UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRÍA EN TELECOMUNICACIONES

DISEÑO DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN CSIRT CON LA FINALIDAD DE ASEGURAR LA INTEGRIDAD DE LA INFORMACIÓN MEDIANTE EL PLANTEAMIENTO DE BUENAS PRÁCTICAS Y POLÍTICAS DE SEGURIDAD

Proyecto del Trabajo de Titulación previo a la obtención del Título de Magíster en Telecomunicaciones

AUTOR:

CARLOS MARIO FERNANDO OBANDO VILLADA

DIRECTOR:

ING. FREDDY MAURICIO TAPIA LEON MSc.

IBARRA - ECUADOR

2021

APROBACIÓN DEL TUTOR

Yo, **Freddy Mauricio Tapia León**, certifico que el estudiante **Carlos Mario Fernando Obando** con Cédula **N° 175854524-6** ha elaborado bajo mi tutoría la sustentación del trabajo de grado titulado: **"Diseño de una guía metodológica para la implementación de un CSIRT con la finalidad de asegurar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad."**

Este trabajo se sujeta a las normas y metodologías dispuestas en el reglamento del título a obtener, por lo tanto, autorizo la presentación a la sustentación para la calificación respectiva.

Ibarra, 27 de abril del 2021

Firmado electrónicamente por:
FREDDY
MAURICIO
TAPIA LEON

MSc. Freddy Mauricio Tapia León

Tutor

CI.: 1714745690

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD	175854524-6
APELLIDOS Y NOMBRES	Obando Villada Carlos Mario Fernando
DIRECCIÓN	Río Chimbo y Princesa Pacha
EMAIL	cmobandov2@utn.edu.ec
TELÉFONO MÓVIL	0986641487

DATOS DE LA OBRA	
TÍTULO	Diseño de una guía metodológica para la implementación de un CSIRT con la finalidad de asegurar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad.
AUTOR	Carlos Mario Fernando Obando Villada
FECHA: DD/MM/AAAA	27 de abril de 2021
PROGRAMA DE POSGRADO	Maestría en Telecomunicaciones
TÍTULO POR EL QUE OPTA	Magister en Telecomunicaciones
TUTOR	MSc. Freddy Mauricio Tapia León

2. CONSTANCIAS

El autor Carlos Mario Fernando Obando Villada, manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 21 días del mes de julio del año 2021.

Firmado electrónicamente por:
CARLOS MARIO FERNANDO OBANDO VILLADA

Carlos Mario Fernando Obando Villada
CI: 1758545246

DEDICATORIA

Este proyecto tiene una mención especial para mis padres y hermanas que siempre están apoyando mis proyectos y desarrollo tanto en el ámbito personal como profesional, sin dejar de lado a mi familia que siempre ha expresado sus mejores deseos.

RECONOCIMIENTO

Agradezco sinceramente al Msc. Freddy Tapia por aportar y guiar mi proyecto de titulación, por los diferentes consejos y predisposición de siempre ayuda y validar cada uno de los avances del trabajo de grado.

Al Msc. Carlos Vásquez por compartir sus conocimientos acertados del tema durante el desarrollo del proyecto de titulación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA EN TELECOMUNICACIONES

"Diseño de una guía metodológica para la implementación de un CSIRT con la finalidad de asegurar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad".

Autor: Ing. Carlos Mario Fernando Obando Villada
Tutor: Msc. Freddy Mauricio Tapia León
Año: 2021

RESUMEN

En la actualidad la disponibilidad del servicio de Internet y el acceso a las aplicaciones a través de la misma se ha convertido en algo indispensable para el área laboral, académica, comercial, entre otras; tanto así que la ausencia de Internet por un largo tiempo afecta a gran parte de las actividades diarias de los usuarios.

