ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Propuesta metodológica basada en ISO 27000, para cumplir requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en micro-empresas proveedoras de internet, caso Maxxnet

DIEGO NOÉ PUSAY VILLARROEL

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

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

AGOSTO DE 2023

DECLARACIÓN DE AUTENTICAD

Yo, Diego Noé Pusay Villarroel, declaro que el presente **Trabajo de Titulación Modalidad Proyecto de Investigación y Desarrollo**, es de mi autoría y que los resultados de este son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

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

Riobamba, agosto de 2023

DIEGO NOÉ PUSAY VILLARROEL
No. Cédula: 060343904-3

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación Modalidad Proyectos de Investigación y Desarrollo**, titulado: Propuesta metodológica basada en ISO 27000,para cumplir requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en micro-empresas proveedoras de internet, caso Maxxnet, de responsabilidad del señor Diego Noé Pusay Villarroel, ha sido minuciosamente revisado por los miembros del tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal autoriza su presentación.

Ing. Luis Eduardo Hidalgo Almeida; PhD.
PRESIDENTE _____

Ing. Carmen Elena Mantilla Cabrera; Mgtr.
DIRECTORA _____

Ing. Raúl Humberto Cuzco Naranjo; Mgtr.
MIEMBRO _____

Ing. Saúl Yasaca Pucuna; Mgtr.
MIEMBRO _____

Riobamba, agosto de 2023

DEDICATORIA

Este trabajo va dedicado a toda mi familia, en particular a mi esposa Patricia y a mis hijos, por su apoyo constante durante el tiempo de estudios presenciales y la realización del trabajo de investigación final.

Diego

AGRADECIMIENTO

Mi profundo y sincero agradecimiento a Dios todopoderoso por permitirme culminar con éxito la meta de obtener un posgrado, a la Escuela Superior Politécnica de Chimborazo por ser la institución alma mater de mi formación profesional.

Mi sentimiento de gratitud a los docentes que compartieron sus conocimientos y experiencias y en especial a la tutora y miembros del tribunal.

Diego

TABLA DE CONTENIDO

CAPÍTULO IV

CAPÍTULO V

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fundamental del presente trabajo de investigación fue proponer una metodología basado en ISO 27000 para el cumplimiento de los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) en las microempresas proveedoras de acceso a internet, aplicada al caso de estudio Maxxnet. En el desarrollo de la investigación se utilizó el método deductivo con un enfoque cuantitativo, asimismo, se realizó revisión documental, observación, análisis de reportes de criticidad, análisis de vulnerabilidades, escaneo de puertos, evidencias de implementación y gestión. Además, fue necesario las hojas de cálculo, openvas, nessus, nmap, comandos de equipos de red, y checklist, que ayudaron a analizar y propone una metodología de gestión de seguridad informática a la microempresa basados en las Normas ISO 27000. Luego del análisis, la alineación de requerimientos y las características particulares, se generó una propuesta metodológica basada en ocho procesos relacionados entre sí, adoptando 58 de los 114 controles sugeridos en la norma ISO 27002 del 2013, además se desarrolló formatos de políticas de seguridad, procedimientos, checklist, manuales y se proponen herramientas open source que permitan evidenciar la ejecución de un sistema de gestión de seguridad, y a la vez generar los documentos de implementación exigidos por las entidades de control. En consecuencia, la implementación de la metodología propuesta en el caso de estudio Maxxnet, permitió medir su eficacia y evidenciar oportunidades de mejora en la gestión de seguridad informática, alcanzando un cumplimiento total de 55% y parcial de 45% de los controles propuestos. En tal sentido, se recomienda ampliar los controles propuestos por la metodología, debido a que esta se centra en el cumplimiento de los requisitos exigidos por la ARCOTEL, sin embargo, las necesidades de las microempresas pueden ser mucho más amplias.

Palabras Clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <SEGURIDAD INFORMÁTICA>, <INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 27000 (ISO)>, <MICROEMPRESAS>, <INTERNET SERVICE PROVIDER (ISP)>, < AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES (ARCOTEL)>, <NETWORK MAPPER (NMAP)>

SUMMARY

The fundamental objective of this research work was to propose a methodology based on ISO 27000 for compliance with the computer security requirements demanded by the Telecommunications Regulation and Control Agency (ARCOTEL) in microenterprises providing Internet access, applied to the Maxxnet case study. In the development of the research, the deductive method was used with a quantitative approach. Likewise, a documentary review, observation, analysis of criticality reports, vulnerability analysis, port scanning, evidence of implementation and management were carried out. In addition, it was necessary to use spreadsheets, openvas, nessus, nmap, network equipment commands, and checklist, which helped analyze and propose a computer security management methodology for microenterprises based on ISO 27000 Standards. After the analysis , the alignment of requirements and the particular characteristics, a methodological proposal was generated based on eight interrelated processes, adopting 58 of the 114 controls suggested in the ISO 27002 standard of 2013, in addition, formats of security policies, procedures, checklists were developed. , manuals and open source tools are proposed that make it possible to demonstrate the execution of a security management system, and at the same time generate the implementation documents required by the control entities. Consequently, the implementation of the proposed methodology in the Maxxnet case study allowed measuring its effectiveness and evidencing opportunities for improvement in computer security management, achieving total compliance of 55% and partial compliance of 45% of the proposed controls. In this sense, it is recommended to expand the controls proposed by the methodology, because it focuses on compliance with the requirements demanded by ARCOTEL; however, the needs of microenterprises can be much broader.

Keywords: <TECHNOLOGY AND ENGINEERING SCIENCES>, <COMPUTER SECURITY>, <INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 27000 (ISO)>, <MICROENTERPRISES>, <INTERNET SERVICE PROVIDER (ISP)>, < TELECOMMUNICATIONS REGULATION AND CONTROL AGENCY (ARCOTEL)>, <NETWORK MAPPER (NMAP)>

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Problema de investigación

El numeral 24 del artículo 24 de la Ley Orgánica de Telecomunicaciones, establece como obligación de los prestadores de servicios de telecomunicaciones: "Contar con planes de contingencia, para ejecutarlos en casos de desastres naturales o conmoción interna para garantizar la continuidad del servicio de acuerdo con las regulaciones respectivas. Asimismo, cumplirá con los servicios requeridos en casos de emergencia, tales como llamadas gratuitas, provisión de servicios auxiliares para Seguridad pública y del Estado y cualquier otro servicio que determine la autoridad competente de conformidad con la Ley". (Ley Orgánica de Telecomunicaciones, 2015)

Mediante Resolución ARCOTEL-2018-0652 se expide la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones", cuyo objeto es "*establecer criterios y mecanismos de coordinación para que los prestadores de servicios de telecomunicaciones, ejecuten las medidas correspondientes para la gestión de vulnerabilidades e incidentes informáticos, para preservar la seguridad de sus servicios y reducir los riesgos de vulnerabilidad de la red, con un nivel de seguridad acorde al riesgo existente, con el fin de salvaguardar el secreto de las comunicaciones y de la información transmitida por sus redes"*. (ARCOTEL-2018-0652, 2018)

Según el boletín estadístico emitido por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) para el cierre del 2018, la participación en el mercado de acceso internet fijo para "Resto Prestadores", alcanza un 8.50% los cuales constituyen la participación de micro y pequeñas empresas proveedoras de internet. (ARCOTEL, 2019).

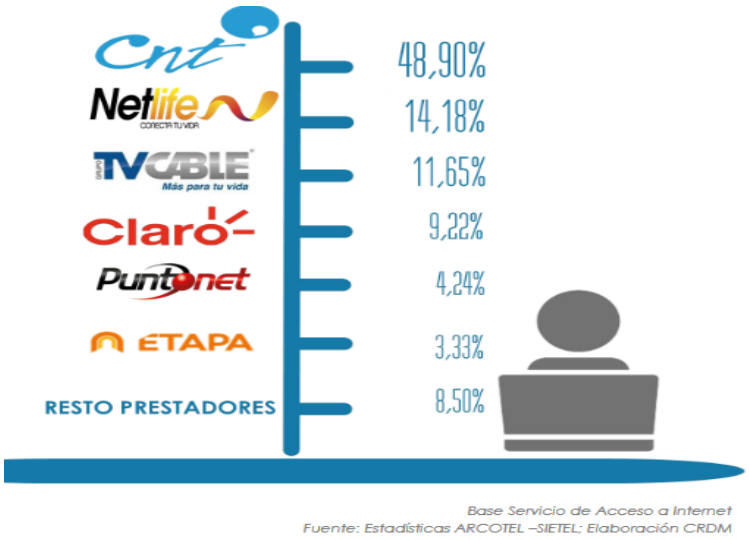


Figura 1-1: Participación de empresas proveedoras de internet
Fuente: ARCOTEL, 2019

La Superintendencia de Compañías, Valores y Seguros, mediante resolución, acogió la clasificación de pequeñas y medianas empresas, PYMES, de acuerdo a la normativa implantada por la Comunidad Andina en su Resolución 1260 y la legislación interna vigente, conforme a la Tabla 1-1: Dimensionamiento de empresas en el Ecuador. (Cámara de Comercio de Quito, 2017).

Tabla 1-1: Dimensionamiento de empresas en el Ecuador

Variables	Microempresa	Pequeña Empresa	Mediana Empresa	Grandes Empresas
Personal Ocupado	De 1-9	De 10-49	De 50-199	>=200
Valor bruto de ventas anuales	<= 100.000	100.001-1.000.000	1.000.001-5.000.000	>5.000.000
Monto de activos	Hasta US$ 100.000	De US$ 100.001 hasta US$ 750.000	De US$ 750.001 hasta US$ 3.999.999	>=4.000.000

Fuente: Cámara de Comercio de Quito, 2017
Realizado por: Pusay, Diego, 2019.

La norma ISO 27000 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Los requerimiento de seguridad informática impuestos por ARCOTEL en 2018, implica niveles de seguridad que no se acoplan a las microempresas por su tamaño, es por esto que al no existir una metodología para este propósito, es necesario generar una, para mejorar la seguridad informática a medida de las micro empresas proveedores de acceso a internet pero basada en normas internacionales que le permita cumplir efectivamente la legislación vigente y fortalecer la seguridad informática de su infraestructura.

1.2 Formulación del problema

¿Qué metodología basada en ISO 27000 se puede aplicar a microempresas proveedoras de acceso a internet para cumplir los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones?

1.3 Sistematización del problema

¿A qué tipos de riesgos están expuestos las mencionadas empresas?
¿Qué controles y buenas prácticas de gestión de seguridad, basados en ISO 27000, se puede implementar para cumplir los requerimientos de seguridad priorizados por las entidades de control?
¿Qué soluciones open source se pueden utilizar para implementar los controles propuestos?
¿Qué tipo de métricas se pueden generar para los controles propuestos?
¿Cómo se comportan los indicadores de seguridad al aplicar la metodología propuesta en el caso de estudio?

1.4 Justificación de la investigación

Los requerimientos de seguridad informática impuestos por la ARCOTEL implican niveles de gestión de seguridad que las microempresas, debido a su tamaño, no pueden permitirse con facilidad.
La creación de una metodología de gestión para la seguridad informática de microempresas proveedoras de acceso a internet basado en ISO 27000, servirá como un referente técnico de alto nivel, para cientos de empresas de este sector productivo, permitiéndoles mejorar la seguridad informática de sus operaciones con estándares internacionales, para el cumplimiento efectivo de las regulaciones nacionales.
La importancia de este tipo de investigaciones radica en el hecho de relacionar los requerimientos técnicos de seguridad informática emitidos por la entidad de control, las particularidades técnicas, operativas y organizacionales de las microempresas proveedoras acceso a internet y los estándares internacionales de gestión de seguridad, todo esto en el contexto nacional.

1.5 Objetivos

1.5.1 *Objetivo General*

Proponer una metodología basado en ISO 27000 para cumplir los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet, aplicada al caso de estudio Maxxnet.

1.5.2 *Objetivos Específicos*

- Diagnosticar los riesgos y vulnerabilidades de microempresa proveedora de servicio: caso de estudio MAXXNET.
- Definir los controles basados en ISO 27001 y 27002 para cumplir los requerimientos de seguridad exigidos por las entidades de control.

- Implementar la metodología propuesta mediante soluciones open-source.
- Evaluar la metodología de seguridad informática propuesta para microempresas proveedoras de acceso a internet en la empresa Maxxnet.

1.6 Hipótesis

La implementación de una metodología basada en ISO 27000 permitirá cumplir con los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes del problema

En el Ecuador la entidad encargada de la administración, regulación y control de las telecomunicaciones a partir del año 2015 es la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

Cumpliendo con su propósito la ARCOTEL, ha emitido requisitos de seguridad informática para cumplimiento obligatorio de todos los prestadores de servicio de acceso a internet, estos prestadores en los últimos años han tenido un crecimiento importante tanto en número como en participación del mercado.

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (Segovia, 2019), en Ecuador se ha adoptado esta norma para la gestión de seguridad informática en las entidades del sector público, a través del Esquema Gubernamental de la Seguridad de la Información (EGSI) y las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000.

2.2 Bases teóricas

Los pilares principales de la familia 27000 son las normas 27001 y 27002. La principal diferencia entre estas dos Normas ISO, es que 27001 se basa en una gestión de la seguridad de forma continuada apoyada en la identificación de los riesgos de forma continuada en el tiempo. En cambio, 27002, es una guía de buenas prácticas que describe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. (Calder, 2017)

ISO 27000: Contiene el vocabulario en el que se apoyan el resto de las normas. Es similar a una guía/diccionario que describe los términos de todas las normas de la familia.

ISO 27001: Es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar.

La norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los cuales se encuentran:

1. **Objeto y campo de aplicación:** Especifica la finalidad de la norma, su uso dentro de una organización y el modo de aplicación del estándar.
2. **Referencias normativas:** recomendación de la consulta a documentos necesarios para la aplicación del estándar.
3. **Término y definiciones:** Los términos y definiciones usados se basan en la norma ISO/IEC 27000.
4. **Contexto de la organización:** Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información (SGSI). Adicional a esto, se debe determinar el alcance.
    - Entendiendo la organización y su contexto
    - Entendiendo las necesidades y expectativas de los implicados
    - Determinando el campo de aplicación del SGSI
    - Sistema de gestión de la seguridad de la información
5. **Liderazgo:** Habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas y asignando a los empleados de la organización roles, responsabilidades y autoridades, asegurando así la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad.
    - Liderazgo y compromiso
    - Políticas
    - Roles organizativos, responsabilidad y autoridades

6. **Planificación:** Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicionalmente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para lograr dichos objetivos también se deben definir en este punto.

    - Acciones para abordar riesgos y oportunidades
    - Objetivos de la seguridad de la información y cómo conseguirlos

7. **Soporte:** Se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada, también se trata en este punto.
    - Recursos
    - Competencias
    - Concienciación
    - Comunicación
    - Información documentación
8. **Operación:** El cómo se debe planificar, implementar y controlar los procesos de la operación, así como la valoración de los riesgos y su tratamiento.
    - Planificación operacional
    - Evaluación de riesgos
    - Tratamiento de los riesgos
9. **Evaluación de desempeño:** Debido a la importancia del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, una medición, un análisis, una evaluación, una auditoría interna y una revisión por la dirección del SGSI del sistema de gestión de la información, para asegurar su correcto funcionamiento.
    - Supervisión, medida, análisis y evaluación
    - Auditorías internas
    - Revisiones de la gestión
10. **Mejora:** Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua.
    - Disconformidades y acciones correctivas
    - Mejora continuada

La segunda parte, está conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia. (Calder, 2017)

ISO 27002: Se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles.
La versión de 2013 del estándar describe los siguientes catorce dominios principales:

1. **Políticas de Seguridad**: Sobre las directrices y conjunto de políticas para la seguridad de la información. Revisión de las políticas para la seguridad de la información.
    - Gestión directiva en seguridad
2. **Organización de la Seguridad de la Información**: Trata sobre la organización interna: asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con grupos de interés especial y seguridad de la información en la gestión de proyectos.

    - Organización interna
    - Dispositivos móviles y teletrabajo

3. **Seguridad de los Recursos Humanos**: Comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Para antes de la contratación se sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo también deben tomarse medidas de seguridad, como lo es des habilitación o actualización de privilegios o accesos.

    - Pre-contratación
    - Durante el contrato
    - Finalización y cambio de contrato

4. **Gestión de los Activos**: En esta parte se toca la responsabilidad sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (directrices, etiquetado y manipulación, manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).

    - Responsabilidad por los activos
    - Clasificación de la información
    - Manejo de los medios de comunicación

5. **Control de Accesos**: Se refiere a los requisitos de la organización para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones.

    - Requisitos empresariales para el control de acceso
    - Gestión del acceso en usuarios
    - Responsabilidades del usuario
    - Control de acceso en sistemas y aplicaciones

6. **Cifrado**: Versa sobre los controles como políticas de uso de controles de cifrado y la gestión de claves.

    - Controles en el cifrado

7. **Seguridad Física y Ambiental**: Habla sobre el establecimiento de áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla).

    - Áreas seguras
    - Equipamiento

8. **Seguridad de las Operaciones**: Procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

    - Procedimientos y responsabilidades operativas
    - Protección ante malware
    - Copias de seguridad
    - Registros y monitoreo
    - Control del software operacional
    - Gestión del as vulnerabilidades técnicas
    - Consideraciones en auditorias de sistemas

9. **Seguridad de las Comunicaciones**: Gestión de la seguridad de la red; gestión de las transferencias de información.

    - Gestión de la seguridad en red
    - Transferencia de información

10. **Adquisición de sistemas, desarrollo y mantenimiento**: Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

    - Requisitos de seguridad en sistemas de la información
    - Seguridad en el desarrollo y proceso de soporte
    - Pruebas

11. **Relaciones con los Proveedores**: Seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.

    - Seguridad de la información en las relaciones con proveedores
    - Gestión de la entrega con proveedores

12. **Gestión de Incidencias que afectan a la Seguridad de la Información**: Gestión de las incidencias que afectan a la seguridad de la información; mejoras.

    - Gestión de incidentes y mejoras

13. **Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio**: Continuidad de la seguridad de la información; redundancias.

    - Continuidad en la seguridad de la información
    - Redundancias

14. **Conformidad**: Conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

    - Conformidad con la ley y los requisitos de contratos
    - Revisiones en la seguridad de la información

ISO 27005: Contiene recomendaciones y directrices enfocadas en la gestión del riesgo, es compatible con los conceptos generales de ISO 27001 y contiene las siguientes secciones:

- Prefacio.
- Introducción.
- Referencias normativas.
- Términos y definiciones.
- Estructura.
- Fondo.
- Descripción del proceso.
- Establecimiento Contexto.
- Información sobre la evaluación de riesgos de seguridad.
- Tratamiento de Riesgos Seguridad de la Información.
- Admisión de Riesgos Seguridad de la información.
- Comunicación de riesgos de seguridad de información.
- Información de seguridad Seguimiento de Riesgos y Revisión.
- Anexos
  - Anexo A: Definición del alcance del proceso.
  - Anexo B: Valoración de activos y evaluación de impacto.
  - Anexo C: Ejemplos de amenazas típicas.
  - Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
  - Anexo E: Enfoques ISRA.

2.3 Marco conceptual

Abonado: Persona que, mediante cuota, tiene derecho a un servicio continuado o periódico a Internet a través de una empresa proveedora. (ARCOTEL, 2016).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ARCOTEL, 2020).

Incidente: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información. (ARCOTEL, 2018).

Seguridad Informática: Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ARCOTEL, 2020)

Metodología: Conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la metodología como el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto. (Eyssautier, 2006)

Normativa: Una normativa es la agrupación de todas aquellas normas que son o pueden ser aplicables en una materia específica, teniendo en cuenta que una norma es un precepto jurídico o ley que regula la conducta de un individuo en una sociedad o espacio determinado, permitiendo así la regulación de ciertas actividades, las normas deben ser respetadas por todos aquellos sujetos hacia los cuales va dirigida, de lo contrario, es decir, el no cumplimiento de la norma acarrea consigo una sanción o pena que deberá ser cumplida por su infractor.

Legal: Que está establecido por la ley o está conforme con ella.

Gestión: El término gestión es utilizado para referirse al conjunto de acciones, o diligencias que permiten la realización de cualquier actividad o deseo. Dicho de otra manera, una gestión se refiere a todos aquellos trámites que se realizan con la finalidad de resolver una situación o materializar un proyecto. En el entorno empresarial o comercial, la gestión es asociada con la administración de un negocio.

Microempresa: Se define como microempresa a la que tiene de 1 a 9 empleados y su volumen de negocio o balance es inferior a los $100.000 USD. (Cámara de Comercio de Quito, 2017)

ISP: Son las siglas de "*Internet Service Provider",* Proveedor de Servicios de Internet, una empresa que proporciona acceso a Internet, es decir que los clientes de un ISP pueden conectarse al internet gracias a la infraestructura aportada por la empresa.

Impacto: El coste para la empresa de un incidente, que puede o no ser medido en términos financieros como pérdida de reputación, implicaciones legales, etc.

Log: Se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.). De esta forma constituye una evidencia del comportamiento del sistema.

IPS/IDS: Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un *software* que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Firewall: Un cortafuego (del término original en inglés *firewall*) es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Calder, 2017)

Puerto: En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

PDCA: El ciclo de Deming (de Edwards Deming), también conocido como ciclo PDCA (del inglés Plan-Do-Check-Act) o PHVA (de la traducción oficial al español como Planificar-Hacer-Verificar-Actuar) o espiral de mejora continua, es una estrategia basada en la mejora continua de la calidad, en cuatro pasos.

Activo Crítico: Para establecer las características de un activo crítico, en el contexto del presente trabajo, se tomará el Artículo 37 de la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones", el cual considera infraestructura crítica aquella que:

- Como resultado de la auditoria se ha determinado que presentan vulnerabilidades.
- Históricamente se ha identificado que son susceptibles a incidentes relacionados con seguridad de las redes y servicios, sobre la base de registros de la propia empresa o de otras empresas.
- Equipos, cuya afectación originada por un incidente o que, como resultado de la materialización de una vulnerabilidad, implique la violación de la seguridad de la red, servicios y de los datos personales de los abonados o clientes, entendiéndose como tal la destrucción, accidental o ilícita, la pérdida, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicio de telecomunicaciones.

Las siguientes definiciones conceptuales son tomadas del Anexo B de la norma ISO 27005 para la gestión de riesgos y parafraseadas en el contexto de las microempresas proveedoras de acceso a internet:

Activos Primarios: Se refieren a los procesos y a la información esencial, central o imprescindible para el negocio, dado el enfoque de la metodología propuesta, en el segmento de las microempresas proveedoras de acceso internet, se debe tener en cuenta que, para identificar los activos primarios se debe tener un enfoque global de la operación del negocio y no solo limitarse a la parte tecnológica.

Procesos Críticos: En el marco de las microempresas podemos encontrar los siguientes: Registro de nuevos clientes, Instalación de servicios, Facturación, Soporte Técnico, Monitoreo de Infraestructura, y otros cuya pérdida o degradación hagan imposible el funcionamiento de la organización.

Información Sensible: Es toda aquella que permite el funcionamiento de la microempresa, generalmente esta almacenada en bases de datos, u hojas de cálculo. Se debe poner énfasis en los registros de datos personales debido al cuidado que exigen las leyes nacionales relacionadas a la privacidad.

Activos de Soporte: Son todos aquellos que permiten la ejecución de procesos críticos, y el acceso a información sensible.

Equipos de procesamiento de datos: Incluye el equipo electrónico para el procesamiento automático de información como son los servidores.

Equipos móviles: Se refiere a equipos de computación portátil como laptops e incluso teléfonos.

Equipos fijos: Son las computadoras utilizadas en las instalaciones de las microempresas.

Sistema Operativo: Lo constituyen todos los programas de un computador que funcionan como base para la ejecución de aplicaciones, servicios o configuraciones, un sistema operativo pone a disposición los recursos de hardware disponibles en un dispositivo electrónico. Tanto las estaciones de trabajo, como servidores y equipos de red administrables cuentan con un sistema operativo que permiten su funcionamiento. Por ejemplo, en servidores es común encontrar sistemas operativos como Centos, Ubuntu, Debían, Windows Server mientras en equipos fijos se encuentra principalmente versiones de escritorio de Windows.

Software de servicio, mantenimiento o administración: Es el software que complementa los servicios del sistema operativo, es importante registrarlos debido a que suelen ser indispensables para el funcionamiento de sistemas de información. En esta categoría encontramos al software de base de datos, servidor de aplicaciones web, etc.

Paquetes de software: Son productos completos, que prestan servicios a los usuarios y a las aplicaciones, pero no son personalizados ni específicos para el negocio, en esta categoría encontramos a las aplicaciones ofimáticas.

Aplicaciones del negocio: Son las aplicaciones que permiten la operación del negocio, como por ejemplo el software de facturación, monitoreo, contabilidad, etc.

Red primaria: La constituye todos los equipos que permiten la conexión a redes externas y la gestión centralizada de los servicios de la red, es denominada también como la red de core, se caracteriza por manejar grandes flujos de datos.

Red secundaria: Está formada por todos equipos que permiten interconectar la red de distribución con la red primaria, en el contexto de las microempresas proveedoras de acceso a internet esta se constituye por los enlaces punto a punto o enlaces de datos con nodos de distribución.

Red distribución: Es el segmento de la red que permite la conexión de los abonados al servicio de internet, generalmente está formada por en transmisor multipunto y un equipo terminal para el cliente.

Personal técnico: Son las personas encargadas de realizar las tareas de gestión técnica en la red como instalaciones, reparaciones, construcción de nodos, monitoreo, etc.

Personal administrativo: Está formado por las personas que se encargan de procesos de venta, facturación, recepción de reclamos, contabilidad, etc.

Instalaciones: La constituye el perímetro de la organización que está en contacto directo con el exterior, generalmente en una microempresa está formada por oficinas de atención a clientes y espacios para los equipos de red.

Servicios esenciales: Normalmente es la energía eléctrica y cualquier otro que sea imprescindible para el funcionamiento de la organización.

Comunicaciones: Son los servicios y equipos de telecomunicaciones suministrados por un operador externo a la organización.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1 Tipo de Investigación

Investigación Cuasi - Experimental: Se podrá observar el comportamiento de las variables dependientes modificando o alterando las variables independientes, sin embargo, no se posee un control total sobre estas variables.

3.2 Diseño de investigación:

Longitudinal: Debido a que se realizará un seguimiento al caso de estudio a lo largo de un periodo completo, para observar la evolución de las características y variables.

