar implementos y equipos de telecomunicaciones, afirma Miguel Izquierdo debido a los altos costos de liquidación arancelaria que encarecen los productos que no se encuentran en el mercado nacional.
- **Económico.-** Pablo Tinoco Gerente Técnico de INTERCON indica que la situación económica del país les afecta directamente debido a que los clientes ya no piden más servicios o simplemente cancelan el servicio de internet a pesar que los precios que tienen son los más bajos del mercado. Por otro lado Miguel Izquierdo se muestra más optimista debido a que indica que a pesar que la economía no es buena las personas buscan los medios necesarios para tener servicio de internet en su domicilio y más si es mediante fibra óptica.
- **Socio-Cultural.-** Geovanny Narea Jefe Técnico de ENFIOP S.A. se muestra seguro al informar que los usuarios no poseen ningún tipo de conocimiento sobre seguridad de la información. Además que el motivo para lo que más pide internet el usuario es para ver Televisión por internet o estar en redes sociales. Pablo Tinoco menciona que hay un índice alto de nuevo hogares y nuevos

sectores donde hay poblaciones importantes y eso representa una oportunidad para su negocio.

- **Tecnológico.-** Al ser una empresa que ofrece servicios de internet Miguel Izquierdo ratifica la amenaza que es el 5G para empresas de este tipo debido a que si tienen la infraestructura tecnológica suficiente y los precios muy bajos podría tener pérdidas en su empresa. Pablo Tinoco en cambio menciona que como las tecnologías evolucionan de forma constante siempre, y eso les va a favorecer para mejorar el servicio y tener mayor participación en el mercado.
- **Legal.-** Las PYMES se ven afectada por la excesiva regulación que existe por parte de la ARCOTEL, esto indica Miguel Izquierdo, Gerente General de EBESTPHONE ECUADOR S.A. donde la ARCOTEL se enfocan en los ISP con título habilitante y no las empresas proveedoras de servicio que trabajan de forma ilegal o sin título habilitante otorgado por la ARCOTEL.
- **Ecológico.-** Geovanny y Pablo indican que el mayor problema ocurre en los inviernos donde se presentan mayor cantidad de cortes de energía causan daño en sus equipos finales que están en el domicilio del usuario o incluso el mal tiempo afecta a los cables eléctricos y estos queman al cable de fibra óptica. Miguel Izquierdo puntualiza que cuando existen lluvias esto causa un retraso en el cronograma debido a que los técnicos no pueden trabajar en posterío cuando llueve por medida de seguridad.

3.1.2.2. Fuerzas de Porter

- **Amenaza de la entrada de los nuevos competidores**.

  Los tres entrevistados consideran que hay muchos factores que hacen difícil entrar en la industria de proveedores de servicio de internet en el Ecuador, algunos factores transcendentales como el poder de penetración en el mercado, la imagen, los gastos de publicidad, el alto costo de equipos de telecomunicaciones que son importados además de los costos operativos y la regulación

excesiva por parte de ARCOTEL. Miguel Izquierdo indica que es costoso cada proyecto de ampliación de red GPON por la mano de obra y los materiales a utilizar. Pablo Tinoco indica que para evitar costos muy elevados importa muchos materiales para la ampliación de red GPON.

- **Poder de Negociación con los proveedores.**
  La proveedores de servicio de Internet tiene como proveedor a empresas con título habilitante otorgado por la ARCOTEL conocidos por Servicios Portadores de Telecomunicaciones (SPT), según datos del SIETEL publicados en Octubre del 2018, el poder de negociación es relativamente bajos de acuerdo a la entrevista con Miguel Izquierdo es debido a que los SPT normalmente poseen precios fijos.
- **Poder de negociación de los clientes.**
  Geovanny Narea indica que la premisa del abonado cada día es más exigente y espera los precios más bajos, el inconveniente es que el cliente puede retirarse en cualquier momento y cambiarse de proveedor de internet. Por eso si se tiene planificado una ampliación de red GPON por realizar se busca que sea en un sector donde no exista o exista sólo uno o dos proveedores de internet, así ratifica Pablo Tinoco.
- **Amenaza de productos sustitutos.**
  Al existir poca eficacia en la regulación y control por parte de la ARCOTEL de proveedores de internet sin permiso habilitante se hace compleja la tarea de mantener precios, más bien la tendencia es hacia la baja.
- **Rivalidad entre los competidores.**
  Pablo Tinoco y Miguel Izquierdo coinciden que empresas como CNT E.P., MEGADATOS S.A., ECUADORTELECOM S.A., PUNTONET S.A. y SETEL S.A. comparten la mayor parte del mercado alrededor del 92%, según datos de ARCOTEL 2015 en su Boletín #6, y que el 8% es compartido entre empresas con menor capital.

Miguel Izquierdo indica que para su empresa si es importante mantener estándares internacionales, procedimientos y procesos bien definidos, además admite que la empresa no ha hecho lo necesario para tener a sus colaboradores bien formados sobre seguridad de la información.

Pablo Tinoco indica que los procedimientos antes, durante y luego del proyecto de ampliación se los realiza de forma manual, debido a que no tiene un software de gestión de procesos. Además informa que los costos de implementación por este tipo de software deben ser altos.

Geovanny Narea indica que como PYME ISP es altamente significativo tener su propia red de fibra óptica además realizar proyectos de ampliación de red GPON, además que si bien no es tan conocida su empresa la velocidad de internet es muy buena para poder visualizar películas online, YouTube y Netflix.

Una vez identificada las amenazas debilidades oportunidades y fortalezas se procede a representar las mismas en la matriz FODA.

3.1.2.3. Análisis de la Matriz FODA

Tabla 3.1 Matriz FODA

Análisis Interno		Análisis Externo	
Debilidades		**Amenazas**	
D01	Limitada capacidad financiera para realizar inversiones para proyecto de ampliacion de red GPON	**A01**	Regulación excesiva por parte del instituciones como ARCOTEL.
D02	Alto procesamiento manual en registro de información de requerimientos (Tablas y documentos físicos) para proyectos de ampliación de red GPON	**A02**	Nuevas tecnologías móviles que compartan mercado con ISP de internet fijo
D03	Falta de cultura empresarial sobre la importancia de la seguridad de la información.	**A03**	Equipos de telecomunicaciones sin seguridad física ante eventos naturales.
Fortalezas		**Oportunidades**	
F01	Red de Fibra Óptica con infraestructura propia.	**O01**	Rápida evolución tecnológica a nivel mundial.
F02	Internet de alta velocidad a más posibles abonados debido a mayor cobertura de red GPON	**O02**	Tendencia favorable en el mercado por un internet mediante fibra óptica.
F03	Escabilidad para nuevos proyectos de ampliación de red GPON	**O03**	Nuevos sectores que requieren internet fijo.

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

De acuerdo a la Tabla 3.1 se analizó la seguridad de la información referente a los proyectos de ampliación de red GPON que lo realizan las

PYMES ISP de Guayaquil donde se visualiza las debilidades, amenazas, fortalezas y oportunidades. Esta matriz fue llenada con la información del análisis PESTEL y PORTER.

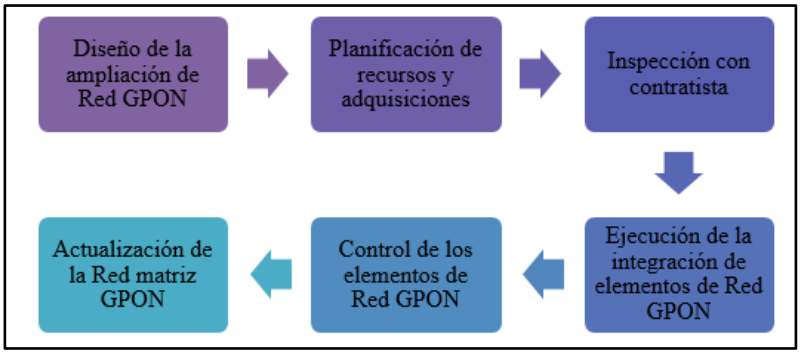
3.1.3. Proyectos de ampliación de red GPON

3.1.3.1. Subproceso proyecto de ampliación de red GPON

Usando la metodología SIPOC (Suppliers, In, Process, Out, Customers), SIPOC es la sigla (en inglés), que simboliza Proveedores, Entradas, Procesos, Salidas y Clientes que es un modelo usado para identificar y aclarar lo que se necesita para crear el producto o servicio.

En el anexo 8 se representa el subproceso de proyecto de ampliación de red GPON en un modelo SIPOC, esta información fue proporcionado por la empresa EBESTPHONE ECUADOR S.A. por lo cual se toma como referencia; sin embargo, esto no indica que el proceso sea idéntico para todas las PYMES ya que dependerá de la estructura organizacional de la empresa más bien sirve para guía de investigación.

Figura 3.4 Subproceso de proyecto de ampliación de la red GPON



Fuente: Datos de la investigación.
Elaborador por: Autor

A continuación se detalla cada uno de los procesos con sus entradas y salidas:

Diseño de la ampliación de red GPON

Para iniciar con el diseño de la ampliación de la red GPON es necesario que el departamento de ventas entregue un documento que especifique el requerimiento de ampliación de la red GPON en un sector específico, el

departamento técnico no es el responsable del cálculo de factibilidad del sector solo ejecuta acorde a lo requerido por el departamento de ventas. Una vez que se realiza el diseño de la red es responsabilidad del jefe de proyecto generar los documentos de listados de materiales, equipos y recursos además de los planos de diseño para presentar a la alta gerencia. Corporación Nacional de Telecomunicaciones. (Febrero 12, 2012)

Tabla 3.2 SIPOC Diseño de la ampliación de la red GPON.

S	I	P	O	C
Departamento de ventas	Requerimiento de ampliación de Red GPON	Diseño de la ampliación de la Red GPON	Listado de materiales, equipo y recursos; y, Planos	Alta Gerencia

Fuente: Datos de la investigación.
Elaborador por: Autor

Planificación de recursos y adquisiciones

Cuando la alta gerencia aprueba los planos de diseño y el listado de materiales, equipos y recursos, el departamento técnico puede proceder con la planificación de recursos y adquisiciones donde se definirá el personal y se monitoreará su desempeño, se realizará la compras de materiales y adquisición de contratistas, donde se define la forma de contrato y los requerimientos mínimos que deben cumplir. Esta información debe ser entregada al departamento de bodega y al departamento de compras para que ejecuten las compras necesarias y procedan con la entrega del material.

Tabla 3.3 SIPOC Planificación de recursos y adquisiciones

S	I	P	O	C
Alta Gerencia	Aprobación de listado de materiales , equipo, recursos y planos del diseño	Planificación de recursos y adquisiciones	Listado de recursos y adquisiciones.	Departamento de bodega
				Departamento de compras

Fuente: Datos de la investigación.
Elaborador por: Autor

Inspección con contratista

Una vez que departamento de bodega y departamento de compras tengan lista la entrega de material y adquisición del contratista se realiza la inspección de campo el jefe técnico de la empresa con el contratista ahí se confirma la geografía donde se va a implementar fibra, donde estarán

instaladas las cajas de distribución y como entregable se tendrá los acuerdos de confidencialidad, planos de diseño de la red GPON y una acta de las observación que se obtuvieron de la inspección.

Tabla 3.4 SIPOC Inspección con contratista

S	I	P	O	C
Departamento de bodega	Materiales de bodega	Inspección con contratista	Acta de inspección; Acuerdo de confidencialidad; y, Planos de diseño de la Red GPON	Departamento técnico
Departamento de compras	Materiales comprados; y, Contratista seleccionado			Contratista

Fuente: Datos de la investigación.
Elaborador por: Autor

Ejecución de la integración de elementos de red GPON

El personal técnico de la PYME debe instalar los elementos de red pasivos y activos de acuerdo los planos As Built entregados por el contratista, en este proceso el personal técnico tiene como entregables el plano As Built ya de toda la red instalada no solamente el cableado que realizó el contratista sino ya implementada en su totalidad. Como salida se tiene plantillas georreferenciadas, fotografías de cómo quedó instalada la fibra y las caja de distribución.

Tabla 3.5 SIPOC Ejecución de la integración de elementos de red GPON

S	I	P	O	C
Departamento técnico	Tendido de fibra y construcción de obra civil; y, Planos As Built y construcción de obra civil	Ejecución de integración de elementos de Red GPON	Planos As Built; Plantillas de levantamiento georreferenciado de los elementos de infraestructura; y, Documentos fotográficos de fusión de fibra y elementos de infraestrutura.	Departamento técnico
Contratista	Copia de certificación de calibración de equipos; y, Orden de trabajo			

Fuente: Datos de la investigación.
Elaborador por: Autor

Control de los elementos de red GPON

Para darle control y monitoreo a la implementación realizada es necesario protocolos de prueba, equipos de medición y la orden de trabajo donde está definida la reparación a realizar de ser necesaria. Como salida de

este proceso se tiene documentos fotográficos, las trazas reflectométricas del 100% de la fibra probada, la orden de pago a contratista la tabla de reparaciones en caso de ser necesario.

Tabla 3.6 SIPOC Control de los elementos de red GPON

S	I	P	O	C
Departamento técnico	Protocolo de prueba; Equipos de medición y control; y, Orden de trabajo.	Control de elementos de Red GPON	Documentos fotográficos de fusión de fibra; Trazas reflectrómeticas del 100% de la fibra probada; Orden de pago a contratista; y, Tabla de reparaciones con valores iniciales y finales de ser el caso.	Departamento técnico

Fuente: Datos de la investigación.
Elaborador por: Autor

Actualización de la red matriz GPON

Finalmente se debe actualizar la red GPON matriz la cual reúne todos los componentes de red de la PYME, una vez actualizado esta red personal de ventas y planificación puede instalar en clientes hogar o clientes corporativos el servicio de internet. Está actualización normalmente se la hace en un software de gestión de la red GPON esto depende del proveedor con el cual trabaja la empresa proveedora de servicios de internet, puede ser programas licenciados como Netnumen u31 de ZTE, u2000 de HUAWEI o ANM2000 de FIBERHOME. ARCOTEL solicita a las empresas proveedoras de servicio de Internet la red implementada total de fibra óptica en ARGIS un software licenciado que permite organizar, gestionar, analizar y distribuir información geográfica.

Tabla 3.7 SIPOC Actualización de la red matriz GPON

S	I	P	O	C
Departamento técnico	Planos As Built; y, Plantillas de levantamiento georreferenciado de los elementos de infraestructura.	Actualización de la red matriz GPON	Archivo actualizado de la red matriz GPON	Departamento técnico

Fuente: Datos de la investigación.
Elaborador por: Autor

Una vez que se tiene conocimiento de las entradas, procesos y salidas se puede identificar al personal que participa en el subproceso, cabe destacar que este proceso sigue el marco de trabajo del PMBOK 6ed.

3.1.3.2. Participantes

A continuación se presenta la matriz de asignación de responsabilidades RACI, que define los roles, responsabilidades y autoridad del equipo de trabajo en el proyecto de ampliación de red GPON. En esta matriz se ubica en la columna las principales tareas del proceso y en las filas se ubica el personal que participa en el mismo. La forma de identificar la participación de cada persona es la siguiente:

R= Responsable; A= Aprobado; C= consultado; e I= Informado.

Tabla 3.8 Matriz RACI de participantes en el proyecto

Tareas	Roles						
	Gerente General	Director del proyecto	Técnico Líder	Técnico de fibra	Contratista	Jefe de Ventas	Ejecutivo de Compras
Definir requerimiento de ampliación de red GPON	A	C	I	I		R	
Enlistar materiales, equipos y recursos.	I	A	R	C			I
Realizar planos donde sera instalada la fibra	I	A	R	C			
Realizar Acta de inspección	I	A	R	I	C		
Efectuar acuerdos de confidencialidad	I	A	R	I	C		
Realizar Presupuesto	A	R	I			C	
Realizar tendido de fibra	I	A	I	I	R		
Efectuar planos as Built	I	A	C	C	R		
georreferenciado de los elementos de infraestructura.	I	A	R	I	C		
Documentar fotografías de fusión de fibra y elementos de infraestructura.	I	A	R	C	R		
Generar orden de Pago a contratista	I	A	R	C	I		
Realizar tabla de reparaciones con valores iniciales y finales de ser el caso.	I	A	R	C	C		
Documentar fotografías de fusión de fibra.	I	A	R	C	C		
Actualizar archivo de la red matriz GPON	I	A	R	C			

Fuente: Datos de la investigación
Elaborado por: Autor

La cantidad de personal inscrita en la matriz RACI puede variar dependiendo del tamaño de la organización además de la cantidad de departamentos que contenga. Este trabajo de investigación está enfocado en PYMES por lo cual se considera reducido el número de servidores, esto a su vez aporta a que un servidor pueda fungir más roles.

3.2. Análisis comparativo, evolución y tendencias.

3.2.1. Análisis de la encuesta

Se efectuó una encuesta a 23 PYMES proveedoras de servicio de internet con título habilitante en la ciudad de Guayaquil, los cuales fueron tomados de la encuesta realizada por el investigador en el año 2019.

Tabla 3.9 Estadística de fiabilidad.

Alfa de Cronbach	N de elementos
,764	27

Fuente: Resultado encuesta a empresarios
Elaborado por: Autor, en herramienta SPSS

Los datos proporcionados por las 23 PYMES en los 27 ítems de la encuesta fueron subidos a la herramienta SPSS para efectuar un análisis de fiabilidad de Alfa de Cronbach; siendo su resultado bueno obteniendo 0,764.

3.2.1.1. Análisis de las tres dimensiones de la variable CONFIDENCIALIDAD en los proyectos de ampliación de red GPON.

La variable independiente CONFIDENCIALIDAD mide la seguridad de la información mediante las tres dimensiones Seguridad del Cableado: El cableado que transmite datos o servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. Requisitos de seguridad en contratos con terceros: Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que tenga acceso, pueda almacenar, comunicar o proporcionar información de la infraestructura de TI. Seguridad de la información en la gestión de proyectos: La seguridad de la información debe tratarse dentro de la gestión de proyectos, de forma independiente de la naturaleza del proyecto.

Análisis de la dimensión SEGURIDAD DEL CABLEADO en función de la variable independiente CONFIDENCIALIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión SEGURIDAD DEL CABLEADO se realizó una investigación de campo, la cual radicó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en sus cableados de fibra óptica cuando son para proyectos de ampliación de red GPON.