Los ISP (Internet Service Provider) están obligados a cumplir las diferentes resoluciones y normativas que la agencia de regulación nacional de las telecomunicaciones ARCOTEL establece para entregar el servicio de Internet a todos sus usuarios; por tal motivo es importante mantener la disponibilidad de la información al menos el 98% del tiempo según la resolución No. 216-09-CONATEL-2009 y resolución No. 2018-0652 de la gestión de incidentes y vulnerabilidades. Con este antecedente existe la necesidad de crear un CSIRT (Computer Security Incident Response Team), éste es un equipo de respuesta a incidentes y su función es minimizar el impacto a las afectaciones de las ausencias de servicio en las empresas prestadoras del servicio de internet, actuando de manera preventiva y proactiva de forma organizada principalmente con la recolección de datos para el análisis y tratamiento de las amenazas y vulnerabilidades.

Este documento es una guía metodológica para implementar un CSIRT que permita afirmar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad para un proveedor de servicios de Internet, tomando en cuenta las diferentes resoluciones que establece el organismo de control de las telecomunicaciones ARCOTEL como exigencias para los ISP en el Ecuador; considerando normas como la de Tecnologías de la información -Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos ISO/IEC 27001 y la Guía Metodológica NIST 802, con la finalidad de mantener el secreto de la información y la continuidad del funcionamiento del negocio.

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA EN TELECOMUNICACIONES

"Diseño de una guía metodológica para la implementación de un CSIRT con la finalidad de asegurar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad".

Autor: Ing. Carlos Mario Fernando Obando Villada
Tutor: Msc. Freddy Mauricio Tapia León
Año: 2021

ABSTRACT

Nowadays, the availability of Internet service and the access to applications through it, has become indispensable for: work, academic, commercial and other areas; so much so, the absence of Internet for a long time affects a large part of the daily activities of the users.

The ISP (Internet Service Provider) are bound to comply with different resolutions and regulations which the National Regulatory of Telecommunications Agency ARCOTEL, establishes to deliver Internet service to all its users; for this reason, it is important to maintain the availability of information at least 98% of the time, according to the resolution No. 216-09-CONATEL-2009 and the resolution No. 2018-0652 of the management of incidents and vulnerabilities. With this background, there is a need to create a CSIRT (Computer Security Incident Response Team), this is an incident response team and its function is to minimize the impact to the affectations of the service absences in the internet service provider companies, acting preventively and proactively in an organized manner, mainly with the collection of data for the analysis and treatment of threats and vulnerabilities.

This document is a methodological guide to implement a CSIRT that allows to affirm the integrity of the information through the approach of good practices and security policies for an Internet service provider, taking into consideration the different resolutions, established by the Telecommunications Control Agency ARCOTEL as requirements for ISPs in Ecuador; considering standards such as Information Technology - Security Techniques - Information Security Management Systems - Requirements ISO/IEC 27001 and the NIST 802 Methodological Guide, in order to maintain the secrecy of the information and the continuity of the business operation.

Keywords: CSIRT, ISP, Security, ACORTEL

CAPITULO I
EL PROBLEMA

En los últimos años el incremento de los ataques informáticos plantea un nuevo panorama a la forma de prevenir incidentes[1], aunque ya se brinda mayor atención a la seguridad de la información aún no es prioridad en las diferentes empresas en el Ecuador, a pesar de que el sector de la banca y seguridad realicen inversiones a la problemática los otros sectores como el de telecomunicaciones no se destacan por presentar un enfoque formal donde se presenten, medidas preventivas que garanticen y minimicen el grado de eventualidades o afectaciones a la integridad de la información. (Medina, 2017b)

Es casi imposible predecir y evadir todos los riesgos[2] que se puedan presentar en una red y su infraestructura, debido a esto, la importancia de tener un equipo de respuesta a incidentes de seguridad (CSIRT), el cual tiene por finalidad solucionar las eventualidades que se presentan y reducir los niveles de impacto en el negocio, en este estudio se enfoca en empresas que brindan servicios de Internet y deben tener de alta disponibilidad. (Mendoza, 2015)

Según la compañía rusa Kaspersky Lab[3], en Latino América en el último periodo evaluado hasta finales del año 2018 el aumento de los ataques cibernéticos ha aumentado un 60% con respecto a los años anteriores, además, se advirtió que Ecuador fue el tercer país con mayor afectación de la región en el año 2017 por WannaCry, siendo México y Brasil las primeras en ser vulneradas (Medina, 2017a), esto debido a la falta de atención a la seguridad de la información.