3.3 Enfoque de la investigación:

Cuantitativo: Se utilizará procedimientos basados en la medición como enumeración de puertos, cuantificación de requisitos, estimación de riesgo, etc. los cuales generan datos cuantificables numéricamente, que se pueden resumir o inferenciar.

3.4 Métodos:

Deductivo: Se pretende generar una metodología para la gestión de seguridad informática basado en estándares internacionales, que debería funcionar para cada caso particular donde se implemente en el Ecuador, es decir que se espera conclusiones particulares a partir de premisas generales.

3.5 Técnicas:

Revisión documental, observación, análisis de reportes de criticidad, análisis de vulnerabilidades, escaneo de puertos, evidencias de implementación y gestión

3.6 Instrumentos

Hojas de cálculo, openvas, nessus, nmap, comandos de equipos de red, checklist.

3.7 Fuentes de Información

Primarias: Observación directa del estado de controles en el caso de estudio.
Secundarias: Bibliografía, Normas técnicas.

3.8 Planteamiento de la Hipótesis

La implementación de una metodología basada en la norma ISO 27000 permitirá cumplir con los requisitos de seguridad informática exigidos por la Arcotel en microempresas proveedoras de acceso a internet

3.9 Identificación de variables

3.9.1 *Variable Dependiente*

Seguridad Informática: Se observará el comportamiento de esta variable en función de la aplicación de metodología propuesta, para verificar la mejora en la seguridad al medir índices de nivel de riesgo, de cumplimiento, impacto y probabilidad de ocurrencia de un incidente de seguridad informática.

3.9.2 *Variables Independientes*

Metodología para mejorar la seguridad informática para microempresas proveedores de acceso a internet basado en ISO 27000: Es el conjunto de procedimientos y técnica basados en ISO 27000, que tiene el fin de mantener la seguridad informática en microempresas proveedoras de acceso a internet, se cuantifica a través de la evaluación del nivel del riesgo y cumplimiento que se aplica al caso de estudio.

3.9.3 *Operacionalización de variables*

Riesgo: Se define como un producto del impacto por la probabilidad, en la investigación propuesta permitirá cuantificar el nivel de mejora de la seguridad informática del caso de estudio, antes y después de aplicar la metodología propuesta.

Impacto: Valor numérico obtenido mediante el análisis de criticidad a los activos de la empresa.

Probabilidad: Valor numérico obtenido mediante el análisis de vulnerabilidades, a más vulnerabilidades mayor probabilidad de un incidente.

Cumplimiento: Número de normas cumplidas respecto a las normas requeridas, permitirá evaluar la efectividad de la metodología propuesta respecto a los requerimientos de las entidades de control.

3.9.4 *Población*

La población de estudio se rige al total de las microempresas proveedoras de acceso a Internet, legalmente autorizadas por las entidades de control, según circulares ARCOTEL-DEDA-2018 007/008/009-C, dando un total de 356 microempresas registradas en Ecuador (ARCOTEL, 2016).

3.9.5 *Unidad de análisis:*

Maxxnet-Internet, servicios de acceso a internet mediante Resolución ARCOTEL-2017-0064, según reportes de facturación y número de empleados la organización cumple en el segmento de las microempresas (Ver Tabla 1-1), la zona de cobertura autorizada cubre los cantones de Riobamba, Alausí, Colta, Chambo y Penipe, empleando tecnología inalámbrica.

Bajo los parámetros descritos, Maxxnet-Internet cumple con las características propuestas en esta investigación, debido a que se encuentra legalmente autorizada, su tamaño corresponde a una microempresa, además posee la infraestructura y tecnología requeridas en relación a la problemática a investigar.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

La metodología propuesta está basada en la familia de estándares ISO 27000, orientada a su aplicación en microempresas proveedoras de internet, para el cumplimiento de los requerimientos de seguridad informática exigidos por la ARCOTEL.

El desarrollo de este capítulo expondrá una serie de fases estructuradas basados en los estándares mencionados, cada fase requiere entradas de datos, cuyas salidas que sirven como entrada para la siguiente.

La propuesta metodológica define modelos de documentos para normalizar cada una de los procesos con el fin de generar evidencias de implementación y disponer de formatos estandarizados.

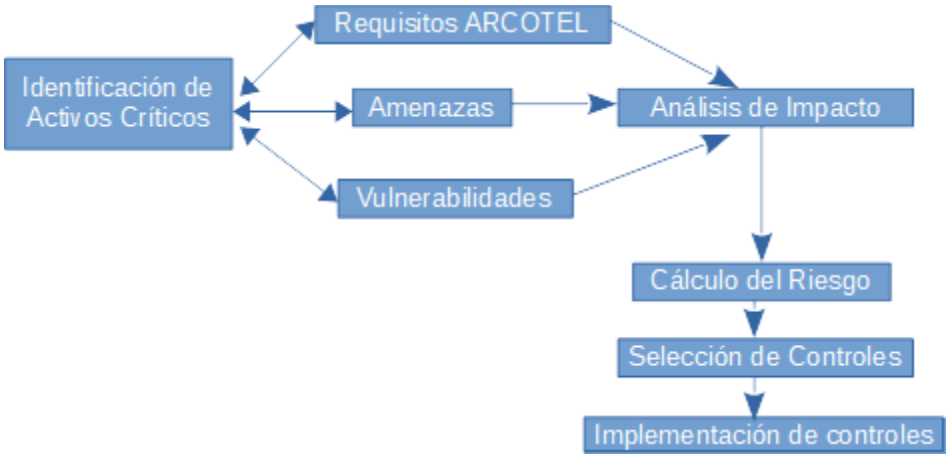


Figura 1-4: Procesos propuesto por la metodología, ISO 27000.
Fuente: ARCOTEL
Realizado por: Pusay, Diego, 2019.

Los resultados de los procesos de gestión de seguridad generan indicadores enmarcados en escalas predefinidas, que facilitan el análisis de niveles de riesgo, y permiten evidenciar los resultados de la gestión de seguridad informática.

Disponer de escalas y procesos predefinidos permite comparar el estado de la seguridad informática de las microempresas a través del tiempo, o incluso compararse con otras de similares características, además podría ser utilizada por las entidades de control como el ARCOTEL, para establecer niveles de gestión regulados en función de las políticas públicas para las telecomunicaciones.

4.1 Análisis de Riesgos

El análisis de riesgos constituye el proceso fundamental para gestionar de manera sistemática la seguridad informática de cualquier organización, nos permite identificar y abordar todos los elementos que influyen en este y la forma en la que estos se relacionan.

Figura 2-4: Relación de factores para la gestión de riesgo
Fuente: ISO 27000, 2015.
Realizado por: Pusay, Diego, 2019.

4.1.1 *Identificación de activos críticos*

La identificación de activos críticos es el primer paso en el desarrollo de la metodología propuesta, proteger estos activos es el objetivo intrínseco de cualquier actividad relacionada a la gestión de seguridad informática.

Para establecer las características de un activo crítico, en el contexto del presente trabajo, se tomará el Artículo 37 de la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones", citado en el Marco conceptual.

Es importante mantener un criterio de clasificación de los activos, para la metodología propuesta se adopta la clasificación propuesta por ISO 27005, en el contexto de las microempresas proveedoras de acceso a internet y su estructura típica.

4.1.1.1 Activos Primarios

- Procesos críticos
- Información sensible

4.1.1.2 *Activos de Soporte*

4.1.1.2.1 *Hardware:*

- Equipos de procesamiento de datos
- Equipos móviles
- Equipos fijos
- Otros dispositivos

4.1.1.2.2 *Software*

- Sistema Operativo
- Software de servicio, mantenimiento o administración
- Paquetes de software
- Aplicaciones del negocio

4.1.1.2.3 *Red*

- Red primaria
- Red secundaria
- Red distribución

4.1.1.2.4 *Personal*

- Personal técnico
- Personal administrativo

4.1.1.2.5 *Sitios*

- Instalaciones
- Servicios esenciales:
- Comunicaciones:

Para la implementación de la metodología conforme a los criterios expuestos se propone el siguiente formulario de identificación de activos críticos:

Tabla 1-4: Plantilla de registro de Activos Críticos

<INSERTE LOGO>	*<NOMBRE DE LA MICROEMPRESA>* **IDENTIFICACIÓN DE ACTIVOS CRÍTICOS** **ACTIVOS** <*PRIMARIOS/SOPORTE*>	**Fecha: _ _ _ _ _ _ _** **Responsable:** **_ _ _ _ _ _ _ _ _ _ _**
UBICACIÓN: _		
COORDENADAS: _		

Ord.	Tipo	Descripción (Nombre, Marca, Modelo)	Cant.	Justificación
1				
2				
3				
…				
n				

Fuente: ARCOTEL, 2016
Realizado por: Pusay Diego, 2019

Indicaciones para el llenado de formulario:

- Se recomienda disponer de un formulario por cada sitio donde se disponga de infraestructura crítica.
- Los espacios con el formato *<CAMPO>* deben ser llenados con los datos particulares de la microempresa.
- Es importante registrar la fecha en la que se levanta la información y el responsable de su ejecución.
- Se recomienda dar nombres únicos a cada ubicación y registrar sus coordenadas geográficas para su rápida localización con un GPS.
- El tipo de activo corresponde a la clasificación pre-establecida.
- La descripción debe incluir un nombre, marca y modelo del activo, cuando corresponda.
- Incluir una breve justificación de la criticidad del activo.

4.11.5 *Identificación de amenazas*

Para evitar tener una larga lista de amenazas y que estas estén relacionadas entre ellas, la norma ISO 27005 recomienda agruparlas por tipo y además identificar su origen por:

- Deliberadas (D)
- Accidentales (A) o
- Ambientales (naturales) (E)

Tabla 2-4: Identificación de amenazas y su origen basado en ISO 27005

Tipo	Amenazas	Origen de la Amenaza
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
Pérdida de los servicios esenciales	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Impulsos electromagnéticos	A, D, E
	Falla del equipo	A
	Mal funcionamiento del equipo	A

Fallas técnicas	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente: ISO 27005, 2015
Realizado por: Pusay Diego, 2019

4.11.6 *Identificación de vulnerabilidades*

Al igual que las amenazas, las vulnerabilidades deben estar agrupadas pero esta vez según el tipo de activo y relacionadas con la amenaza que puede explotarla, considerando que un tipo de activo puede tener muchas vulnerabilidades y una vulnerabilidad puede ser explotada por una amenaza.

Tabla 3-4: Amenazas y Vulnerabilidades basado en ISO 27005.

Tipo de activo	Vulnerabilidad	Amenaza
Hardware	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
Red	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones

	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Gestión inadecuada de la red	Saturación del sistema de información
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Entrenamiento insuficiente en seguridad	Error en el uso
	Falla en los mecanismos de monitoreo	Desconocimiento del estado real de la infraestructura
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Red eléctrica inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo
Organización	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de planes de continuidad	Falla del equipo
	Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo

Fuente: ISO 27005, 2015
Realizado por: Pusay Diego, 2019

4.11.6.1*Análisis automatizado de vulnerabilidades:*

Además de la identificación de vulnerabilidades categorizadas según la Tabla 5-4: Relación entre Amenazas, Vulnerabilidades y tipo de activo basado en ISO 27005, es importante que las microempresas generen capacidades de detección y gestión interna, para lograr estos propósitos se propone tres herramientas, dos de ellas open source y una con licencia comercial (nessus).

Zenmap/Nmap:

Zenmap es la interfaz gráfica de nmap, este software es de código abierto y multiplataforma, permite evaluar el estado de los puertos TCP/UDP de cualquier dispositivo en la red, con el fin de detectar equipos activos, servicios publicados e incluso sistemas operativos.

Es una herramienta básica y esencial para evaluar el nivel de exposición de servicios sin embargo si se requiere un análisis más profundo que incluya reportes, estadísticas y recomendaciones es necesario la implementación de otro tipo de software.

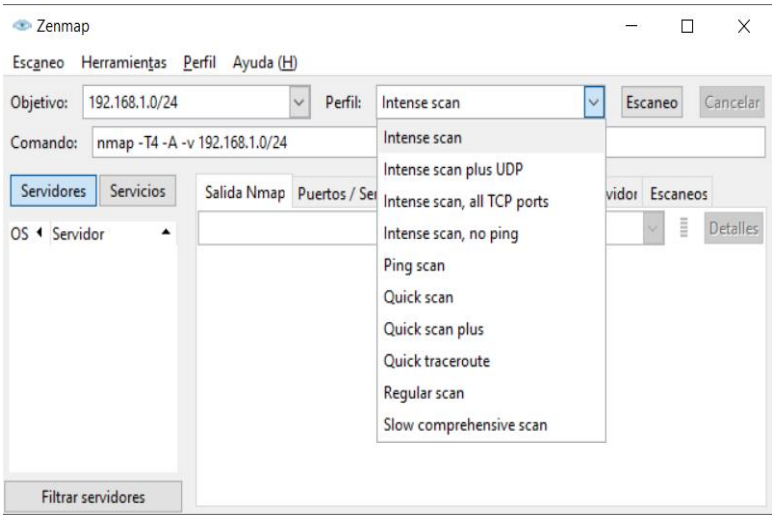


Figura 3-4: Interfaz de Zenmap
Fuente: Zenmap, 2019
Realizado por: Pusay Diego, 2019

Openvas:

Open Vulnerability Assesment System o Sistema Abierto de Evaluación de Vulnerabilidades, es un software open source, que permite identificar de manera profunda las vulnerabilidades que podrían existir y además brinda facilidades para la gestión de estas.

Figura 4-4: Logo OPENVAS
Fuente: Openvas, 2020.

Nessus:

Al igual que OpenVAS, permite realizar análisis automatizados de vulnerabilidades en los equipos críticos de una organización, dispone de una versión comercial y una de uso gratuito con algunas limitaciones, sin embargo, para el contexto de las microempresas es una herramienta que se recomienda.

Figura 5-4: Logo Nessus
Fuente: Tenable, 2019

4.11.7 *Requerimientos de la ARCOTEL (requisitos legales).*

Dentro del marco propuesto para la presente investigación, se analizará el conjunto de requisitos definidos en:

- Numeral 24 del artículo 24 de la Ley Orgánica de Telecomunicaciones.
- Resolución ARCOTEL-2018-0652 se expide la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones"

El numeral 24 del artículo 24 de la Ley Orgánica de Telecomunicaciones, establece como obligación de los prestadores de servicios de telecomunicaciones: "Contar con planes de contingencia, para ejecutarlos en casos de desastres naturales o conmoción interna para garantizar la continuidad del servicio de acuerdo con las regulaciones respectivas. Asimismo, cumplirá con los servicios requeridos en casos de emergencia, tales como llamadas gratuitas, provisión de servicios auxiliares para Seguridad pública y del Estado y cualquier otro servicio que determine la autoridad competente de conformidad con la Ley". (Ley Orgánica de Telecomunicaciones, 2015), por lo tanto, el requerimiento expresado en la ley es que los proveedores de acceso a internet cuenten con planes de contingencia; este tema será abordado durante la implementación de controles alineados a la norma ISO 27002.

La resolución ARCOTEL-2018-0652 expide la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones", cuyo objeto es "*establecer criterios y mecanismos de coordinación para que los prestadores de servicios de telecomunicaciones, ejecuten las medidas correspondientes para la gestión de vulnerabilidades e incidentes informáticos, para preservar la seguridad de sus servicios y reducir los riesgos de vulnerabilidad de la red, con un nivel de seguridad acorde al*

riesgo existente, con el fin de salvaguardar el secreto de las comunicaciones y de la información transmitida por sus redes". (ARCOTEL, 2018)

Análisis de los requerimientos de la norma técnica, enfocado en la generación de un procedimiento interno dentro de las microempresas que sea compatible con lo exigido por la entidad de control:

Tabla 4-4: Análisis de Requerimientos ARCOTEL

Requerimiento ARCOTEL	**Características del procedimiento**
Artículo 6.- Procedimientos de Gestión. - Para preservar la seguridad de sus servicios, reducir el impacto de la ocurrencia de una vulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes, es obligación de los prestadores de servicio de telecomunicaciones establecer procedimientos relacionados con vulnerabilidades e incidentes, en los que se considere al menos el registro, priorización, análisis, escalamiento y gestión.	Al menos: registro, priorización, análisis, escalamiento y gestión.
Artículo 7.- Generación de Notificaciones. - Las notificaciones de vulnerabilidades e incidentes de seguridad de las redes o servicios de telecomunicaciones pueden generarse por: 1. Notificaciones de la ARCOTEL a los prestadores de servicios de telecomunicaciones 2. Notificaciones de los prestadores de servicios de telecomunicaciones a la ARCOTEL	Entradas por notificación desde la ARCOTEL y salidas hacia la ARCOTEL de ser el caso.
Artículo 8.- Categorización y Priorización. - Las notificaciones y reportes que se intercambian entre el ARCOTEL y los prestadores de servicio de telecomunicaciones, así como la información contenida en las mismas, relacionada con la gestión de incidentes y vulnerabilidades, deberán ser categorizadas acorde a los siguientes criterios: 1. Prioridad 2. Categorización	Priorización: Crítica, Alta, Media, Baja, en función del impacto y la urgencia Categorización con Protocolo TLP: Pública General (Blanco), Pública Comunitaria (Verde), Sensible (Ámbar), Confidencial (Rojo)
Artículo 14.- Consideraciones para el intercambio de información a través de correo electrónico. - Los mensajes de correo electrónico generados por la ARCOTEL hacia los prestadores de servicios de telecomunicaciones, y de los prestadores hacia la ARCOTEL, deberán incluir una Cláusula de Confidencialidad…	Controles de seguridad, para el intercambio cifrado de los mensajes de correo electrónico.

La ARCOTEL y los prestadores de servicios de telecomunicaciones, implementarán controles de seguridad; para el intercambio cifrado de los mensajes de correo electrónico y otros documentos necesarios en la gestión de vulnerabilidades e incidentes, tanto para la transmisión de información como para su almacenamiento…	
Artículo 16.- Respaldo. - La información referente a la gestión de incidentes y vulnerabilidades, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios de telecomunicaciones, será respaldada de manera que se garantice la confidencialidad, integridad y disponibilidad de la misma; es obligación del prestador el mantener la evidencia documentada.	Mantener la evidencia documentada, garantizando la confidencialidad, integridad y disponibilidad
Artículo 17.-Conservación. - La información referente a la gestión de vulnerabilidades e incidentes, ya sea notificada por la ARCOTEL o los casos detectados por los prestadores de servicios de telecomunicaciones, será conservada por estos últimos de acuerdo al siguiente detalle: 1. Información Pública General o Pública Comunitaria: durante 6 (seis) meses; 2. Información Sensible: durante un (1) año; 3. Información Confidencial: durante tres (3) años.	Conservar documentación durante el tiempo indicado, dependiendo de la clasificación de la información.
Artículo 18.- Identificación de abonados o clientes relacionados con incidentes y vulnerabilidades.- Con la finalidad de que se puedan gestionar las vulnerabilidades o incidentes, el prestador de servicios de telecomunicaciones deberá almacenar, por un lapso de 1 (un) año, la información relativa a la asignación de direcciones ip de sus clientes o abonados, con el propósito de identificar a clientes o abonados que poseían una dirección IP pública o la dirección IP privada en caso de estar disponible, la información incluirá la fecha y hora en que la IP fue asignada, independientemente de la tecnología o protocolo utilizado para la asignación de direcciones.	Conservar el registro de asignación de direcciones ip públicas o privadas durante un año.
Artículo 19.- Obligación de Información. - En caso de presentarse el riesgo de violación de seguridad a la red pública o de un servicio de telecomunicaciones, los prestadores de servicio de telecomunicaciones informarán dentro de los términos establecidos en el artículo 22 de la presente norma técnica, a sus abonados o clientes sobre dicha vulnerabilidad o incidente y las medidas que adoptará para atenuar o mitigar el riesgo.	Salidas con notificaciones hacia los clientes o abonados con los plazos previstos.
Artículo 22.- Tiempos de recepción, gestión y respuesta de notificaciones. - Los prestadores de servicios de telecomunicaciones deberán cumplir con los siguientes	Tareas de reporte y solución de acuerdo con plazos establecidos.

<table>
<tr>
<td>términos para notificar las acciones implementadas o a implementarse para la gestión de los incidentes y vulnerabilidades reportadas por la ARCOTEL.

a) Para Vulnerabilidades. -
<table>
<tr><th>Prioridad</th><th>Tiempo máximo</th></tr>
<tr><td>Crítica</td><td>4 días hábiles</td></tr>
<tr><td>Alta</td><td>8 días hábiles</td></tr>
<tr><td>Media</td><td>Informativa</td></tr>
<tr><td>Baja</td><td>Informativa</td></tr>
</table>
b) Para Incidentes. -
<table>
<tr><th>Prioridad</th><th>Tiempo máximo</th></tr>
<tr><td>Crítica</td><td>1 día calendario</td></tr>
<tr><td>Alta</td><td>2 días hábiles</td></tr>
<tr><td>Media</td><td>4 días hábiles</td></tr>
<tr><td>Baja</td><td>Informativa</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>Artículo 23.- Estados de Gestión. - La gestión de vulnerabilidades o incidentes por parte del prestador de servicios de telecomunicaciones podrá tener los siguientes estados: Atendido, Pendiente, En análisis.</td>
<td>Identificación del estado de la gestión.</td>
</tr>
<tr>
<td>Artículo 30.- Gestión de incidentes y vulnerabilidades que involucren las redes de los abonados o clientes. Si la gestión al problema presentado en la red del abonado o cliente, consiste en el bloqueo o limitación de ciertos contenidos o aplicaciones,…, el prestador de servicios de telecomunicaciones podrá proceder con dicho bloqueo o limitación siempre y cuando el abonado o cliente manifieste expresamente su consentimiento, o por disposición de la autoridad competente…

1. Para los casos en los que la gestión de incidentes o vulnerabilidades de las redes públicas de telecomunicaciones requiera correctivos por parte del cliente o abonado, el prestador de servicio informará al abonado o cliente acerca del particular, indicándole las medidas técnicas que debe tomar para solucionar el problema…</td>
<td>Informar a los clientes de las medidas tomadas o solicitar la remediación en sus redes.</td>
</tr>
</table>

Fuente: ARCOTEL, 2018
Elaboración: Pusay Diego, 2019

4.11.8 *Identificación y valoración de impacto*

El impacto es uno de los factores que definen directamente el riesgo, el propósito de la metodología es definir una escala cuantitativa basada en un criterio cualitativo asociado a un nivel de impacto, entendible por quien realiza un análisis.

La definición de la escala de impacto adopta un criterio basado en la infraestructura típica de una microempresa proveedora de acceso a internet.

Tabla 5-4: Valoración del Impacto

Impacto	Criterio	Valor
Bajo	Afecta a un solo radio transmisor	1
Medio Bajo	Afecta a varios radios transmisores de un nodo	2
Medio	Afecta totalmente a un nodo de transmisión	3
Medio Alto	Afecta a varios nodos de transmisión	4
Alto	Afecta a toda la red	5

Fuente: ARCOTEL, 2018
Realizado por: Pusay Diego, 2019

4.11.9 *Cálculo del riesgo*

El valor del riesgo para la metodología propuesta adopta su definición más común, es simplemente el producto del impacto por la probabilidad.

$$Riesgo = Impacto\ x\ Probabilidad$$

La cuantificación del impacto fue definida en la sección anterior Tabla 6-4, mientras la escala cualitativa de la probabilidad es definida en la siguiente tabla:

Tabla 6-4: Valoración de la probabilidad

Probabilidad	Criterio	Frecuencia	Valor
Improbable	Más de 10 años	Muy Poco frecuente	1
Remoto	Cada varios años	Poco Frecuente	2
Posible	Una a tres veces al año	Normal	3
Probable	Mensual o más de tres veces al año	Frecuente	4
Muy Probable	A diario o semanal	Muy Frecuente	5

Fuente: ARCOTEL, 2018.
Realizado por: Pusay Diego, 2019.

La valoración de la probabilidad asocia criterios basados en la frecuencia de ocurrencia de un evento o incidente que comprometa la seguridad informática de un activo, y le asigna un valor numérico que permitirá multiplicarlo por el valor establecido para el impacto y de esta forma obtener un valor numérico para el riesgo.

Una vez establecidas las escalas para el impacto y la probabilidad debemos relacionarlas con las categorías de amenazas identificadas, para lograrlo se utiliza la siguiente tabla:

Tabla 7-4: Matriz de relación entre impacto y probabilidad

Ord.	Activos	Impacto	Probabilidad de que se materialice una Amenaza			
			Amenaza 1	Amenaza 2	…	Amenaza m
1	Activo 1	x_1	p_{11}	p_{21}	…	p_{m1}
2	Activo 2	x_2	p_{12}	p_{22}	…	p_{m2}
3	Activo 3	x_3	p_{13}	p_{23}	…	p_{m3}
…	…	…	…	…	..	..
n	Activo n	x_n	p_{1n}	p_{2n}	…	p_{mn}

Fuente: ISP, 2019
Realizado por: Pusay Diego, 2019

Siendo m el número de categorías de amenazas identificadas y n el número de activos críticos de la microempresa. x_n el valor del impacto del activo n y p_{mn} la probabilidad de que la amenaza m se materialice en el activo n.

Finalmente se construye la matriz de riesgo, en la cual se multiplica el valor x_n del impacto por p_{mn} de la probabilidad, obteniendo un valor numérico para el riesgo.

Tabla 8-4: Matriz de Riesgo

Ord.	Activos	RIESGO			
		Amenaza 1	Amenaza 2	…	Amenaza m
1	Activo 1	$x_1 * p_{11}$	$x_1 * p_{21}$	…	$x_1 * p_{m1}$
2	Activo 2	$x_2 * P_{12}$	$x_2 * p_{22}$	…	$x_2 * p_{m2}$
3	Activo 3	$x_3 * P_{13}$	$x_3 * p_{23}$	…	$x_3 * p_{m3}$
…	…	…	…	…	…
n	Activo n	$x_n * P_{1n}$	$x_n * p_{2n}$	…	$x_n * p_{mn}$

Fuente: Pusay Diego, 2019
Realizado por: Pusay Diego, 2019

Obtenidos valores cuantitativos para el riesgo es necesario fijar una escala cualitativa, que facilite su análisis y la generación de un mapa de calor, con el fin de priorizar la atención de aquellos riesgos que se encuentren en niveles inaceptables para la microempresa.