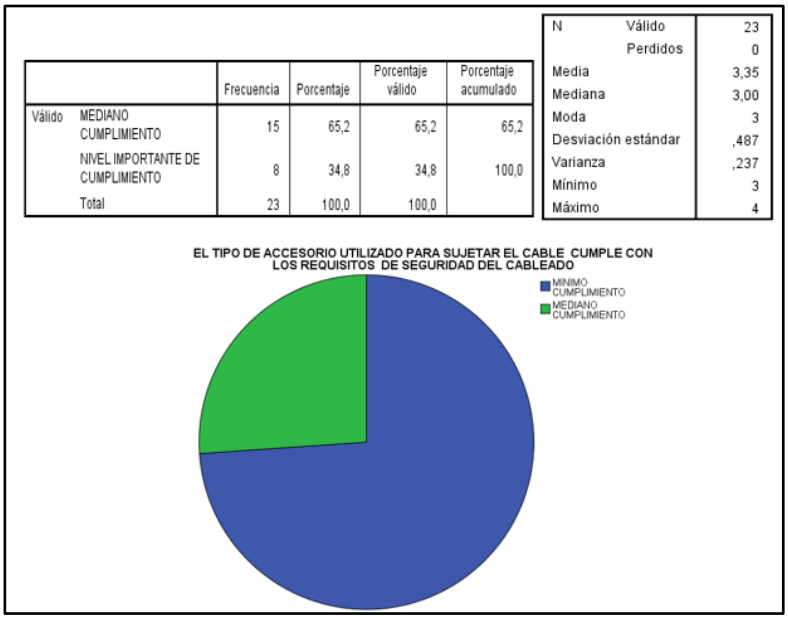
Nombre de la variable: VI01confidencialidad_SeguridadCableado

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.1 Valoración de la importancia de la seguridad del cableado (Tipo de accesorio)



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MEDIANO CUMPLIMIENTO	15	65,2	65,2	65,2
	NIVEL IMPORTANTE DE CUMPLIMIENTO	8	34,8	34,8	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,35
Mediana		3,00
Moda		3
Desviación estándar		,487
Varianza		,237
Mínimo		3
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

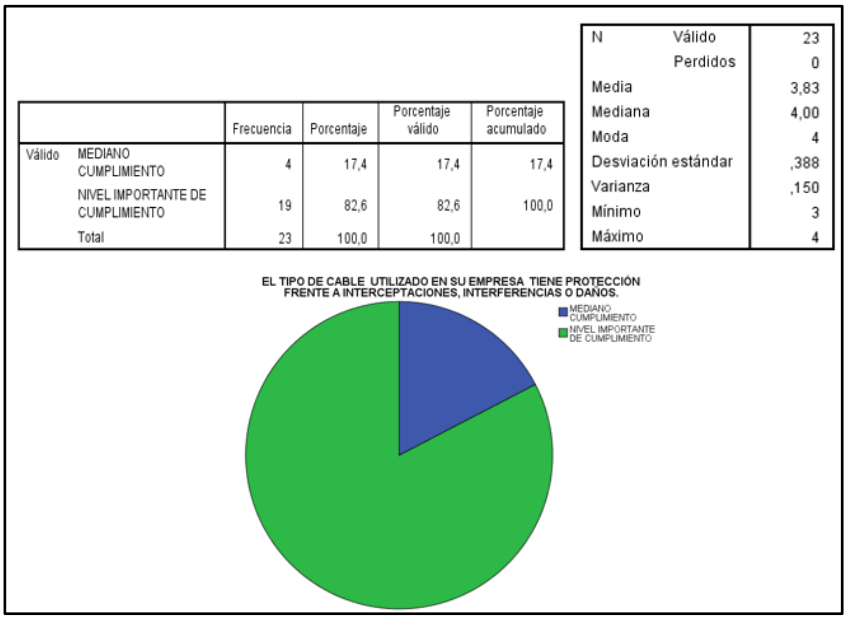
En el Gráfico 3.1 se valora la importancia de la SEGURIDAD DEL CABLEADO para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas sobre “El tipo de accesorio utilizado para

sujetar el cable cumple con los requisitos de seguridad del cableado" se encuentra una distribución según la escala de Likert de:

- 8 empresas indican un nivel importante de cumplimiento; y,
- 15 empresas un mediano cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica MEDIANO CUMPLIMIENTO y el valor máximo es de 4 puntos que indica NIVEL IMPORTANTE DE CUMPLIMIENTO. La media es de 3,35 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a un MEDIANO CUMPLIMIENTO, y representa en 65,2% referente al tipo de accesorio utilizado para sujetar el cable de fibra óptica tiene un mínimo cumplimiento con los requisitos de seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.487 respecto a la media.

Gráfico 3.2 **Valoración de la importancia de la seguridad del cableado (Tipo de *cable)***



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MEDIANO CUMPLIMIENTO	4	17,4	17,4	17,4
	NIVEL IMPORTANTE DE CUMPLIMIENTO	19	82,6	82,6	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,83
Mediana		4,00
Moda		4
Desviación estándar		,388
Varianza		,150
Mínimo		3
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.2 se valora la importancia de la SEGURIDAD DEL CABLEADO para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de

muestra de 23 empresas consultadas sobre “El tipo de cable utilizado en su empresa tiene protección frente a interceptaciones, interferencias o daños” se encuentra una distribución según la escala de Likert de:

- 19 empresas indican un nivel importante de cumplimiento; y,
- 04 empresas un mediano cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica MEDIANO CUMPLIMIENTO y el valor máximo es de 4 puntos que indica NIVEL IMPORTANTE DE CUMPLIMIENTO. La media es de 3,83 es decir el promedio se encuentra más aproximado a 4 equivalente a un NIVEL IMPORTANTE DE CUMPLIMIENTO, y representa que el 82,6% de empresas tienen un mediano cumplimento en relación al tipo de cable de fibra óptica utilizado para evitar interceptaciones, interferencias o daños referente a la seguridad de la información considerando la confidencialidad. La desviación Estándar presenta una dispersión de 0.388 respecto a la media.

Análisis de la dimensión REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS en función de la variable independiente CONFIDENCIALIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS se realizó una investigación de campo, la cual radicó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en sus contratos con terceos cuando son para proyectos de ampliación de red GPON.

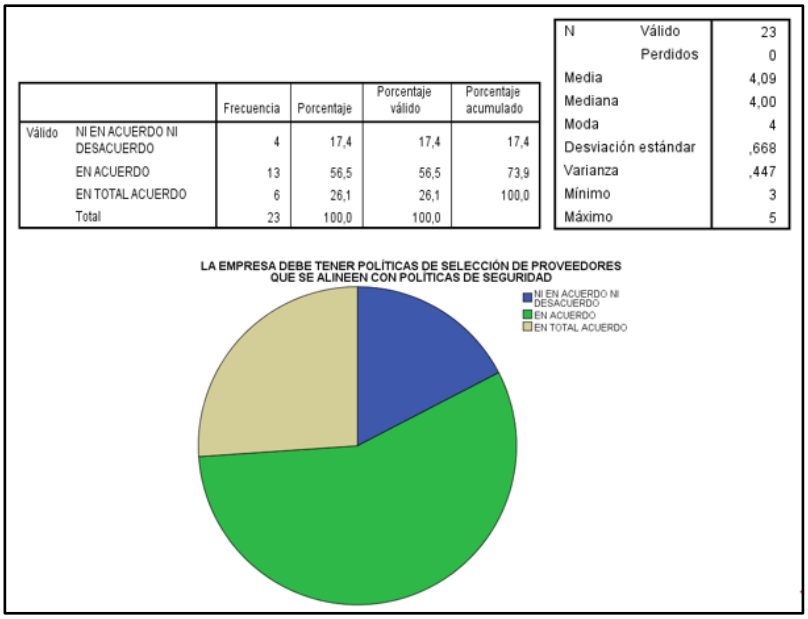
Nombre de la variable: VI01confidencialidad_SeguridadConTerceros

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.3 Valoración de la importancia de los requisitos de seguridad en contratos con terceros



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	4	17,4	17,4	17,4
	EN ACUERDO	13	56,5	56,5	73,9
	EN TOTAL ACUERDO	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		4,09
Mediana		4,00
Moda		4
Desviación estándar		,668
Varianza		,447
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

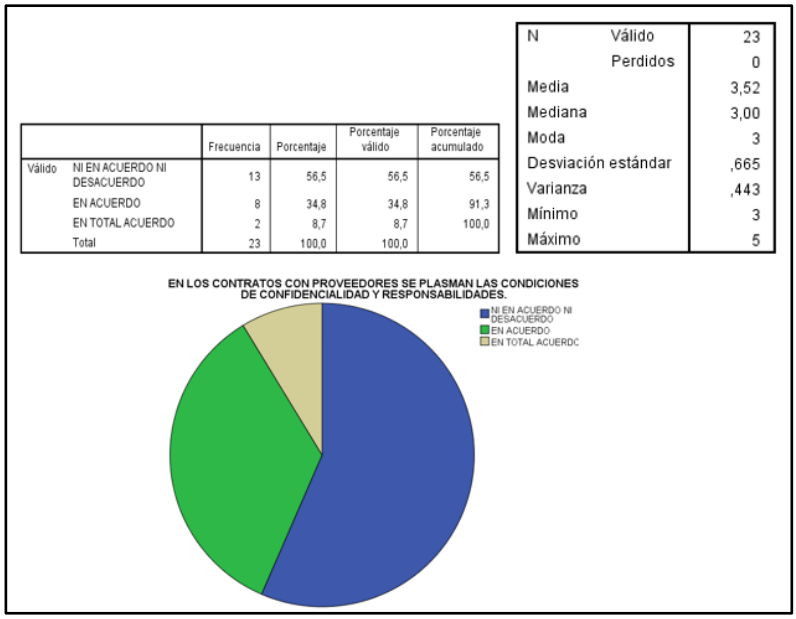
En el Gráfico 3.3 se valora la importancia de la LOS REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo sobre “La empresa debe tener políticas de selección de proveedores que se alineen con políticas de seguridad” se encuentra una distribución según la escala de Likert de:

- 4 empresas que indican que están ni en acuerdo ni desacuerdo;
- 13 empresas indica estar en acuerdo; y,
- 6 indican estar en total de acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL DE ACUERDO. La media es de 4,09 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representada que el 56,5% de empresas que están en acuerdo a la necesidad de tener políticas de selección de proveedores que se alineen con políticas de

seguridad referente a la seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.668 respecto a la media.

Gráfico 3.4 Valoración de la importancia de los requisitos de seguridad en contratos con terceros



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	13	56,5	56,5	56,5
	EN ACUERDO	8	34,8	34,8	91,3
	EN TOTAL ACUERDO	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,52
Mediana		3,00
Moda		3
Desviación estándar		,665
Varianza		,443
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

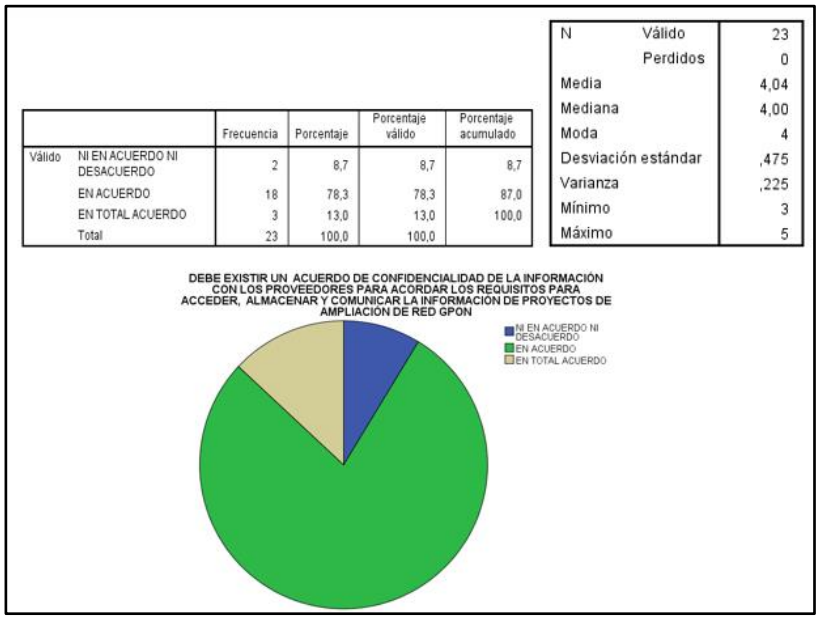
En el Gráfico 3.4 se valora la importancia de la LOS REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo sobre “En los contratos con proveedores se plasman las condiciones de confidencialidad y responsabilidades.” se encuentra una distribución según la escala de Likert de:

- 13 empresas indican estar ni en acuerdo ni desacuerdo;
- 8 empresas indican estar en acuerdo; y,
- 2 empresas indican estar en total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI EN DESACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 3,52 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a NI EN

ACUERDO NI DESACUERDO, y representa en 56,5% de empresas que les es indiferente que en los contratos con proveedores se plasman las condiciones de confidencialidad y responsabilidad referente a la seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.665 respecto a la media.

Gráfico 3.5 Valoración de la importancia de los requisitos de seguridad en contratos con terceros



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	2	8,7	8,7	8,7
	EN ACUERDO	18	78,3	78,3	87,0
	EN TOTAL ACUERDO	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		4,04
Mediana		4,00
Moda		4
Desviación estándar		,475
Varianza		,225
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.5 se valora la importancia de la LOS REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que "Debe existir un acuerdo de confidencialidad de la información con los proveedores para acordar los requerimientos para acceder, almacenar y comunicar la información de proyectos de ampliación de red GPON" se encuentra una distribución según la escala de Likert de:

- 2 empresas que indican que están ni en acuerdo ni desacuerdo.
- 18 empresas indican en acuerdo; y,
- 3 empresas indican total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 4,04 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representa 78,3% a las empresas están de acuerdo que debe existir un acuerdo de confidencialidad de la información con los proveedores para acordad los requisitos para acceder, almacenar y comunicar la información de proyectos de ampliación de red GPON referente a la seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.475 respecto a la media.

Análisis de la dimensión SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS en función de la variable independiente CONFIDENCIALIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

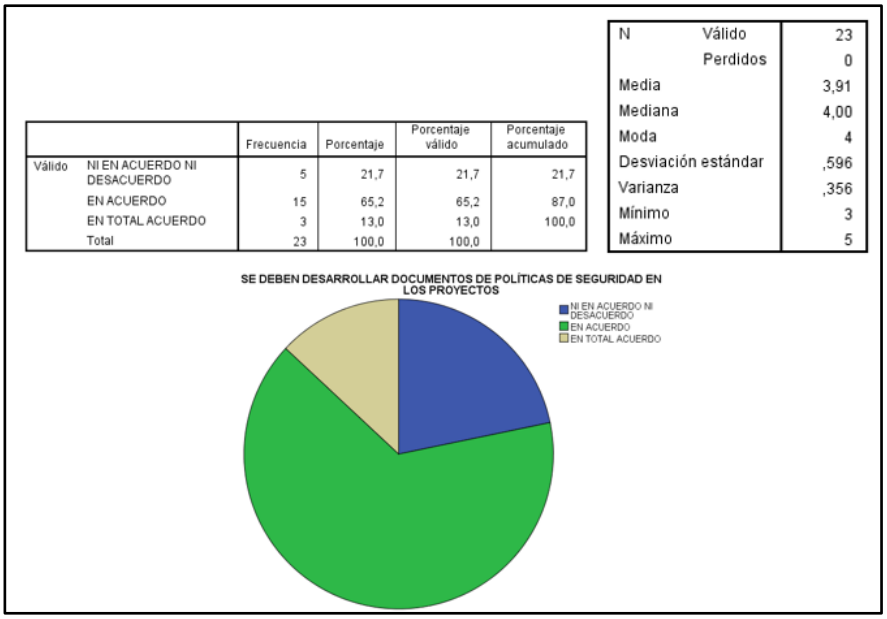
Nombre de la variable: VI01confidencialidad_SeguridadConTerceros

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.6 Valoración de la importancia de la seguridad de la información en la gestión de proyectos



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	5	21,7	21,7	21,7
	EN ACUERDO	15	65,2	65,2	87,0
	EN TOTAL ACUERDO	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,91
Mediana		4,00
Moda		4
Desviación estándar		,596
Varianza		,356
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

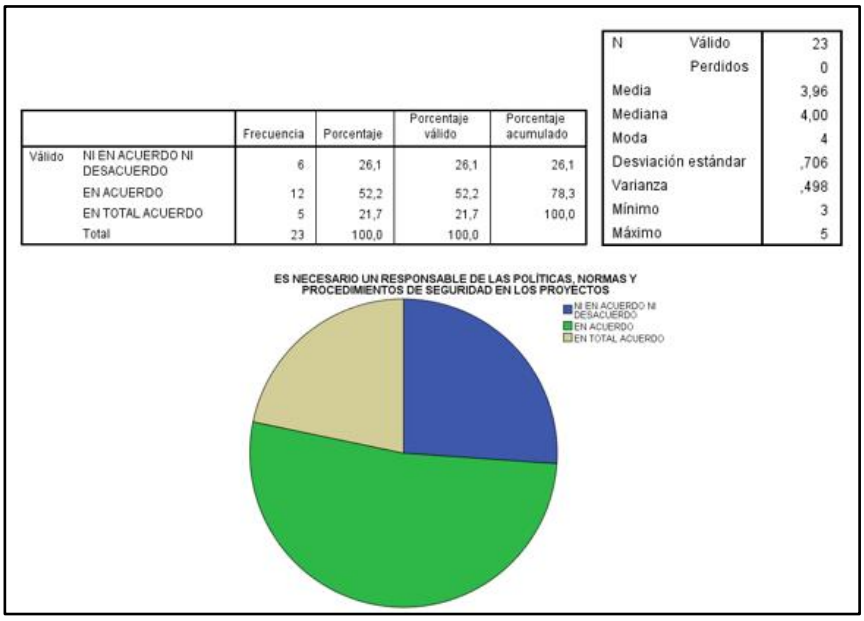
En el Gráfico 3.6 se valora la importancia de la SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Se deben desarrollar documentos de políticas de seguridad en los proyectos” se encuentra una distribución según la escala de Likert de:

- 5 empresas que indican que están ni en acuerdo ni desacuerdo,
- 15 empresas indican en acuerdo, y;
- 3 empresas en total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 3,91 es decir el promedio se encuentra más aproximado a 4 puntos equivalente EN ACUERDO, y representa 65,2% de empresas que están en acuerdo que se deben desarrollar documentos de políticas de seguridad en los proyectos referente a la seguridad

de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.596 respecto a la media.