---

[1] Incidentes según la definición de RAE se comprende que son hechos ya ocurridos.
[2] La RAE define Riesgo se define como la proximidad de un daño y este sujeto a una probabilidad de que pueda suceder o no
[3] Kaspersky es la mayor compañía privada de ciberseguridad. Opera en 200 países y dispone de 35 oficinas en 31 países. Recuperado de https://www.kaspersky.es/about/company#_edn1

AEPROVI, es una Asociación que busca el progreso del sector de las telecomunicaciones y las tecnologías de la información dentro del territorio ecuatoriano, en la actualidad registra sus políticas de seguridad en NAP.EC[4] pero no se especifica que las empresas proveedoras de internet deban tener unas, este organismo se centra en asegurar el enrutamiento de internet o simplemente definir accesos, pero no existe una normativa que regule la inclusión de un equipo técnico de prevención de riesgos a la seguridad de la información. (AEPROVI, 2020)

Bajo este precepto, los ISP's del Ecuador no cuentan con una guía de conformación de un CSIRT o uno debidamente documentado y registrado en el organismo de control de telecomunicaciones como ARCOTEL. lo que ocasiona que los procesos sean desarrollados por personal no calificado y ejecuten acciones que no estén reguladas, Por ejemplo, la asignación de personal inadecuado para atender ocasionando conflictos y malas respuestas a los incidentes reportados.

1.1.Problema de investigación

La filtración de información de los datos personales de casi toda la población ecuatoriana en septiembre del 2019, ha evidenciado una problemática en la importancia que se le da a la seguridad de la información, que desde años atrás está descuidada, pasados estos acontecimientos y en conocimiento de los incidentes en Ecuador se plantea un plan de protección de datos.(Salamanca, 2019)

El ente regulador de las telecomunicaciones en Ecuador ha instaurado un centro de respuestas a incidentes informáticos para las empresas de telecomunicaciones, el propósito

[4] "Oficialmente, NAP.EC fue creado y entró en operación el 4 de julio de 2001 con aval del CONATEL", existe un acuerdo para intercambio de tráfico local. Recuperado de http://aeprovi.org.ec/es/napec/presentacion

de EcuCERT[5] es contribuir a la seguridad de la información y cooperar con los diferentes equipos CSIRT dentro y fuera del Ecuador.(EcuCERT, 2018)

El presente trabajo inicia con la necesidad de obtener una metodología de generar un equipo de respuesta rápida a incidentes de seguridad (CSIRT), teniendo en cuenta que la ARCOTEL reportó a los proveedores de servicios de telecomunicaciones acerca del centro de respuesta a incidentes, es de gran importancia generar un CSIRT en las empresas prestadoras del servicio de Internet o ISP's con la finalidad de mantener el contacto y cumplir con las disposiciones del ente de regulación nacional. (EcuCERT, 2018)

Otro elemento a considerar es la cantidad de información que se transporta por Intranet o hacia el Internet, y la necesidad de salvaguardar los datos almacenados en los dispositivos que se encuentran interconectados a través de la infraestructura de red y que circulan a través de la misma; los proveedores de servicios de Internet deben cumplir con parámetros de disponibilidad de servicio, con un 98% que se exige a las empresas de telecomunicaciones.(Reformada et al., 2006)[6]

Debido a la necesidad de un menor tiempo de respuestas a la solución de inconvenientes que se puedan presentar a diario por problemas en la infraestructura de red física o lógica del ISP, es vital prestar una gran atención a la generación del personal adecuado para solventar estas necesidades. (Mendoza, 2015)