Debido a que el riesgo está conformado por dos factores (impacto y probabilidad), y la escala predefinida para estos está entre 1 y 5 el valor máximo no superará 25, este valor es distribuido en una escala cualitativa conformada por: Bajo, Moderado, Alto, Extremo.

Tabla 9-4: Escala de nivel de riesgo

Escala	Nivel de Riesgo
1-7	Bajo
8-14	Moderado
15-20	Alto
20-25	Extremo

Fuente: Pusay Diego, 2019
Realizado por: Pusay Diego, 2019

4.12 Selección de controles ISO 27002

La selección de controles propuesta se centra en el cumplimiento de los requisitos exigidos por la ARCOTEL y en los riesgos identificados, sin embargo, este criterio puede variar dependiendo de las microempresas, para su desarrollo se toma como referencia la "declaración de aplicabilidad", que es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información.

El objetivo de este proceso es definir cuáles de los 133 controles sugeridos son los que se implementará y cuáles no, en función del análisis de riesgos y requerimientos del ARCOTEL presentado en las secciones anteriores.

El criterio de selección es:

- **SI:** El control permite gestionar el riesgo identificado y/o cumplir con lo exigido por el ARCOTEL.
- **NO:** El control puede ser implementado a futuro, bajo el contexto de la metodología propuesta no es de aplicación obligatoria.

Tabla 10-4: Selección de controles ISO 27002

Sección	Controles	Seleccionado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	SI
A5.1.2	Revisión de las políticas para la seguridad de la información	SI
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	SI
A6.1.2	Segregación de tareas	SI
A6.1.3	Contacto con las autoridades	SI
A6.1.4	Contacto con grupos de interés especial	NO
A6.1.5	Seguridad de la información en la gestión de proyectos	NO
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	NO
A6.2.2	Teletrabajo	NO
A7	**Seguridad relativa a los recursos humanos**	
A7.1	**Antes del empleo**	
A7.1.1	Investigación de antecedentes	NO
A7.1.2	Términos y condiciones del empleo	NO
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	SI
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	NO
A7.2.3	Proceso disciplinario	NO
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	
A7.3.1	Responsabilidades ante la finalización o cambio	NO
A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	SI
A8.1.2	Propiedad de los activos	NO
A8.1.3	Uso aceptable de los activos	NO
A8.1.4	Devolución de activos	NO
A8.2	**Clasificación de la información**	

A8.2.1	Clasificación de la información	SI
A8.2.2	Etiquetado de la información	SI
A8.2.3	Manipulado de la información	SI
A8.3	**Manipulación de los soportes**	
A8.3.1	Gestión de soportes extraíbles	NO
A8.3.2	Eliminación de soportes	NO
A8.3.3	Soportes físicos en tránsito	SI
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
A9.1.1	Política de control de acceso	SI
A9.1.2	Acceso a las redes y a los servicios de red	SI
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	SI
A9.2.2	Provisión de acceso de usuario	SI
A9.2.3	Gestión de privilegios de acceso	SI
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	SI
A9.2.5	Revisión de los derechos de acceso de usuario	SI
A9.2.6	Retirada o reasignación de los derechos de acceso	SI
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	NO
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	SI
A9.4.2	Procedimientos seguros de inicio de sesión	NO
A9.4.3	Sistema de gestión de contraseñas	SI
A9.4.4	Uso de utilidades con privilegios del sistema	SI
A9.4.5	Control de acceso al código fuente de los programas	NO
A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	SI
A10.1.2	Gestión de claves	SI
A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.1	Perímetro de seguridad física	SI
A11.1.2	Controles físicos de entrada	SI

A11.1.3	Seguridad de oficinas, despachos y recursos	SI
A11.1.4	Protección contra las amenazas externas y ambientales	SI
A11.1.5	El trabajo en áreas seguras	NO
A11.1.6	Áreas de carga y descarga	NO
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	SI
A11.2.2	Instalaciones de suministro	NO
A11.2.3	Seguridad del cableado	NO
A11.2.4	Mantenimiento de los equipos	NO
A11.2.5	Retirada de materiales propiedad de la empresa	NO
A11.2.6	Seguridad de los equipos fuera de las instalaciones	NO
A11.2.7	Reutilización o eliminación segura de equipos	NO
A11.2.8	Equipo de usuario desatendido	NO
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	NO
A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	SI
A12.1.2	Gestión de cambios	NO
A12.1.3	Gestión de capacidades	NO
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	NO
A12.2	**Protección contra el software malicioso (malware)**	
A12.2.1	Controles contra el código malicioso	SI
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	SI
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	SI
A12.4.2	Protección de la información del registro	SI
A12.4.3	Registros de administración y operación	SI
A12.4.4	Sincronización del reloj	SI
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en explotación	NO
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	SI
A12.6.2	Restricción en la instalación de software	NO

A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	NO
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	SI
A13.1.2	Seguridad de los servicios de red	SI
A13.1.3	Segregación en redes	SI
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	SI
A13.2.2	Acuerdos de intercambio de información	SI
A13.2.3	Mensajería electrónica	SI
A13.2.4	Acuerdos de confidencialidad o no revelación	SI
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	
A14.1	**Requisitos de seguridad en los sistemas de información**	
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	NO
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	NO
A14.1.3	Protección de las transacciones de servicios de aplicaciones	NO
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	
A14.2.1	Política de desarrollo seguro	NO
A14.2.2	Procedimiento de control de cambios en sistemas	NO
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	NO
A14.2.4	Restricciones a los cambios en los paquetes de software	NO
A14.2.5	Principios de ingeniería de sistemas seguros	NO
A14.2.6	Entorno de desarrollo seguro	NO
A14.2.7	Externalización del desarrollo de software	NO
A14.2.8	Pruebas funcionales de seguridad de sistemas	NO
A14.2.9	Pruebas de aceptación de sistemas	NO
A14.3	**Datos de prueba**	
A14.3.1	Protección de los datos de prueba	NO
A15	**Relación con proveedores**	
A15.1	**Seguridad en las relaciones con proveedores**	

A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	NO
A15.1.2	Requisitos de seguridad en contratos con terceros	NO
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	NO
A15.2	**Gestión de la provisión de servicios del proveedor**	
A15.2.1	Control y revisión de la provisión de servicios del proveedor	NO
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	NO
A16	**Gestión de incidentes de seguridad de la información**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	SI
A16.1.2	Notificación de los eventos de seguridad de la información	SI
A16.1.3	Notificación de puntos débiles de la seguridad	SI
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	SI
A16.1.5	Respuesta a incidentes de seguridad de la información	SI
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI
A16.1.7	Recopilación de evidencias	SI
A17	**Gestión de la continuidad de negocio**	
A17.1	**Continuidad de la seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI
A17.1.2	Implementar la continuidad de la seguridad de la información	SI
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	SI
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI
A18.1.2	Derechos de Propiedad Intelectual (DPI)	NO
A18.1.3	Protección de los registros de la organización	NO
A18.1.4	Protección y privacidad de la información de carácter personal	SI
A18.1.5	Regulación de los controles criptográficos	SI

A18.2	Revisiones de la seguridad de la información	
A18.2.1	Revisión independiente de la seguridad de la información	SI
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI
A18.2.3	Comprobación del cumplimiento técnico	SI

Fuente: ISO 27002
Realizado por: Pusay Diego, 2019

4.13 Implementación de controles

La implementación de controles constituye la fase que más esfuerzo técnico requiere, además es el paso final, según la metodología propuesta. Después de la identificación y valoración de los riesgos junto a los requerimientos del ARCOTEL y la selección de controles alineados a la norma ISO 27002 finalmente en esta etapa se propone un conjunto de herramientas y configuraciones que permitirán el cumplimiento de los controles propuestos.

Para el desarrollo de esta etapa final, se propone utilizar la pirámide documental de cuatro niveles sugerida por la norma ISO 9001 para la gestión de calidad, pero enfocada a la gestión de seguridad informática:

Figura 6-4: Pirámide documental ISO 9001
Fuente: ISO 9001
Elaborado por: *Pusay Diego, 2019*

4.13.5 Manual de gestión de seguridad

El manual de gestión de seguridad es el documento del cual parten y deben alinearse, todas las actividades relacionadas a la gestión de seguridad.

Para fines de la metodología propuesta el manual de gestión de seguridad está constituido por la "Política de Seguridad de la Información", la cual consta de las siguientes partes:

- Objetivos
- Alcance
- Marco Legal
- Política de Seguridad

Entre las características que destacan en la política propuesta es su alineación a los 14 dominios sugeridos por la norma ISO 27002:2013, además su marco legal se ajusta a los requerimientos de seguridad exigidos por el ARCOTEL.

El detalle de la política propuesta, así como los campos que se recomienda llenar se detalla en el Anexo A.

4.13.6 *Procedimientos*

4.13.6.1Plan de contingencia

El plan de contingencia es un instrumento de gestión que contiene las medidas técnicas, humanas y organizativas para procurar la continuidad del negocio y las operaciones de una organización, el requerimiento de este plan por parte de la ARCOTEL viene acompañado de un modelo de formato que debe ser llenado y aprobado por el representante legal de la microempresa.

La estructura del modelo es la siguiente:

- Aprobación del Plan
- Marco Legal
- Introducción
  - Presentación Institucional
  - Presentación Técnica
  - Diagrama Operacional de la Red
- Principios, Metas y Objetivos
- Análisis de Amenazas, Vulnerabilidades y Riesgos
- Planes y acciones institucionales
  - Planes y Acciones para la Prevención
  - Procedimientos y acciones para la recuperación
  - Planes y Acciones de resiliencia

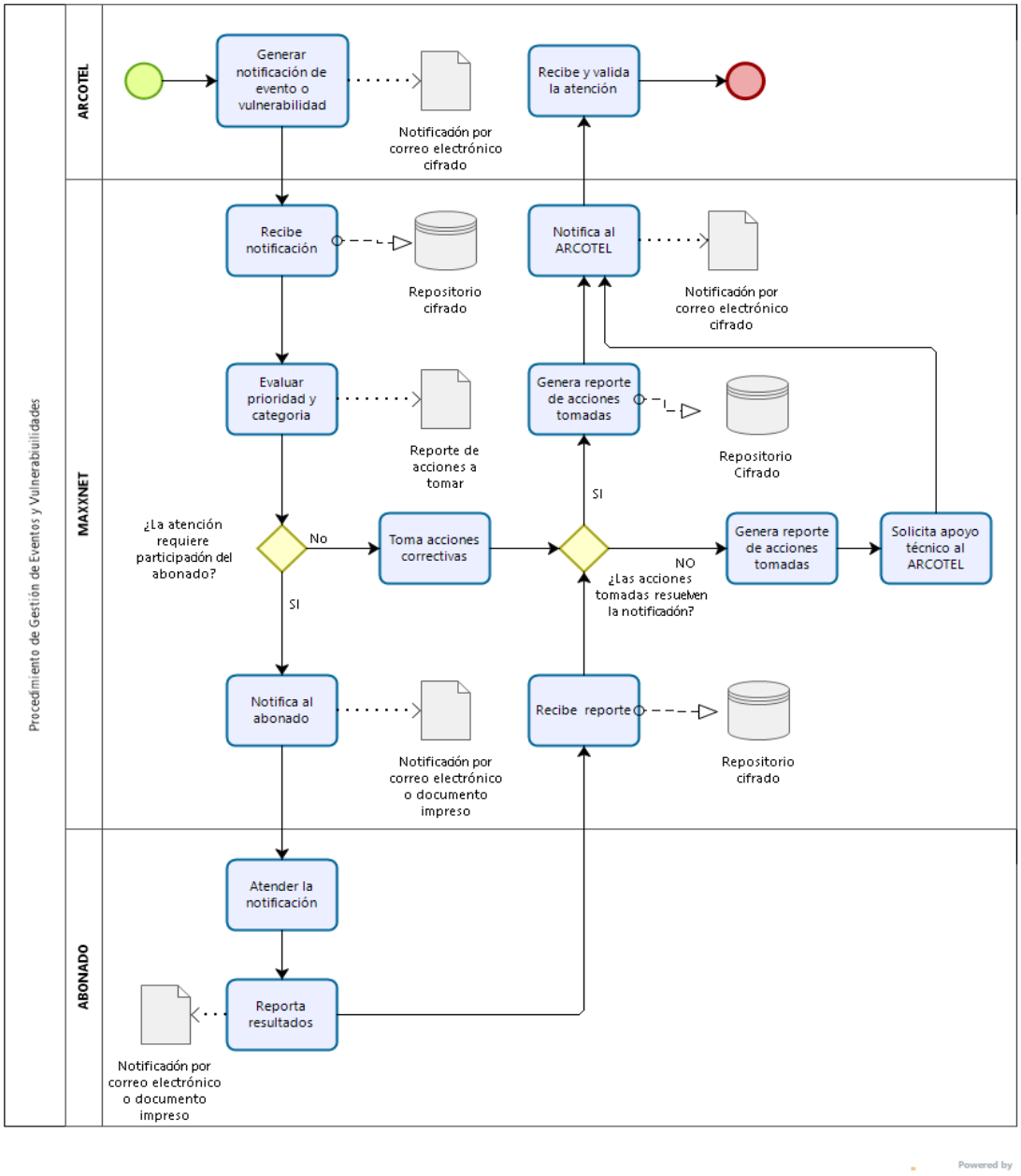
- Estimado de recursos (humanos, técnicos, logísticos, económicos), para la ejecución de las actividades del plan de contingencia
- Responsabilidades y funciones para el personal encargado de la ejecución del plan de contingencia, e información de contacto
- Planes de capacitación para el personal involucrado en el plan de contingencia, respecto a la ejecución de este.
- Planificación para la realización de simulacros o pruebas relacionadas con la aplicación del Plan de Contingencia.
- Informe de ejecución de las pruebas de la evaluación del Plan de Contingencia del año inmediato anterior.
- Apéndices

El desarrollo del formato modelo se expone detalladamente en el Anexo B: Plan de Contingencia, donde destaca el uso de la metodología propuesta en este trabajo para determinar el nivel de riesgo.

4.13.6.2Procedimiento de gestión de eventos

La metodología propuesta se centra en el procedimiento de gestión de eventos y vulnerabilidades debido a que es uno de los principales requisitos del ARCOTEL, por lo cual, el procedimiento planteado cumple con los requerimientos analizados en la sección 4.1.4, resumidos en la tabla 5-4.

PROCEDIMIENTO DE GESTIÓN DE EVENTOS Y VULNERABILIDADES	***Versión:***	*1.0*
	Fecha:	*10/10/2019*
Objetivos: Establecer criterios y mecanismos de coordinación para ejecutar las medidas correspondientes para la gestión de vulnerabilidades e incidentes informáticos.		
Desarrollo:		



Canales de Comunicación:

- Correo electrónico normal/cifrado

4.13.6.3Check list, instrucciones, formularios

4.13.6.3.1 Checklist de respaldos periódicos de configuración.

Los Checklists nos permiten llevar un registro de cumplimiento de tareas periódicas que deben ser realizadas conforme lo estipulen las políticas, manuales o procedimientos de seguridad.

Por ejemplo, si el procedimiento de seguridad indica que se debe hacer respaldos de los archivos de configuración de los equipos de la red primaria cada mes, se debe generar un checklist donde

se pueda registrar el cumplimiento de esta tarea, es importante que el documento especifique claramente su título, el responsable y las indicaciones de la tarea a cumplir.

Tabla 11-4: *Ejemplo de Checklist*

MaxxNet Internet	**CHECK LIST DE RESPALDO DE CONFIGURACIÓN**							**Responsable:** Ing. Paola Pérez					
Marque con una X en el mes que corresponda, una vez que haya realizado el respaldo completo de configuración de los equipos y después de respaldar los archivos en el repositorio designado													
No	**Equipo**	**EN**	**FE**	**MA**	**AB**	**MA**	**JU**	**JL**	**AG**	**SE**	**OC**	**NO**	**DI**
1	Firewall de Borde, Pfsense, XG-1541 1U												
2	Ruteador Principal Multipuerto, Mikrotik, CCR1036-12G-4S												
3	Servidor Facturación/Monitoreo, HP, DL325												
4	Switch POE, Ubiquiti, EdgeSwitch 8												
5	Radio Transmisor Punto Punto con antena, Ubiquiti, airFiber 5XHD												
6	Radio Transmisor Multipunto con antena, Ubiquiti, Rocket M5												
7	Switch de Core, Mikrotik, CRS125-24G-1S-IN												

Fuente: Maxxnet, 2019
Realizado por: Pusay Diego, 2019

4.13.6.3.2 Instrucciones de configuración de firewall perimetral.

El firewall perimetral es uno de los componentes fundamentales para mantener niveles de seguridad informática adecuados, para el caso de estudio se utilizó Pfsense debido a que es uno de las soluciones open source más utilizadas, además dispone de soporte comercial.

Figura 7-4: Logo de pfsense
Fuente: Pfsense

Para facilitar la implementación de controles de acceso, y supervisar tanto el tráfico interno como el externo hacia los servidores de la microempresa, se debe ubicar el firewall perimetral con al menos tres interfaces de alta velocidad de la siguiente manera:

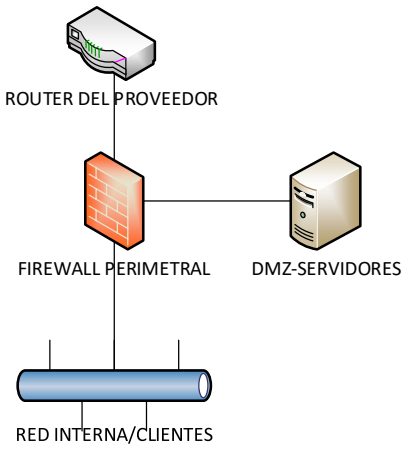


Figura 8-4: Ubicación del Firewall perimetral
Fuente: Pfsense
Realizado por: Pusay Diego, 2019

Todos los servidores deben estar en el segmento de red DMZ-SERVIDORES, y el acceso debe estar limitado mediante una regla de firewall, solamente se debe acceder a este segmento desde la red administrativa o la red de oficinas.

La regla por defecto del firewall debe ser bloquear todo, y abrir solo los puertos necesarios, cada regla debe llevar un comentario que resuma su uso de manera entendible.

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	0 /4.59 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
☐ ✔	0 /0 B	IPv4 TCP	192.168.0.0/24	*	172.16.99.2	80 (HTTP)	*	none		Acceso aplicativo de cobros
☐ ✖	0 /2 KiB	IPv4 *	*	*	172.16.99.0/24	*	*	none		Bloqueo el acceso a la DMZ

Figura 9-4: Ejemplo de regla de acceso a la DMZ

Realizado por: Pusay Diego, 2019

4.13.6.3.3 Instrucciones de generación y configuración de correo cifrado

Para la gestión de correo cifrado se recomienda el uso de thunderbird más el complemento enigmail.

1. Descargue e instale el software thunderbird (https://www.thunderbird.net/en-US/download/)

Figura 10-4: Logo de cliente de correo Thunderbird

Fuente: Thunderbird

2. Configure el software con la cuenta de correo con la cual va a intercambiar correo cifrado.

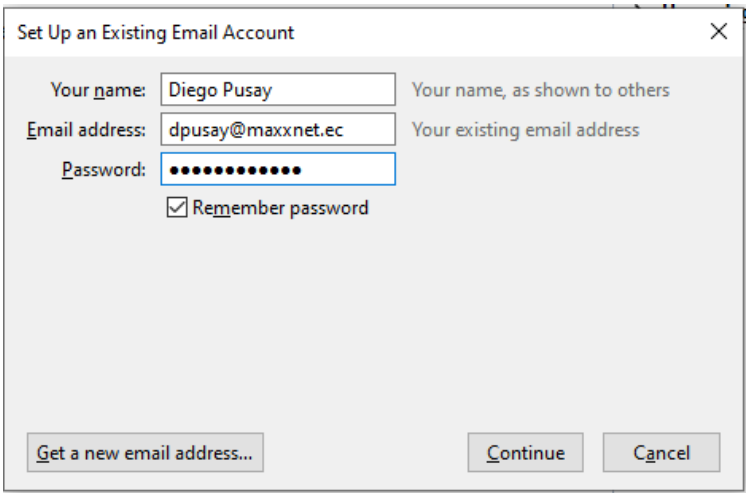


Figura 11-4: Configuración de correo en Thunderbird

Realizado por: Pusay Diego, 2019

3. *Agregue el Addon Enigmail en Thunderbird*

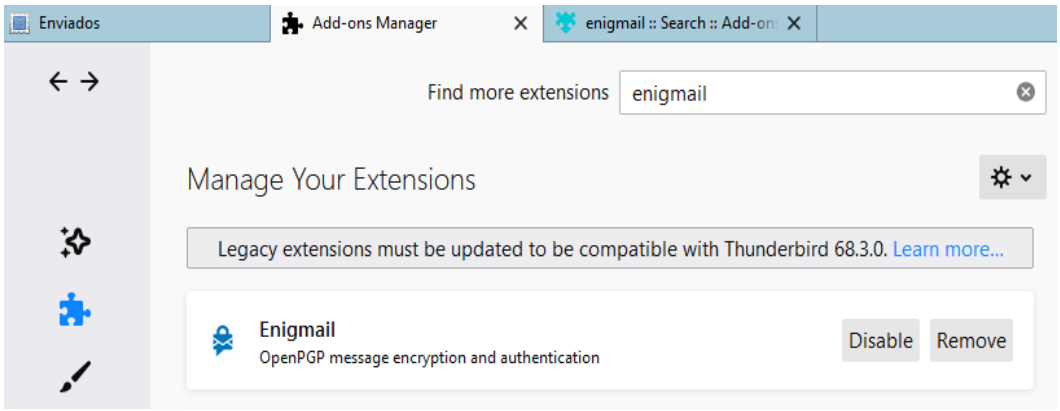


Figura 12-4: Addon Enigmail en Thunderbird
Realizado por: Pusay Diego, 2019

4. Instale GPG4win (https://gpg4win.org/thanks-for-download.html)

Figura 13-4: Logo de GNUPG
Realizado por: Pusay Diego, 2019

5. Ejecute el Setup Wizard de GnuPG
6. Utilice Enigmail Key Management para exportar su clave pública e importar claves públicas de sus contactos.

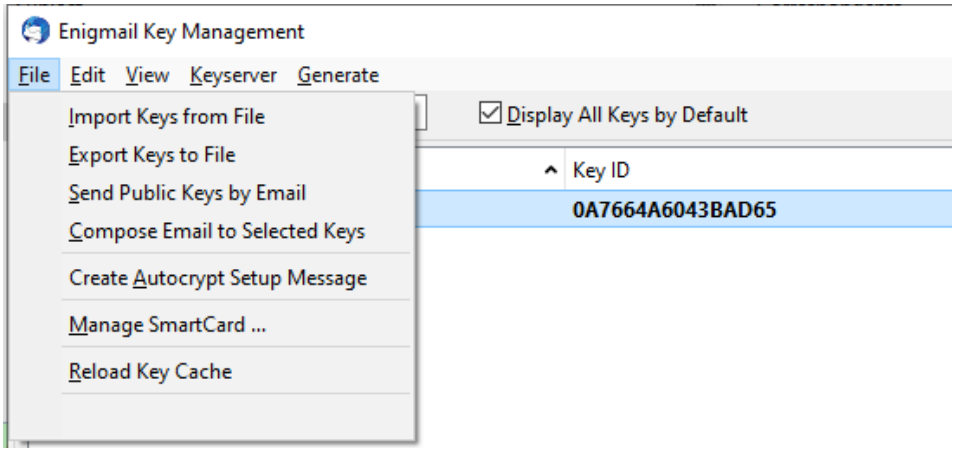


Figura 14-4: Interface Enigmail Key Management
Realizado por: Pusay Diego, 2019

7. Utilice la función cifrar y firmar para intercambiar correos cifrados.

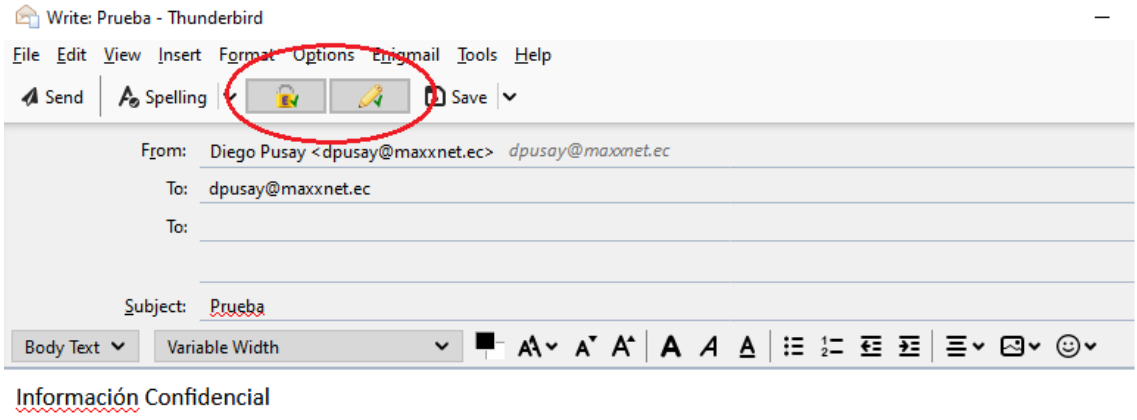


Figura 15-4: Opciones de Cifrado y Firmado en Thunderbird
Realizado por: Pusay Diego, 2019

4.13.6.3.4 Instrucciones de generación y administración de contraseñas seguras

Para la gestión de contraseñas seguras se recomienda el uso de KeePass en su versión más reciente, este software permite almacenar credenciales en una base de datos cifrada, además permite la generación de contraseñas fuertes.

1. Descargue e instale KeePass (https://sourceforge.net/projects/keepass/files/KeePass%202.x/2.43/KeePass-2.43-Setup.exe/download)

Figura 16-4: Logo de KeePass
Fuente: keepass.info
Realizado por: Pusay Diego, 2019

2. Ejecute el programa y cree una base de datos en blanco, le solicitarán una “Master Password”, sea cuidadoso al elegirla porque con esta clave se cifrará la Base de Datos de credenciales.