Gráfico 3.7 Valoración de la importancia de la seguridad de la información en la gestión de proyectos



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	6	26,1	26,1	26,1
	EN ACUERDO	12	52,2	52,2	78,3
	EN TOTAL ACUERDO	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,96
Mediana		4,00
Moda		4
Desviación estándar		,706
Varianza		,498
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.7 se valora la importancia de la SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Es necesario un responsable de las políticas, normas y procedimientos de seguridad de la información” se encuentra una distribución según la escala de Likert de:

- 06 empresas indican estar ni en acuerdo ni desacuerdo;
- 12 empresas indican estar en acuerdo; y,
- 05 empresas indican en acuerdo.

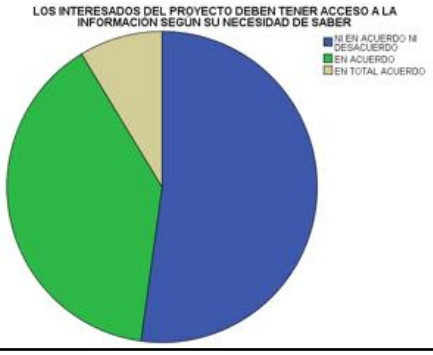
El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica EN DESACUERDO y el valor máximo es de 5 puntos que indica EN ACUERDO. La media es de 3,96 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representada en 52,2%

de las empresas les es indiferente la necesidad de un responsable de las políticas, normas y procedimientos de seguridad en los proyectos referente a la seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.706 respecto a la media.

Gráfico 3.8 Valoración de la importancia de la seguridad de la información en la gestión de proyectos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	12	52,2	52,2	52,2
	EN ACUERDO	9	39,1	39,1	91,3
	EN TOTAL ACUERDO	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,57
Mediana		3,00
Moda		3
Desviación estándar		,662
Varianza		,439
Mínimo		3
Máximo		5



Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.8 se valora la importancia de la SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Los interesados del proyecto deben tener acceso a la información según su necesidad de saber” se encuentra una distribución según la escala de Likert de:

- 12 empresas que indican estar ni en acuerdo ni desacuerdo;
- 9 empresas indican estar ni en acuerdo ni desacuerdo; y,
- 2 empresas indican en acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos

que indica EN TOTAL ACUERDO. La media es de 3,57 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a NI EN ACUERDO NI DESACUERDO y representada en 52,2% de empresas son indiferentes a que los interesados del proyecto deben tener acceso a la información según su necesidad de saber referente a la seguridad de la información considerando la confidencialidad. La desviación estándar presenta una dispersión de 0.662 respecto a la media.

3.2.1.2. Análisis de las tres dimensiones de la variable INTEGRIDAD en los proyectos de ampliación de red GPON.

La variable independiente INTEGRIDAD mide la seguridad de la información mediante las tres dimensiones RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN: Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. RESPONSABILIDADES DE GESTIÓN: La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. ACCESO A LA REDES Y A LOS SERVICIOS DE RED. Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

Análisis de la dimensión RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN en función de la variable independiente INTEGRIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

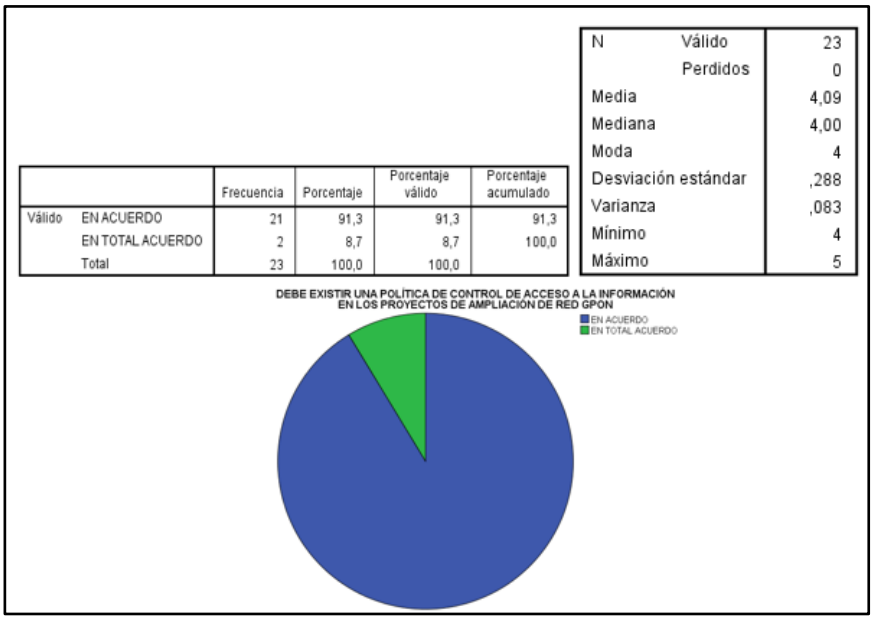
Nombre de la variable: VI02integridad_Restricción

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.9 Restricción del acceso a la información



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	EN ACUERDO	21	91,3	91,3	91,3
	EN TOTAL ACUERDO	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		4,09
Mediana		4,00
Moda		4
Desviación estándar		,288
Varianza		,083
Mínimo		4
Máximo		5

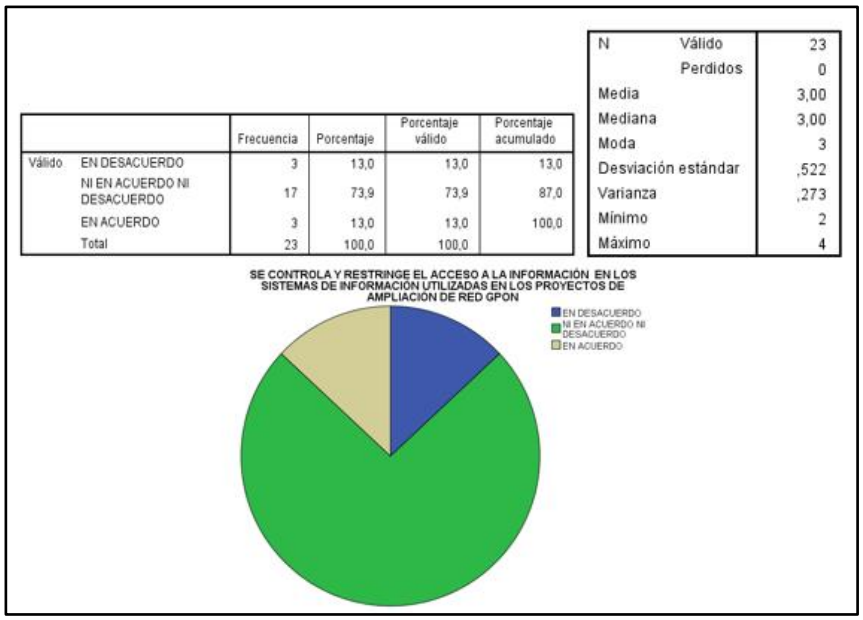
Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.9 se valora la importancia de la RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Debe existir una política de control de acceso a la información en los proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 21 empresas indican estar en acuerdo; y,
- 2 empresas indican en total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 4 puntos que indica EN ACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 4,09 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representa 91,3% de empresas que consideran que debe existir una política de control de acceso a la información referente a la seguridad de la información considerando la integridad. La desviación estándar presenta una dispersión de 0.288 respecto a la media.

Gráfico 3.10 Restricción del acceso a la información



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	EN DESACUERDO	3	13,0	13,0	13,0
	NI EN ACUERDO NI DESACUERDO	17	73,9	73,9	87,0
	EN ACUERDO	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,00
Mediana		3,00
Moda		3
Desviación estándar		,522
Varianza		,273
Mínimo		2
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

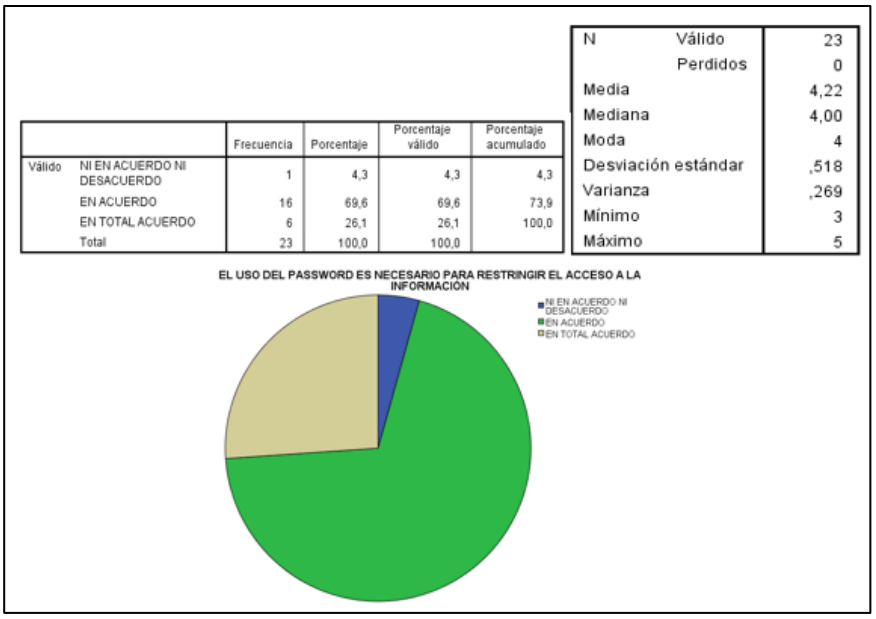
En el Gráfico 3.10 se valora la importancia de la RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Se controla y restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 03 empresas que indican estar en desacuerdo,
- 16 empresas indican estar en ni en acuerdo ni en desacuerdo; y,
- 03 empresas que indican estar en acuerdo.

El valor mínimo encontrado según la escala de Likert es de 2 punto que indica EN DESACUERDO y el valor máximo es de 4 puntos que indica EN ACUERDO. La media es de 3,00 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a NI EN ACUERDO NI DESACUERDO, y representa 79,9% está en desacuerdo que se controle y restringe el acceso a la información en los sistemas de información utilizados en los proyectos de ampliación de red GPON referente a la seguridad de la información

considerando la integridad. La desviación estándar presenta una dispersión de 0.522 respecto a la media.

Gráfico 3.11 Restricción del acceso a la información



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	1	4,3	4,3	4,3
	EN ACUERDO	16	69,6	69,6	73,9
	EN TOTAL ACUERDO	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		4,22
Mediana		4,00
Moda		4
Desviación estándar		,518
Varianza		,269
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.11 se valora la importancia de la RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “El uso del password es necesario para restringir el acceso a la información” se encuentra una distribución según la escala de Likert de:

- 1 empresas que indican estar ni en acuerdo ni desacuerdo;
- 16 empresas indican estar en acuerdo; y,
- 6 empresas indican estar en total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos que indica EN ACUERDO. La media es de 4,22 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representa 69,6% de empresas indiferentes en el uso del password necesario para restringir el acceso a la información a que referente a la seguridad de la

información considerando la integridad. La desviación estándar presenta una dispersión de 0.518 respecto a la media.

Análisis de la dimensión RESPONSABILIDADES DE GESTIÓN en función de la variable independiente INTEGRIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión RESPONSABILIDADES DE GESTIÓN se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

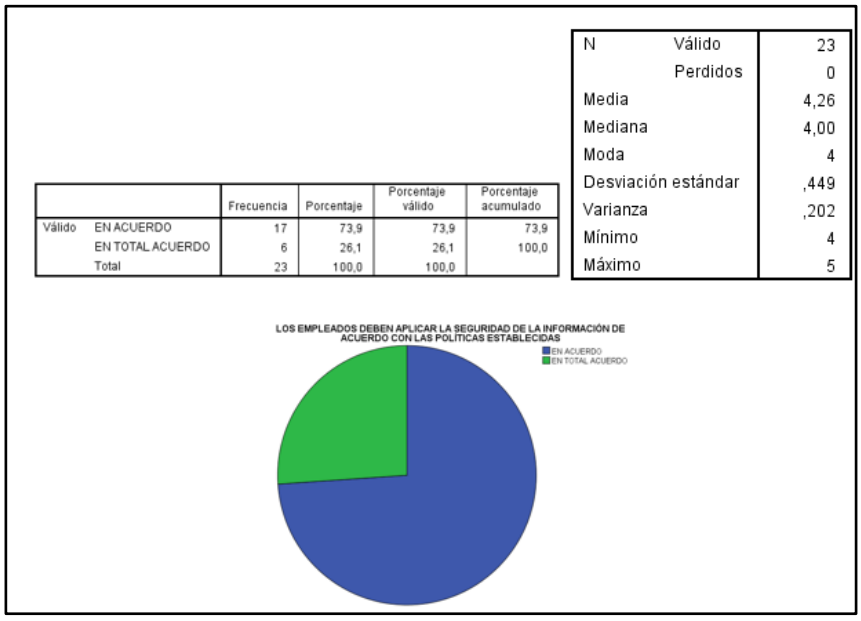
Nombre de la variable: VI02 integridad_responsabilidades

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.12 Valoración de responsabilidades de gestión



Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.12 se valora la importancia de la VALORACION DE RESPONSABILIDADES DE GESTIÓN para los proyectos de ampliación de

red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Es necesario establecer una política de control de accesos para los proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 17 empresas indican están en acuerdo; y,
- 6 empresas indican estar en total acuerdo.

El valor mínimo encontrado según la escala de Likert es de 4 puntos que indica EN ACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 4,26 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representa en 73,9% que las empresa consideran indiferente la necesidad de establecer una política de control de Accesos para los proyectos de ampliación de red GPON referente a la seguridad de la información considerando la integridad. La desviación estándar presenta una dispersión de 0.449 respecto a la media.

Análisis de la dimensión ACCESO A LA REDES Y A LOS SERVICIOS DE RED en función de la variable independiente INTEGRIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión ACCESO A LA REDES Y A LOS SERVICIOS DE RED se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

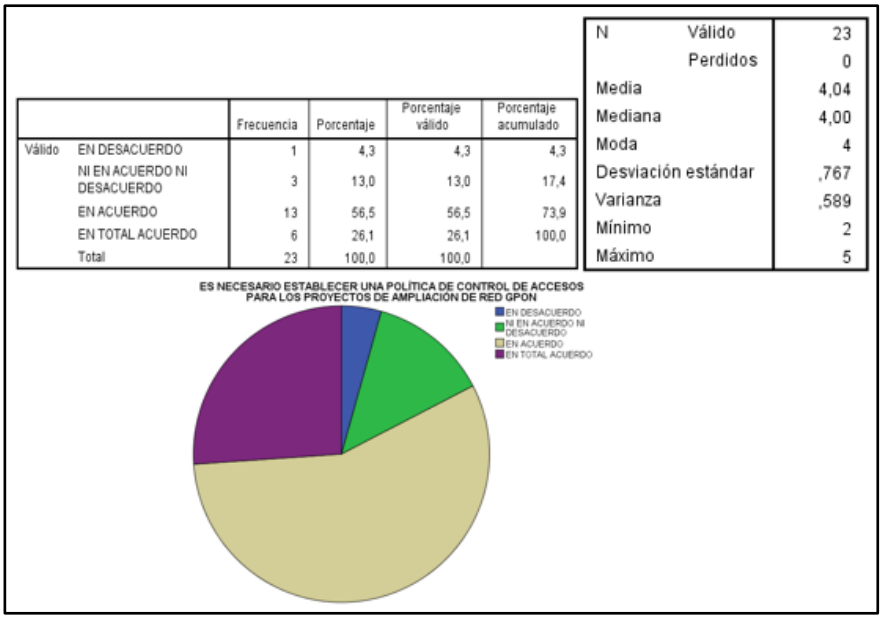
Nombre de la variable: VI02integridad_Acceso_Redes

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

***Gráfico 3.13 Valoración de la importancia* del acceso a la redes y a los servicios de red**



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	EN DESACUERDO	1	4,3	4,3	4,3
	NI EN ACUERDO NI DESACUERDO	3	13,0	13,0	17,4
	EN ACUERDO	13	56,5	56,5	73,9
	EN TOTAL ACUERDO	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		4,04
Mediana		4,00
Moda		4
Desviación estándar		,767
Varianza		,589
Mínimo		2
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

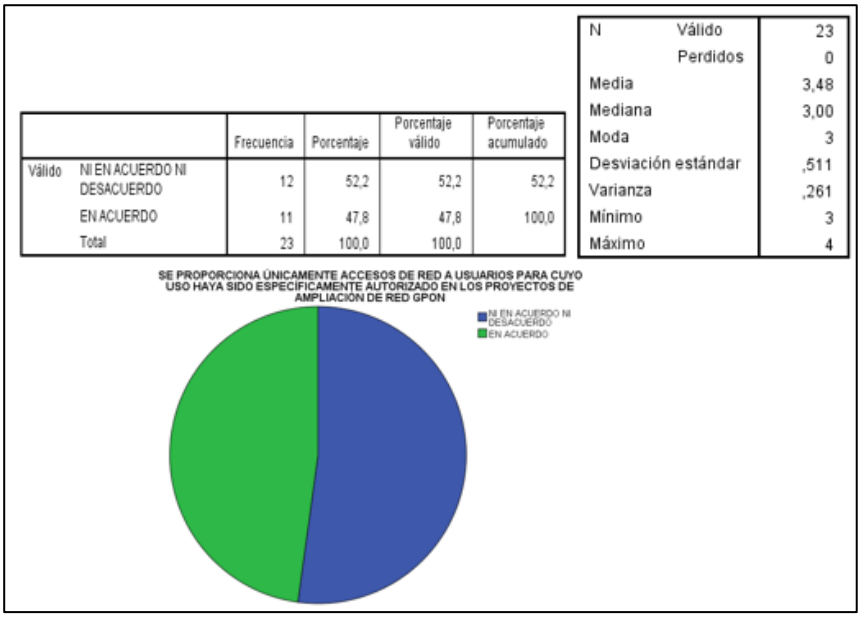
En el Gráfico 3.13 se valora la importancia de la VALORACION DE RESPONSABILIDADES DE GESTIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo que “Los interesados del proyecto deben tener acceso a la información según su necesidad de saber” se encuentra una distribución según la escala de Likert de:

- 1 empresa que indican estar en desacuerdo;
- 3 empresas que indican estar ni en acuerdo ni desacuerdo;
- 13 empresas indican estar en acuerdo; y,
- 6 empresas indican estar en desacuerdo.