Los ISP actualmente deben de cumplir con algunas exigencias que se han determinado por la ARCOTEL, debido a los diferentes incidentes presentados en los últimos años, existe varias normativas y leyes con las que se debe cumplir, además de tener una constante comunicación con el EcuCert sobre los incidentes en las redes de los proveedores de servicios de Internet, por lo cual es importante generar un CSIRT centrado en los

[5] EcuCERT, es el Centro de Respuestas a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones (EcuCERT, 2018)
[6] Normativa vigente por la ARCOTEL

prestadores de servicio, con la finalidad de preservar el funcionamiento de la red física como lógica del ISP.

1.2. Objetivos de la investigación

1.2.1. Objetivo general

Asegurar la integridad de la información mediante el planteamiento de buenas prácticas y políticas de seguridad para un proveedor de servicios de Internet

1.2.2. Objetivos específicos

- Revisar la literatura asociada a los aspectos de seguridad informática y específicamente en la implementación de un CSIRT, en el Ecuador.
- Determinar los riesgos físicos y lógicos de la infraestructura de la red en un proveedor de servicios de Internet (ISP), a través de un estudio de campo.
- Analizar la norma ISO/IEC 27001 y la Guía de manejo de incidentes de seguridad informática (NIST.v. R2), por medio de una revisión bibliográfica de cada normativa.
- Implementar políticas de seguridad basado en el análisis previo de las normativas propuestas y los resultados obtenidos en las matrices de vulnerabilidad.
- Realizar pruebas de control y vulnerabilidad a través de un software específico validado por un cuadrante de Gartner, para probar la implementación de la seguridad planteada.

1.3. Justificación

La ARCOTEL a nivel nacional exige que todas las empresas telecomunicaciones cumplan con ciertos lineamientos para poder funcionar correctamente, entre las cuales se encuentran las proveedoras de y transportadoras de Internet (Carrier), según la ley orgánica de telecomunicaciones, “El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad

de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información" debe establecer "políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información" (Asamblea Nacional, 2015).

Cada ISP tiene establecido un plazo para desarrollar e implementar en cada empresa un sistema de seguridad de la información vigente y listo para ser auditado, por tal razón es necesario organizar las actividades y formar un equipo especializado sobre cada área y plantear las actividades que se deben realizar para cumplir con estas exigencias del organismo de regulación hacia los ISP's.

El Diseño de una guía metodológica para la implementación de un CSIRT contribuirá a generar lineamientos que pueden ser adaptados a las diferentes necesidades que tengan o se presenten en las diferentes empresas de telecomunicaciones, así como a departamentos en donde se proveen servicios de forma similar a un ISP con el cual se pretende asegurar la integridad de la información, aportando a las áreas de investigación de Diseño y análisis organizacional.

CAPITULO II
MARCO REFERENCIAL

2.1. Antecedentes

La generación de una metodología para la implementación de un equipo de respuesta a incidentes de seguridad no tiene un precedente para empresas de telecomunicaciones puntualmente para un ISP, pero si hay estudios que pueden ayudar a la formación de una, como los artículos generados para los CSIRT[7] de CEDIA(Valladares et al., 2017), y la Escuela Politécnica Nacional en Ecuador(Mendoza, 2015), así como también un modelo de una compañía Irán (Naseri & Azmoon, 2012), y una "Propuesta de Marco de Trabajo para la Protección de un CSIRT" (Mejía et al., 2016).

2.2. Marco teórico

Los sistemas informáticos actualmente son un parte esencial en el día a día, en el área de las telecomunicaciones, la alta disponibilidad y la fiabilidad de la información son parámetros seriamente considerables para los Proveedores de Servicios de Internet – ISP, con lo cual es importante contar con equipos de respuesta a eventualidades y minimización a la ausencia del servicio.