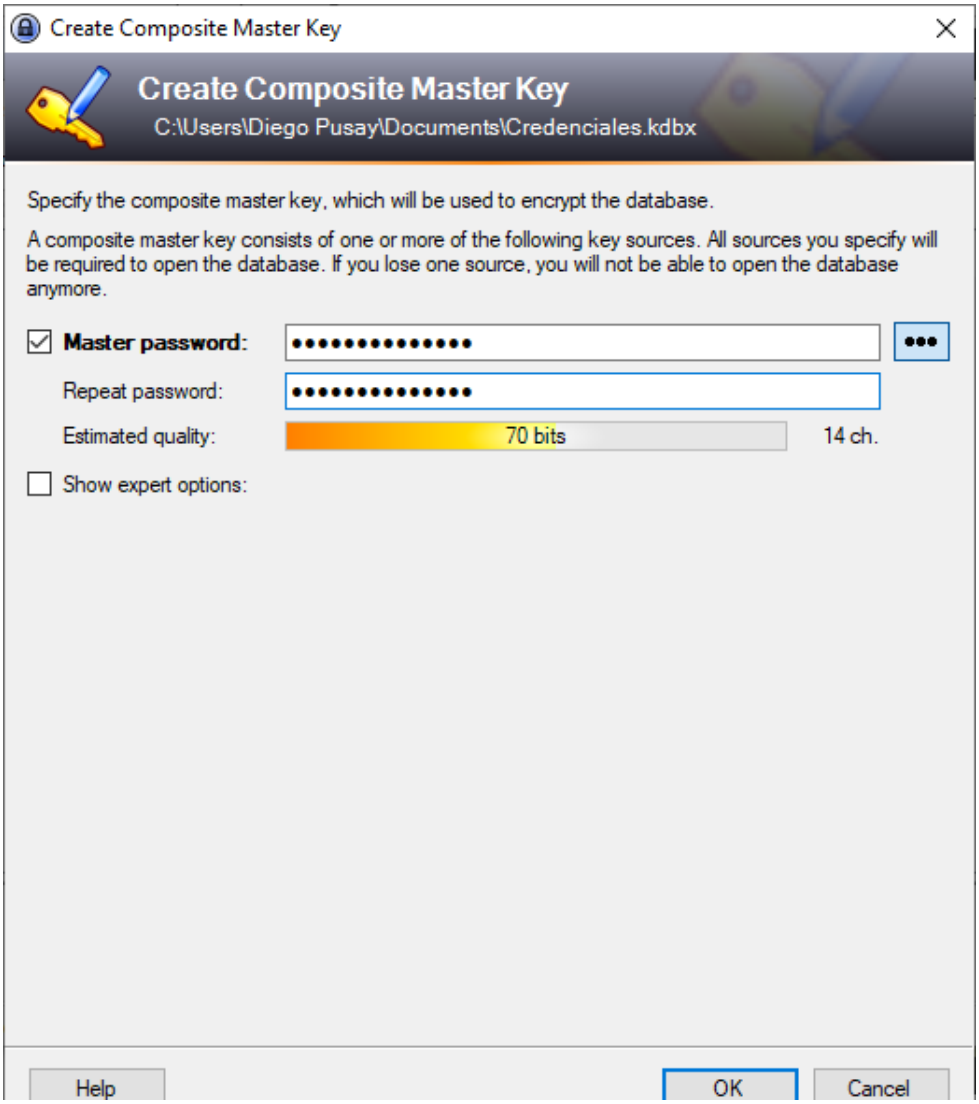


Figura 17-4: Master Password para base de datos de KeePass
Realizado por: Pusay Diego, 2019

3. Ingrese en el software las credenciales con privilegios de equipos y sistemas críticos de su organización.

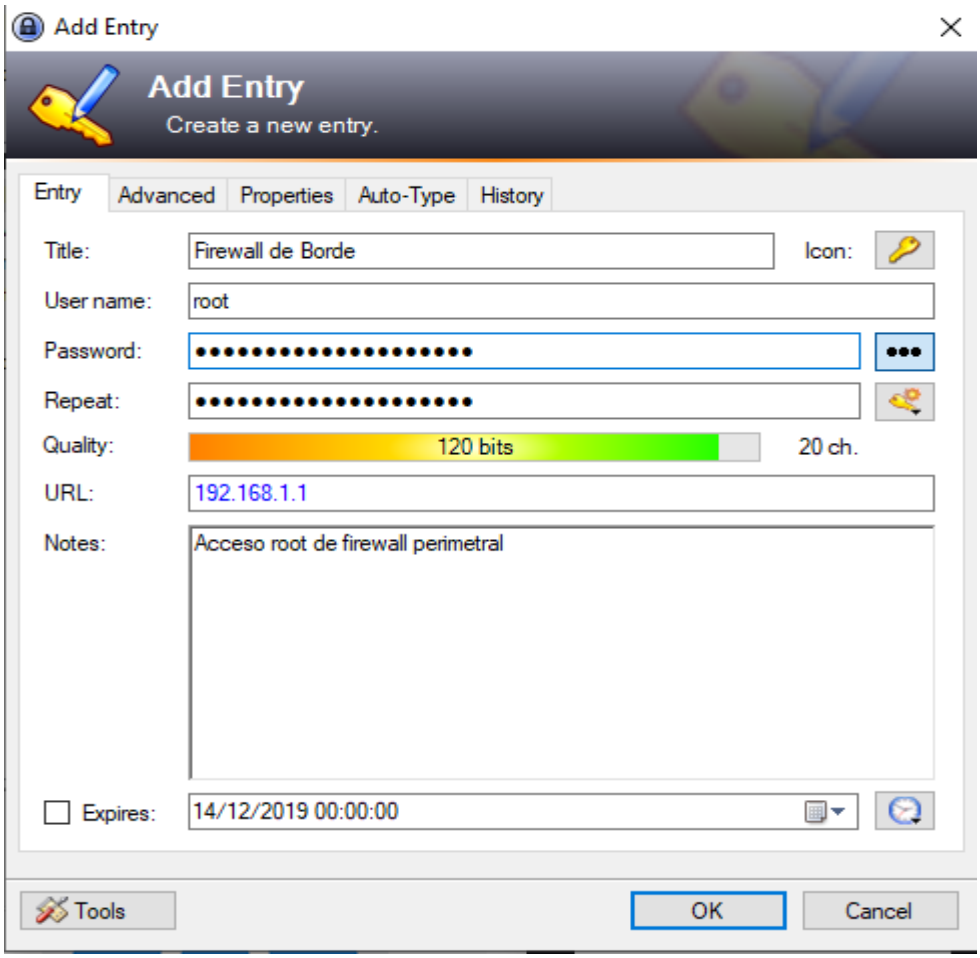


Figura 18-4: Generación e Ingreso de credenciales en KeePass
Realizado por: Pusay Diego, 2019

4. Una vez completada la información respalde la BD de datos en un lugar seguro, y utilice credenciales que identifiquen a cada una de las personas que ingresan a los equipos y sistemas, evitando usuarios y claves genéricas como user, admin, técnicos, etc.

4.13.7 *Registro de eventos*

4.13.7.1Almacenamiento de logs con logalyze.

Para la gestión de logs de activos críticos se recomienda LOGalyze, debido a su facilidad de instalación y funcionalidades para el análisis y almacenamiento de logs.

Figura 19-4: Logo de Logalyze
Fuente: Logalyze
Realizado por: Pusay Diego, 2019

1. Descargue e instale la herramienta de su sitio oficial http://www.logalyze.com/
2. Siga el proceso indicado en los manuales, al terminar la instalación podrá acceder al sistema mediante un navegador web, apuntando a la dirección ip del servidor en el puerto 8080.

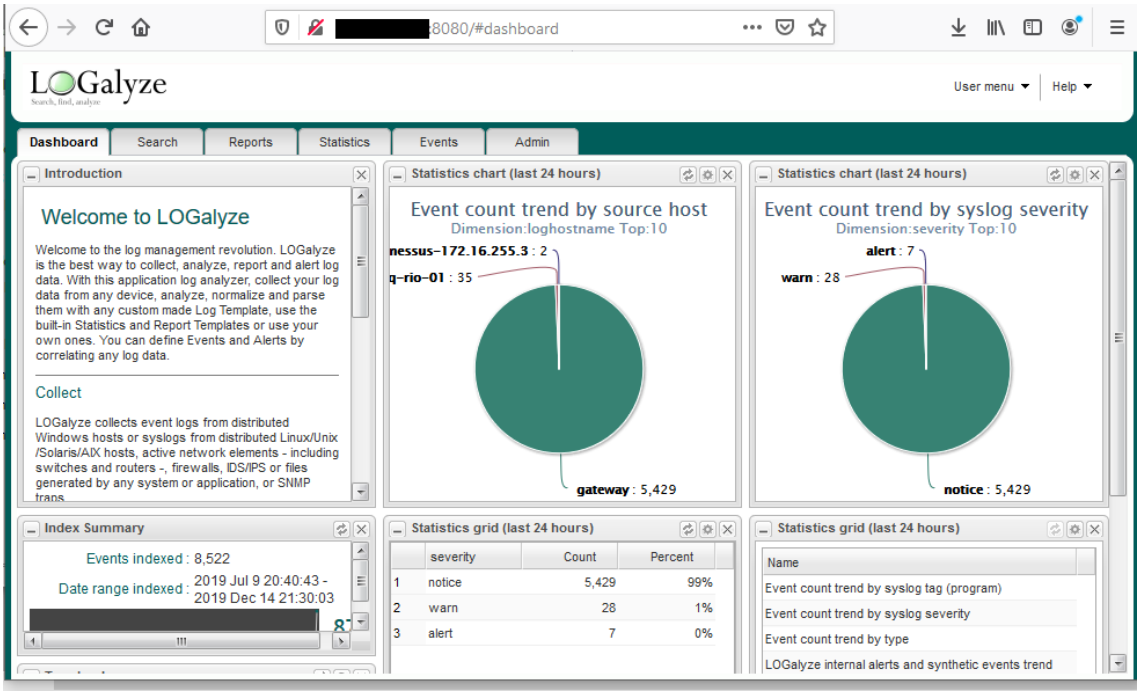


Figura 20-4: Interface de Logalyze
Fuente: Logalyze, 2019
Realizado por: Pusay Diego, 2019

3. Asegúrese de que el servidor es accesible solo desde segmentos de red administrativos y desde los equipos que necesite almacenar logs.
4. Configure sus equipos para que envíen sus logs al servidor remoto.
5. Para equipos Mikrotik: dentro de winbox elija la opción system/logging y configure la acción remota con la dirección ip y el puerto de escucha de logs del servidor, por defecto logalyze recepta logs en el puerto TCP/UDP 1670.

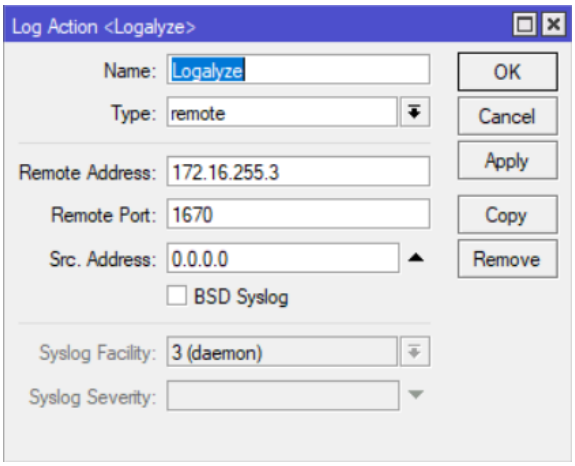


Figura 21-4: Configuración de envío de logs mikrotik
Realizado por: Pusay Diego, 2019

6. Seleccione los topics de logs que serán enviados a logalyze.
7. Para equipos ubiquiti en la pestaña Services configure la dirección IP y el puerto de logalyze.

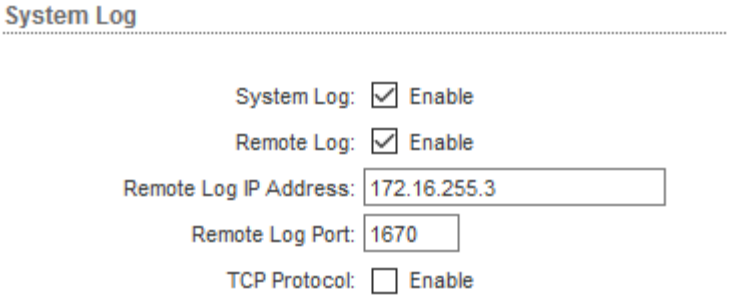


Figura 22-4: Envío de Logs ubiquiti
Realizado por: Pusay Diego, 2019

CAPÍTULO V

5. PROPUESTA

5.1 Análisis de resultados

Para la presentación de resultados se evaluará la implementación de la metodología propuesta en el caso de estudio Maxxnet la cual presta servicios de acceso a internet a hogares y pymes, a través de redes inalámbricas, en los cantones de Alausí y Riobamba pertenecientes a la provincia de Chimborazo.

La matriz se encuentra en la ciudad de Riobamba, en las calles Espejo y Chimborazo, se dispone de los siguientes números telefónicos de contacto: 0999060601, 032 376690, del correo electrónico info@maxxnet.ec y del sitio web: www.maxxnet.ec

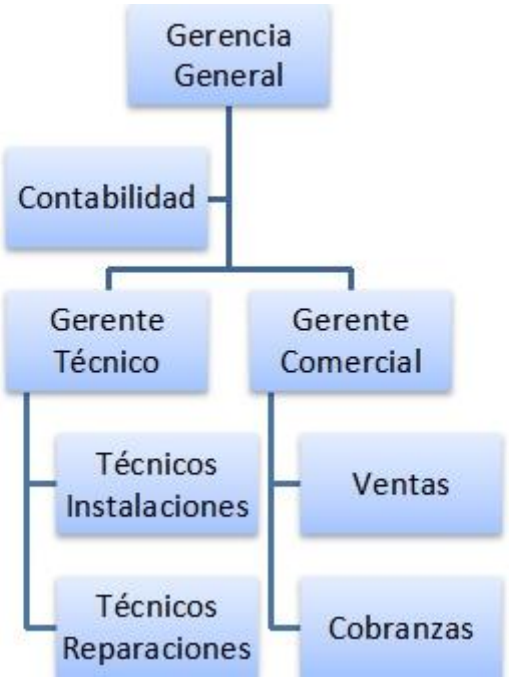


Figura 1-5 Estructura organizacional Maxxnet
Realizado por: Pusay Diego, 2019

Descripción del Sistema:

- La red de transporte cuenta con dos nodos centrales uno en Alausí y otro en Riobamba, a los cuales se conectan nodos secundarios desde donde se conectan los abonados.
- En los nodos principales también existen abonados directamente conectados.
- Los únicos puntos de salida hacia el Internet son los nodos principales, desde donde se accede a través de fibra óptica.

- La conexión entre los nodos es a través de radio enlaces.
- Los nodos centrales cuentan con UPS, banco de baterías y generador eléctrico, para mantenerlos operativos.
- Los nodos secundarios disponen de UPS con banco de baterías y un sistema de alarma en caso de corte de energía.
- En los nodos centrales se dispone de generadores eléctricos portable para ser trasladados a los nodos secundarios en caso de cortes de energía.

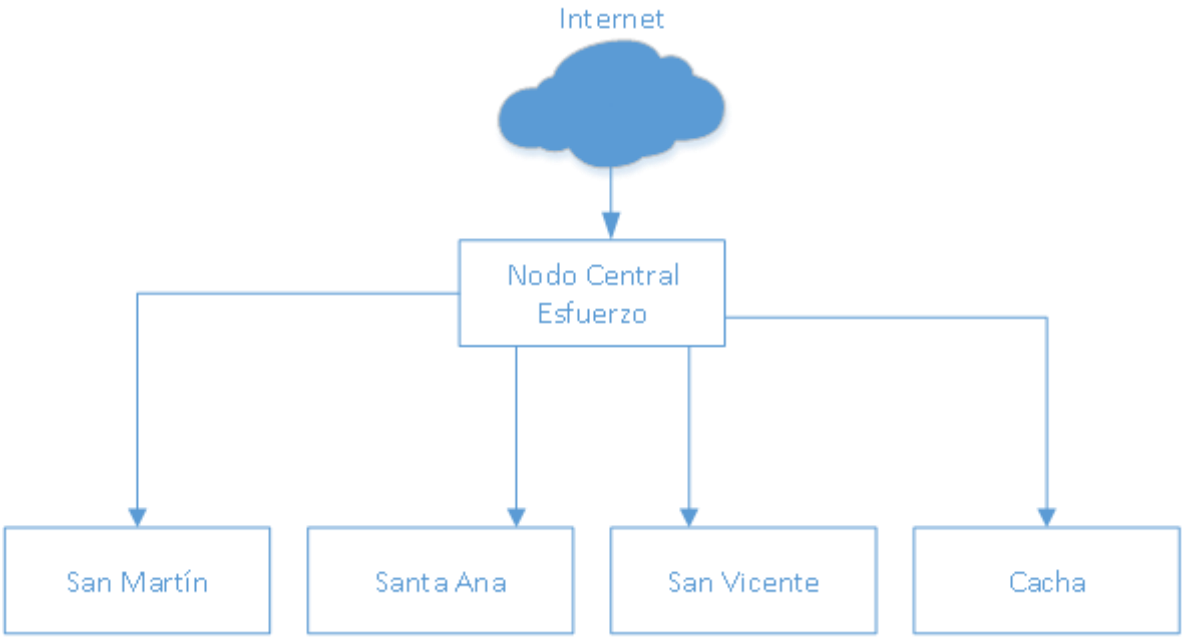


Figura 2-5: Nodos de transmisión Riobamba
Realizado por: Pusay Diego, 2019

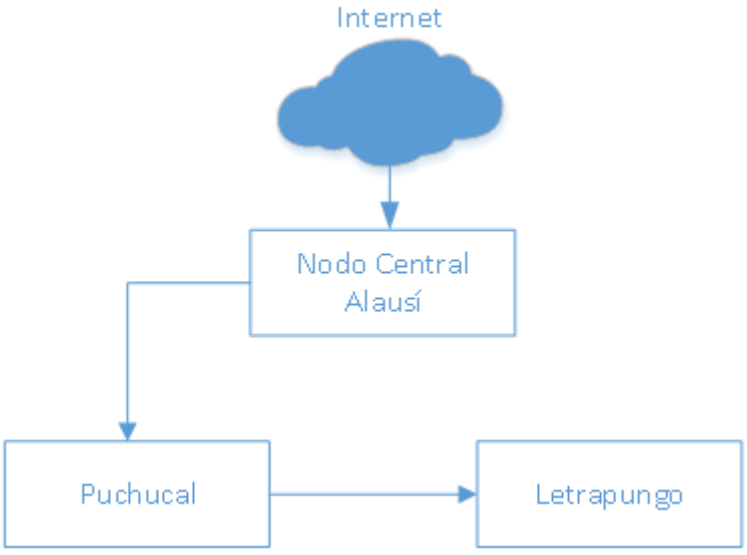


Figura 3-5: Nodos de transmisión Alausí
Realizado por: Pusay Diego, 2019

Según lo mostrado en la Figura 2-4: Flujo de procesos propuesto por la metodología, y desarrollada cada una de las etapas en el capítulo anterior podemos resumir lo siguiente:

Tabla 1-5: Resumen de la metodología propuesta.

Ord.	Etapa	Entradas y Actividades	Salida
1	Identificación de Activos Críticos	**Actividad:** Enumeración y categorización de activos críticos	**Tabla 1-4:** Plantilla de registro de Activos Críticos.
2	Identificación de Requisitos, Amenazas y Vulnerabilidades		
2.1	Requisitos ARCOTEL	Numeral 24 del artículo 24 de la Ley Orgánica de Telecomunicaciones. Resolución ARCOTEL-2018-0652: "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones" **Actividad:** Identificación de características y evidencias para demostrar el cumplimiento.	**Anexo 2:** Modelo de plan de contingencia. **Tabla 4-4:** Análisis de Requerimientos ARCOTEL
2.2	Amenazas	**Tabla 1-4:** Plantilla de registro de Activos Críticos. **Actividad:** Identificación y categorización de amenazas	**Tabla 13-4:** Identificación de amenazas y su origen basado en ISO 27005
2.3	Vulnerabilidades	**Tabla 1-4:** Plantilla de registro de Activos Críticos. **Actividad:** Relación entre amenazas y vulnerabilidades, identificación automatizada de vulnerabilidades.	**Tabla 14-4:** Relación entre Amenazas, Vulnerabilidades y tipo de activo basado en ISO 27005. Herramientas para la detección automatizada de vulnerabilidades: nessus, zenmap, openvas.
3	Análisis de Impacto	**Tabla 1-4:** Plantilla de registro de Activos Críticos. **Tabla 15-4:** Relación entre Amenazas, Vulnerabilidades y tipo de activo basado en ISO 27005. **Actividad:** Ponderación del impacto basado en la identificación, categorización y relación de activos, amenazas y vulnerabilidades.	**Tabla 16-4:** Valoración de la probabilidad **Tabla 19-4:** Valoración del Impacto

4	Cálculo de Riesgo	**Tabla 18-4:** Valoración de la probabilidad **Tabla 19-4:** Valoración del Impacto	**Tabla 20-4:** Matriz de relación entre impacto y probabilidad **Tabla 21-4:** Matriz de Riesgo **Tabla 22-4:** Escala de nivel de riesgo
5	Selección de Controles	**Tabla 23-4:** Matriz de Riesgo	**Tabla 24-4:** Selección de controles ISO 27002
6	Implementación de Controles	**Tabla 25-4:** Selección de controles ISO 27002	Manual de gestión de seguridad Plan de contingencia Procedimiento de gestión de eventos Procedimiento de gestión de vulnerabilidades Check list, instrucciones, formularios Registro de eventos

Fuente: Pusay, Diego, 2019

Realizado por: Pusay Diego, 2019

*5.1.1 **Identificación de Activos Críticos***

La identificación de activos se realizó con el formulario propuesto por la metodología, llenando los campos con los datos obtenidos del caso de estudio.

Tabla 2-5: Identificación de activos críticos Maxxnet.

LEONARDO BENALCAZAR-MAXXNET **IDENTIFICACIÓN DE ACTIVOS CRÍTICOS** **ACTIVOS DE SOPORTE**				**Fecha:** 28/08/20219 **Responsable:** Ing. Paola Pérez
Ord.	**Tipo**	**Descripción**	**Cant.**	**Justificación**
1	Red Primaria	Ruteador del Proveedor, CISCO, 800 Series	1	Equipo mediante el cual se recibe el servicio por parte de los proveedores.

2	Red Primaria	Firewall de Borde, Pfsense, XG-1541 1U	1	NAT de direcciones y controles de seguridad, publicación de servicios.
3	Red Primaria	Ruteador Principal Multipuerto, Mikrotik, CCR1036-12G-4S	1	Equipo para controlar velocidades, y cortes de servicio a clientes impagos.
4	Equipo de procesamiento de datos	Servidor Facturación/Monitoreo, HP, DL325	1	Equipo con máquinas virtuales que ejecutan los sistemas de cobros, registro de clientes y monitoreo de la infraestructura.
5	Red Primaria	Switch POE, Ubiquiti, EdgeSwitch 8	3	Equipos L2, con POE para dar conectividad y energía a los equipos montados en la torre.
6	Red Primaria	Radio Transmisor Punto Punto con antena, Ubiquiti, airFiber 5XHD	10	Equipos para enlazar nodos secundarios.
7	Red Primaria	Radio Transmisor Multipunto con antena, Ubiquiti, Rocket M5	8	Equipos para conectar clientes finales.
8	Red Primaria	Switch de Core, Mikrotik, CRS125-24G-1S-IN	1	Equipo para concetar la red de core.
9	Otros dispositivos	Generador Eléctrico,	1	Equipo para suplir de energía en caso de cortes eléctricos prolongados.
10	Otros dispositivos	UPS, APC, SURTA1500XL	1	Equipo para soportar cortes de energía.
11	Otros dispositivos	Banco de Baterías	1	Suministran energía para el UPS en caso de cortes prolongados.
12	Instalaciones	Torre metálica	1	Sostiene los equipos y antenas de transmisión.

Fuente: Maxxnet, 2019
Realizado por: Pusay Diego, 2019

*5.1.2 **Identificación de Requisitos, Amenazas y Vulnerabilidades***

Para cumplir con los requisitos de seguridad informática exigidos por la ARCOTEL, y mitigar las amenazas y vulnerabilidades detectadas, para el caso de estudio Maxxnet se categorizaron 6 tipos de amenazas:

- Daño Físico
- Eventos Naturales
- Pérdida de servicios esenciales

- Perturbación radio eléctrica
- Fallas técnicas
- Compromisos de funciones

La categorización de amenazas se realizó conforme a lo propuesto en el capítulo 4.

Además, mediante el escaneo de puertos con nmap se detectó gran cantidad de puertos y servicios abiertos sin la debida segregación.

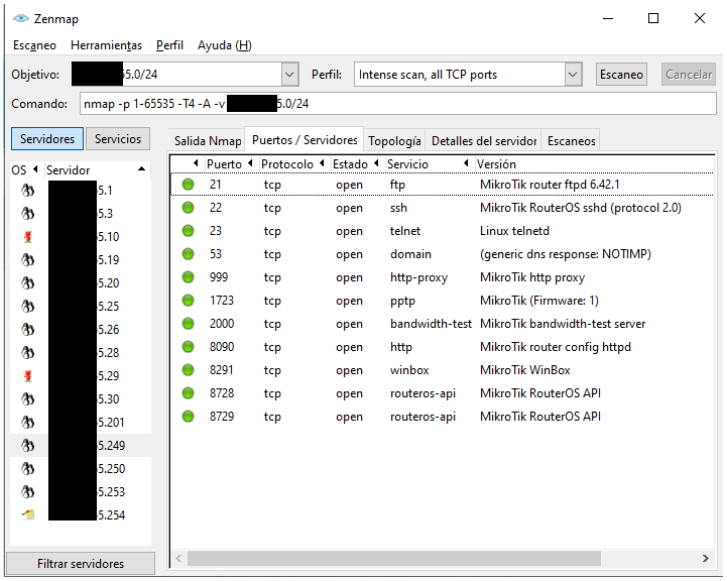


Figura 4-5: Resultados nmap, caso Maxxnet
Fuente: Zenmap, 2019
Realizado por: Pusay Diego, 2019

El análisis automatizado mediante Nessus detectó vulnerabilidades que deben ser tratadas a la brevedad posible, la mayor parte de ellas relacionadas a la actualización de versiones de firmware, certificados de seguridad auto firmados y servicios expuestos, que se utilizan para acceder a la gestión de los equipos mediante entornos web.

Por motivos de confidencialidad no se expondrán todos los hallazgos encontrados en el caso de estudio.