El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 5 puntos que indica EN TOTAL ACUERDO. La media es de 4,04 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a EN ACUERDO, y representa en 56,5% de las empresas consideran indiferente que los

empleados deban aplicar la seguridad de la información de acuerdo con las políticas establecidas referente a la seguridad de la información considerando la integridad. La desviación estándar presenta una dispersión de 0.767 respecto a la media.

Gráfico 3.14 Valoración de la importancia del acceso a la redes y a los servicios de red



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NI EN ACUERDO NI DESACUERDO	12	52,2	52,2	52,2
	EN ACUERDO	11	47,8	47,8	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,48
Mediana		3,00
Moda		3
Desviación estándar		,511
Varianza		,261
Mínimo		3
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.14 se valora la importancia de la VALORACION DE RESPONSABILIDADES DE GESTIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que “Se proporcione únicamente acceso de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 12 empresas que indican estar ni en acuerdo ni desacuerdo; y,
- 11 empresas indican estar en acuerdo.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica NI EN ACUERDO NI DESACUERDO y el valor máximo es de 4 puntos que indica EN ACUERDO. La media es de 3,48 es decir el promedio se

encuentra más aproximado a 3 puntos equivalente a NI EN ACUERDO NI DESACUERDO, y representa en 52,2% a empresas que consideran indiferente que a se proporcione únicamente acceso de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON referente a la seguridad de la información considerando la integridad. La desviación estándar presenta una dispersión de 0.511 respecto a la media.

3.2.1.3. Análisis de las tres dimensiones de la variable DISPONIBILIDAD en los proyectos de ampliación de red GPON.

La variable independiente DISPONIBILIDAD mide la seguridad de la información mediante las tres dimensiones INVENTARIO DE ACTIVOS: Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse el inventario. DOCUMENTACION DE PROCEDIMIENTOS DE LA OPERACIÓN: Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten. COPIAS DE SEGURIDAD DE LA INFORMACIÓN: Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

Análisis de la dimensión INVENTARIO DE ACTIVOS en función de la variable independiente DISPONIBILIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión INVENTARIO DE ACTIVOS se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

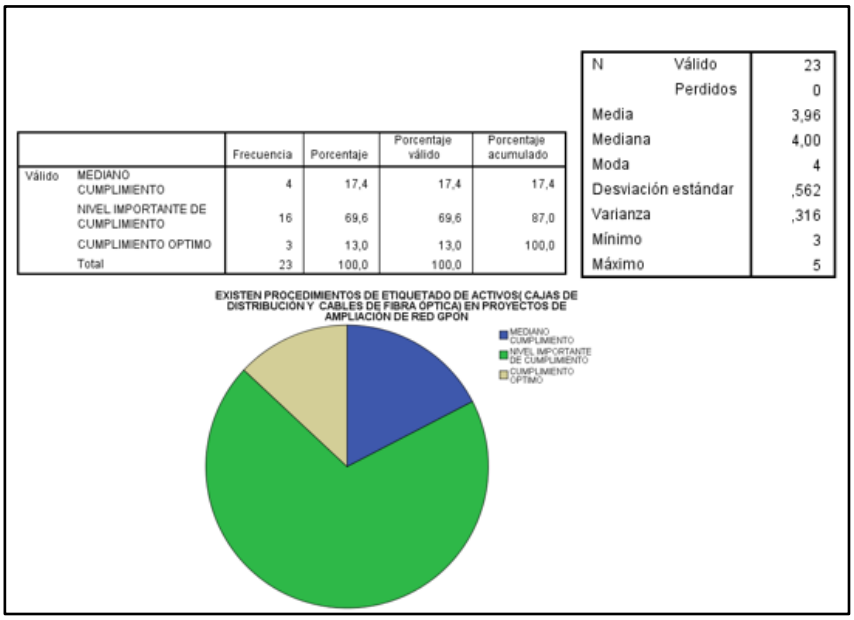
Nombre de la variable: VI03disponibilidad_Inventario_Activos

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.15 Valoración de la importancia inventario de activos



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MEDIANO CUMPLIMIENTO	4	17,4	17,4	17,4
	NIVEL IMPORTANTE DE CUMPLIMIENTO	16	69,6	69,6	87,0
	CUMPLIMIENTO OPTIMO	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,96
Mediana		4,00
Moda		4
Desviación estándar		,562
Varianza		,316
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.15 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA INVENTARIO DE ACTIVOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que “Existen procedimientos de etiquetado de activos (Cajas de distribución y cables de fibra óptica) en proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 4 empresas indican estar en mediano cumplimiento;
- 16 empresas indican estar en nivel importante de cumplimiento; y,
- 3 empresas indican estar en cumplimiento óptimo.

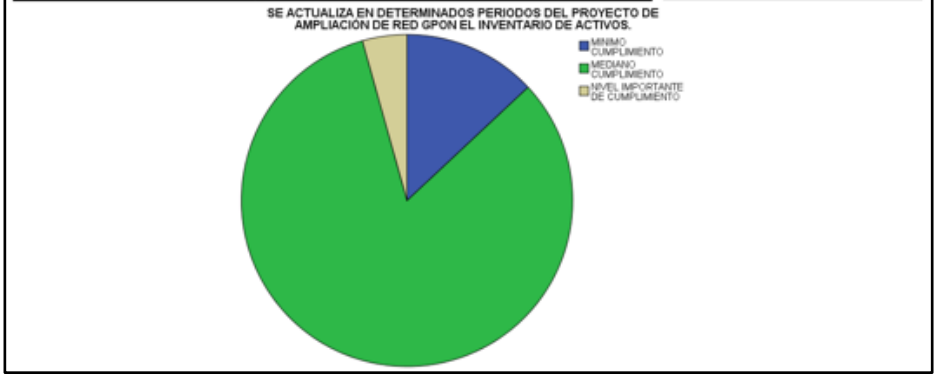
El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica MEDIANO CUMPLIMIENTO y el valor máximo es de 5 puntos que indica CUMPLIMIENTO ÓPTIMO. La media es de 3,96 es decir el promedio se encuentra más aproximado a 4 puntos equivalente a MINIMO CUMPLIMIENTO, y representa en 69,6% empresas que tienen un mínimo cumplimiento en la existencia de procedimientos de etiquetado de activos

(Cajas de distribución y cables de fibra óptica) en proyectos de ampliación de red GPON referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.562 respecto a la media.

Gráfico 3.16 Valoración de la importancia inventario de activos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MINIMO CUMPLIMIENTO	3	13,0	13,0	13,0
	MEDIANO CUMPLIMIENTO	19	82,6	82,6	95,7
	NIVEL IMPORTANTE DE CUMPLIMIENTO	1	4,3	4,3	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		2,91
Mediana		3,00
Moda		3
Desviación estándar		,417
Varianza		,174
Mínimo		2
Máximo		4



Fuente: Recolección de datos de la investigación
Elaborado por: Autor

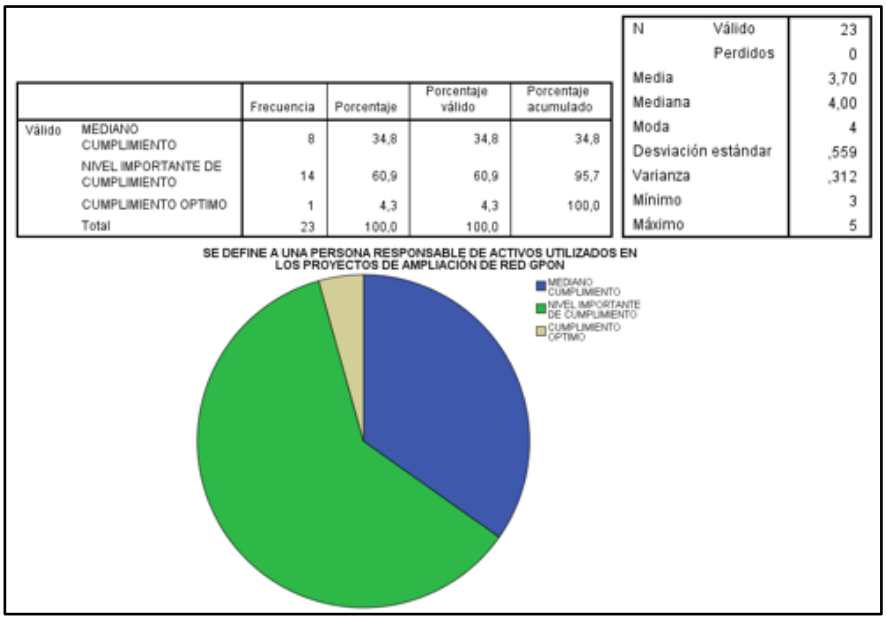
En el Gráfico 3.16 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA INVENTARIO DE ACTIVOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que "Se actualiza en determinados periodos del proyecto de ampliación de red GPON el inventario de activos" se encuentra una distribución según la escala de Likert de:

- 3 empresas que indican mínimo cumplimiento;
- 19 empresas que indican mediano cumplimiento y,
- 1 empresas indican nivel importante de cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica MÍNIMO CUMMPLIMIENTO y el valor máximo es de 4 puntos que indica el NIVEL IMPORTANTE CUMPLIMIENTO. La media es de 2,91 es decir el

promedio se encuentra más aproximado a 3 puntos equivalente a MEDIANO CUMPLIMIENTO, y representa en 82,6% empresas tienen un mínimo cumplimento en actualizar en determinados periodos del proyecto el inventario de activos referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.417 respecto a la media.

Gráfico 3.17 Valoración de la importancia inventario de activos



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MEDIANO CUMPLIMIENTO	8	34,8	34,8	34,8
	NIVEL IMPORTANTE DE CUMPLIMIENTO	14	60,9	60,9	95,7
	CUMPLIMIENTO OPTIMO	1	4,3	4,3	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,70
Mediana		4,00
Moda		4
Desviación estándar		,559
Varianza		,312
Mínimo		3
Máximo		5

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.17 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA INVENTARIO DE ACTIVOS para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que “Se define a una persona responsable de activos utilizados en los proyectos de ampliación de red GPON” se encuentra una distribución según la escala de Likert de:

- 10 empresas indican mínimo cumplimiento; y,
- 13 empresas indican mediano cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica MÍNIMO CUMPLIMIENTO y el valor máximo es de 3 puntos que indica MEDIANO CUMPLIMIENTO. La media es de 2,57 es decir el promedio se

encuentra más aproximado a 3 puntos equivalente a MEDIANO CUMPLIMIENTO, y representa en 56,5% empresas tienen un mediano cumplimiento en definir a una persona responsable de activos utilizados en los proyectos de ampliación de red GPON referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.507 respecto a la media.

Análisis de la dimensión DOCUMENTACION DE PROCEDIMIENTOS DE LA OPERACIÓN en función de la variable independiente DISPONIBILIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión DOCUMENTACIÓN DE PROCEDIMIENTOS DE LA OPERACIÓN se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

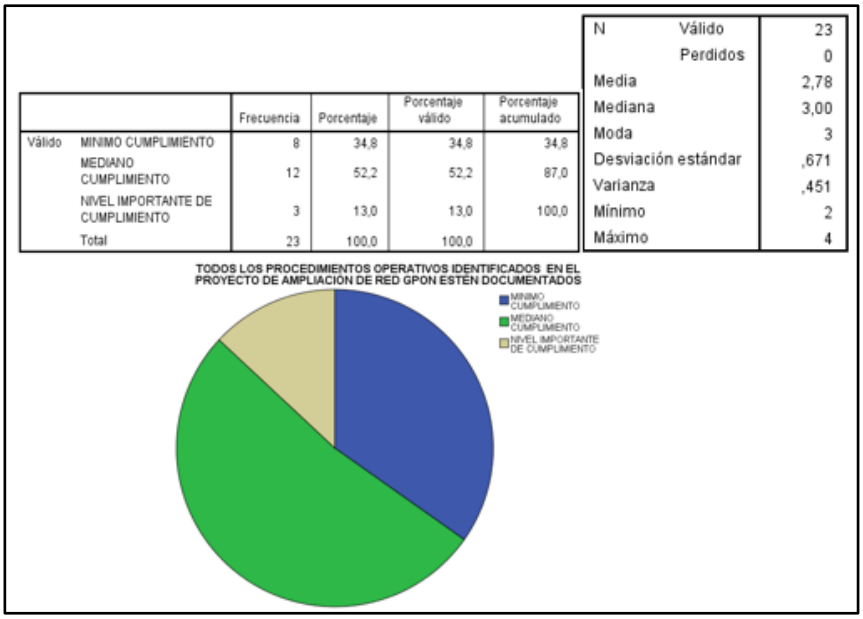
Nombre de la variable: VI03disponibilidad_Doc_Procedimientos

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.18 Valoración de la importancia de la documentación de procedimientos de la operación



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MINIMO CUMPLIMIENTO	8	34,8	34,8	34,8
	MEDIANO CUMPLIMIENTO	12	52,2	52,2	87,0
	NIVEL IMPORTANTE DE CUMPLIMIENTO	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		2,78
Mediana		3,00
Moda		3
Desviación estándar		,671
Varianza		,451
Mínimo		2
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.18 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA DE LA DOCUMENTACIÓN DE PROCEDIMIENTOS DE LA OPERACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que “Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON estén documentados” se encuentra una distribución según la escala de Likert de:

- 8 empresas indican que hay mínimo cumplimiento;
- 12 empresas indican un mediano cumplimento; y,
- 3 empresas indican un nivel de importante cumplimiento.

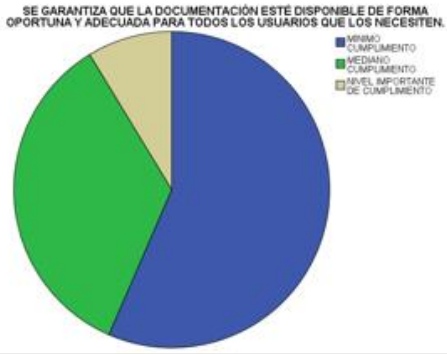
El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica HAY MÍNIMO CUMPLIMIENTO y el valor máximo es de 4 puntos que indica MEDIANO CUMPLIMIENTO. La media es de 2,78 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a MEDIANO CUMPLIMIENTO, y representa en 52,2% a Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON estén

documentados referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.671 respecto a la media.

Gráfico 3.19 Valoración de la importancia de la documentación de procedimientos de la operación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MINIMO CUMPLIMIENTO	13	56,5	56,5	56,5
	MEDIANO CUMPLIMIENTO	8	34,8	34,8	91,3
	NIVEL IMPORTANTE DE CUMPLIMIENTO	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		2,52
Mediana		2,00
Moda		2
Desviación estándar		,665
Varianza		,443
Mínimo		2
Máximo		4



Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.19 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA DE LA DOCUMENTACIÓN DE PROCEDIMIENTOS DE LA OPERACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que "se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que lo necesiten" se encuentra una distribución según la escala de Likert de:

- 13 empresas que indican hay mínimo cumplimiento,
- 8 empresas indican un mediano cumplimiento; y,
- 2 empresas indican un nivel importante de cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica HAY MÍNIMO CUMPLIMIENTO y el valor máximo es de 4 puntos que

indica NIVEL IMPORTANTE DE CUMPLIMIENTO. La media es de 2,52 es decir el promedio se encuentra más aproximado a 2 puntos equivalente a que HAY MÍNIMO CUMPLIMIENTO, y representa en 56,5% que se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que lo necesiten referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.665 respecto a la media.

Análisis de la dimensión COPIAS DE SEGURIDAD DE LA INFORMACIÓN en función de la variable independiente DISPONIBILIDAD en los proyectos de ampliación de red GPON.

Para el análisis de la dimensión COPIAS DE SEGURIDAD DE LA INFORMACIÓN se realizó una investigación de campo, la cual se fundamentó en ejecutar una encuesta basada en los datos de la investigación referentes a los aspectos principales de seguridad implementado por las PYMES en la seguridad de la información dentro de la gestión de proyectos aplicados a proyectos de ampliación de red GPON.