Todas las empresas de telecomunicaciones se rigen a los diferentes organismos de control, de acuerdo a el país y las actividades que desempeña, estas instituciones se rigen bajo normativas nacionales e internacionales en las cuales se destaca la seguridad e integridad de la información. En el caso particular de ecuador el ente regulador es la Agencia de Regulación y Control de las Telecomunicaciones – ARCOTEL.

[7] CSIRT por sus siglas en ingles Computer Security Incident Response Team (Equipo de Respuesta ante Incidencias de Seguridad Informáticas) (Mendoza, 2015)

2.2.1. Normativas de Telecomunicaciones

Las normativas son un conjunto de normas, reglas o leyes que se deben cumplir por las diferentes empresas de telecomunicaciones y sus usuarios, en las que se encuentran: Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27001:2013 (27001:2013, 2015), Security Computer Incident Handling Guide Revision 2 (Cichonski et al., 2012) Ley Orgánica Nacional de telecomunicaciones (Asamblea Nacional, 2015), La Resolución (0652, 2015a) ARCOTEL2018-0652, Agencia de regulación y control de las telecomunicaciones y la Guía de uso del protocolo TLP. (ARCOTEL, 2019)

2.2.2. ¿Qué es un CSIRT?

Los CSIRT son equipos de respuesta a incidentes de seguridad, buscan restituir las actividades con el impacto mínimo aceptable para las organizaciones, Su importancia tiene que ver con distintos factores (Csirt, 2015), entre los que destacan:

- El incremento del tipo y número de amenazas informáticas
- La aparición de leyes y regulaciones orientadas a la protección de la información
- La contribución en los procesos de gestión de riesgos y seguridad de la información

A nivel general existe una gran cantidad de servicios que un CSIRT puede brindar, pero actualmente ninguno brinda todos, en la tabla 1 se muestra algunos servicios:

Tabla 1

Servicios de un CSIRT (Mejía et al., 2016)

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alerta y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias
Tratamiento de incidentes	Evaluaciones o auditoría de la seguridad	Coordinación de la respuesta a las instancias

Apoyo a la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Gestión de la calidad de la seguridad
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad	Análisis de riesgos
Respuesta a incidentes	Servicios de detección de intrusos	Continuidad de negocio y recuperación tras un desastre
Respuesta a incidentes en el sitio	Difusión de información relacionada con la seguridad	Consultoría de seguridad
Tratamiento de la vulnerabilidad		Sensibilización
Análisis de la vulnerabilidad		Educación/Formación
Respuesta a la vulnerabilidad		Evaluación o certificación de productos

Nota: Se listan los servicios reactivos, proactivos y las instancias que puede tener un CSIRT.

Con los diferentes servicios del CSIRT, se propone apoyar a los diferentes departamentos de la empresa o comunidades para las cuales fue conformado, con la finalidad de implementar medidas para prevenir y reducir riesgos además de, responder a la resolución de incidentes con nuevas técnicas y tecnologías de la seguridad en redes de comunicación. (Valladares et al., 2017)

En una empresa proveedora de servicios de Internet es importante contar con algunos de los servicios que se encuentran en la tabla 1, tales como la gestión de notificaciones (alertas y advertencias), tratamiento y respuesta a incidentes, además de, el análisis y tratamiento de vulnerabilidades.