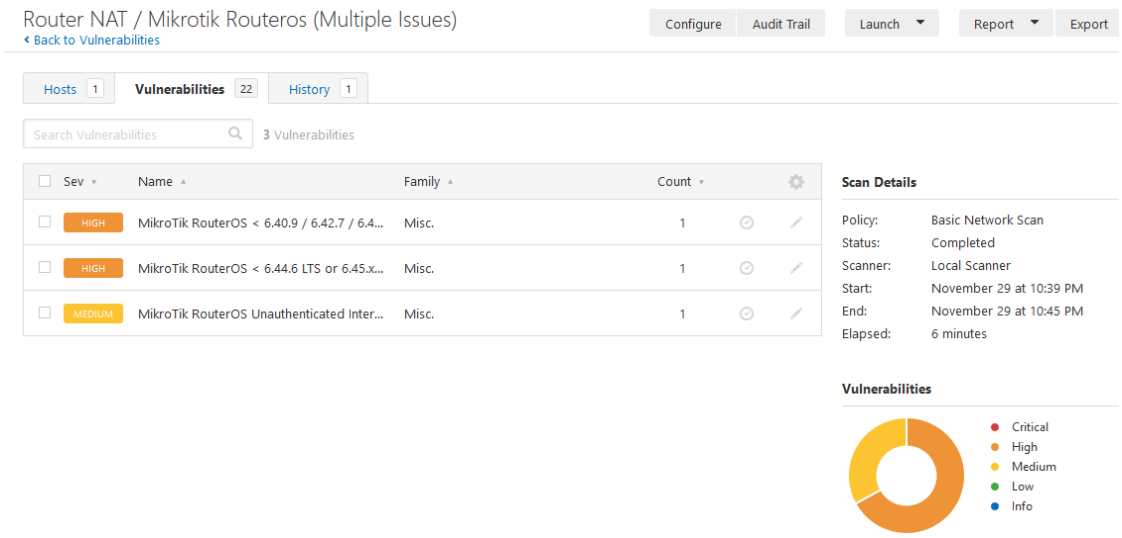


Figura 5-5: Resultados nessus, caso Maxxnet
Fuente: Router NAT, 2019
Realizado por: Pusay Diego, 2019

*5.1.3 **Análisis de impacto***

Se analizó los activos enumerados en la fase anterior y se asignó un valor de acuerdo con la escala generada por la metodología.

Tabla 3-5: Análisis de impacto.

Activos de Soporte	**Impacto**	**Probabilidad de materialización de Amenazas**					
		Daño Físico	**Eventos Naturales**	**Pérdida de servicios esenciales**	**Perturbación Radio-eléctrica**	**Fallas Técnicas**	**Compromiso de las funciones**
Ruteador del Proveedor	5	2	1	3	2	2	2
Firewall de Borde	5	2	1	3	2	2	3
Ruteador Principal Multipuerto	5	2	1	3	2	2	3
Servidor de Facturación/Monitoreo	1	2	1	3	2	2	2
Switch POE	4	2	1	3	2	2	2
Radio Transmisor Punto Punto	3	3	2	3	4	3	3

Radio Transmisor Multipunto	3	3	2	3	4	3	3
Switch de Core	5	2	1	3	2	2	3
Generador Eléctrico	1	3	1	1	1	2	1
UPS	1	2	1	1	1	2	1
Banco de Baterías	1	2	1	1	1	2	1
Torre metálica	5	2	2	1	1	1	1

Fuente: Maxxnet, 2019
Realizado por: Pusay Diego, 2019

5.1.4 Cálculo de Riesgo

El cálculo del riesgo se realizó conforme a la escala y a la fórmula propuesta por la metodología, además para su mejor análisis se implementó formato condicional a cada celda conforme a la Tabla 11-4: Escala de nivel de riesgo, permitiéndonos obtener un mapa de calor del nivel de riesgo de los activos críticos de la microempresa.

Tabla 4-5: Mapa de calor del riesgo, Caso Maxxnet.

Activos	Riesgo					
	Daño Físico	**Eventos Naturales**	**Pérdida de servicios esenciales**	**Perturbación debido a la radiación**	**Fallas Técnicas**	**Compromiso de las funciones**
Ruteador del Proveedor	10	5	15	10	10	10
Firewall de Borde	10	5	15	10	10	15
Ruteador Principal Multipuerto	10	5	15	10	10	15
Servidor de Facturación/Monitoreo	2	1	3	2	2	2
Switch POE	8	4	12	8	8	8
Radio Transmisor Punto Punto con antena	9	6	9	12	9	9

Radio Transmisor Multipunto con antena	9	6	9	12	9	9
Switch de Core	10	5	15	10	10	15
Generador Eléctrico	3	1	1	1	2	1
UPS	2	1	1	1	2	1
Banco de Baterías	2	1	1	1	2	1
Torre metálica	10	10	5	5	5	5

Fuente: Maxxnet, 2019

Realizado por: Pusay Diego, 2019

*5.1.5 **Selección de Controles***

La metodología propone la selección de 58 de los 114 controles enunciados por la ISO 27002, los insumos para el cumplimiento de esos controles se detallan en el capítulo 4, sin embargo, se debe notar que el enfoque propuesto se centra en el cumplimiento de los requisitos exigidos por la ARCOTEL, mientras las ISO 27002 los aborda de manera más general.

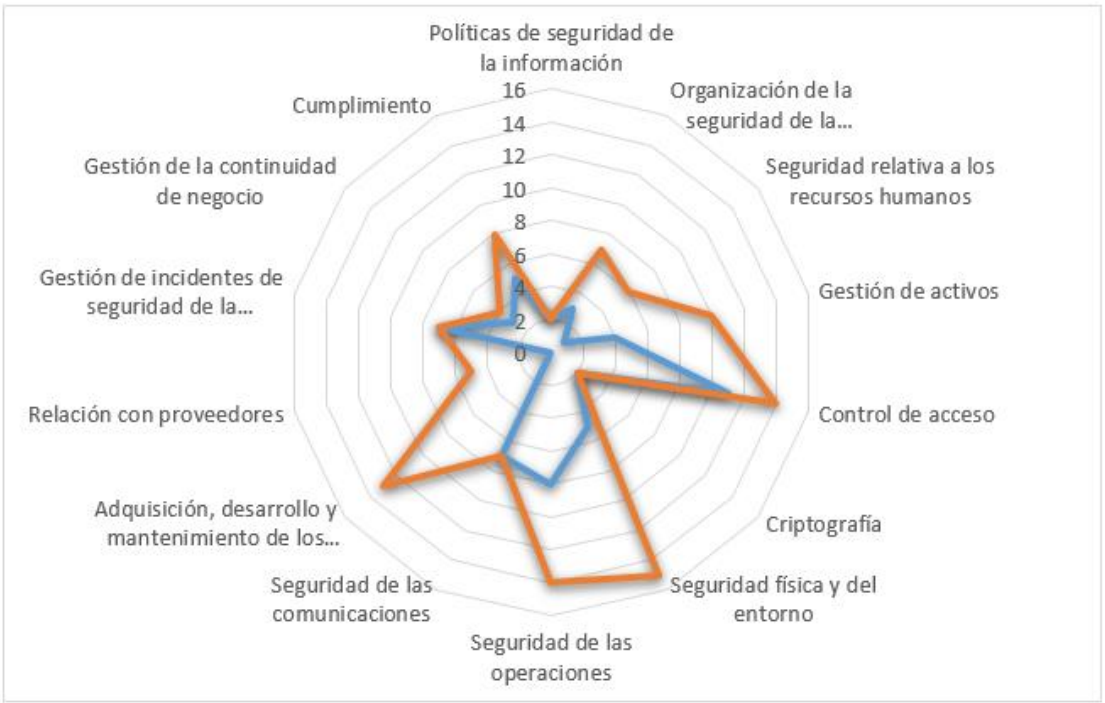


Figura 6-5: Controles adoptados por dominio vs Total de controles ISO 27002

Fuente: Maxxnet, 2019.

Realizado por: Pusay Diego, 2019

En la Figura 6-5 se puede observar de color azul la cobertura de controles que adopta la metodología propuesta, en comparación con el total de controles ISO 27002 de color anaranjado, los controles están agrupados en cada uno de los 14 dominios que define el estándar internacional. La selección de controles apenas constituye uno de los primeros pasos en la gestión sistemática

de la seguridad informática de una microempresa, la forma en que se los implementa, el seguimiento que se los da y el nivel de automatización en la implementación de estos controles, dan lugar a la definición del nivel madurez que es un tema que está fuera del alcance de este trabajo.

*5.1.6 **Implementación de Controles***

La implementación de controles propuestos por la metodología en el caso de estudio Maxxnet, permitió cumplir con los requisitos exigidos por la ARCOTEL, sin embargo, el enfoque de las normas ISO 27000 abarca los dominios de forma integral, lo cual conlleva un cumplimiento parcial de sus objetivos en el contexto de la metodología propuesta.

Para la evaluación cualitativa del nivel de implementación de controles se propone una escala de tres estados:

- **NULO:** No existen evidencia documental y/o aplicación práctica que sustente la aplicación del control.
- **PARCIAL:** Existe evidencia documental y/o aplicación práctica del control, sin embargo, este no se ejecuta de manera integral en la microempresa, o no está alineado a la gestión de seguridad.
- **COMPLETA:** Existe evidencia documental y/o aplicación práctica del control, se ejecuta de manera integral en la microempresa, y está alineado a la gestión de seguridad.

La evaluación propuesta no implica determinar el nivel de madurez de los controles, se limita a determinar el nivel inicial con la que una microempresa podría iniciar su gestión de seguridad informática, al aplicar la metodología propuesta.
La tabla a continuación resume el estado de cumplimiento de controles ISO 27002 antes y después de la aplicación de la metodología en el caso de estudio.

Tabla 5-5: Cumplimiento de controles utilizando la metodología propuesta.

Sección	Controles	Antes	Después
A5.1.1	Políticas para la seguridad de la información	NULO	COMPLETO
A5.1.2	Revisión de las políticas para la seguridad de la información	NULO	COMPLETO

A6.1.1	Roles y responsabilidades en seguridad de la información	NULO	COMPLETO
A6.1.2	Segregación de tareas	NULO	PARCIAL
A6.1.3	Contacto con las autoridades	PARCIAL	COMPLETO
A7.2.1	Responsabilidades de gestión	NULO	PARCIAL
A8.1.1	Inventario de activos	PARCIAL	COMPLETO
A8.2.1	Clasificación de la información	NULO	PARCIAL
A8.2.2	Etiquetado de la información	NULO	PARCIAL
A8.2.3	Manipulado de la información	NULO	PARCIAL
A9.1.1	Política de control de acceso	PARCIAL	COMPLETO
A9.1.2	Acceso a las redes y a los servicios de red	PARCIAL	COMPLETO
A9.2.1	Registro y baja de usuario	PARCIAL	PARCIAL
A9.2.2	Provisión de acceso de usuario	PARCIAL	PARCIAL
A9.2.3	Gestión de privilegios de acceso	NULO	PARCIAL
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	NULO	PARCIAL
A9.2.5	Revisión de los derechos de acceso de usuario	PARCIAL	PARCIAL
A9.2.6	Retirada o reasignación de los derechos de acceso	NULO	PARCIAL
A9.4.1	Restricción del acceso a la información	PARCIAL	COMPLETO
A9.4.3	Sistema de gestión de contraseñas	NULO	COMPLETO
A9.4.4	Uso de utilidades con privilegios del sistema	NULO	PARCIAL
NULO	Política de uso de los controles criptográficos		PARCIAL
NULO	Gestión de claves		COMPLETO
PARCIAL	Perímetro de seguridad física		COMPLETO
PARCIAL	Controles físicos de entrada		COMPLETO
PARCIAL	Seguridad de oficinas, despachos y recursos		PARCIAL
PARCIAL	Protección contra las amenazas externas y ambientales		COMPLETO
A11.2.1	Emplazamiento y protección de equipos	PARCIAL	COMPLETO
A12.1.1	Documentación de procedimientos operacionales	NULO	PARCIAL
A12.2.1	Controles contra el código malicioso	PARCIAL	COMPLETO
A12.3.1	Copias de seguridad de la información	PARCIAL	COMPLETO
A12.4.1	Registro de eventos	NULO	PARCIAL
A12.4.2	Protección de la información del registro	NULO	PARCIAL
A12.4.3	Registros de administración y operación	NULO	PARCIAL
A12.4.4	Sincronización del reloj	NULO	COMPLETO
A12.6.1	Gestión de las vulnerabilidades técnicas	NULO	COMPLETO
A13.1.1	Controles de red	PARCIAL	COMPLETO
A13.1.2	Seguridad de los servicios de red	PARCIAL	COMPLETO
A13.1.3	Segregación en redes	PARCIAL	COMPLETO

A13.2.1	Políticas y procedimientos de intercambio de información	NULO	PARCIAL
A13.2.2	Acuerdos de intercambio de información	NULO	PARCIAL
A13.2.3	Mensajería electrónica	NULO	PARCIAL
A13.2.4	Acuerdos de confidencialidad o no revelación	NULO	PARCIAL
A16.1.1	Responsabilidades y procedimientos	NULO	COMPLETO
A16.1.2	Notificación de los eventos de seguridad de la información	NULO	COMPLETO
A16.1.3	Notificación de puntos débiles de la seguridad	NULO	COMPLETO
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	NULO	COMPLETO
A16.1.5	Respuesta a incidentes de seguridad de la información	NULO	COMPLETO
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	NULO	COMPLETO
A16.1.7	Recopilación de evidencias	NULO	COMPLETO
A17.1.1	Planificación de la continuidad de la seguridad de la información	PARCIAL	COMPLETO
A17.1.2	Implementar la continuidad de la seguridad de la información	NULO	PARCIAL
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	NULO	PARCIAL
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	PARCIAL	COMPLETO
A18.1.4	Protección y privacidad de la información de carácter personal	PARCIAL	COMPLETO
A18.2.1	Revisión independiente de la seguridad de la información	NULO	PARCIAL
A18.2.2	Cumplimiento de las políticas y normas de seguridad	PARCIAL	COMPLETO
A18.2.3	Comprobación del cumplimiento técnico	NULO	PARCIAL

Fuente: Pusay Diego, 2019
Realizado por: Pusay Diego, 2019

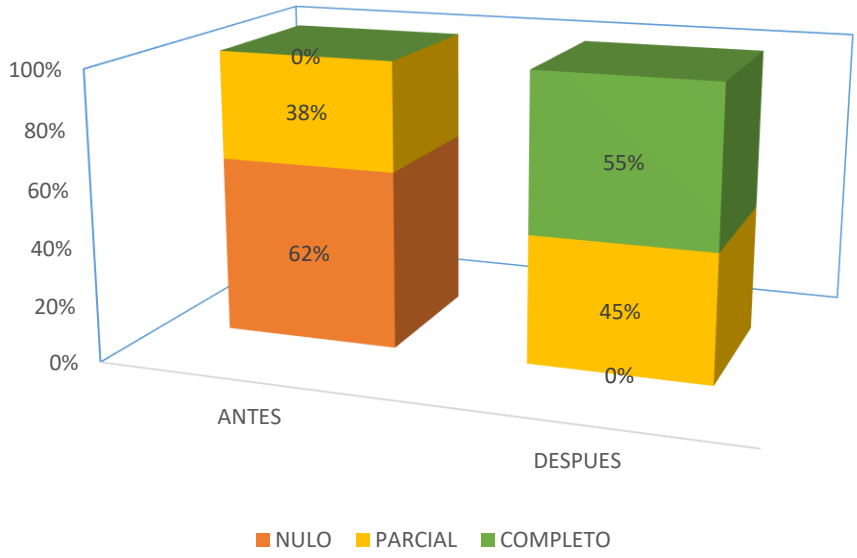


Gráfico 1-5: Comparativa de implementación de controles ISO 27002:2013.
Realizado por: Pusay Diego, 2019

En la figura anterior se aprecia el nivel de implementación de controles antes y después de la aplicación de la metodología propuesta, se observa que, después de la aplicación de la metodología los controles con implementación nula desaparecen, los de cumplimiento parcial pasan de 38% a 45% y los de implementación completa alcanzan un 55%.

5.2 Prueba de hipótesis

Para la comprobación de la hipótesis "La implementación de una metodología basada en ISO 27000 permitirá cumplir con los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet", se utilizó la prueba Chi-Cuadrado con un valor de significancia de 0.05%.

Hipótesis Nula H_0: "La implementación de una metodología basada en ISO 27000 **NO** permitirá cumplir con los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet".

Hipótesis de Investigación H_1: "La implementación de una metodología basada en ISO 27000 **SI** permitirá cumplir con los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet".

La Tabla 30-5 muestra las frecuencias de valores, que reflejan el estado del cumplimiento de los controles ISO 27002 alineados a los requerimientos de la ARCOTEL, observados en el caso de estudio antes y después de la aplicación de la metodología propuesta.

Tabla 6-5: Niveles de cumplimiento

	Nivel de cumplimiento			
	Nulo	**Parcial**	**Completo**	**Total**
Sin Metodología	36	22	0	58
Con Metodología	0	26	32	58
Total:	36	48	32	116

Fuente: Maxxnet, 2019.
Realizado por: Pusay Diego, 2019

La tabla de frecuencias esperadas se obtiene al aplicar la siguiente fórmula:

$$F_e = \frac{total\ columna\ x\ total\ fila}{suma\ total}$$

Tabla 7-5: Frecuencias esperadas chi cuadrado.

	Nivel de cumplimiento			
	Nulo	**Parcial**	**Completo**	**Total**
Sin Metodología	18	24	16	58
Con Metodología	18	24	16	58
Total:	36	48	32	116

Fuente: Maxxnet, 2019.
Realizado por: Pusay Diego, 2019

El valor de chi cuadrado está definido por la fórmula:

$$x^2 = \sum \frac{(F_o - F_e)^2}{F_e}$$

Dónde:

F_0: Frecuencia Observada

F_e: Frecuencia Esperada

$$x^2 = \frac{(36-18)^2}{18} + \frac{(22-24)^2}{24} + \frac{(0-16)^2}{16} + \frac{(0-18)^2}{18} + \frac{(26-24)^2}{24} + \frac{(32-16)^2}{16}$$

$$x^2 = 18 + 0.167 + 16 + 18 + 0.167 + 16$$

$$x^2 = 68.3$$

Los grados de libertad están definidos por:

$$v = (r - 1) * (k - 1)$$

Dónde:

r: número de filas

k: número de columnas

$$v = (2 - 1) * (3 - 1)$$

$$v = 2$$

Tabla 8-5: Tabla de Distribución Chi Cuadrado.

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, v = Grados de Libertad

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807

$$x^2\ crítico = 5{,}9915$$

H_0 se acepta si:

$$x^2\ calculado \leq x^2\ crítico$$

Caso contrario se rechaza H_0 y se acepta H_1.

Según los datos obtenidos tenemos que:

$$x^2\ calculado\ >\ x^2\ crítico$$
$$68.3\ >\ 5{,}9915$$

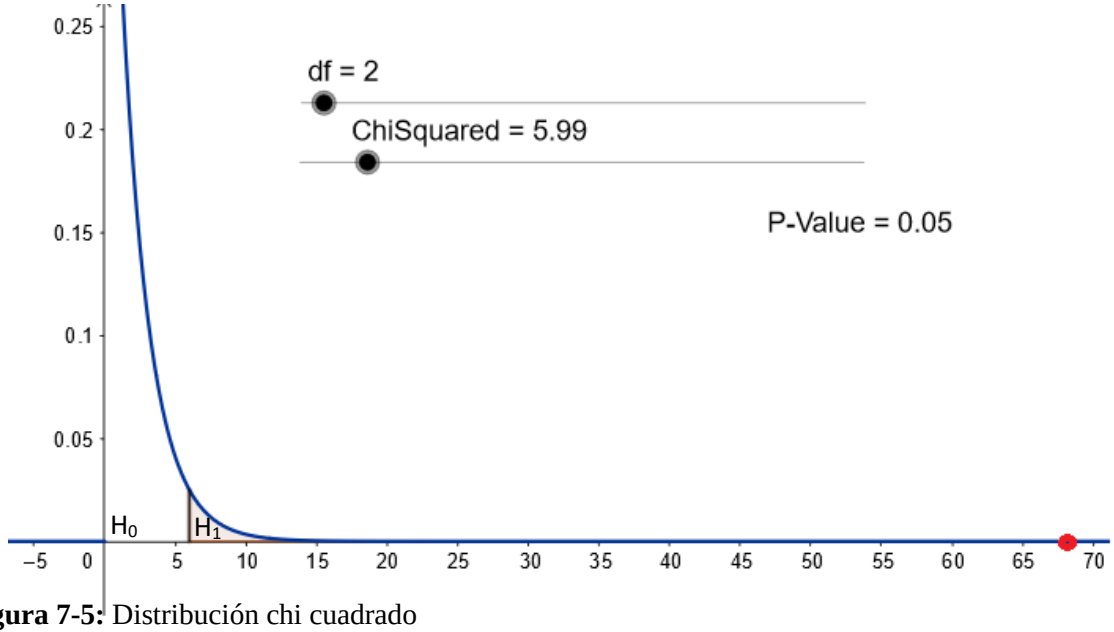


Figura 7-5: Distribución chi cuadrado
Fuente: Lifeder, 2019.
Realizado por: Pusay Diego, 2019

Por tanto, se rechaza H_0 y se acepta H_1: "La implementación de una metodología basada en ISO 27000 **SI** permitirá cumplir con los requerimientos de seguridad informática exigidos por la Agencia de Regulación y Control de las Telecomunicaciones en microempresas proveedoras de acceso a internet"

CONCLUSIONES

- La metodología de gestión de seguridad informática basada en ISO 27000 propuesta en este proyecto de investigación, facilita el cumplimiento de las regulaciones exigidas por la ARCOTEL en microempresas proveedoras de acceso a internet, debido a que desarrolla un marco de gestión en ocho etapas interrelacionadas entre sí, que proporcionan los documentos y herramientas necesarias para la implementación de controles, alineados a estándares internacionales para el cumplimiento de la legislación nacional.

- La metodología propuesta permite evaluar el nivel de riesgo al que podrían estar expuestas las microempresas proveedoras de acceso a internet, al proponer un método cuantitativo y cualitativo con escalas adecuadas para el contexto de las operaciones de este segmento empresarial. La evaluación del riesgo permitió seleccionar los controles adecuados para su tratamiento y generar la documentación de sustento para la ARCOTEL.

- Los riesgos y requerimientos de la ARCOTEL, fueron tratados mediante 58 de los 114 controles ISO 27002:2013, los cuales son desarrollados y documentados en la propuesta metodológica.

- El estudio desarrollado permitió implementar una metodología usando software open source, además de plantillas, formularios, procedimientos y checklist, todos personalizables para facilitar su implantación y generación de evidencias en caso de ser requeridas por las entidades de control.

- La implementación de la metodología propuesta en el caso de estudio Maxxnet, permitió medir su eficacia y evidenciar oportunidades de mejora en la gestión de seguridad informática, alcanzando un cumplimiento total de 55% y parcial de 45% de los controles propuestos.

RECOMENDACIONES

- La implementación de metodologías de gestión de seguridad informática basada en ISO 27000, como parte de los procesos operativos de las microempresas proveedoras de acceso a internet con el fin de responder de manera proactiva a los riesgos a los que están expuestas y a los requisitos exigidos por las entidades de control.
- La adopción de buenas prácticas de gestión de seguridad informática desde los inicios de las microempresas con el fin de generar valor agregado que permitan su permanencia y crecimiento en el mercado.
- El desarrollo de los controles propuestos con el fin de alcanzar niveles de madurez acorde al crecimiento de la microempresa.
- La ampliación de los controles propuestos por la metodología debido a que esta se centra en el cumplimiento de los requisitos exigidos por la ARCOTEL, sin embargo, las necesidades de las microempresas pueden ser mucho más amplias.

GLOSARIO

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones.

Checklist: Un instrumento que revisa de forma ordenada el cumplimiento de procedimientos que se llevan a cabo.

Cifrado: Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.

Firewall: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora.

Datagrama: Paquete de datos que constituye el mínimo bloque de información en una red de conmutación

GNU: Es un sistema operativo de tipo Unix, así como una gran colección de programas informáticos que componen al sistema

IP: Es una dirección única que identifica a un dispositivo en Internet o en una red local.

ISO: Norma definida por la Organización Internacional de normalización que se aplica a los productos y servicios.

Logs: Se refiere a la grabación secuencial en un archivo o en una base de datos.

NAT: Son las siglas de Network Address Translator, o en español traductor de direcciones de red.

Nmap: Es un programa de código abierto que sirve para efectuar rastreo de puertos.

Nodo: Punto de intersección, conexión o unión de varios elementos.

Pymes: Empresa pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y número de trabajadores.

TCP: Protocolo de Control de Transmisión, es protocolo de red importante que permite que dos usuarios se conecten e intercambien flujos de datos.

UDP: El protocolo de datagramas de usuario, es un protocolo que permite la transmisión sin conexión de datagramas en redes basadas en IP.

UPS: (Uninterruptable Power Supply) Dispositivo que permite tener flujo de energía eléctrica mediante baterías.

BIBLIOGRAFÍA

ARCOTEL. (2019). *Boletín Estadístico Cierre 2018.* Recuperado de: http://www.arcotel.gob.ec/wp-content/uploads/2015/01/BOLETIN-ESTADISTICO-FEBRERO-2019-Cierre-2018.pdf

ARCOTEL. (2016). *Boletín Estadístico Número 6 del Sector de las Telecomunicaciones*. Recuperado de: http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf

ARCOTE. (2020). *Guía para la gestión de riesgos de seguridad de la información*. Recuperado de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

ARCOTEL. (2018) *Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afectan a la seguridad de las redes y servicios de telecomunicaciones.* Recuperado de: https://www.arcotel.gob.ec/norma-tecnica-para-coordinar-la-gestion-de-incidentes-y-vulnerabilidades-que-afecten-a-la-seguridad-de-las-redes-y-servicios-de-telecomunicaciones/

Asamblea Nacional. (2015). *Ley Orgánica de Telecomunicaciones*. Publicada en el Registro Oficial Suplemento No. 149, Quito, Ecuador, 18 de febrero del 2015. Ecuador. Recuperado de: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Calder, A. (2017). *ISO 27001/27002: Una guía de bolsillo*. Recuperado de: https://www.perlego.com/book/1284177/iso27001iso27002-una-gua-de-bolsillo-pdf

Cámara de Comercio de Quito. (2017). *Boletín Jurídico: Clasificación de las PYMES, PEQUEÑA Y MEDIANA EMPRESA.* Recuperado de: http://www.ccq.ec/wp-content/uploads/2017/06/Consulta_Societaria_Junio_2017.pdf

Eyssautier, M. (2006). *Metodología de la investigación: desarrollo de la inteligencia*. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/4714108.pdf

Segovia, A. (2019). *¿Qué es norma ISO 27001?.* Recuperado de: https://advisera.com/27001academy/es/que-es-iso-27001/

ANEXOS

Anexo A: Modelo de Política de Seguridad de la Información.