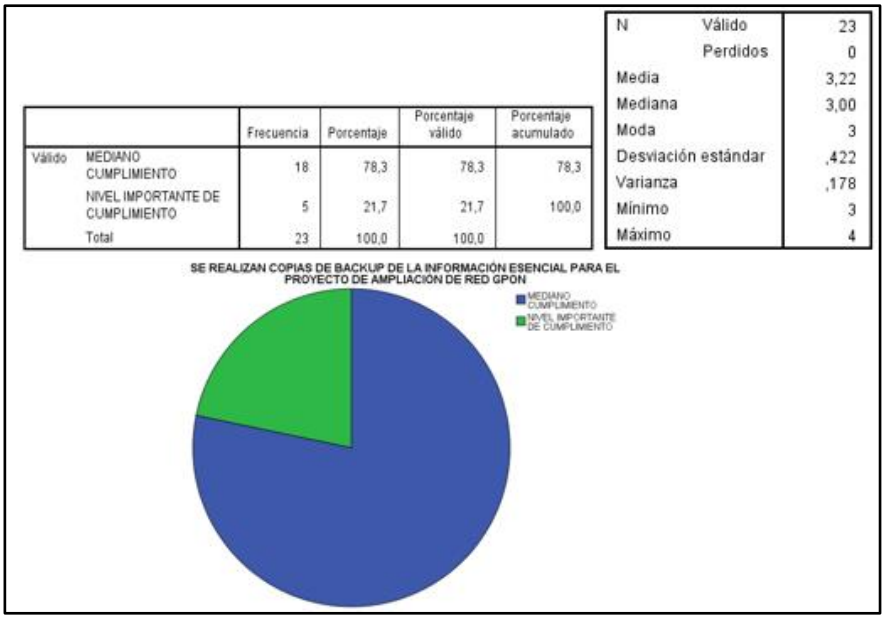
Nombre de la variable: VI03disponibilidad_Copias_Seguridad

Técnica de investigación: Recolección de campo

Instrumento: Encuesta

Fuente: Primaria

Gráfico 3.20 Valoración de la importancia de copias de seguridad de la información



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MEDIANO CUMPLIMIENTO	18	78,3	78,3	78,3
	NIVEL IMPORTANTE DE CUMPLIMIENTO	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		3,22
Mediana		3,00
Moda		3
Desviación estándar		,422
Varianza		,178
Mínimo		3
Máximo		4

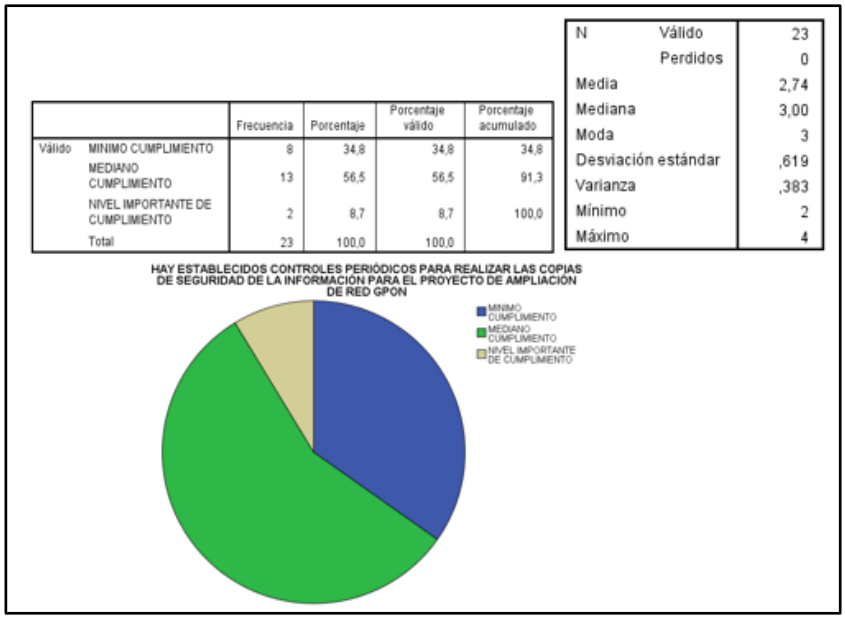
Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.20 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que "Se realizan copias de backup de la información esencial para el proyecto de ampliación de red GPON" se encuentra una distribución según la escala de Likert de:

- 18 empresas indican mediano cumplimiento; y,
- 5 personas indican nivel importante de cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 3 puntos que indica HAY MEDIANO CUMPLIMIENTO y el valor máximo es de 4 puntos que indica NIVEL IMPORTANTE DE CUMPLIENTO. La media es de 3,22 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a MEDIANO CUMPLIMIENTO, y representa en 78,3% a Se realizan copias de backup de la información esencial para el proyecto de ampliación de red GPON referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.422 respecto a la media.

Gráfico 3.21 Valoración de la importancia de copias de seguridad de la información



		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	MINIMO CUMPLIMIENTO	8	34,8	34,8	34,8
	MEDIANO CUMPLIMIENTO	13	56,5	56,5	91,3
	NIVEL IMPORTANTE DE CUMPLIMIENTO	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

N	Válido	23
	Perdidos	0
Media		2,74
Mediana		3,00
Moda		3
Desviación estándar		,619
Varianza		,383
Mínimo		2
Máximo		4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

En el Gráfico 3.21 se valora la importancia de la VALORACIÓN DE LA IMPORTANCIA DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN para los proyectos de ampliación de red GPON, basándose en las recomendaciones y controles de la Norma ISO/IEC 27001:2013. De un total de muestra de 23 empresas consultadas si están de acuerdo en que "Hay establecidos controles periódicos para realizar las copias de seguridad de la información para el proyecto de ampliación de red GPON" se encuentra una distribución según la escala de Likert de:

- 8 empresas que indican mínimo cumplimiento; y,
- 13 empresas indican mediano cumplimiento; y,
- 2 empresas indican nivel importante de cumplimiento.

El valor mínimo encontrado según la escala de Likert es de 2 puntos que indica MÍNIMO CUMPLIMIENTO y el valor máximo es de 4 puntos que indica un NIVEL IMPORTANTE CUMPLIMIENTO. La media es de 2,74 es decir el promedio se encuentra más aproximado a 3 puntos equivalente a MEDIANO CUMPLIMIENTO, y representa en 56,5% a Hay establecidos controles periódicos para realizar las copias de seguridad de la información para el

proyecto de ampliación de red GPON referente a la seguridad de la información considerando la disponibilidad. La desviación estándar presenta una dispersión de 0.619 respecto a la media.

3.2.2. Correlación de las variables cualitativas

Las variables identificadas para el estudio correlativo responde a la necesidad de evidenciar el nivel de asociación entre ítem: “el uso de password para restringir el acceso a la información” y el ítem: “se proporcionada únicamente accesos de red a usuarios autorizados” debido a la contradicción que existe entre los resultados ya que el 69,6% de los encuestados indica que está de acuerdo en que el uso de password es necesario para restringir el acceso de la información mientras que sólo un 47,8% de los encuestados indicó estar de acuerdo en que se proporcione únicamente accesos de red a usuarios para cuyo uso haya sido específicamente autorizado.

En el segundo estudio correlativo descrito en la sección 3.2.2.2 se justifica debido a que el ítem “se deben desarrollar documentos de políticas de seguridad en los proyectos” presentó un 65,2% de los encuestados en estar de acuerdo mientras que el ítem “Se controla y se restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON” presentó un 73,9% de los encuestados indicó no estar de acuerdo ni en desacuerdo es decir existe una indiferencia total ante esta consulta.

3.2.2.1. Correlación del ítem “Uso del password es necesario para restringir el acceso a la información” con el ítem “Se proporciona únicamente accesos de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON”.

Se establece la asociación aplicando tablas de contingencia o tablas cruzadas para las variables cualitativas en este ejemplo el “uso del password” y “se proporciona únicamente accesos de red a usuarios autorizados”, tal como se muestra en la siguiente gráfica:

Gráfico 3.22 Nivel de asociación entre variables

EL USO DEL PASSWORD ES NECESARIO PARA RESTRINGIR EL ACCESO A LA INFORMACIÓN *SE PROPORCIONA ÚNICAMENTE ACCESOS DE RED A USUARIOS PARA CUYO USO HAYA SIDO ESPECÍFICAMENTE AUTORIZADO EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON tabulación cruzada

			SE PROPORCIONA ÚNICAMENTE ACCESOS DE RED A USUARIOS PARA CUYO USO HAYA SIDO ESPECÍFICAMENTE AUTORIZADO EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON		
			NI EN ACUERDO NI DESACUERDO	EN ACUERDO	Total
EL USO DEL PASSWORD ES NECESARIO PARA RESTRINGIR EL ACCESO A LA INFORMACIÓN	NI EN ACUERDO NI DESACUERDO	Recuento	0	1	1
		% del total	0,0%	4,3%	4,3%
	EN ACUERDO	Recuento	10	6	16
		% del total	43,5%	26,1%	69,6%
	EN TOTAL ACUERDO	Recuento	2	4	6
		% del total	8,7%	17,4%	26,1%
Total		Recuento	12	11	23
		% del total	52,2%	47,8%	100,0%

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

El **¡Error! No se encuentra el origen de la referencia.** determina el grado de asociación lineal, entre el uso de *password* si es necesario para restringir el acceso a la información y se proporciona únicamente accesos de red a usuarios autorizados.

CHI CUADRADO.- El estadístico observado 2,628 en el Gráfico 3.22 se presenta una distribución de dos grados de libertad (gl=2) con una probabilidad de asociación de significancia de 0,269 lo que informa que existe una relación de independencia entre el uso de *password* y con que se proporciona únicamente accesos de red a usuarios autorizados.

Gráfico 3.22 Prueba de Chi Cuadrado sobre datos de variables categóricas.

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	2,628[a]	2	,269
Razón de verosimilitud	3,033	2	,219
Asociación lineal por lineal	,240	1	,624
N de casos válidos	23		

a. 4 casillas (66,7%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,48.

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

COEFICIENTE DE CONTINGENCIA C (KARL PEARSON).- Este medida sirve para calcular el grado de aceptación de asociación de dos conjuntos en la escala nominal en la tabla cruzada tomando valores de 0 a 1. El valor de 1 indica que existe asociación de la variable y el 0 señala que existe independencia de la variable por lo tanto mientras exista un valor cercano a 1 mayor será la intensidad entre variables.

Gráfico 3.23 Nivel de asociación coeficiente de contingencia

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	Coeficiente de contingencia	,320	,269
N de casos válidos		23	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el Gráfico 3.23 se observa que no existe una relación fuerte debido a que el valor resultante es de 0.320 que se encuentra en la zona de aceptación entre la el uso de password y con que se proporciona únicamente accesos de red a usuarios autorizados.

COEFICIENTE DE CRAMER.- Mide el nivel asociación de variables nominales o cualitativas cuando las categorías varían de dos a tres clases. El valor puede ser entre 0 y 1.

Gráfico 3.24 Nivel asociación del coeficiente de Cramer

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	Phi	,338	,269
	V de Cramer	,338	,269
N de casos válidos		23	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el Gráfico 3.24 se observa una asociación débil y que existe independencia de las variables por el valor de 0,338 que está más cercano a cero que a uno.

COEFICIENTE PHI.- Este tipo de correlación no se aplica debido a que la asociación es para variables de tipo binario.

3.2.2.2. Correlación del ítem "Se deben desarrollar documentos de políticas de seguridad en los proyectos" con el ítem "Se controla y se restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON".

Se establece la asociación aplicando tablas de contingencia para variables cualitativas "se deben desarrollar documentos de políticas de seguridad en los proyectos" y "se controla y se restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON":

Gráfico 3.25 Nivel de asociación entre variables

SE DEBEN DESARROLLAR DOCUMENTOS DE POLÍTICAS DE SEGURIDAD EN LOS PROYECTOS *SE CONTROLA Y RESTRINGE EL ACCESO A LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN UTILIZADAS EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON tabulación cruzada

			SE CONTROLA Y RESTRINGE EL ACCESO A LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN UTILIZADAS EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON			
			EN DESACUERDO	NI EN ACUERDO NI DESACUERDO	EN ACUERDO	Total
SE DEBEN DESARROLLAR DOCUMENTOS DE POLÍTICAS DE SEGURIDAD EN LOS PROYECTOS	NI EN ACUERDO NI DESACUERDO	Recuento	1	4	0	5
		% del total	4,3%	17,4%	0,0%	21,7%
	EN ACUERDO	Recuento	1	13	1	15
		% del total	4,3%	56,5%	4,3%	65,2%
	EN TOTAL ACUERDO	Recuento	1	0	2	3
		% del total	4,3%	0,0%	8,7%	13,0%
Total		Recuento	3	17	3	23
		% del total	13,0%	73,9%	13,0%	100,0%

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

El Gráfico 3.25 determina el grado de asociación lineal, se deben desarrollar documentos de políticas de seguridad en los proyectos y se controla y se restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON.

Gráfico 3.26 Prueba De Chi Cuadrado Sobre Datos Variables Categóricas.

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	11,906[a]	4	,018
Razón de verosimilitud	11,344	4	,023
Asociación lineal por lineal	1,874	1	,171
N de casos válidos	23		

a. 8 casillas (88,9%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,39.

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

Gráfico 3.27 Nivel De Asociación Coeficiente De Contingencia

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	Coeficiente de contingencia	,584	,018
N de casos válidos		23	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el Gráfico 3.27 se observa que existe una relación relativamente fuerte debido a que el valor resultante es de 0.584 que se encuentra en la zona de asociación entre que se deben desarrollar documentos de políticas de seguridad con que se controla y restringe el acceso a la información en los sistemas de información.

Gráfico 3.28 Nivel de asociación coeficiente de CRAMER

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	Phi	,719	,018
	V de Cramer	,509	,018
N de casos válidos		23	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el Gráfico 3.28 se observa una asociación relativamente fuerte y que existe dependencia de las variables por el valor de 0,509 está más cercano a uno que a cero.

3.3. Presentación de resultados y discusión

3.3.1. Resultado y discusión de la variable dependiente

3.3.1.1. Análisis de la matriz FOFA-DODA

A partir del análisis FODA en la seguridad de la información en proyectos de ampliación de red GPON, se identificó los factores externos e internos a ser analizados. La priorización o ranking de los factores se realizará mediante la siguiente escala.

Tabla 3.9 Criterios de priorización

Escala	Condición	Condición
4	Cuando la Fortaleza es mayor	Cuando la Oportunidad es mayor
3	Cuando la Fortaleza es menor	Cuando la Oportunidad es menor
2	Cuando la Debilidad es menor	Cuando la Amenaza es menor
1	Cuando la Debilidad es mayor	Cuando la Amenaza es mayor

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

La ponderación o peso de factores define una calificación de cero a uno de cada uno de los factores mediante los análisis cualitativos de los participantes.

Definida esta ponderación se procede a multiplicarla por la priorización o ranking, dando un resultado que en sumatoria total permitirá ubicarnos en los ejes para conocer las estrategias.

Tabla 3.10 Análisis Interno – Fortalezas y Debilidades

Cod.	Análisis Interno- Fortalezas y Debilidades	Peso (0-1)	Ranking (1-4)	Resutado
D01	Limitada capacidad financiera para realizar inversiones para proyecto de ampliacion de red GPON	0,2	1	0,2
D02	Alto procesamiento manual en registro de información de requerimientos (Tablas y documentos físicos) para proyectos de ampliación de red GPON	0,1	2	0,2
D03	Falta de cultura empresarial sobre la importancia de la seguridad de la información.	0,1	2	0,2
F01	Red de Fibra Óptica con infraestructura propia.	0,2	3	0,6
F02	Internet de alta velocidad a más posibles abonados debido a mayor cobertura de red GPON	0,2	4	0,8
F03	Escabilidad para nuevos proyectos de ampliación de red GPON	0,2	4	0,8
			Total	2,8

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

Tabla 3.11 Análisis externo- Oportunidades y Amenazas

Cod.	Análisis Externo - Oportunidades y Amenazas	Peso (0-1)	Ranking (1-4)	Resutado
A01	Regulación excesiva por parte del instituciones como ARCOTEL.	0,1	2	0,2
A02	Nuevas tecnologias móviles que compartan mercado con ISP de internet fijo	0,2	1	0,2
A03	Equipos de telecomunicaciones sin seguridad física ante eventos naturales.	0,2	2	0,4
O01	Rápida evolución tecnológica a nivel mundial.	0,1	4	0,4
O02	Tendencia favorable en el mercado por un internet mediante fibra óptica.	0,2	3	0,6
O03	Nuevos sectores que requieren internet fijo.	0,2	3	0,6
				0
				0
		1	Total	2,4

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

Del análisis de factores externos se obtuvo un valor de 2,4 mientras que del análisis de los factores internos se obtuvo un valor de 2,8 dando como resultado la necesidad de implementar estrategias agresivas con respecto a los proyectos de ampliación de red GPON aplicado a un modelo de la seguridad de la información basado en la Norma ISO/IEC 27011:2016.

Figura 3.5 Análisis de la matriz FOFA-DODA

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

De acuerdo a las oportunidades y fortalezas indicadas en el punto anterior se llega a las estrategias para las PYMES ISP que se presenta a continuación:

Tabla 3.12 Estrategias obtenidas a partir del análisis FODA

		Oportunidades	
		O01	Rápida evolución tecnológica a nivel mundial.
		O02	Tendencia favorable en el mercado por un internet mediante fibra
		O03	Nuevos sectores que requieren internet fijo.
Fortalezas		**ESTRATEGIAS F-O**	
F01	Red de Fibra Óptica con infraestructura propia.	FO01	Planificar proyectos de ampliación de forma periódica.
F02	Internet de alta velocidad a más posibles abonados debido a mayor cobertura de red GPON	FO02	Ofrecer servicios que complementen el uso del internet, como Antivirus y software
F03	Escabilidad para nuevos proyectos de ampliación de red GPON	FO03	Realizar mantenimientos preventivos de acuerdo a la ISO 27001 aplicado en ISP certificados.

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

Estás estrategias van a depender del flujo de caja de cada PYME, se prioriza los proyectos de inversión debido a que logran captar clientes y con eso generar rentabilidad para futuros proyectos de ampliación u ofrecer servicios que se complementen al uso del internet.

3.3.1.2. Discusión de las entrevistas

De las tres entrevistas se pudo conseguir que la alta gerencia está consciente de la importancia de la Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para los Proyectos de Ampliación de Red GPON según los entrevistados las empresas si están implementado o buscando soluciones para la seguridad de la información, los detalles son reservados debido a que no dan a conocer sus mejoras en los procesos para evitar que la competencia conozca y copie sus estrategias de negocio.

Además los entrevistados concuerdan en que las restricciones legales, los impuestos de importación y la falta de capital es un problema inherente en la ampliación de red GPON.

Acerca de las PYMES concluyen que hay mucho interés en desarrollar un sistema de gestión en seguridad de la información incluso tener certificaciones de seguridad de la información lo complejo de obtener una certificación serían los costos de implementación además indican que como software el más conocido es el programa ISOTools, lo que deben tener en cuenta la alta gerencia es el costo beneficio que obtendrá implementando una certificación internacional mejorando así sus procesos y capacitando a sus colaboradores ya que son vitales para lograr una seguridad de la información de forma total en la empresa.

Además indican que hay poco conocimiento sobre seguridad de la información por parte de los participantes de los proyectos de ampliación de red GPON, la alta gerencia y los participantes en los proyectos deben tener conocimiento y prácticas para que la seguridad de la información sea una ventaja competitiva y genere proyectos exitosos.

Los entrevistados concuerdan que los gastos son grandes en lo que respecta a equipos de telecomunicación debido a que deben importarlos, deben considerar que al comprar en otros países demanda el tiempo de traslado y que por lo general estos equipos existen localmente pero con precios más altos, una alternativa es comprar estos equipos con una debida

planificación para así ahorrar costos por transporte aéreo sino por transporte marítimo.

3.3.2. Resultados de las variables independientes

En el anexo 4 se presentan el formato de encuesta realizada y en el anexo 9 y 10 los resultados obtenidos y tabulados en el programa SPSS, estos resultados fueron utilizados para el análisis estadístico de las variables y sus dimensiones. Además se puede realizar la correlación de variables y el método de la muestra.