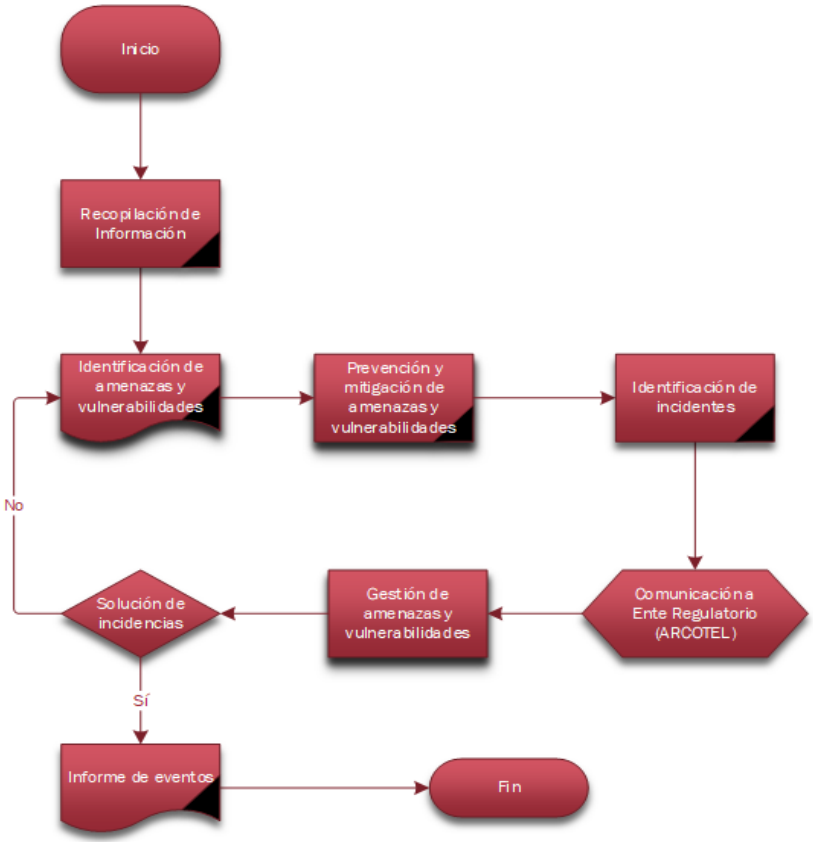
Para cumplir con los procesos generales, un CSIRT actúa de manera preventiva y proactiva (Valladares et al., 2017), siguiendo de manera precisa las diferentes normativas que se registran por las instituciones o agencias de control correspondientes a cada país; en Ecuador la ARCOTEL como agente de control en las telecomunicaciones establece la

"norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones" (0652, 2015a), el objeto es establecer criterios y mecanismos para preservar y mantener la seguridad de los servicios prestados por las empresas de telecomunicaciones, resguardando el secreto de las comunicaciones y de la información transmitida a través de sus redes (0652, 2015b).

La labor de un CSIRT debe ser organizada y precisa para su buen funcionamiento, principalmente con la recolección de datos, ya que bajo esto se realiza el análisis y el tratamiento de las amenazas y vulnerabilidades, las cuales se deben de informar al ente regulador como parte del proceso de solución, en la **figura 1** se determina un diagrama de flujo del comportamiento de un CSIRT

Figura. 1

Diagrama de bloques comportamiento de un CSIRT



Nota: basado en el artículo de (Valladares et al., 2017)

La finalidad de un CSIRT es disminuir las incidencias y aumentar la disponibilidad de la información y continuidad del servicio, en este caso en el área de las telecomunicaciones, así como, ayudar a la comunidad compartiendo conocimientos generales de la solución de los diferentes problemas que se puede suscitar y las soluciones de los mismos.

Por tal motivo entre las obligaciones de los prestadores de servicios de telecomunicaciones se ha dispuesto bajo la Resolución ARCOTEL-2018- 0652, el reporte de incidencias y vulnerabilidades que afectan a la seguridad de la información y las soluciones ejecutadas, el cual se debe realizar bajo los formularios dispuestos por EcuCERT, con esto se busca generar los servicios que se muestran en la **tabla 2**

Tabla 2

Servicios de EcuCERT (EcuCERT, 2018)

Reactivos	**Proactivos**	**Valor Agregado**
Alertas de seguridad	Comunicación y anuncios Tempranos	Sensibilización
Manejo de Incidentes Coordinación a la respuesta de incidentes	Apoyo en la formación de los equipos de respuesta a incidentes informáticos, CSIRT's	
Manejo de vulnerabilidades Coordinación a la respuesta de vulnerabilidades		

Nota: Lista de los servicios propuestos por EcuCERT para las empresas de telecomunicaciones.