<INSERTE LOGO>

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

<Ciudad, Fecha>

Ver: <X.Y.Z>

ACCESO PÚBLICO

Firmas de Responsabilidad

Elaborado por:	_____ **Nombre:** *<Nombre y Apellido>* **Cargo:** *<Cargo>*
Revisado por:	_____ **Nombre:** *<Nombre y Apellido>* **Cargo:** *<Cargo>*
Aprobado por:	_____ **Nombre:** *<Nombre y Apellido>* **Cargo:** Gerente

<*INSERTE LOGO*>	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	***<Identificador>***

1. OBJETIVO:

Establecer los lineamientos, objetivos y requisitos generales para la gestión de seguridad de la información alineados a los requerimientos legales exigidos por las entidades de control de las telecomunicaciones, con el fin de cumplir con la normativa legal vigente y garantizar la integridad, confidencialidad y disponibilidad de los servicios y sistemas con los que opera la organización.

2. ALCANCE:

Las políticas descritas en este documento aplican a todo el personal que presta sus servicios en la organización, así como a los procesos que estos ejecutan.

Se limita a la gestión de seguridad de la información producida dentro de la infraestructura de la organización y que circula a través de cualquier medio electrónico, escrito o verbal dentro de esta.

3. MARCO LEGAL:

Resolución ARCOTEL-2018-0652 esta Agencia de Regulación y Control Técnico expidió la "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES DE TELECOMUNICACIONES" misma que fue publicada mediante Registro Oficial No. 331, el 20 de septiembre de 2018.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

4.1 NORMAS GENERALES

a) Todo el personal que preste servicios bajo cualquier modalidad en la organización está sometido al cumplimiento de la política de seguridad de la información.
b) La política de seguridad debe ser revisada al menos una vez al año, en función de los requerimientos legales de las entidades de control o en caso de detectarse amenazas y vulnerabilidades importantes.
c) Todos los procedimientos operativos y demás regulaciones que se generen posteriormente deben estar alineadas a la presente política de seguridad de la información, procurando su cumplimiento y generando insumos que permitan medir su efectividad.

4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a) La gerencia será la responsable de la aplicación, difusión, seguimiento y actualización de la política de seguridad de la información.
b) El personal es responsable del cuidado y cumplimiento de las políticas de seguridad dentro del ámbito de sus competencias.
c) Los incidentes que atenten contra los derechos de los clientes de la organización deben ser comunicados a las autoridades de control conforme a los mecanismos y procedimientos establecidos.
d) La gerencia deberá mantenerse informada y procurar el contacto con grupos, organizaciones, asociaciones profesionales especializados en seguridad con el fin de disponer información actualizada sobre amenazas y vulnerabilidades que pongan en riesgo a la organización.
e) Anualmente se dispondrá una auditoría de seguridad conforme los requerimientos de las entidades de control.
f) La gerencia es responsable de catalogar la información confidencial y resguardarla adecuadamente.

4.3 TALENTO HUMANO

a) Todo el personal que preste sus servicios debe firmar un acuerdo de confidencialidad y renovarlos anualmente.
b) Dentro de las funciones asignadas al personal, se entenderán implícita o explícitamente el cumplimiento de la política de seguridad.
c) La organización se reserva el derecho de investigar los antecedentes del personal.
d) Todo el personal debe recibir al menos una vez al año, capacitación o concientización respecto a la seguridad de la información.
e) En caso de incumplimiento de la política de seguridad por parte del personal, la organización deberá seguir el procedimiento de sanción conforme a la legislación laboral vigente.

4.4 GESTIÓN DE ACTIVOS

a) Todos los activos deben estar claramente identificados, elaborando y manteniendo un inventario con los más importantes.
b) Todos los activos de la organización deben tener asignado una persona responsable, la cual puede hacer uso, mantenimiento y cuidado del activo.
c) La Gerencia debe identificar, documentar e implantar regulaciones para el uso adecuado de la información y sus activos asociados.
d) Se prohíbe el uso de medios de almacenamiento extraíbles para transportar información comercial, datos de clientes, configuraciones, topologías y credenciales de acceso.

4.5 CONTROL DE ACCESO

a) El acceso a la información se restringe al ámbito de las funciones y competencias de cada uno de los empleados de la organización.
b) Los responsables de los activos de información son responsables de la protección de los activos bajo su custodia.
c) Se prohíbe el uso de usuarios y contraseñas genéricas para el acceso administrativo a equipos y sistemas críticos de la organización.
d) El acceso administrativo a equipos y sistemas de la organización estarán regulados y autorizados por la gerencia, a través de un procedimiento formal.
e) Los nombres de usuario deben identificar de manera única a la persona que accede y sus contraseñas debe contener al menos 8 caracteres incluyendo letras mayúsculas, minúsculas, números y caracteres especiales.

4.6 CIFRADO

a) Las credenciales de acceso privilegiado a equipos, sistemas operativos, y sistemas críticos de la organización deben ser almacenados en archivos cifrados, se prohíbe el almacenamiento en texto plano.
b) El acceso remoto a la red de la organización debe hacerse a través de enlaces cifrados con credenciales que identifiquen adecuadamente al usuario.
c) Todos los respaldos de información digital, que incluyan información personal o comercial de clientes y proveedores deben resguardarse en archivos cifrados.

4.7 SEGURIDAD FÍSICA Y DEL ENTORNO

a) Las instalaciones que albergan infraestructura crítica están restringidas para todo el personal, la autorización de acceso será controlada por la gerencia.
b) El centro de procesamiento de datos principal deberá contar con alarmas contra incendios, cerraduras adecuadas, extintor, alarmas de acceso, sensores de movimiento, aire acondicionado, cámaras de seguridad y circuito eléctrico puesto a tierra.
c) Se prohíbe al personal realizar copias de llaves de cerraduras y candados de cualquiera de las instalaciones de la organización.
d) En las áreas de atención a clientes se debe evitar exponer por cualquier medio información personal de clientes y comercial de proveedores.

4.8 SEGURIDAD EN LAS OPERACIONES

a) Todo el personal recibirá un manual de funciones donde se establecerá sus responsabilidades, atribuciones, nivel de acceso y difusión de información y los procedimientos de operación rutinarios de acuerdo con sus funciones procurando la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso deliberado o por negligencia.
b) Todos los equipos informáticos con los que se opera la red y los servicios de la organización deben contar con antivirus actualizado y licencia vigente.
c) Se debe realizar regularmente copias de seguridad de los activos de información considerados críticos.
d) Realizar copias de seguridad antes de cualquier cambio en la infraestructura crítica.
e) Todos los cambios en la infraestructura crítica deben documentarse y aprobarse por gerencia.
f) Las pruebas de funcionamiento o desarrollo de nuevas arquitecturas o sistemas se deben realizar en ambientes separados a los de producción.
g) La gestión de vulnerabilidades técnicas debe hacerse con la prioridad que amerite evitando comprometer los equipos y sistemas en producción.
h) Se debe monitorear permanentemente y emitirse informes mensuales de la capacidad de los activos críticos.

i) Se debe realizar anualmente o cuando las entidades de control lo dispongan auditorías de seguridad informática a las redes y servicios críticos de la organización.

4.9 SEGURIDAD EN LAS TELECOMUNICACIONES

a) Los controles de seguridad en las redes se implementarán en los routers y firewalls que delimiten cada dominio de broadcast, aplicando el principio de segregación de redes.
b) El acceso a sistemas informáticos y configuración de equipos será restringido mediante el firewall del perímetro de su dominio de broadcast.
c) Los servicios publicados hacia el internet y el tráfico proveniente desde este, debe ser monitoreado por un Firewall perimetral y un IDS/IPS.
d) La red de administración debe ser separada e inaccesible desde la red de clientes.
e) El acceso administrativo a equipos y sistemas debe estar limitado exclusivamente a la red de administración.
f) Cualquier intercambio de información o acceso remoto a las redes y servicios de la organización deben realizarse por canales cifrados.

4.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

a) Para la adquisición de sistemas o equipos informáticos se debe tener en cuenta la compatibilidad con la infraestructura existente, las capacidades presentes y futuras así como los costos indirectos de su implementación.
b) Para el desarrollo de sistemas informáticos se debe realizar un proceso formal para definir los requerimientos de la organización, criterios de aceptación y propiedad intelectual.
c) Durante el mantenimiento de sistemas informáticos se debe notificar previamente a los afectados procurando que la suspensión de servicios sea mínima.

4.11 RELACIÓN CON LOS PROVEEDORES

a) Se debe monitorear permanentemente y emitir reportes mensuales del cumplimiento de los niveles de servicio contratados por los proveedores.
b) Los proveedores que tengan acceso a los activos de la organización deben someterse a la presente política de seguridad.

4.12 GESTIÓN DE INCIDENTES

a) La gestión de incidentes de seguridad está a cargo de la Gerencia la cual definirá responsabilidades y procedimientos conforme las necesidades de la organización y requisitos de las entidades de control.
b) Las actividades de gestión de incidentes deben incluir como mínimo las siguientes fases:
    - Preparación
    - Detección y Análisis
    - Contención, erradicación, recuperación y respuesta.
    - Actividades post-incidentes.
c) Todos los activos críticos deben tener habilitados los registros de auditoría y centralizar sus logs en un equipo diferente.

4.13 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

a) La gestión de continuidad del negocio está a cargo de la Gerencia la cual definirá responsabilidades y procedimientos conforme las necesidades de la organización y requisitos de las entidades de control.
b) Se debe procurar que la infraestructura crítica de la organización disponga de equipos para redundancia.

4.14 CUMPLIMIENTO

a) La Gerencia será la responsable de identificar la legislación aplicable a la organización en temas de gestión de seguridad de la información.
b) Se debe evaluar el cumplimiento de la política de seguridad al menos una vez al año.

5. CASOS ESPECIALES.

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por la Gerencia, quien evaluará la pertinencia y los riesgos asociados y permitirán o negarán la excepción por escrito.

Anexo B: Plan de Contingencia- formato ARCOTEL.

MODELO DE PLAN DE CONTINGENCIA PARA LOS PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES

PROCESO: GESTIÓN DE CONTROL DE SERVICIOS DE TELECOMUNICACIONES

Contenido

1.0 Resumen

La intención de un Plan de Contingencia, es la de asegurar la disponibilidad de los sistemas de los prestadores de servicios del régimen general de telecomunicaciones bajo toda circunstancia. Un Plan de Contingencia provee la capacidad para responder a emergencias, recuperarse de ellas, y reanudar las operaciones normales, posiblemente en una ubicación alterna, en el evento de una emergencia, falla del sistema, o desastre.

SERVICIOS DEL REGIMEN GENERAL DE TELECOMUNICACIONES

LEONARDO ISRAEL BENALCAZAR ROMERO

Plan de Contingencia

Preparado por:
Diego Noé Pusay Villarroel
Riobamba, Chimborazo

Versión <1.0>
30/01/2020

1. Aprobación del Plan

Como autoridad designada por Leonardo Israel Benalcazar Romero, por la presente se certifica que el presente plan de contingencia para sistemas del régimen general de telecomunicaciones se encuentra completo, y que la información contenida provee una representación exacta del hardware, software y demás componentes de telecomunicaciones de nuestro sistema, de acuerdo a lo establecido en la normativa correspondiente.

Certifico además que las estrategias de recuperación identificadas proveerán las habilidades para recuperar las funcionalidades del sistema con los métodos más convenientes y rentables de acuerdo al nivel de criticidad del sistema.

Me comprometo para que este Plan de Contingencia sea probado como mínimo cada año, y los resultados de la verificación se incluirán como parte del Plan de Contingencia del año subsiguiente. El presente documento será actualizado y mejorado de manera anual.

_____ Fecha 30/01/2020

Ing. Leonardo Israel Benalcazar Romero

Gerente Técnico

2.0 MARCO LEGAL

Los sistemas de telecomunicaciones son vitales, de acuerdo a la Constitución son considerados parte de los sectores estratégicos, por tanto, es crítico que los servicios ofrecidos por los proveedores del régimen general de telecomunicaciones estén aptos para operar de manera efectiva sin excesivas interrupciones. El presente plan de contingencia establece procedimientos comprensivos para recuperar los sistemas de telecomunicaciones y los servicios de manera rápida y efectiva posterior a la afectación del servicio en caso de desastres naturales o conmoción interna.

Ley Orgánica de Telecomunicaciones

El numeral 24 del artículo 24 de la Ley Orgánica de Telecomunicaciones, establece como obligación de los prestadores de servicios de telecomunicaciones: *"Contar con planes de contingencia, para ejecutarlos en casos de desastres naturales o conmoción interna para garantizar la continuidad del servicio de acuerdo con las regulaciones respectivas. Asimismo, cumplirá con los servicios requeridos en casos de emergencia, tales como llamadas gratuitas, provisión de servicios auxiliares para Seguridad pública y del Estado y cualquier otro servicio que determine la autoridad competente de conformidad con la Ley"*.

Reglamento General a la Ley Orgánica de Telecomunicaciones

El numeral 12 del artículo 59 del Reglamento General a la Ley Orgánica de Telecomunicaciones, establece: "*Las obligaciones previstas en el artículo 24 numeral 24 de la LOT serán cumplidas por todos los prestadores de servicios del régimen general de telecomunicaciones. Respecto a los servicios requeridos en casos de emergencia, los prestadores de servicios de telecomunicaciones proporcionarán de forma gratuita lo siguiente: i) Acceso a llamadas de emergencia por parte del abonado, cliente y usuario, independientemente de la disponibilidad de saldo; ii) Difusión por cualquier medio, plataforma o tecnología, de información de alertas de emergencia a la población, conforme la regulación que emita para el efecto la ARCOTEL. Dichos servicios se prestarán gratuitamente, sin perjuicio de la declaratoria de Estado de Excepción establecida en el artículo 8 de la LOT. También deberán prestar de manera obligatoria, con el pago del valor justo, lo siguiente: i) Integración de sus redes a cualquier plataforma o tecnología, para la atención de servicios de emergencias, conforme a la normativa que emita la ARCOTEL; ii) Servicios auxiliares para la seguridad pública y del Estado; iii) Cualquier otro servicio que determine la ARCOTEL"*.

El numeral 14 del artículo 59 del Reglamento General a la Ley Orgánica de Telecomunicaciones, establece: "*El o los planes de contingencia previstos en el artículo 24*

numeral 24 de la LOT serán presentados en enero de cada año para conocimiento y revisión de la ARCOTEL".

Norma que regula la presentación de los Planes de Contingencia para la Operación de las Redes Públicas de Telecomunicaciones por parte de los Prestadores de Servicios del Régimen General de Telecomunicaciones

3.0 Introducción

4.0 Presentación Institucional

Leonardo Israel Benalcazar Romero (Maxxnet), presta servicios de acceso a internet a hogares y pymes, a través de redes inalámbricas, en los cantones de Alausí y Riobamba pertenecientes a la provincia de Chimborazo.

Actualmente la matriz se encuentra en la ciudad de Riobamba, en las calles Espejo y Chimborazo, se dispone de los siguientes números telefónicos de contacto: 0999060601, 032 376690, del correo electrónico info@maxxnet.ec y del sitio web: www.maxxnet.ec

5.0 Estructura Organizacional

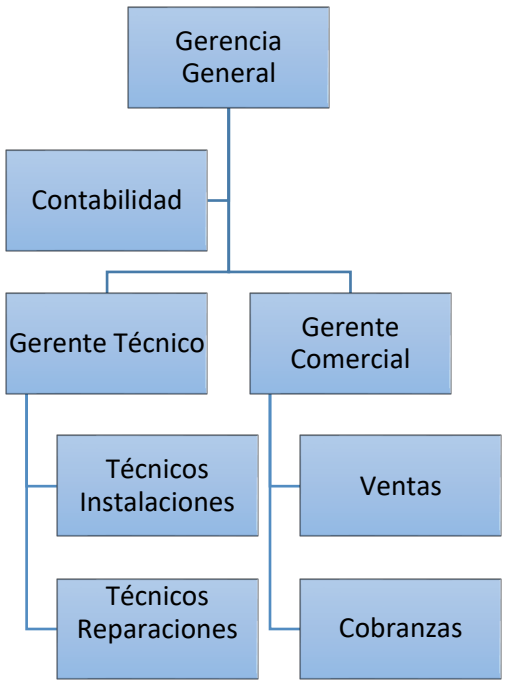


Fig 1. Estructura Organizacional Maxxnet.

6.0 Presentación Técnica

Descripción del Sistema:

- La red de transporte cuenta con dos nodos centrales uno en Alausí y otro en Riobamba, a los cuales se conectan nodos secundarios desde donde se conectan los abonados.

- En los nodos principales también existen abonados directamente conectados.
- Los únicos puntos de salida hacia el Internet son los nodos principales, desde donde se accede a través de fibra óptica.
- La conexión entre los nodos es a través de radio enlaces.
- Los nodos centrales cuentan con UPS, banco de baterías y generador eléctrico, para mantenerlos operativos.
- Los nodos secundarios disponen de UPS con banco de baterías y un sistema de alarma en caso de corte de energía.
- En los nodos centrales se dispone de generadores eléctricos portable para ser trasladados a los nodos secundarios en caso de cortes de energía.

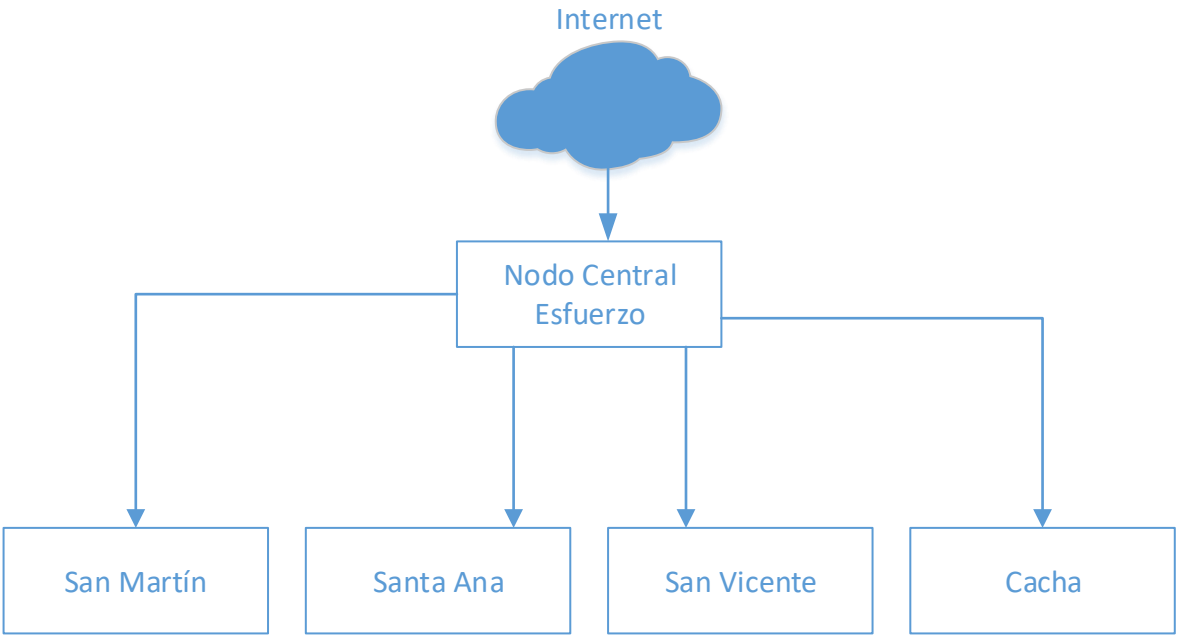


Fig 2. Esquema de Conexiones del nodo central de Riobamba

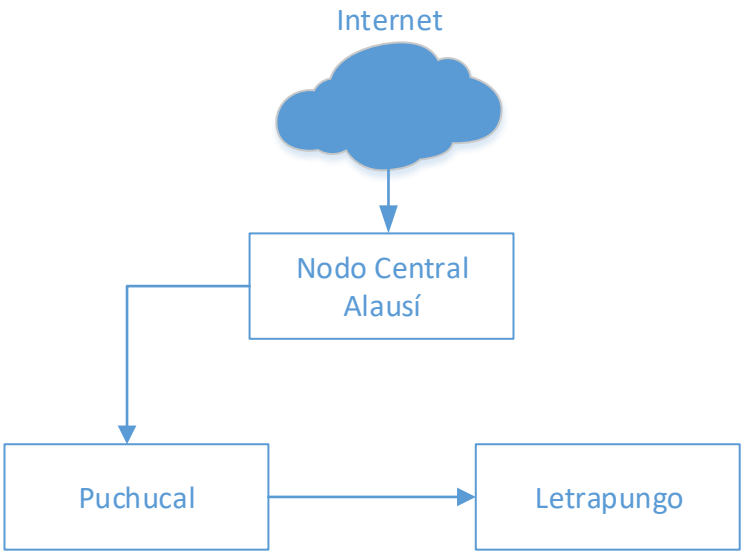


Fig 3. Esquema de Conexiones del nodo central de Alausí

7.0 Diagrama Operacional de la Red

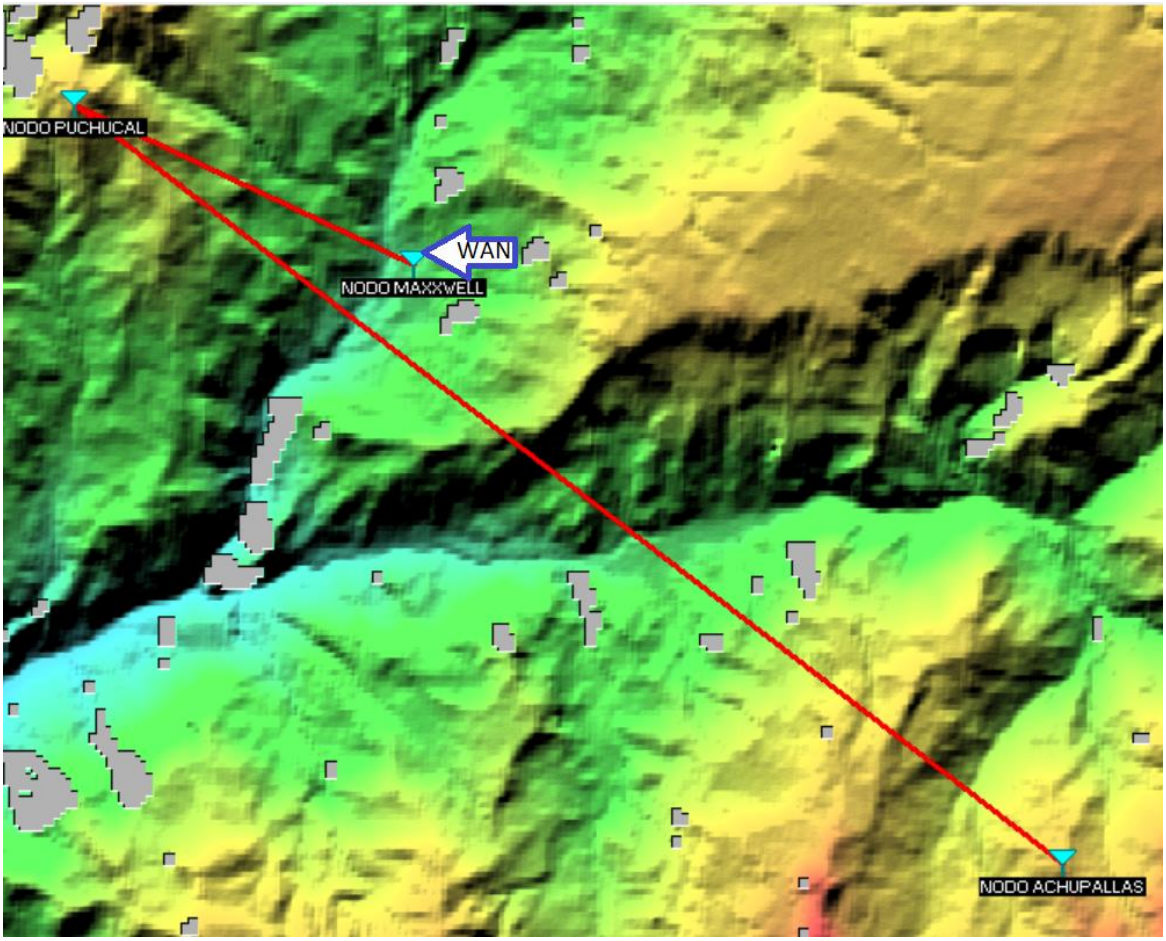


Fig 3. Red de trasnporte Alausí

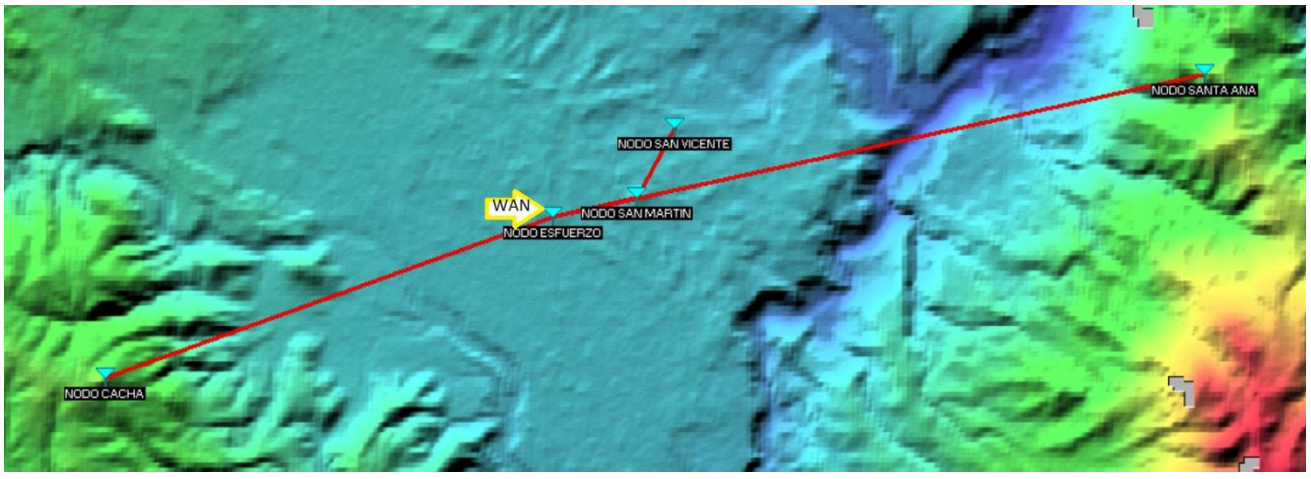


Fig 4. Red de transporte Riobamba

8.0 Principios, Metas y Objetivos

Este plan de contingencia aplicable al {nombre del sistema o proveedor} establece procedimientos para recuperar la red y los servicios de telecomunicaciones utilizada para la prestación de servicios del régimen general de telecomunicaciones luego de una afectación producida en casos de desastres naturales o conmoción interna. Se han establecido los siguientes objetivos para el plan:

- Maximizar la efectividad de las operaciones de contingencia en tres fases:
  - Fase preventiva y de activación y notificación — Acciones para reducir el riesgo. Activación del plan, en caso de presentarse un evento, se activa y se determina la magnitud de los daños.
  - Fase de Recuperación — Se recuperan las operaciones del sistema y la prestación de (los) servicio (s).
  - Fase de Reconstitución (Resiliencia) — Se valida la operación del sistema de telecomunicaciones para la prestación del (los) servicio (s) del régimen general de telecomunicaciones mediante pruebas de verificación pre establecidas, y se reanudan las operaciones normales.
- Identificar actividades, recursos, y procedimientos necesarios para aplicar en el sistema durante interrupciones prolongadas de la operación normal debido a casos de desastres naturales o conmoción interna.
- Asignar responsabilidades al personal designado en cada componente del sistema y proveer instrucciones para la recuperación del sistema,
- Garantizar la coordinación entre todo el personal responsable de implementar las estrategias de recuperación planificadas para cada componente del sistema.
- Garantizar la coordinación con puntos de contacto externos y proveedores cuya participación es necesaria para la ejecución del plan de contingencia.