3.3.2.1. Resultado de la aplicación del método sobre la muestra

En la Tabla 3.13 se presenta el resultado de la ponderación de la escala de Likert sobre las variables con respectivas dimensiones que se han utilizado

Tabla 3.13 Resultado de la investigación

Nombre variable independiente	Preguntas o ítems	5	4	3	2	1
V01	El tipo de cable utilizado en su empresa tiene protección frente a interceptaciones, interferencias o daños.			x		
	El tipo de accesorio utilizado para sujetar el cable cumple con los requisitos de seguridad del cableado		x			
	La empresa debe tener políticas de selección de proveedores que se alineen con políticas de seguridad		x			
	En los contratos con proveedores se plasman las condiciones de confidencialidad y responsabilidades.			x		
	Debe existir un acuerdo de confidencialidad de la información con los proveedores para acordar los requisitos para acceder, almacenar y comunicar la información de proyectos de ampliación de red GPON		x			
	Se deben desarrollar documentos de políticas de seguridad en los proyectos		x			
	Es necesario un responsable de las políticas, normas y procedimientos de seguridad en los proyectos		x			
	Los interesados del proyecto deben tener acceso a la información según su necesidad de saber			x		
V02	Existen procedimientos de etiquetado de activos(cajas de distribución y cables de fibra óptica) en proyectos de ampliación de red GPON		x			
	Se actualiza en determinados periodos del proyecto de ampliación de red GPON el inventario de activos.			x		
	Se define a una persona responsable de activos utilizados en los proyectos de ampliación de red GPON		x			
	Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON estén documentados			x		
	Se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que los necesiten.				x	
	Se realizan copias de backup de la información esencial para el proyecto de ampliación de red GPON			x		
	Hay establecidos controles periódicos para realizar las copias de seguridad de la información para el proyecto de ampliación de red GPON			x		
V03	Debe existir una política de control de acceso a la información en los proyectos de ampliación de red GPON		x			
	Se controla y restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON			x		
	El uso del password es necesario para restringir el acceso a la información		x			
	Los empleados deben aplicar la seguridad de la información de acuerdo con las políticas establecidas		x			
	Es necesario establecer una política de control de accesos para los proyectos de ampliación de red GPON		x			
	Se proporciona únicamente accesos de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON			x		

Fuente: Datos de investigación
Elaborado por: Autor

. Se observa que 10 indicadores se encuentran en los niveles de “3· y “2” que representan el 47,6% de todos los ítems.

Entre los indicadores que requieren atención inmediata se encuentran confianza en la seguridad del cableado, requisitos de seguridad en contratos con terceros, seguridad de información en la gestión de proyectos, inventario de activos, copias de seguridad de la información y accedo a las redes y los servicios.

3.3.2.2. Discusión de las encuestas

Al efectuar y realizar el cálculo de estadísticas descriptivas con la herramienta SPSS se observa aquellos ítems que obtuvieron puntuaciones más bajas “2” y “3” en la moda y con sus medianas cercana a “3”, fueron:

1. No se realiza de forma constante una actualización del inventario de activos durante los proyectos de ampliación de red GPON.
2. No todos los procedimientos operativos dentro de un proyecto de ampliación de red GPON se encuentran documentados.
3. Existe una baja garantía que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que los necesiten.
4. Se cuenta con pocos controles periódicos para realizar las copias de seguridad de la información para el proyecto de ampliación de red GPON.
5. Existe desconocimiento si se controla o restriegue el acceso a la información a los sistemas de información utilizados en los proyectos de ampliación de red GPON.

Son muchos aspectos que se deben mejorar teniendo en cuenta que solo es un proceso estudiado en este trabajo de investigación, como el de Proyectos de TI y que podrían ser solventados con la implementación de un sistema de seguridad de la información basada en la Norma ISO/IEC 27011:2016.

3.3.2.3. Resultados de la agrupación de las PYMES ISP

Es necesario agrupar las variables en el SPSS de acuerdo al puntaje total obtenido como resultado de la sumatoria total de los 21 ítems de las respuestas de los participantes.

En la variable SUMA, se obtiene una nota máxima de 105 puntos (21*5) que es la sumatoria total que pueden llegar a obtener.

En la variable AGRUPACIÓN, se agrupó los resultados de la variable SUMA en 5 rangos que se detallan a continuación:

Tabla 3.14 Estrategias obtenidas a partir del análisis

Pyme calificada	Rango de la suma	Descripción de la agrupación
Infeciente	1-21	Cumple menos del 20% ítems de la encuesta
Deficiente	22-42	Cumple menos del 40% ítems de la encuesta
Regular	43-63	Cumple menos del 60% ítems de la encuesta
Organizada	64-84	Cumple menos del 80% ítems de la encuesta
Eficiente	85-105	Cumple menos del 100% ítems de la encuesta

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

Como resultado se obtuvo que el 13,04% de las PYMES ISP mostraron un puntaje eficiente con respecto a seguridad de la información en sus proyectos de ampliación de red GPON mientras que el restante es decir un 86,96% son empresas que poseen una organizada seguridad de la información.

Tabla 3.15 Resultado de la agrupación de las PYMES

Empresa	Frecuencia	Porcentaje	Porcentaje acumulado
Organizada	20	86,96	86,96
Eficiente	3	13,04	100
Total	23	100	

Fuente: Recolección de datos de la investigación
Elaborado por: Autor

Es decir que el 86,96% de las PYMES ISP en el Norte de Guayaquil deben mejorar para llegar a un rango de eficiente en la seguridad de la información en sus proyectos de ampliación de red GPON.

CONCLUSIONES

El objetivo planteado en la investigación si permite identificar la aplicación del modelo de seguridad de la información con base científica por la Norma ISO/IEC 27011:2016 para proyectos de ampliación de red GPON además se tomó información del marco de referencia para proyectos el PMBOK sexta edición publicada por el PMI en el 2017.

Se concluye que luego de analizar, dimensiones, indicadores e ítems del modelo de seguridad de la información basado en la Norma ISO/IEC 27011:2016 para los proyectos de ampliación de la red GPON, que las PYMES proveedoras de servicio de Internet no utilizan procedimientos o procesos dentro de sus proyectos que garanticen la disponibilidad, integridad y confidencialidad. Además de acuerdo a las encuestas se verifica que los participantes de proyectos de ampliación de red GPON ponderan con mayor calificación de acuerdo a las escalas de Likert la confidencialidad y no la disponibilidad, siendo este último primordial para futuros proyectos debido a que el PMBOK sexta edición indica que la información que se obtiene de proyectos previos además de los procedimientos y procesos propios de la organización ayudan para la buena gestión del proyecto; por ejemplo estándares de la organización, políticas, plantillas y todo tipo de procedimientos.

Los controles encontrados en este modelo mediante las 9 dimensiones de función de la seguridad de la información mediante la Norma ISO/IEC 27002:2013 fue por medio de estadística descriptiva, estadística correlacional, análisis situacional y cálculos de porcentajes, se estableció escalas de valor para cada dimensión que se consideran como un factor crítico que incide de forma directa en la seguridad de la información en los proyectos de ampliación de red GPON en las PYMES ISP del norte de Guayaquil.

Aun se cree que por tener un cable más robusto o de mayor costo se tiene más protección cuando en realidad quien evita que el cable se desprenda del poste o que pierda fijación aérea es el accesorio quien sostiene y soporta el cable en la postería; esto se evidencia en las encuestas donde el ítem TIPO

DE ACCESORIO representa solo 34,8% de nivel de cumplimiento importante mientras que el ítem TIPO DEL CABLE representa un 82,6% de nivel de importante de cumplimiento; ambos forman parte de una misma dimensión SEGURIDAD DEL CABLEADO por lo cual se justifica que CNT considere necesario certificar cada uno de los accesorios que se utilizan a nivel nacional en los proyectos de ampliación de red GPON.

La variable DISPONIBILIDAD tiene 3 dimensiones de la cuales se identificó ponderación baja en la dimensión DOCUMENTACIÓN DE PROCEDIMIENTOS DE LA OPERACIÓN donde se verifica que el ítem “Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON están documentados” representa un 34,8% de mínimo cumplimiento y que el ítem “Se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que los necesiten” representa un 56.6% de mínimo cumplimiento lo cual evidencia que no existe una corresponsabilidad de la organización y sus colaboradores en generar la documentación, además de tener disponible la información.

Se pudo concluir que al existir un nivel de asociación de 0.584 entre dos ítem de diferentes variables confidencialidad e integridad, se demuestra una relación relativamente fuerte lo cual evidencia que hay una correlación entre estos dos ítem seleccionados del modelo encontrado en la sección 1.5.3.1

RECOMENDACIONES

La adopción de recomendaciones por parte de la ISO/IEC 27001:2013 en seguridad de la información debe garantizar la confidencialidad, disponibilidad e integridad por lo que se sugiere realizar capacitaciones del personal involucrado en todos los procesos que tienen relación con los proyectos de ampliación de red GPON.

Es necesario que exista documentación de procesos y procedimientos de la operación de los proyectos de ampliación de red GPON que involucren lecciones aprendidas, mejora contínua para que de esta manera se asegure el éxito en cada proyecto.

Este trabajo de investigación servirá de contribución en las futuras investigaciones y se plantea la sugerencia de considerar los aspectos en los controles y dimensiones encontrados, considerando la necesidad de modificarlos de acuerdo al giro de del negocio y al tipo de proyecto de la empresa.

Es recomendable que la organización sin importar su tamaño adopte un modelo de seguridad de la información, no solamente para proyectos para que así tenga políticas internas que aseguren la disponibilidad, confidencialidad e integridad de la información.

Se recomienda considerar las dimensiones e ítems del modelo presentado basado en la Norma ISO/IEC 27011:2016 para proveer seguridad de la información de forma holística y transversal en la organización en proyectos de ampliación de red GPON no solamente para PYMES sino para empresas de mayor tamaño.

Además se debe considerar para futuras investigaciones realizar una auditoria basada en la Norma ISO/IEC 27011:2016 en las PYME ISP de esta manera se verificará si están o no aplicando el modelo de seguridad de la información hallado en la presenta investigación.

REFERENCIAS BIBLIOGRAFÍAS

Alcivar Mendoza David Andrés. (2015). Estudio Para La Implementación De Una Red Gpon De Telconet S.A En La Comunidad De Juan Gómez Rendón (Progreso).. Recuperado De Http://Repositorio.Ug.Edu.Ec/Bitstream/Redug/6970/1/Estudio%20para%20la%20implementacion%20de%20una%20red%20gpon%20de%20telconet%20e.Pdf

Al-dhahri, S. (2017). Information Security Management System, (October). https://doi.org/10.5120/ijca2017912851

Al-quzwini, M. M. (2017). Design and implementation of a Fiber to the Home FTTH access network based on GPON Design and Implementation of a Fiber to the Home FTTH Access Network based on GPON, (March 2014). https://doi.org/10.5120/16015-5050

Ali, S. M. (2014). Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework, (February).

Arcotel. (2017). Geo Referenciación Y Soterramiento De Redes Físicas De Telecomunicaciones. Julio 25, 2019, De Arcotel Sitio Web: Http://Www.Arcotel.Gob.Ec/Wp-Content/Uploads/Downloads/2017/08/Resolucion-0584-Arcotel-2017.Pdf

Arcotel. (2018). Resolución Arcotel-2018- 0652. Julio 29, 2019, De Arcotel Recuperado de Http://Www.Arcotel.Gob.Ec/Wp-Content/Uploads/Downloads/2018/08/Arcotel-2018-0652-2018-07-31-Telecomunicaciones-Matriz.Pdf

Asamblea Nacional Del Ecuador . (2018). Registro Oficial No. 331. Julio 25, 2019, De Asamblea Nacional Del Ecuador Recuperado de Https://Www.Derechoecuador.Com/Registro-Oficial/2018/09/Registro-Oficial-No331--Jueves-20-De-Septiembre-De-2018

Asanka, N., Arachchilage, G., & Love, S. (2014). Computers in Human Behavior Security awareness of computer users : A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Committee ISO. (2018). ISO Survey Of Certifications To Management System Standards - Full Results. . ISO TC Recuperado De Https://Isotc.Iso.Org/Livelink/Livelink?Func=Ll&Objid=18808772&Objaction=Browse&Viewtype=1

comware S.A.. (2019). Servicios De Seguridad Informática, Aplicable Para Cualquier Tipo De Compañía.. Https://Www.Guiadesolucionestic.Com Recuperado De Https://Www.Guiadesolucionestic.Com/Seguridad/-Seguridad-De-La-Informacion-Servicios-Especializados-En/3546-Comware-Seguridad-Como-Servicio-Saas

Corporación Nacional De Telecomunicaciones. (2012). NORMAS DE DISEÑO Y CONSTRUCCIÓN DE REDES DE TELECOMUNICACIONES CON FIBRA ÓPTICA. Ecuador Recuperado De Https://Www.Compraspublicas.Gob.Ec/Procesocontratacion/Compras/PC/Bajararchivo.Cpe?Archivo=82hgsid48dvfwdm_QO0Xekkqa9d1D5n_2alkn-Jglkm.

Deloitte. (2018). Encuesta 2018 Sobre Tendencias De Cyber Riesgos Y Seguridad De La Información En Ecuador. Ecuador: Deloitte Touche Tohmatsu Limited.

Fernández, Luis Gómez, And Ana Andrés Álvarez. Guía De Aplicación De La Norma UNEISO/IEC 27001 Sobre Seguridad En Sistemas De Información Para PYMES. Asociación Española De Normalización Y Certificación (2012)

GF Sistemas. (2014). Empresa Implementada Y Certificada. Recuperado De Https://Www.Gfm.Ec/Index.Php/Servicio/Iso-27001-Consultorias

Isaca. (2012). Contenidos De La Guía De Referencia De Procesos De Cobit 5. Recuperado De

Https://Www.Isaca.Org/Chapters7/Monterrey/Events/Documents/20120305%20cobit%205.Pdf

ISO 27001:2013. (2013) Recuperado de, Http://Www.Iso.Org/Iso/Iso27001

ISO/IEC 27001:2013. (2013) Information Technology E Security Techniques E Code Of Practice For Information Security Controls. 2013

ISO/IEC 27002:2005. (2005) Information Technology E Security Techniques E Code Of Practice For Information Security Controls. 2005.

Isotools. (2019). PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA. Recuperado De Https://Www.Isotools.Org/Casos-De-Exito/Interoil-Soluciones-Isotools-Gestion-Sistemas-Integrados/

Isotools. (2014). Normas ISO. Recuperado De Https://Www.Isotools.Org/Normas/

ITU. (2017). Code Of Practice For Information Security Controls Based On Itu-T X.1051 For Small And Medium-Sized Telecommunication Organizations. Julio 27, 2019, De Telecommunication Standardization Sector Of Itu Sitio Web: Https://Www.Itu.Int/Rec/T-Rec-X.1053/en

Jaramillo, L. (2018). Interconexión mediante tecnología GPON en una ciudad Inteligente : Caso de estudio Ciudad de Loja (Ecuador).

Juan Carlos León. (2014). Propuesta De Una Nueva Estructura De La Red De Acceso GPON De La Empresa ETAPA EP Para La Provisión De Nuevos Servicios De Telecomunicaciones Para Usuarios De Tipo Residencial Y Comercial.. Recuperado De Https://Dspace.Ups.Edu.Ec/Bitstream/123456789/6451/1/UPS-CT003084.Pdf

La Republica. (2018). Astilleros Navales Ecuatorianos Reciben Certificación ISO 27001. Recuperado De Https://Www.Larepublica.Ec/Blog/Sociedad/2018/05/31/Astilleros-Navales-Ecuatorianos-Reciben-Certificacion-Iso-27001/

Mahecha & Coello. (2016). Desarrollo De Un Sistema De Información Para Gestionar La Implantación, Mantenimiento Y Mejora Continua De Un

Sistema De Gestión De Seguridad De La Información Basado En La Norma Iso 27001:2013. Recuperado De Https://Www.Dspace.Espol.Edu.Ec/Retrieve/98956/D-106133.Pdf

Malagón-Barinas, Jaime. (2014). Factores En El Éxito De Proyectos. Aproximación Al Impacto En La Organización. Paper Presented At The Encuentro Internacional De Investigadores En Administración 2014. Investigación En Administración Y Redes Globales De Conocimiento., Cali, Colombia.

Nº, A. I. I., Hugo, I. N. G., & Pozo, D. E. L. (2015). Ley orgánica de telecomunicaciones, 1–40.

Obtenci, L. A., Maestr, T. D. E., Red, D. E. U. N. A., & Fibra, C. D. E. (2015). Pontifícia universidad católica del ecuador facultad de ingeniería maestría en redes de comunicaciones.

Oriol Llauradó. (2014). La Escala De Likert: Qué Es Y Cómo Utilizarla. Recuperado De Https://Www.Netquest.Com/Blog/Es/La-Escala-De-Likert-Que-Es-Y-Como-Utilizarla

Project Management Institute, (2017). La Guía De Los Fundamentos Para La Dirección De Proyectos (Guía Del PMBOK). EEUU: Inc., Editor.

Project Management Institute. 2017. A Guide To The Project Management Body Of Knowledge (PMBOK Guide—Sixth Edition). Newtown Square, PA: Project Management Institute.

Recomendación Uit-Tg.984.1- Redes Ópticas Pasivas Con Capacidad De Gigabits Características Generales

Registro Oficial Del Ecuador. (2015). LEY ORGÁNICA DE TELECOMUNICACIONES. Agosto 3, 2019, De Asamblea Nacional Del Ecuador Recuperado de Https://Www.Telecomunicaciones.Gob.Ec/Wp-Content/Uploads/Downloads/2016/05/Ley-Org%C3%A1nica-De-Telecomunicaciones.Pdf

Rodríguez & Vásquez. (2016). Análisis Y Diseño Para La Implementación De Un Sistema De Servicios Convergentes De Telecomunicaciones Con Modelo De Red Ftth Basado En La Tipología Gpon

En El Sector De Banife Del Cantón Daule, De La Provincia Del Guayas. Recuperado De Https://Www.Dspace.Espol.Edu.Ec/Retrieve/97536/D-103429.Pdf

Safa, N. S., & Ismail, M. A. (2013). A customer loyalty formation model in electronic commerce. Economic Modelling, 35, 559–564. https://doi.org/10.1016/j.econmod.2013.08.011

Said, J. (2015). Information Security : Risk , Governance and Implementation Setback. Procedia Economics and Finance, 28(April), 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Schatz, D., Wall, J., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security, 12(2).