9.0 Análisis de Amenazas, Vulnerabilidades y Riesgos

Se desarrolla el análisis enfocado en el plan de contingencia propuesto por el Arcotel.

a) Identificación de activos de hardware:

Ord.	Descripción	Cant.	Propietario
1	Ruteador del Proveedor	1	Nedetel S.A
2	Firewall de Borde	1	Maxxnet
3	Ruteador Principal Multipuerto	1	Maxxnet
4	Servidor Facturación/Monitoreo	1	Maxxnet
5	Switch POE	1	Maxxnet
6	Radio Transmisor Punto Punto con antena	4	Maxxnet
7	Radio Transmisor Multipunto con antena	3	Maxxnet
8	Switch de Core	1	Maxxnet

9	Generador Eléctrico	1	Maxxnet
10	UPS 1,7 kVA	1	Maxxnet
11	Banco de Baterías	1	Maxxnet
12	Torre metálica	1	Maxxnet

Tabla 1: Nodo Central Riobamba

Nodo San Martín/Santa Ana/Cacha/San Vicente:

Ord.	**Descripción**	**Cant.**	**Propietario**
1	Radio Receptor Punto Punto	1	Maxxnet
2	Radio Transmisor multipunto	3	Maxxnet
3	UPS	1	Maxxnet
4	Banco de baterias	1	Maxxnet
5	Ruteador multipuerto	1	Maxxnet
6	Torre metálica	1	Maxxnet,Wilson Soto (Cacha)

Tabla 2: Nodo San Martín/Santa Ana/Cacha/San Vicente:

Ord.	**Descripción**	**Cant.**	**Propietario**
1	Ruteador	1	Nedetel S.A
2	Ruteador Multipuerto	1	Maxxnet
3	Radio Transmisor Punto Punto con antena	1	Maxxnet
4	Radio Transmisor Multipunto con antena	2	Maxxnet
5	Generador Eléctrico	1	Maxxnet
6	UPS 500 VA	1	Maxxnet
7	Banco de Baterías	1	Maxxnet

Tabla 3: Nodo Central Alausí

Nodo Puchucal/Letrapungo:

Ord.	Descripción	Cant.	Propietario
1	Radio Receptor Punto Punto	1	Maxxnet
2	Radio Transmisor multipunto	3	Maxxnet
3	UPS	1	Maxxnet
4	Banco de baterias	1	Maxxnet
5	Ruteador multipuerto	1	Maxxnet
6	Torre metálica	1	Maxxnet,Radio Alausí

Tabla 4: Nodo Puchucal/Letrapungo:

b) Identificación de Amenazas

Origen de la Amenaza:

- Deliberadas (D)
- Accidentales (A) o
- Ambientales (naturales) (E)

Tipo	Amenazas	Origen de la Amenaza
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
Pérdida de los servicios esenciales	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D

Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Impulsos electromagnéticos	A, D, E
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Incumplimiento en la disponibilidad del personal	A, D, E

Tabla 5: Identificación de Amenazas y su origen

c) Identificación de Vulnerabilidades

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización,
- Personal,
- Lugar,
- Hardware,
- Red

Tipo de activo	Vulnerabilidad	Amenaza
Hardware	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética

	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
Red	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Gestión inadecuada de la red	Saturación del sistema de información
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Entrenamiento insuficiente en seguridad	Error en el uso
	Falla en los mecanismos de monitoreo	Desconocimiento del estado real de la infraestructura
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Red eléctrica inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo
Organización	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información

	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de planes de continuidad	Falla del equipo
	Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo

Tabla 6: Relación entre Amenazas, Vulnerabilidades y tipo de activo

d) Evaluación de la probabilidad e Impacto de incidentes

Probabilidad	Criterio	Frecuencia	Valor
Improbable	Más de 10 años	Muy Poco frecuente	1
Remoto	Cada varios años	Poco Frecuente	2
Posible	Una a tres vez al año	Normal	3
Probable	Mensual o más de tres veces al año	Frecuente	4
Muy Probable	A diario	Muy Frecuente	5

Tabla 7: Valoración de la Probabilidad

Impacto	Criterio	Valor
Bajo	Afecta a un solo radio transmisor	1
Medio Bajo	Afecta a varios radio transmisores de un nodo	2
Medio	Afecta totalmente a un nodo de transmisión	3
Medio Alto	Afecta a varios nodos de transmisión	4
Alto	Afecta a toda la red	5

Tabla 8: Escala de Impacto

Activos de Soporte	Impacto	Probabilidad de materialización de Amenazas					
		Daño Físico	Eventos Naturales	Pérdida de servicios esenciales	Perturbación debido a la radiación	Fallas Técnicas	Compromiso de las funciones
Ruteador del Proveedor	5	2	1	3	2	2	2
Firewall de Borde	5	2	1	3	2	2	3
Ruteador Principal Multipuerto	5	2	1	3	2	2	3
Servidor de Facturación/Monitoreo	1	2	1	3	2	2	2
Switch POE	4	2	1	3	2	2	2
Radio Transmisor Punto Punto con antena	3	3	2	3	4	3	3
Radio Transmisor Multipunto con antena	3	3	2	3	4	3	3
Switch de Core	5	2	1	3	2	2	3
Generador Eléctrico	1	3	1	1	1	2	1
UPS	1	2	1	1	1	2	1
Banco de Baterías	1	2	1	1	1	2	1
Torre metálica	5	2	2	1	1	1	1

Tabla 9: Relación Impacto y probabilidad de materialización de amenazas

e) Estimación del riesgo

Escala	Nivel de Riesgo
01-07	Bajo
08-14	Moderado
15-20	Alto
20-25	Extremo

Tabla 10: Escala de nivel de riesgo

Activos	Riesgo					
	Daño Físico	**Eventos Naturales**	**Pérdida de servicios esenciales**	**Perturbación debido a la radiación**	**Fallas Técnicas**	**Compromiso de las funciones**
Ruteador del Proveedor	10	5	15	10	10	10
Firewall de Borde	10	5	15	10	10	15
Ruteador Principal Multipuerto	10	5	15	10	10	15
Servidor de Facturación/Monitoreo	2	1	3	2	2	2
Switch POE	8	4	12	8	8	8
Radio Transmisor Punto Punto con antena	9	6	9	12	9	9
Radio Transmisor Multipunto con antena	9	6	9	12	9	9
Switch de Core	10	5	15	10	10	15
Generador Eléctrico	3	1	1	1	2	1
UPS	2	1	1	1	2	1
Banco de Baterías	2	1	1	1	2	1
Torre metálica	10	10	5	5	5	5

Tabla 10: Cálculo del Riesgo (Impacto x Probabilidad)

10.0 Planes y acciones institucionales

Este plan de contingencia ha sido elaborado para recuperar el (los) Sistema (s) de Telecomunicaciones (s) del prestador de servicios del régimen general de telecomunicaciones MAxxnet en tres fases. Un enfoque que busca garantizar que la recuperación del Sistema se realice siguiendo una secuencia metódica que maximice la efectividad de los esfuerzos de recuperación y minimice el tiempo de interrupción debido a errores y omisiones. Las tres fases para recuperación del Sistema son:

- Fase de Prevención y Activación/Notificación
  - Incluye actividades necesarias para reducir el impacto de la ocurrencia
  - Este Plan de Contingencia se activa al momento de producirse un evento de desastres naturales o conmoción interna. Como resultado del evento se pueden producir daños severos a las facilidades que acogen al sistema de telecomunicaciones; daños severos o pérdidas de equipamiento; u otros daños que típicamente resultan en pérdidas a largo plazo.
  - Luego de la activación del plan de Contingencia, el propietario del Sistema y los usuarios serán notificados de un posible corte de los servicios, y se dispondrá una evaluación a fondo del problema. Los resultados de la evaluación serán presentados al propietario del Sistema, y podrán ser utilizados para modificar los procedimientos de recuperación para enfocarse específicamente en las causas de la interrupción.
- Fase de Recuperación
  - Durante la fase de recuperación, se ejecutarán las actividades y procedimientos, que se incluyen en el presente documento, por parte de los técnicos debidamente capacitados en la recuperación del Sistema, sin necesidad de un conocimiento de los aspectos considerados como confidenciales del mismo. Esta fase incluye notificación y procedimientos de escalamiento de notificación hacia los propietarios y usuarios, acerca del estatus de recuperación del sistema.
- Fase de Reconstitución/Resiliencia
  - Define las acciones tomadas para probar y validar las capacidades y funcionalidades del Sistema en la ubicación original o en una nueva ubicación permanente. Los procedimientos de validación pueden incluir pruebas de funcionalidad o regresión respecto de las operaciones en condiciones normales. Procesamiento concurrente, y/o validación de datos. Una vez completada la validación, el Sistema será declarado como recuperado y operacional por parte de los propietarios del sistema.
  - La desactivación del plan es el paso final, durante el cual los usuarios del Sistema son informados acerca del estado operacional del Sistema; se cierra la documentación de registro de los esfuerzos de recuperación; y se documentan las lecciones aprendidas para ser incorporadas en las actualizaciones del plan. Se realiza la reposición de los recursos utilizados (equipos de repuesto, repuestos, materiales, etc.) para futuros eventos.

11.0 Planes y Acciones para la Prevención

12.0 Identificación de infraestructura crítica

Conforme lo establece la Norma Técnica: “Se considera como infraestructura crítica mínima, a la red de transporte independientemente del medio o tecnología que se utilice para la misma” y en base al análisis de vulnerabilidades, amenazas y riesgos del presente Plan de adjunta en el Apéndice D la infraestructura crítica del sistema.

13.0 Planes de mantenimiento preventivos de la infraestructura crítica, detallando la periodicidad y ámbito de los mismos, considerando los grupos electrógenos y respaldo de bancos de baterías.

Apéndice G

14.0 Reportes de mantenimientos preventivos, correctivos y emergentes realizados en la infraestructura crítica el año previo al de la presentación del Plan de Contingencias, detallando fechas de ejecución, relacionados con la infraestructura crítica, incluyendo los grupos electrógenos y bancos de baterías.

Apéndice H

15.0 Sistemas de respaldo de energía con el que se cuente para la infraestructura crítica (generadores, bancos de batería, etc.), especificando la capacidad de los elementos de respaldo expresado en tiempo.

Apéndice D

16.0 Inventario de repuestos y equipamiento de respaldo disponibles para la infraestructura crítica.

Apéndice E

17.0 Procedimientos y acciones para la recuperación (durante la contingencia), especificando el tiempo aproximado asociado para la ejecución de cada actividad.

18.0 Procedimiento para la activación del plan de contingencia

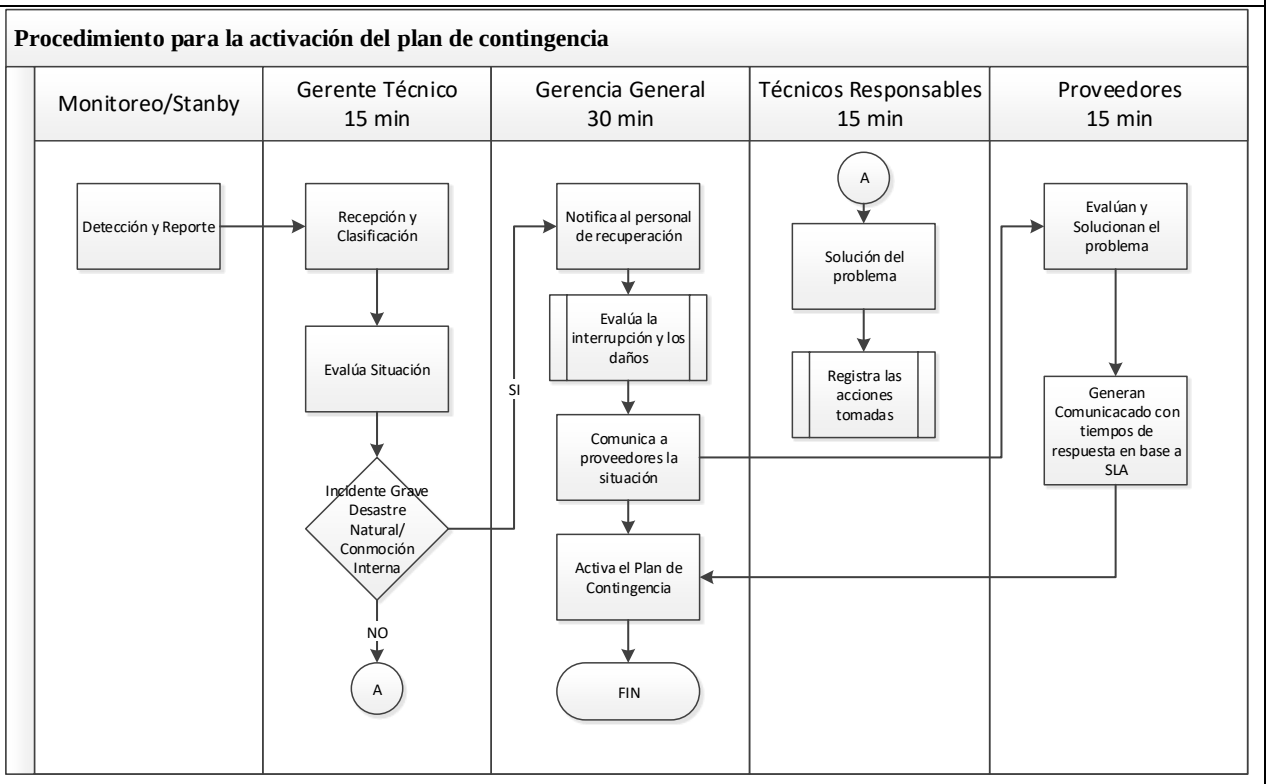
La fase de Activación y Notificación define las acciones iniciales tomadas una vez que se ha presentado un evento de desastre natural o conmoción interna. Esta fase incluye actividades para notificar al personal de recuperación, conducir una evaluación de interrupción y daños, y activar el PC. Una vez completadas las actividades de la fase de Activación y Notificación, el personal involucrado en el Plan de Contingencias (PC) deberá iniciar las medidas de recuperación.

Los roles y responsabilidades de los actores de los procedimientos se detallan en el Apéndice I.

Procedimiento para la activación del plan de contingencia	***Versión:***	*1.0*
	Fecha:	*20/02/2018*

Objetivos: Definir las acciones iniciales tomadas una vez que se ha presentado un evento de desastre natural o conmoción interna

Desarrollo:



Canales de Comunicación:

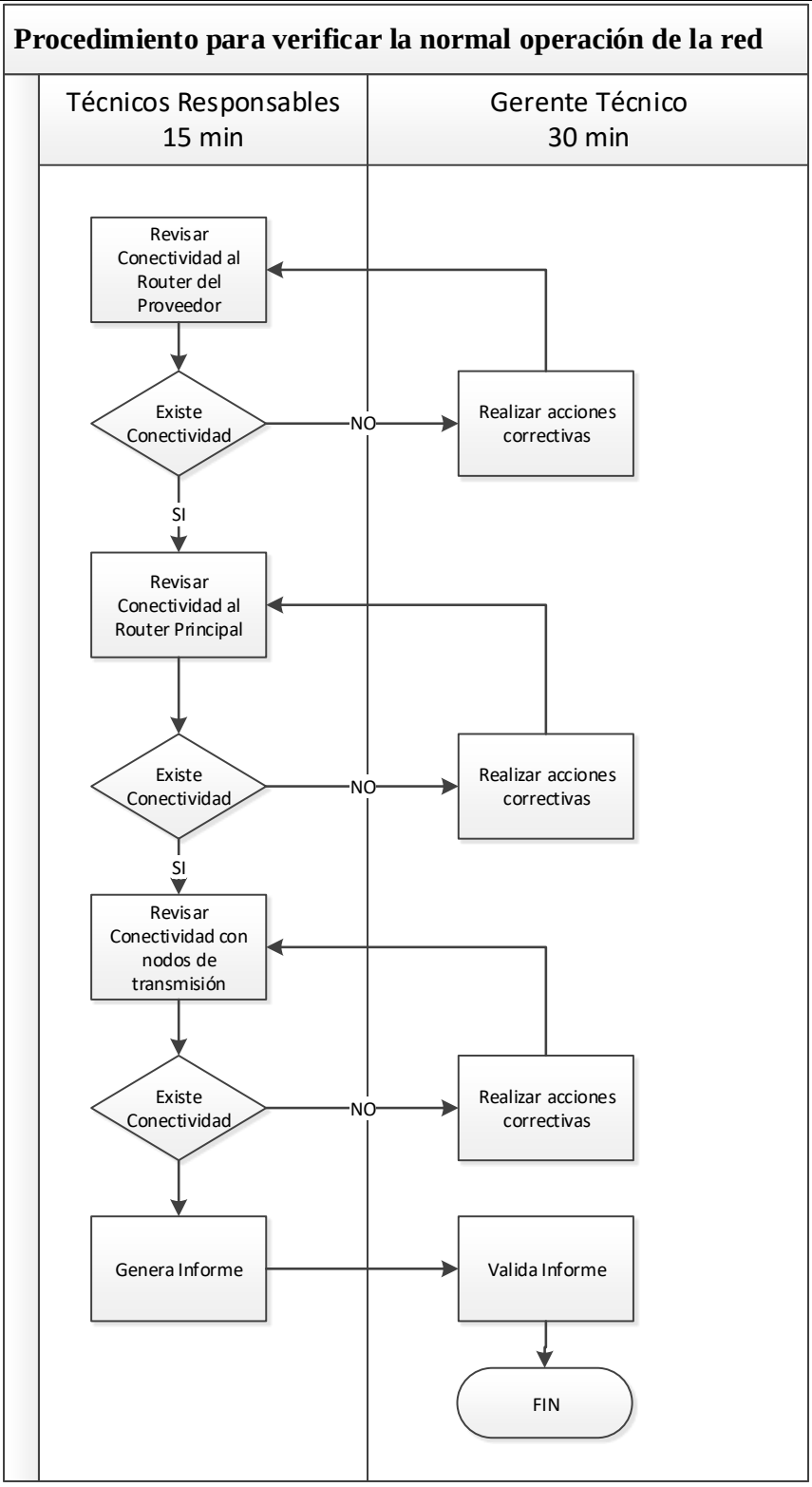
- Llamada Telefónica
- SMS, Chat
- Correo Electrónico

19.0 Procedimiento para verificar la normal operación de la red y de los servicios hacia los abonados, usuarios o clientes.

Procedimiento para verificar la normal operación de la red y de los servicios hacia los abonados, usuarios o clientes.	***Versión:***	*1.0*
	Fecha:	*20/02/2018*

Objetivos: Definir las acciones para verificar la normal operación de la red y de los servicios hacia los abonados, usuarios o clientes.

Desarrollo:



Canales de Comunicación:

- Llamada Telefónica

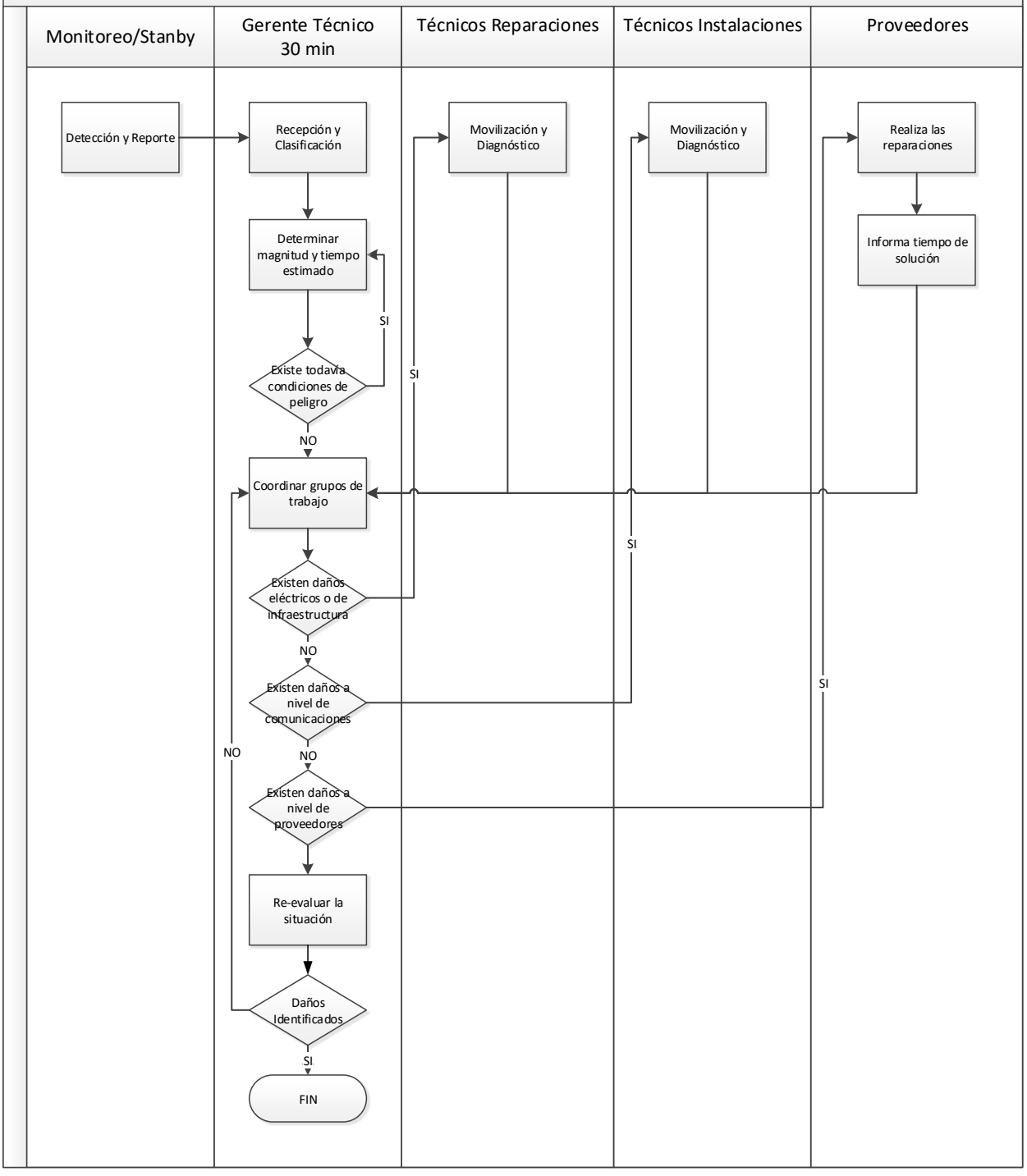
- SMS, Chat
- Correo Electrónico

20.0 Procedimiento para identificación de daños.

Luego de la notificación, el Equipo de evaluación de Daños o el personal delegado para la identificación de daños, determinará la magnitud de los daños y el tiempo estimado de recuperación. Los resultados de la evaluación se proporcionarán al encargado o coordinador del PC. Si la evaluación de daños no puede realizarse debido a condiciones de peligro, se tomarán medidas alternativas según lo establecido en el presente PC.

Procedimiento para identificación de daños.	***Versión:***	*1.0*
	Fecha:	*20/02/2018*
Objetivos: Definir las acciones para identificar daños.		
Desarrollo:		

Procedimiento para identificación de daños



Canales de Comunicación:

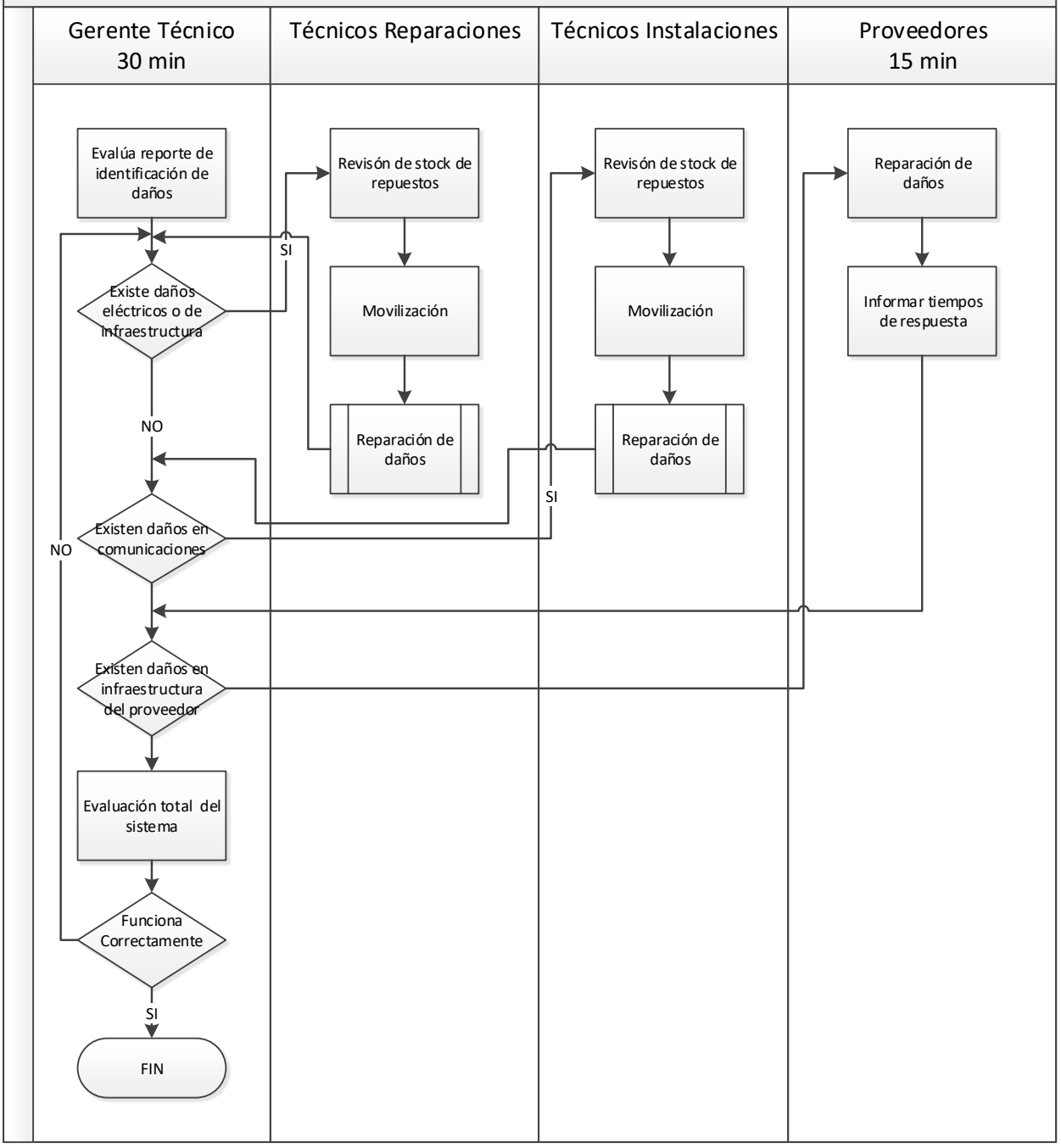
- Llamada Telefónica
- SMS, Chat
- Correo Electrónico

21.0 Procedimiento para reparación y restablecimiento de los servicios.

Durante la fase de Recuperación se llevan a cabo las operaciones formales de recuperación, empezando luego de que el PC ha sido activado y completada la fase de notificación; se han completado las evaluaciones de los daños (de ser posible); y se han movilizado los equipos adecuados. Las actividades de la fase de recuperación se centran en la aplicación de estrategias de recuperación para restaurar las capacidades del sistema, reparar los daños, y reanudar las capacidades operativas en la ubicación original o alternativa. Una vez completada la fase de recuperación, el Sistema de Telecomunicaciones será funcional.

Procedimiento para reparación y restablecimiento de los servicios	***Versión:***	*1.0*
	Fecha:	*20/02/2018*
Objetivos: Definir las acciones para reparar y restablecer los servicios		
Desarrollo:		

Procedimiento para Reparación restablecimiento de servicios



Canales de Comunicación:

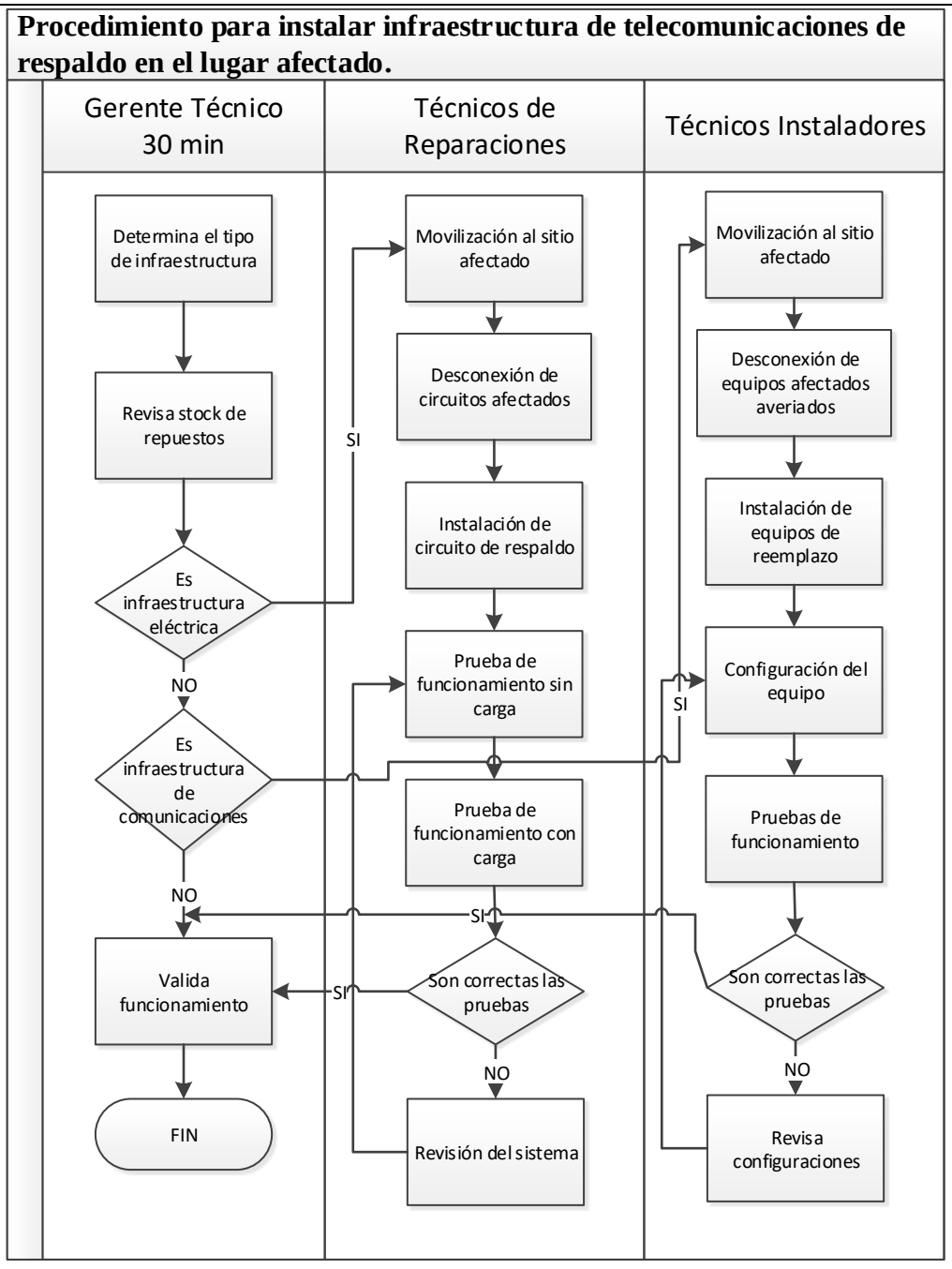
- Llamada Telefónica
- SMS, Chat
- Correo Electrónico

22.0 Procedimiento para instalar infraestructura de telecomunicaciones de respaldo en el lugar afectado.

Procedimiento para instalar infraestructura de telecomunicaciones de respaldo en el lugar afectado.	***Versión:***	*1.0*
	Fecha:	*20/02/2018*

Objetivos: Definir las acciones para instalar infraestructura de telecomunicaciones de respaldo en el lugar afectado

Desarrollo:



Canales de Comunicación:

• Llamada Telefónica • SMS, Chat • Correo Electrónico

23.0 Procedimiento para instalar infraestructura de telecomunicaciones de respaldo o permanente en un lugar alterno, en caso de ser requerido.

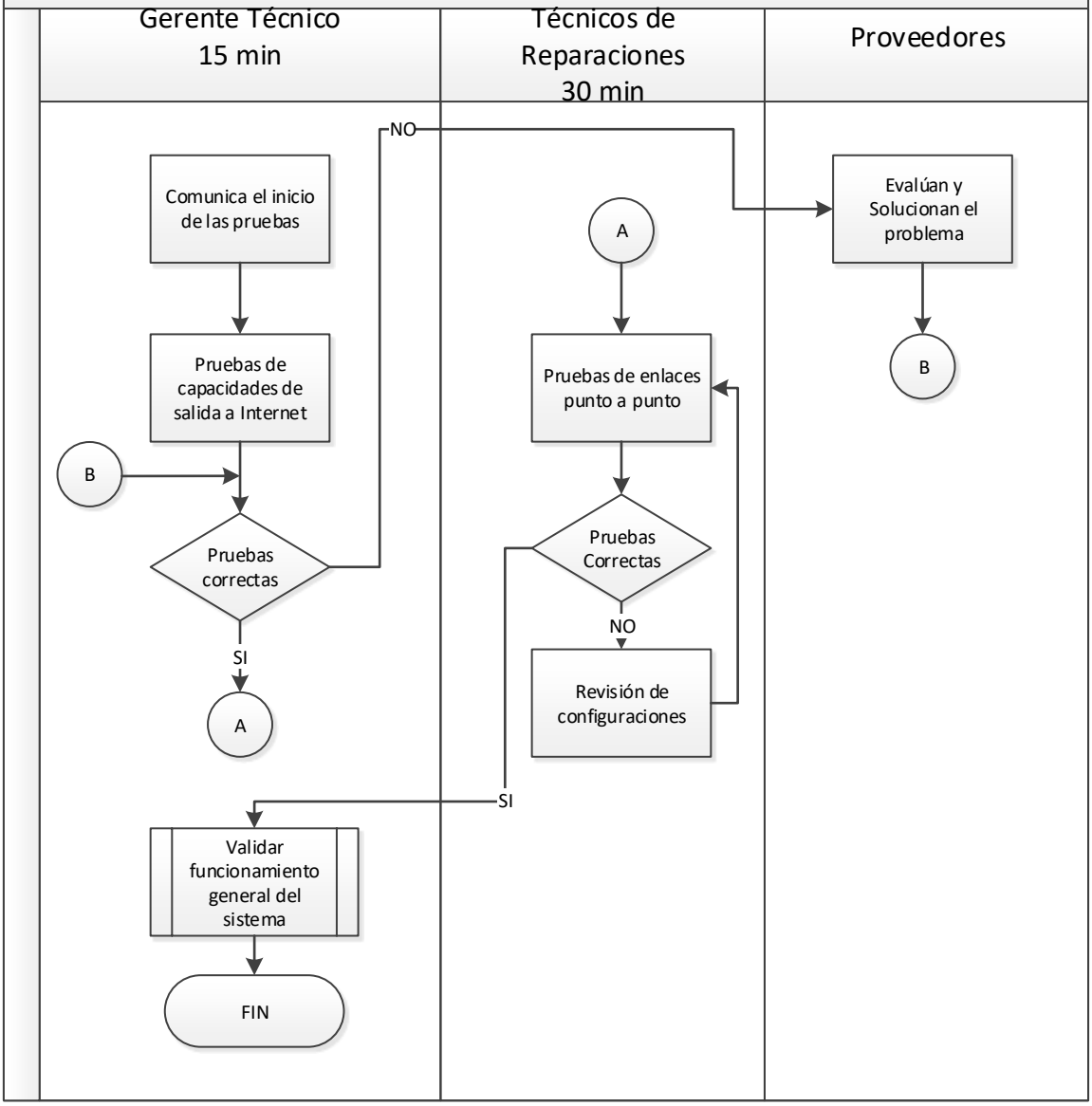
No aplica para este plan

24.0 Planes y Acciones de resiliencia (posterior a la contingencia)

25.0 Procedimiento para probar y validar las capacidades del sistema en la ubicación original, o en la ubicación alterna en caso de que existiere, detallando el tiempo aproximado asociado a cada actividad.

Procedimiento para probar y validar las capacidades del sistema.	***Versión:***	*1.0*
	Fecha:	*20/02/2018*
Objetivos: Definir las acciones para probar y validar las capacidades del sistema		
Desarrollo:		

Procedimiento para Validar las capacidades del sistema



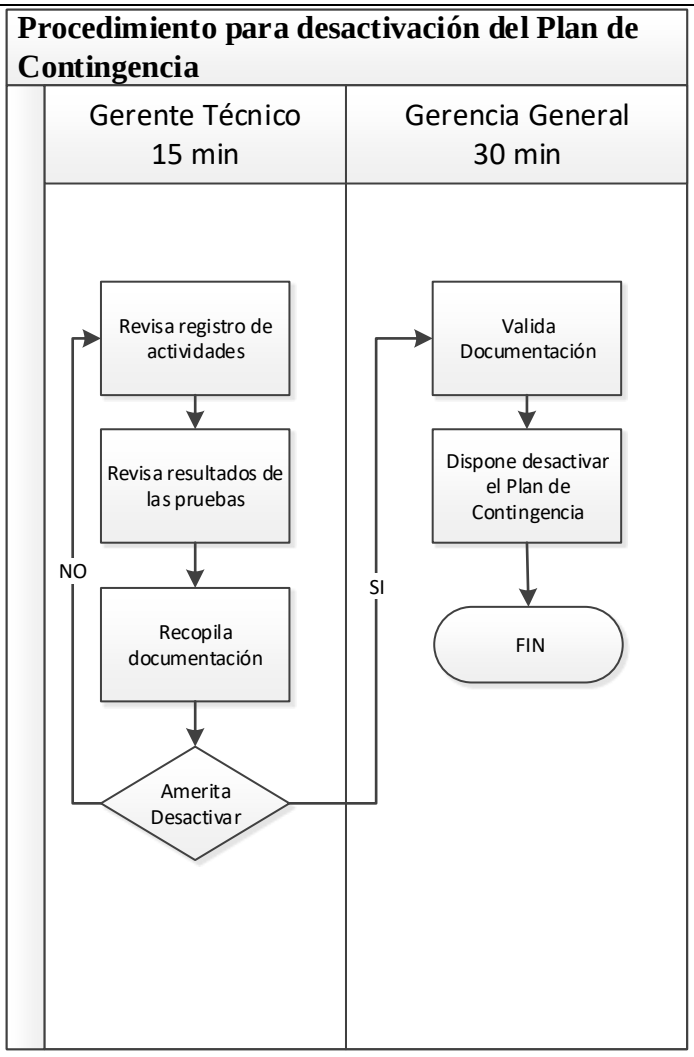
Canales de Comunicación:

- Llamada Telefónica
- SMS, Chat
- Correo Electrónico

Detalle de ejecución de pruebas en el Apéndice J

26.0 Procedimiento para la desactivación o finalización de la aplicación del plan de contingencia y registro de información a tomar en cuenta para la actualización de dicho plan.

Procedimiento para la desactivación o finalización de la aplicación del plan de contingencia	***Versión:***	*1.0*
	Fecha:	*20/02/2018*
Objetivos: Definir las acciones para desactivación o finalización de la aplicación del plan de contingencia		
Desarrollo:		



Canales de Comunicación:

- Correo Electrónico

27.0 Estimado de recursos (humanos, técnicos, logísticos, económicos), para la ejecución de las actividades del plan de contingencia, tanto para las que se realicen de manera remota como para las que se efectúen en sitio, en caso de requerirse.
Apéndices B y J, técnicos (Infraestructura Crítica), logísticos y económicos.

28.0 Responsabilidades y funciones para el personal encargado de la ejecución del plan de contingencia, e información de contacto.

Apéndices A, B y J

29.0 Planes de capacitación para el personal involucrado en el Plan de Contingencia, respecto a la ejecución del mismo.

Temas	Asistentes	Responsable	Frecuencia
Introducción al Plan de Contingencia Vulnerabilidades, Amenazas, Riesgos Identificación de daños Mecanismos de pruebas	Técnicos Reparaciones, Técnicos Instalaciones, Monitoreo/Stanby	Gerente Técnico	Cada 6 meses

30.0 Planificación para la realización de simulacros o pruebas relacionadas con la aplicación del Plan de Contingencia.

Simulacro de riesgo materializado	Responsable	Fecha
Pérdida de servicio en Firewall de Borde	Gerente Técnico	Abril-2020
Pérdida de servicios Radio Transmisor Punto Punto con antena	Gerente Técnico	Junio-2020
Pérdida de servicio Radio Transmisor Multipunto con antena	Gerente Técnico	Agosto-2020
Compromiso de funciones Ruteador Principal Multipuerto	Gerente Técnico	Octubre-2020

31.0 Informe de ejecución de las pruebas de la evaluación del Plan de Contingencia del año inmediato anterior.

Responsable: Gerente Técnico

Desarrollo: Se evalúa el tiempo de respuesta y el cumplimiento del procedimiento establecido, simulando fallas en la configuración y problemas eléctricos.

Fecha	Prueba de Evaluación	Observaciones	Recomendaciones
Junio-2019	Pérdida de servicio en Firewall de Borde	Los tiempos de respuesta no son los adecuados, y dependen de una sola persona para ejecutar el procedimiento.	Capacitar al personal y establecer los accesos necesarios que permitan diagnosticar y ejecutar los procedimientos con celeridad.
Julio-2019	Pérdida de servicios Radio Transmisor Punto Punto con antena	Los equipos de respaldo de energía no conmutan automáticamente y el tiempo de respaldo del sistema UPS es limitado. No se dispone de backups actualizados de configuración de equipos.	Implementar un sistema de conmutación automática de energía para evitar el apagado de los equipos. Evaluar las capacidades de soporte de energía actuales del UPS y reemplazarlo de ser necesario. Realizar respaldo de configuración de equipos con mayor frecuencia y dejarlos al alcance de los responsables de ejecutar los procedimientos de contingencia.
Agosto-2019	Pérdida de servicio Radio Transmisor Multipunto con antena	La falta de equipos electrógenos portables no permite atender simultáneamente cortes eléctricos masivos. No se dispone de backups actualizados de configuración de equipos	Adquirir más equipos electrógenos portables para atender de forma simultanea más nodos de transmisión multipunto. Realizar respaldo de configuración de equipos con mayor frecuencia y dejarlos al alcance de los responsables de ejecutar los procedimientos de contingencia.
Septiembre-2019	Compromiso de funciones Ruteador Principal Multipuerto	El diagnóstico y aplicación del procedimiento está centrado en una solo persona	Capacitar al personal y establecer los accesos necesarios que permitan diagnosticar y ejecutar los

			procedimientos con celeridad.

32.0 Apéndices

Apéndice A: Información de contacto del personal encargado de aplicación y ejecución del Plan de Contingencia (al menos 3, con orden de prelación para el contacto).

Apéndice B: Información de contacto del personal adicional involucrado en las tareas del plan de contingencia (personal de proveedores relacionada con infraestructura crítica).

Esta información no se incluirá en el documento que se presente a la ARCOTEL, sin embargo de lo cual el prestador de servicios deberá mantener dicha información en el formato indicado y deberá ser reportada a la ARCOTEL en caso de ser requerida o presentada durante las tareas de verificación.

Apéndice C: Identificación de proveedores

Esta información no se incluirá en el documento que se presente a la ARCOTEL, sin embargo de lo cual el prestador de servicios deberá mantener dicha información en el formato indicado y deberá ser reportada a la ARCOTEL en caso de ser requerida o presentada durante las tareas de verificación.

Apéndice D: Información geográfica de la Infraestructura Crítica y Sistemas de respaldo de energía para la infraestructura crítica

Apéndice E: Inventario de repuestos y equipamiento de respaldo, en relación con la infraestructura crítica

Esta información no se incluirá en el documento que se presente a la ARCOTEL; sin embargo, de lo cual el prestador de servicios deberá mantener dicha información en el formato que se establezca para tal fin, y deberá ser remitido a la ARCOTEL en caso de ser requerida, o ser presentado durante las tareas de verificación.

Apéndice F: Sistemas portátiles de respaldo de energía - generadores o grupos electrógenos

Esta información no se incluirá en el documento que se presente a la ARCOTEL; sin embargo, de lo cual el prestador de servicios deberá mantener dicha información en el formato que se establezca para tal fin, y deberá ser remitido a la ARCOTEL en caso de ser requerida, o ser presentado durante las tareas de verificación.

Apéndice G: Planes de mantenimiento preventivo programados para el año de aplicación del Plan de contingencia

Apéndice H: Reportes de ejecución del último año, de mantenimientos preventivos, correctivos y emergentes

Apéndice I: Roles y Responsabilidades

J.1. Gerente General o Responsable del Plan de Contingencias (PC)

Es el gerente de administración y es responsable de la administración ejecutiva de todas las facetas del plan de contingencia y ejercicios de prueba del mismo, así como de las operaciones de recuperación, viene a ser el Responsable de Nivel 1 a contactar en caso de desastre natural o conmoción interna. Sus actividades son las siguientes:

- Previo al evento
  - Aprobar el Plan
  - Asegurar que el plan sea mantenido y actualizado
  - Asegurar que se ejecute el plan de entrenamiento y capacitación
  - Autorizar los ejercicios periódicos de prueba del plan
- Posterior al Evento
  - Es el encargado de realizar la declaración de ocurrencia de eventos de desastres naturales o conmoción interna
  - Autorizar el desplazamiento y estadía para los miembros de los equipos
  - Autorizar los gastos a través del equipo de Administración.
  - Administrar y monitorear todo el proceso de recuperación.

J.2. Equipo de Administración de Contingencia

El Equipo de Administración de Contingencia es el responsable de administrar los esfuerzos o tareas de recuperación; para asegurar que otros equipos y personal ejecuten todas las actividades del plan; proveer un "Centro de Comando" para coordinación y todas las comunicaciones; para asegurar que las actividades son ejecutadas entre todos los equipos dentro de los tiempos planificados y para proveer asistencia en la resolución de problemas que puedan presentarse.

Este equipo es activado por el Gerente de Administración del PC o el propietario del sistema.

Todos los demás equipos reportan directamente al equipo de Contingencia/Administración, cuyos deberes específicos son:

J.2.1 Líder del Equipo de Administración de Contingencia o Gerente Técnico

- Previo al Evento
  - Mantener y actualizar el plan de acuerdo a lo requerido o programado, lo cual no debe ser mayor a un año
  - Distribuir copias del plan a los miembros de los equipos
  - Coordinar pruebas requeridas o programadas en un tiempo no mayor a un año
  - Entrenar a los miembros del equipo
- Posterior al Evento
  - Cumplir con la notificación inicial a los miembros del equipo
  - Establecer un centro de comando para las operaciones de recuperación

- Asistir en la evaluación de daños
- Coordinará actividades de los equipos de recuperación
- Notificar de un sitio alterno para reactivación del sistema en caso de requerirse
- Notificar a los líderes de los equipos acerca de la activación del Plan de Contingencia
- Autorizar al Equipo de Administración para realizar los arreglos necesarios para el viaje y hospedaje de los miembros del equipo de recuperación.
- Reportar periódicamente al Gerente de Administración del PC acerca del estado de las actividades de recuperación y otros detalles de acuerdo a o requerido

J.2.2 Miembros del Equipo de Administración de Contingencia:

- **Previo al Evento**
  - Asistir al Líder del Equipo de acuerdo a lo dispuesto
  - Participar en los ejercicios de contingencia
  - Entender todos los roles y responsabilidades del Plan de Contingencia
- **Posterior al Evento**
  - Ejecutar funciones del centro de comando
  - Mantener un historial de todas las comunicaciones utilizando las formas provistas

J.3. Técnicos de Reparaciones e Instalaciones

Los técnicos de reparaciones son los responsables del equipamiento físico y eléctrico de las todas las instalaciones.

Los técnicos de instalaciones son los responsables del equipamiento de comunicaciones de toda la red.

Los técnicos de reparación e instalación son los responsables de evaluar los daños en la infraestructura, equipos y redes, tan pronto como sea posible luego de la activación del Plan de Contingencia, y reportar el nivel de daños al equipo de Administración de Contingencia/Emergencia. El equipo además, provee asistencia cuando sea posible en los trabajos de limpieza y reparación requeridas. Específicamente las responsabilidades del equipo son:

- Previo al evento
  - Entender su rol y responsabilidades bajo el Plan de Contingencia
  - Trabajar para reducir la probabilidad de eventos que requieran la activación del Plan de Contingencia.
  -
  - Participar en los ejercicios y pruebas del Plan de Contingencia.
  - Tener un conocimiento profundo de los procedimientos de evaluación de daños

- Posterior al Desastre
  - Determinar la accesibilidad a la infraestructura, oficinas, y a las áreas/estaciones de trabajo
  - Evaluar la extensión del daño al sistema de telecomunicaciones
  - Evaluar las necesidades y/o adecuaciones físicas de seguridad/protección
  - Estimar el tiempo para recuperar las facilidades primarias y del Sistema
  - Identificar el hardware rescatable
  - Informar al Equipo de Administración de Contingencia acerca del grado de los daños, tiempo estimado de recuperación, la necesidad de seguridad física, y detalle de los equipos recuperables.
  - Mantener un registro de equipo recuperable
  - Coordinar con los proveedores la restauración, reparación o reemplazo del equipamiento que no está bajo la responsabilidad de otros equipos.
  - Colaborar con la limpieza de las facilidades luego del incidente

Apéndice J: Plan de pruebas de Validación del Sistema

Una vez que se ha recuperado el Sistema, se deben ejecutar los siguientes pasos para validar los datos y funcionalidad del Sistema:

Procedimiento	Resultados Esperados	Resultados Actuales	OK?	Responsable
Test de velocidad entre el firewall de borde y la salida a Internetr	Anchos de Banda conforme a lo contratado			Gerente Técnico
Test de velocidad entre el nodo central y los nodos de distribución	Ancho de Banda estable conforme a las necesidades de la red en todos los enlaces			Técnicos de Reparaciones/Instalaciones
Acceso Administrativo a todos los equipos	Acceso correcto			Gerente Técnico
Conexión de clientes a equipos de transmisión	Número de clientes conectados en base a registro de facturación			Monitoreo y Stanby
Sistema de monitoreo de enlaces y eléctrico sin alertas	Ninguna alerta no gestionada			Monitoreo y Stanby

Apéndice K: Historial de Revisión del Documento

Registro de Cambios			
Fecha	**Sección**	**Descripción**	**Cambio realizado por**