Sector, S., & Itu, O. F. (2017). ITU-T. Telecommunication Standardization Sector

Servicio Ecuatoriano De Normalización. (2016). MiPYMES Y Organizaciones De Economía Popular Y Solidaria Son Una Pieza Clave Para La Economía Del País. Recuperado De Https://Www.Normalizacion.Gob.Ec/MiPYMES-Y-Organizaciones-De-Economia-Popular-Y-Solidaria-Son-Una-Pieza-Clave-Para-La-Economia-Del-Pais/

Sohrabi, N., Solms, R. Von, Furnell, S., Elizabeth, P., & Africa, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70–82 Recuperado de. https://doi.org/10.1016/j.cose.2015.10.006

Systems, D. (2012). ITU-T, 1(2008).

Telégrafo. (2017). El 42% De Las Compañías Registradas En El País Son PYMES. Recuperado De Https://Www.Eltelegrafo.Com.Ec/Noticias/Economia/1/El-42-De-Las-Companias-Registradas-En-El-Pais-Son-PYMES.

Timesaver, P. (2018). Índice.

Too, E. G., & Weaver, P. (2014). ScienceDirect The management of project management : A conceptual framework for project governance. JPMA, 32(8), 1382–1394. Recuperado de https://doi.org/10.1016/j.ijproman.2013.07.006

Too, Eric G., & Weaver, Patrick. (2013). The Management Of Project Management: A Conceptual Framework For Project Governance

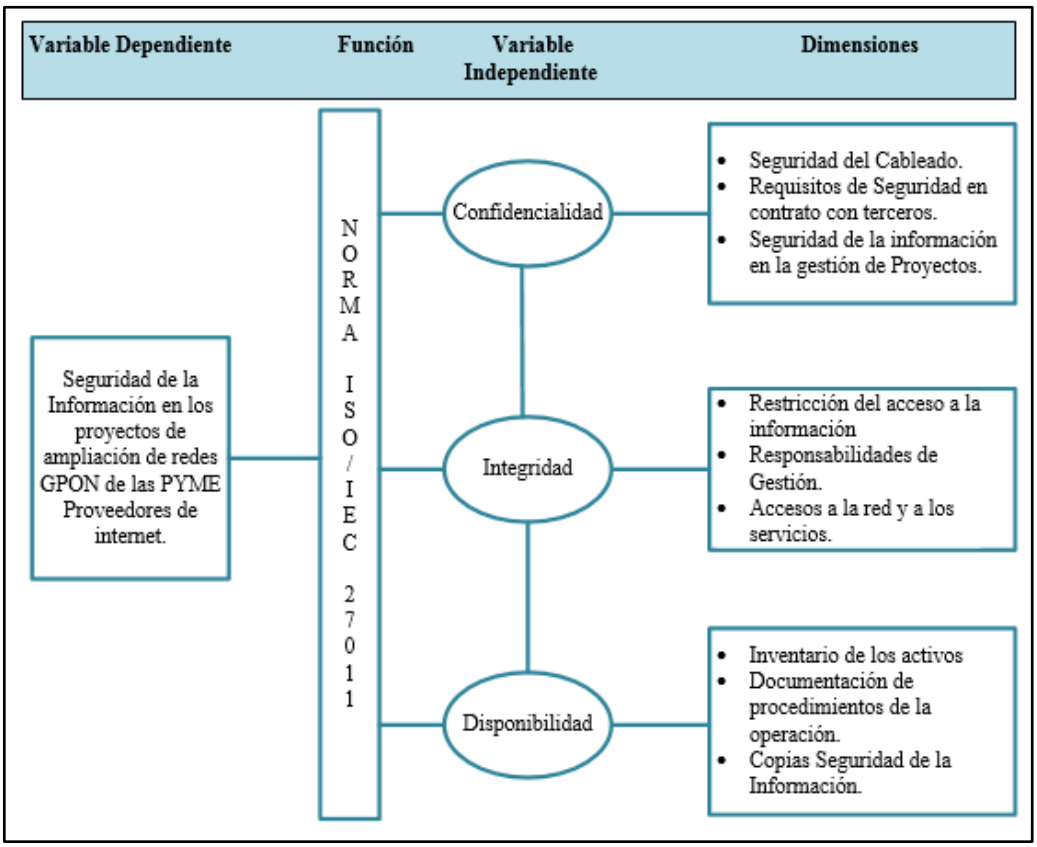
Too, Eric G., & Weaver, Patrick. (2013). The management of project management: A conceptual framework for project governance. International Journal of Project Management(0). doi: 10.1016/j.ijproman.2013.07.006.

ANEXOS

Anexo N° 1 Matriz Auxiliar de Operación de Diseño del Trabajo de Investigación.

Problema	Objetivo	Operacionalización de variables		Dimensión	Indicador
Formulación del problema	**General**	**Variable dependiente**	**Variable independiente**		
¿Cómo incide un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27000 en el proyecto de ampliación redes GPON en los proveedores de Internet del sector PYME del norte de la ciudad de Guayaquil?	Evaluar un modelo de sistema de seguridad de la información bajo la norma ISO/IEC 27001 para los proyectos de ampliación de la red GPON en las PYME ISP del norte de Guayaquil.	Seguridad de la información	Confidencialidad	Seguridad del cableado	Confianza en la seguridad del cableado
				Requisitos de seguridad en contratos con terceros	Confianza en la información respaldada
				Seguridad de información en la gestión de proyectos	Establecer controles y procedimientos para evitar problemas en la seguridad de la información
Sistematización	**Específicos**		Disponibilidad	Inventario de los activos	Garantía de actualización de activos
1. ¿La falta de confidencialidad de la información en el proyecto de ampliación de redes GPON pueden superarse aplicando la norma ISO/IEC 2700?; 2. ¿Los proveedores de Internet PYME pueden continuar sin tener disponible la información sobre el proyecto de ampliación de Redes GPON?; y, 3. ¿Existen procedimientos que eviten la manipulación y alteración la información en el proyecto de ampliación de red GPON?	1. Identificar un modelo de seguridad de la información basado a los requerimientos de la norma ISO/IEC 27000 para los proyectos de ampliación de la red GPON; 2. Analizar las prácticas de la Seguridad de la Información existentes en las PYME ISP para los proyectos de ampliación de la red GPON; y, 3. Encontrar controles de seguridad de la información basados en la ISO/IEC 27002 para los proyectos de ampliación de la red GPON en Guayaquil.			Documentación de procedimientos de la operación	Nivel de disponibilidad de la información
				Copias de seguridad de la información	Nivel de aseguramiento de la información
			Integridad	Restricción del acceso a la información	Monitoreo de acceso a la información de la red de GPON
				Responsabilidades de gestión	Confianza de participación de personal autorizado
				Acceso a las redes y los servicios de red	Asignación de personal para la función de acuerdo a su Rol

Anexo N° 2 Modelo Conceptual Aplicado a la Metodología



Anexo N° 3 Antecedentes bibliográficos de las variables, dimensiones e indicadores

Operacionalización de variables					
Variable dependiente	**Variable independiente**	**N°**	**Dimensión**	**Indicador**	**Antecedentes Técnicos**
Seguridad de la información	Confidencialidad	1	Seguridad del cableado	Confianza en la seguridad del cableado	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		2	Requisitos de seguridad en contratos con terceros	Confianza en la información respaldada	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		3	Seguridad de información en la gestión de proyectos	Establecer controles y procedimientos para evitar problemas en la seguridad de la información	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
	Disponibilidad	4	Inventario de activos	Garantía de actualización de activos	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		5	Documentación de procedimientos de la operación	Nivel de disponibilidad de la información	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		6	Copias de seguridad de la información	Nivel de aseguramiento de la información	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
	Integridad	7	Restricción del acceso a la información	Monitoreo de acceso a la información de la red de GPON	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		8	Responsabilidades de ges	Confianza de participación de personal autorizado	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html
		9	Acceso a las redes y los servicios de red	Asignación de personal para la función de acuerdo a su Rol	Organización Intermacional de Normalización, ISO (2013) Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54553.html

Anexo N° 4 Matriz de operacionalización de las variables investigadas.

Operacionalización de variables										
Variable dependiente	**Variable independiente**	**N°**	**Dimensión**	**Indicador**	**Preguntas o ítems**	**Técnicas**	**Instrumento**	**Fuente**	**Procesamiento**	**Tipo de Información**
Seguridad de la información	Confidencialidad	1	Seguridad del cableado	Confianza en la seguridad del cableado	El tipo de cable utilizado en su empresa tiene protección frente a interceptaciones, interferencias o daños.	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					El tipo de accesorio utilizado para sujetar el cable cumple con los requisitos de seguridad del cableado	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		2	Requisitos de seguridad en contratos con terceros	Confianza en la información respaldada	La empresa debe tener políticas de selección de proveedores que se alineen con políticas de seguridad	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					En los contratos con proveedores se plasman las condiciones de confidencialidad y responsabilidades.	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Debe existir un acuerdo de confidencialidad de la información con los proveedores para acordar los requisitos para acceder, almacenar y comunicar la información de proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		3	Seguridad de información en la gestión de proyectos	Establecer controles y procedimientos para evitar problemas en la seguridad de la información	Se deben desarrollar documentos de políticas de seguridad en los proyectos	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Es necesario un responsable de las políticas, normas y procedimientos de seguridad en los proyectos	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Los interesados del proyecto deben tener acceso a la información según su necesidad de saber	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
	Disponibilidad	4	Inventario de activos	Garantía de actualización de activos	Existen procedimientos de etiquetado de activos(cajas de distribución y cables de fibra óptica) en proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Se actualiza en determinados periodos del proyecto de ampliación de red GPON el inventario de activos.	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Se define a una persona responsable de activos utilizados en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		5	Documentación de procedimientos de la operación	Nivel de disponibilidad de la información	Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON estén documentados	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que los necesiten.	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		6	Copias de seguridad de la información	Nivel de aseguramiento de la información	Se realizan copias de backup de la información esencial para el proyecto de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Hay establecidos controles periódicos para realizar las copias de seguridad de la información para el proyecto de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
	Integridad	7	Restricción del acceso a la información	Monitoreo de acceso a la información de la red de GPON	Debe existir una política de control de acceso a la información en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Se controla y restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					El uso del password es necesario para restringir el acceso a la información	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		8	Responsabilidades de gestión	Confianza de participación de personal autorizado	Los empleados deben aplicar la seguridad de la información de acuerdo con las políticas establecidas	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		9	Acceso a las redes y los servicios de red	Asignación de personal para la función de acuerdo a su Rol	Es necesario establecer una política de control de accesos para los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
					Se proporciona únicamente accesos de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa

Anexo N° 5 Matriz de conversión de datos

Operacionalización de variables												
Variable dependiente	**Variable independiente**	**N°**	**Dimensión**	**Preguntas o ítems**	**Técnicas**	**Instrumento**	**Fuente**	**Nombre variable**	**Procesamiento**	**Tipo de fuente**	**Tipo de Información**	**Descripción de la variable**
Seguridad de la información	Confidencialidad	1	Seguridad del cableado	El tipo de cable utilizado en su empresa tiene protección frente a interceptaciones, interferencias o daños.	Recolección de campo	Encuesta	Primaria	Seg_Cable_01	No aplica	No aplica	Cuantitativa	Detalle de la seguridad del cableado
				El tipo de accesorio utilizado para sujetar el cable cumple con los requisitos de seguridad del cableado	Recolección de campo	Encuesta	Primaria	Seg_Cable_02	No aplica	No aplica	Cuantitativa	Detalle de lo que sostiene al cableado
		2	Requisitos de seguridad en contratos con terceros	La empresa debe tener políticas de selección de proveedores que se alineen con políticas de seguridad	Recolección de campo	Encuesta	Primaria	Req_Seg_01	No aplica	No aplica	Cuantitativa	Selección de proveedor
				En los contratos con proveedores se plasman las condiciones de confidencialidad y responsabilidades.	Recolección de campo	Encuesta	Secundaria	Reg_Seg_02	No aplica	No aplica	Cuantitativa	Acuerdo de confidencialidad y responsabiliad
				Debe existir un acuerdo de confidencialidad de la información con los proveedores para acordar los requisitos para acceder, almacenar y comunicar la información de proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Reg_Seg_03	No aplica	No aplica	Cuantitativa	Acuerdo de confidencialiad
		3	Seguridad de información en la gestión de proyectos	Se deben desarrollar documentos de políticas de seguridad en los proyectos	Recolección de campo	Encuesta	Primaria	Seg_Pro_01	No aplica	No aplica	Cuantitativa	Seguridad en los proyectos
				Es necesario un responsable de las políticas, normas y procedimientos de seguridad en los proyectos	Recolección de campo	Encuesta	Primaria	Seg_Pro_02	No aplica	No aplica	Cuantitativa	Responsable de Seguridad de la información.
				Los interesados del proyecto deben tener acceso a la información según su necesidad de saber	Recolección de campo	Encuesta	Primaria	Seg_Pro_03	No aplica	No aplica	Cuantitativa	Interesados del proyecto
	Disponibilidad	4	Inventario de activos	Existen procedimientos de etiquetado de activos(cajas de distribución y cables de fibra óptica) en proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Inv_Act_01	No aplica	No aplica	Cuantitativa	Procedimientos de etiquetado
				Se actualiza en determinados periodos del proyecto de ampliación de red GPON el inventario de activos.	Recolección de campo	Encuesta	Primaria	Inv_Act_02	No aplica	No aplica	Cuantitativa	Inventarios de Activos
				Se define a una persona responsable de activos utilizados en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Inv_Act_03	No aplica	No aplica	Cuantitativa	Responsable de activos
		5	Documentación de procedimientos de la operación	Todos los procedimientos operativos identificados en el proyecto de ampliación de red GPON estén documentados	Recolección de campo	Encuesta	Primaria	Doc_Pro_01	No aplica	No aplica	Cuantitativa	Procedimientos operativos
				Se garantiza que la documentación esté disponible de forma oportuna y adecuada para todos los usuarios que los necesiten.	Recolección de campo	Encuesta	Primaria	Doc_Pro_02	No aplica	No aplica	Cuantitativa	Documentación disponible
		6	Copias de seguridad de la información	Se realizan copias de backup de la información esencial para el proyecto de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Cop_Seg_01	No aplica	No aplica	Cuantitativa	Copias de backup
				Hay establecidos controles periódicos para realizar las copias de seguridad de la información para el proyecto de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Cop_Seg_02	No aplica	No aplica	Cuantitativa	Controles periódicos
	Integridad	7	Restricción del acceso a la información	Debe existir una política de control de acceso a la información en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Res_Acc_01	No aplica	No aplica	Cuantitativa	Políticas de control de acceso
				Se controla y restringe el acceso a la información en los sistemas de información utilizadas en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Res_Acc_02	No aplica	No aplica	Cuantitativa	Restricción de acceso a la información
				El uso del password es necesario para restringir el acceso a la información	Recolección de campo	Encuesta	Primaria	Res_Acc_03	No aplica	No aplica	Cuantitativa	Uso de password
		8	Responsabilidades de gestión	Los empleados deben aplicar la seguridad de la información de acuerdo con las políticas establecidas	Recolección de campo	Encuesta	Primaria	Res_Ges_01	No aplica	No aplica	Cuantitativa	Responsabilidades de Gestión
		9	Acceso a las redes y los servicios de red	Es necesario establecer una política de control de accesos para los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Acc_Red_01	No aplica	No aplica	Cuantitativa	Políticas de control de acceso
				Se proporciona únicamente accesos de red a usuarios para cuyo uso haya sido específicamente autorizado en los proyectos de ampliación de red GPON	Recolección de campo	Encuesta	Primaria	Acc_Red_02	No aplica	No aplica	Cuantitativa	Accesos de red a usuarios específicos

Anexo N° 6 Estructura de variables - Programa estadístico IBM SPSS

	Nombres	Tipo	Medida	Anchura
1	Trabajo	Numérico	Nominal	8
2	Numero	Numérico	Nominal	8
3	Funcion	Numérico	Nominal	8
4	Proyectos	Numérico	Nominal	8
5	Certificación	Numérico	Nominal	9
6	Conocimiento	Numérico	Nominal	8
7	Seg_Cable_01	Numérico	Nominal	8
8	Seg_Cable_02	Numérico	Nominal	8
9	Req_Seg_01	Numérico	Nominal	8
10	Reg_Seg_02	Numérico	Nominal	8
11	Reg_Seg_03	Numérico	Nominal	8
12	Seg_Pro_01	Numérico	Nominal	8
13	Seg_Pro_02	Numérico	Nominal	8
14	Seg_Pro_03	Numérico	Nominal	8
15	Inv_Act_01	Numérico	Nominal	8
16	Inv_Act_02	Numérico	Nominal	8
17	Inv_Act_03	Numérico	Nominal	8
18	Doc_Pro_01	Numérico	Nominal	8
19	Doc_Pro_02	Numérico	Nominal	8
20	Cop_Seg_01	Numérico	Nominal	8
21	Cop_Seg_02	Numérico	Nominal	8
22	Res_Acc_01	Numérico	Nominal	8
23	Res_Acc_02	Numérico	Nominal	8
24	Res_Acc_03	Numérico	Nominal	8
25	Res_Ges_01	Numérico	Nominal	8
26	Acc_Red_01	Numérico	Nominal	8
27	Acc_Red_02	Numérico	Nominal	8

Anexo N° 7 Listado de Empresas Proveedoras de servicio de Internet registradas con contrato habilitante en la Agencia de Regulación y Control de las Telecomunicaciones

Nombre	Tipo compañía	Nº.OFICIO AUTORIZACIÓN
ARTIANEXOS S.A.	Anónima	ARCOTEL-CZ5-2016-0192-OF
BAJAÑA ANA DENNI CHRISTIAN	Anónima	ARCOTEL-2018-1263
CHAVEZ HOLGUIN RUBEN MILTON	Anónima	ARCOTEL-CZ5-2015-0263-OF
COMM&NET S.A.	Anónima	ARCOTEL-CZ5-2016-0492-OF
EBESTPHONE ECUADOR S.A.	Anónima	ARCOTEL-CZ5-2017-0044
ENLACES CON FIBRA OPTICA ENFIOP S.A.	Anónima	ARCOTEL-CZ5-2015-0262-OF
GIGATEL S.A.	Anónima	ARCOTEL-2018-1130
LK TRO-KOM S.A.	Anónima	ARCOTEL-CZO5-2018-0614-OF
MAILLOT S.A.	Anónima	SENATEL-DRL-2014-1293
NUÑEZ DE LA ROSA RICHARD DALTON	Anónima	SENATEL-2014-006930
PIOVESAN AMPUERO EMILIO	Anónima	ARCOTEL-2018-1293
TECNOBIS S.A.	Anónima	ARCOTEL-CZ5-2015-0234-OF
TRANSCORPORACION S.A.	Anónima	ARCOTEL-2018-1010
UFINET ECUADOR UFIEC S.A.	Anónima	ARCOTEL-2017-0067
ASAPTEL S.A.	Anónima	DRL-2014-1313-OF
CODGREC S.A.	Anónima	DRL-2013-1078-OF
COMPUTECNICSNET S.A.	Anónima	DRL-2014-1316-OF
FLASHNET S.A.	Anónima	ARCOTEL-CZO5-2018-0923-OF
GALARZA PORRAS RAFAEL LUIS	Anónima	ARCOTEL-CTDS-2018-0140-OF
GEDATECU S.A.	Anónima	ARCOTEL-2018-1141
INKAVISION S.A.	Anónima	ARCOTEL-DRS-2016-0326-OF
LANDETA QUIMI DARIO RENE	Anónima	S/N SOLO EN PERMISO
NETESERVICE S.A.	Anónima	ARCOTEL-CZ5-2016-0116-M
NEW ACCESS S.A.	Anónima	GGST-2013-2385

Anexo N° 8 Formato de Encuesta

ENCUESTA DE OPINIÓN SOBRE SEGURIDAD DE LA INFORMACIÓN A PYME PROVEEDORAS DE SERVICIOS DE INTERNET EN EL NORTE DE GUAYAQUIL.

La presente encuesta está dirigida a las PYME proveedoras de servicio de internet, para conocer su nivel de manejo en proyectos de ampliación de redes GPON, frecuencia de implementación de red GPON y opinión sobre el uso de la normativa; por lo tanto, solicitamos que usted responda con sinceridad a todos los ítems formulados.

1. **¿USTED SE ENCUETRA LABORANDO EN UNA EMPRESA PYME ISP DEL NORTE DE GUAYAQUIL?**
   Mark only one oval.
   - ◯ SI
   - ◯ No

2. **¿INDICAR EL NÚMERO APROXIMADO DE EMPLEADOS EN SU EMPRESA?**
   Mark only one oval.
   - ◯ MENO DE 10
   - ◯ DE 11 A 50
   - ◯ MÁS DE 11

3. **¿FUNCIÓN DENTRO DE LA EMPRESA?**
   Mark only one oval.
   - ◯ GERENTE GENERAL
   - ◯ GERENTE TÉCNICO
   - ◯ GERENTE FINANCIERO
   - ◯ JEFE DE PROYECTO
   - ◯ JEFE TÉCNICO
   - ◯ TÉCNICO

4. **¿INDICAR EL NÚMERO DE VECES AL AÑO QUE SU EMPRESA REALIZA PROYECTOS DE AMPLIACIÓN DE RED GPON?**
   Mark only one oval.
   - ◯ 1 VEZ AL AÑO
   - ◯ DE 2 A 4 VECES AL AÑO
   - ◯ MAS DE 4 VECES AL AÑO
   - ◯ NINGUNA

5. **¿SU EMPRESA CUENTA CON CERTIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN?**
   Mark only one oval.
   - ◯ SI
   - ◯ NO

6. **¿TIENE CONOCIMIENTO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27000?**

Mark only one oval.

- ◯ Sí
- ◯ No

7. **EL TIPO DE CABLE UTILIZADO EN SU EMPRESA TIENE PROTECCIÓN FRENTE A INTERCEPTACIONES, INTERFERENCIAS O DAÑOS.**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MINIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO OPTIMO

8. **EL TIPO DE ACCESORIO UTILIZADO PARA SUJETAR EL CABLE CUMPLE CON LOS REQUISITOS DE SEGURIDAD DEL CABLEADO**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MINIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO OPTIMO

9. **LA EMPRESA DEBE TENER POLÍTICAS DE SELECCIÓN DE PROVEEDORES QUE SE ALINEEN CON POLÍTICAS DE SEGURIDAD**

Mark only one oval.

- ◯ EN TOTAL DESACUERDO
- ◯ EN DESACUERDO
- ◯ NI EN ACUERDO NI EN DESACUERDO
- ◯ EN ACUERDO
- ◯ EN TOTAL ACUERDO

10. **EN LOS CONTRATOS CON PROVEEDORES SE PLASMAN LAS CONDICIONES DE CONFIDENCIALIDAD Y RESPONSABILIDADES.**

Mark only one oval.

- ◯ EN TOTAL DESACUERDO
- ◯ EN DESACUERDO
- ◯ NI EN ACUERDO NI EN DESACUERDO
- ◯ EN ACUERDO
- ◯ EN TOTAL ACUERDO

11. **DEBE EXISTIR UN ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN CON LOS PROVEEDORES PARA ACORDAR LOS REQUISITOS PARA ACCEDER, ALMACENAR Y COMUNICAR LA INFORMACIÓN DE PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ EN TOTAL DESACUERDO
- ◯ EN DESACUERDO
- ◯ NI EN ACUERDO NI EN DESACUERDO
- ◯ EN ACUERDO
- ◯ EN TOTAL ACUERDO

12. **EXISTEN PROCEDIMIENTOS DE ETIQUETADO DE ACTIVOS(CAJAS DE DISTRIBUCIÓN Y CABLES DE FIBRA ÓPTICA) EN PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MÍNIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO ÓPTIMO

13. **SE DEFINE A UNA PERSONA RESPONSABLE DE ACTIVOS UTILIZADOS EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MÍNIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO ÓPTIMO

14. **SE REALIZAN COPIAS DE BACKUP DE LA INFORMACIÓN ESENCIAL PARA EL PROYECTO DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MÍNIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO ÓPTIMO

15. **HAY ESTABLECIDOS CONTROLES PERIÓDICOS PARA REALIZAR LAS COPIAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROYECTO DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ NO HAY CUMPLIMIENTO
- ◯ MÍNIMO CUMPLIMIENTO
- ◯ MEDIANO CUMPLIMIENTO
- ◯ NIVEL IMPORTANTE DE CUMPLIMIENTO
- ◯ CUMPLIMIENTO ÓPTIMO

16. **DEBE EXISTIR UNA POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- EN TOTAL DESACUERDO
- EN DESACUERDO
- NI EN ACUERDO NI EN DESACUERDO
- EN ACUERDO
- EN TOTAL ACUERDO

17. **SE CONTROLA Y RESTRINGE EL ACCESO A LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN UTILIZADAS EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- EN TOTAL DESACUERDO
- EN DESACUERDO
- NI EN ACUERDO NI EN DESACUERDO
- EN ACUERDO
- EN TOTAL ACUERDO

18. **EL USO DEL PASSWORD ES NECESARIO PARA RESTRINGIR EL ACCESO A LA INFORMACIÓN**

Mark only one oval.

- EN TOTAL DESACUERDO
- EN DESACUERDO
- NI EN ACUERDO NI EN DESACUERDO
- EN ACUERDO
- EN TOTAL ACUERDO

19. **LOS EMPLEADOS DEBEN APLICAR LA SEGURIDAD DE LA INFORMACIÓN DE ACUERDO CON LAS POLÍTICAS ESTABLECIDAS**

Mark only one oval.

- EN TOTAL DESACUERDO
- EN DESACUERDO
- NI EN ACUERDO NI EN DESACUERDO
- EN ACUERDO
- EN TOTAL ACUERDO

20. **ES NECESARIO ESTABLECER UNA POLÍTICA DE CONTROL DE ACCESOS PARA LOS PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- EN TOTAL DESACUERDO
- EN DESACUERDO
- NI EN ACUERDO NI EN DESACUERDO
- EN ACUERDO
- EN TOTAL ACUERDO

21. **SE PROPORCIONA ÚNICAMENTE ACCESOS DE RED A USUARIOS PARA CUYO USO HAYA SIDO ESPECÍFICAMENTE AUTORIZADO EN LOS PROYECTOS DE AMPLIACIÓN DE RED GPON**

Mark only one oval.

- ◯ EN TOTAL DESACUERDO
- ◯ EN DESACUERDO
- ◯ NI EN ACUERDO NI EN DESACUERDO
- ◯ EN ACUERDO
- ◯ EN TOTAL ACUERDO

Anexo N° 9 Entrevista Miguel Izquierdo

ENTREVISTA		
Fecha	05/08/2019	
Nombre del entrevistado	Miguel Izquierdo	
Ocupación actual	Gerente General de Empresa “A”	
Años experiencia profesional	5	
OBJETIVO DE LA ENTREVISTA		
El objetivo de la entrevista es recopilar información sobre la seguridad de la información en una empresa proveedora de servicios de internet.		
PREGUNTAS Y RESPUESTAS DE LA ENTREVISTA		
1	**Como describe usted el nivel de conocimiento sobre seguridad de la información de los participantes en un proyecto de ampliación de red GPON**	Los contratistas y personal técnico por lo general no posee un conocimiento de proteger la información, o de la importancia que esto genera para las empresas.
2	**¿Cuáles son las principales dificultades para entrar al mercado cuando empieza una ampliación de red GPON?**	Tener la certeza que si en realidad la ampliación que se hace tendrá su retorno a lo invertido.
3	**¿Pueden los compradores disminuir drásticamente los precios del servicio de internet?**	Antes un plan el mínimo superaba los $30,00 ahora el mínimo tiene el costo de $23,93 es difícil competir con precios más bajos y el cliente siempre se inclina hacia un costo menor. Quizás no puedan drásticamente pero el precio del internet esta de caída.
4	**¿Cómo Gerente General y máxima autoridad que tan importante es la seguridad de la información en sus proyectos de ampliación de red GPON?**	Cada proyecto debe tener su rentabilidad sino es así no tiene sentido que se gaste en él, la seguridad de la información es importante debido a que hemos tenido ataques de terceros y si se hubieran implementado más políticas de seguridad de la información quizás muchos problemas hubieran sido evitados, es importantísima la seguridad.
5	**¿Existe un líder absoluto de mercado en este sector de proveedores de internet?**	No creo eso, CNT tiene muchos usuarios pero es debido a que estuvo primero, pero muchos de nuestros clientes salen de CNT y contratan con nosotros, así mismo Netlife. La competencia es para todos.
6	**¿Su empresa cuantos proyectos de ampliación de red GPON hace al año?**	Se podría decir que de 2 a 4 al año, con una capacidad de 200 a 400 clientes.
7	**¿En su empresa se utiliza algún sistema de información basado en la gestión de la seguridad de la información?**	No. Lo que tenemos son CRM, sistema de facturación electrónica y sistemas de monitoreo de los equipos en los nodos de internet.
8	**¿Por qué?**	Los costos son altos. He preguntado y son de $10,000 al año y pueden variar según los módulos que queremos utilizar.
9	**¿Conoce usted algún proveedor de un sistema de información para seguridad de la información?**	ISOTools. También hay un programa colombiano no recuerdo el nombre.

10	**¿Qué ventajas y desventajas tiene al documentar todo el proceso de la forma actual que lo hace para los proyectos de ampliación de red GPON?**	Ventajas como tener disponible esa información, un respaldo que es necesario para futuros proyectos. Desventajas puede ser el tiempo que se dedica en aquello.
11	**¿Cómo la seguridad de la información le daría una ventaja competitiva a su empresa cuando se implemente una red GPON?**	Trabajar sobre normas internacionales de calidad es lo que siempre tratamos de hacer día a día. Trabajar de esta forma si nos puede dar una ventaja para que un proyecto finalice en el tiempo planificado incluso que sea más rentable.
12	**¿Qué amenazas afectan a un proyecto de ampliación de red GPON?**	La ARCOTEL, las condiciones que imponen el mercado, cuando existen técnicos de otras empresas rompen nuestros cables, cuando las redes eléctricas son deficientes y pueden producir un corto circuito.
La información proporcionada en esta entrevista es para fines académicos		
Firma del entrevistado		Firma del entrevistador

Anexo N° 10 Entrevista Geovanny Narea

ENTREVISTA		
Fecha	25/08/2019	
Nombre del entrevistado	Geovanny Narea	
Ocupación actual	Jefe Técnico de Empresa “B”	
Años experiencia profesional	3	
OBJETIVO DE LA ENTREVISTA		
El objetivo de la entrevista es recopilar información sobre la seguridad de la información en una empresa proveedora de servicios de internet.		
PREGUNTAS Y RESPUESTAS DE LA ENTREVISTA		
1	**Como describe usted el nivel de conocimiento sobre seguridad de la información de los del servicio de internet**	El usuario no posee conocimiento de seguridad informática, incluso cree que la empresa proveedora de internet es responsable del contenido que ven y de los virus que existan mientras navegan.
2	**¿Cuáles son las principales dificultades para entrar al mercado cuando empieza una ampliación de red GPON?**	Los costos de implementar fibra aún siguen siendo caros, a pesar que hubo un leve decremento por la mano de obra sigue siendo caro por las herramientas y la mano de obra.
3	**¿Pueden los compradores disminuir drásticamente los precios del servicio de internet?**	Si pueden, nosotros tratamos de ingresar en una zona mediante precios bajos, no es por dañar el mercado sino que así inicialmente se hace conocer el nombre de la empresa.
4	**¿Cree usted que la seguridad de la información en proyectos de ampliación de red GPON le ayudará a tener más clientes?**	No sabría indicarle con seguridad si voy a tener más o menos clientes, pero si tengo conocimiento que una política de confidencialidad será muy útil para cada proyecto que empiece la empresa.
5	**¿Existe un líder absoluto de mercado en este sector?**	Creería que es CNT, TV Cable y Netlife tienen gran parte del mercado.
6	**¿El mercado en el que opera su empresa está en crecimiento?**	Claro que sí, el consumo del internet va en aumento en lugares perimetrales de la ciudad y en suburbios donde no llegan las grandes compañías.
7	**¿En su empresa se utiliza algún sistema de información basado en la gestión de la seguridad de la información? Si su respuesta es no, ¿podría indicar el por qué?**	No.
8	**¿Por qué?**	Imagino que deben ser por los costos de algún software de esos.
9	**¿Conoce usted algún proveedor de un sistema de información para seguridad de la información?**	No.
10	**¿Qué ventajas y desventajas tiene al documentar todo el proceso de la forma actual que lo hace para los proyectos de ampliación de red GPON?**	Nosotros tenemos ciertas plantillas o procedimiento de trabajo, además de registro de cómo queda la red GPON. Como ventaja es tenerlo disponible ante cualquier evento y desventaja que sería mejor tener todo eso en digital.

11	**¿Cómo la seguridad de la información le daría una ventaja competitiva a su empresa cuando se implemente una red GPON?**	Pienso que nos dará más herramientas y conocimiento para competir ante empresas grandes.
12	**¿Qué amenazas afectan a un proyecto de ampliación de red GPON?**	La tramitología, si queremos implementar una red en un área de regeneración urbana se nos complica por los procesos que debemos cumplir y esto depende de cada proceso. También factores ambientales como lluvias podrían detener lo planificado para un proyecto.

La información proporcionada en esta entrevista es para fines académicos

Firma del entrevistado	Firma del entrevistador

Anexo N° 11 Entrevista Pablo Tinoco

ENTREVISTA		
Fecha	05/08/2019	
Nombre del entrevistado	Pablo Tinoco	
Ocupación actual	Gerente Técnico de Empresa “C”	
Años experiencia profesional	8	
OBJETIVO DE LA ENTREVISTA		
El objetivo de la entrevista es recopilar información sobre la seguridad de la información en una empresa proveedora de servicios de internet.		
PREGUNTAS Y RESPUESTAS DE LA ENTREVISTA		
1	**Como describe usted el nivel de conocimiento sobre seguridad de la información de los del servicio de internet**	El ciudadano común normalmente no tiene precaución al momento de navegar en internet y la seguridad de su información se puede poner expuesta.
2	**¿Cuáles son las principales dificultades para entrar al mercado cuando empieza una ampliación de red GPON?**	El costo por implementación de una red GPON es alto dependiendo de la zona de cobertura, además los materiales e implementos son más baratos si se los importan. Lo difícil de entrar en este mercado es hacerse conocer y los costos de marketing y publicidad que pueden representar.
3	**¿Pueden los compradores disminuir drásticamente los precios del servicio de internet?**	Si existe una competencia bien agresiva si porque el cliente siempre quiere pagar menos y si esta una nueva compañía lo primero que hace es bajar precios para tener nuevos clientes.
4	**¿Existen algunos que tienen control sobre los precios?**	No sé si control pero hay ciertos proveedores de servicios de internet que trabajan de forma ilegal es decir sin autorización de la ARCOTEL.
5	**¿Existe un líder absoluto de mercado en este sector?**	No, absoluto no, lo que si ocurre que CNT y Netlife tienen un gran poder al tener una maquinaria de publicidad.
6	**¿El mercado en el que opera su empresa está en crecimiento?**	Sí, pero hay que buscar los clientes y mientras tengas buenos precios y visión se puede crecer.
7	**¿En su empresa se utiliza algún sistema de información basado en la gestión de la seguridad de la información? Si su respuesta es no, ¿podría indicar el por qué?**	No.
8	**¿Por qué?**	Porque los costos de implementación deben ser altos además todavía se puede avanzar con procesos y procedimientos manuales no automatizados.
9	**¿Conoce usted algún proveedor de un sistema de información para seguridad de la información?**	ISOTools.
10	**¿Qué ventajas y desventajas tiene al documentar todo el proceso de la forma actual que lo hace para los proyectos de ampliación de red GPON?**	La ventaja que se tiene una bitácora importante para futuros proyectos, lo tedioso son las tablas, los informes, toda la documentación necesaria para registrar cada evento en un proyecto de ampliación de red GPON.

11	**¿Cómo la seguridad de la información le daría una ventaja competitiva a su empresa cuando se implemente una red GPON?**	Si bien es cierto que una certificación en seguridad de información si nos daría una ventaja, considero que los principales participantes son los empleados que deben tener ese hábito de salvaguardar la información delicada de la empresa.
12	**¿Qué amenazas afectan a un proyecto de ampliación de red GPON?**	La burocracia que existe al momento de cada trámite en el ente regulador, riesgo que un equipo se dañe o queme ante un evento natural emergente, que la información no sea confidencial entre los empleados. Que se pierda información de la base de datos de nuestras aplicaciones para la gestión de equipos de fibra.

La información proporcionada en esta entrevista es para fines académicos

Firma del entrevistado	Firma del entrevistador

Anexo N° 12 Diagrama SIPOC del subproceso Proyecto de ampliación de GPON