Teniendo en cuenta cuales son los servicios que los diferentes equipos de respuesta a incidentes y los parámetros indicados por el ente de regulación de las telecomunicaciones, tablas 1 y 2 respectivamente, se obtiene cuáles son los servicios que un CSIRT para un ISP como se indica en la **tabla 3.**

Tabla 3

Servicios de CSIRT en un ISP

Servicios Proactivos	Servicios Reactivos	Manejo de instancias
Alertas y advertencias	Comunicación y anuncios Tempranos	Análisis de instancias
Tratamiento y manejo de incidentes	Apoyo en la formación de los equipos de respuesta a incidentes informáticos, CSIRT's	Coordinación de la respuesta a las instancias
Tratamiento y manejo de vulnerabilidades	Sensibilización, educación y formación	Evaluación o certificación de productos

Nota: se observa los servicios proactivos, reactivos y el manejo de instancias de un CSIRT para las empresas proveedoras de servicio de Internet.

2.2.3. Sistema de Gestión de la Seguridad de la Información (SGSI)

Según ISO 27001, un SGSI consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. (Licencia, Para, Mario, Obando, & Inen, 2015)

De un sistema de seguridad de la información se espera que su implementación se integre y sea parte de la estructura general del diseño de los procesos y se desarrolle de acuerdo a las necesidades de la organización, además de, la constante mejora del sistema de gestión de la información.

2.2.4. Proveedor de Servicios de Internet (ISP)

Es una empresa u organización que vende a los usuarios servicios de telecomunicaciones como la conexión a Internet. En un mismo país o región pueden existir diversos ISP y cada uno puede utilizar diferentes formas de transportar el servicio de Internet.

Existen varios permisos de portador de servicios, entre los cuales se encuentran los de servicio de valor agregado, en esa categoría se encuentran los ISP's, estas organizaciones en Ecuador están reguladas por la ARCOTEL, la cual ha emitido distintas ordenanzas y normativas con los derechos y obligaciones que deben de cumplir, entre las cuales : i) uso del espectro radioeléctrico[8] (Telecomunicaciones, n.d.); ii) Normativa para el tendido físico de redes aéreas de servicios de telecomunicaciones (Agencia de regulación y Control de las Telecomunicaciones, n.d.); iii) despliegue de redes físicas soterradas de redes de telecomunicaciones (Ministerio del trabajo, 2017); iv) Parámetros de calidad de carácter obligatorio de las empresas portadoras (ARCOTEL, 2002).

Unos de los parámetros importantes que deben de cumplir los ISP es la alta disponibilidad del servicio de Internet, este es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado de continuidad operacional durante un período de medición dado. (Plan de servicio universal 2018 - 2021, 2018)

2.3. Marco legal

Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27001:2013 (27001:2013, 2015) es una guía metodológica en donde se encuentran los diferentes dominios y procedimientos para realizar el análisis y tratamiento de la información.

[8] El espectro radioeléctrico constituye un subconjunto de ondas electromagnéticas, donde es posible brindar una variedad de servicios de telecomunicaciones que tienen una importancia creciente para el desarrollo social y económico de un país. Recuperado de: http://www.arcotel.gob.ec/espectro-radioelectrico-2/

Security Computer Incident Handling Guide Revision 2 (Cichonski et al., 2012), proporcionada por la NIST (National Institute of Standards and Technology), en donde se destacan los parámetros que se deben considerar para la gestión y prevención de eventos en el área de las telecomunicaciones.

Ley Orgánica Nacional de telecomunicaciones (Asamblea Nacional, 2015), EN donde se encuentran los derechos y obligaciones que tiene cada empresa de telecomunicaciones y sus usuarios.

La resolución ARCOTEL-2018-0652, Agencia de regulación y control de las telecomunicaciones(0652, 2015b) y la Guía de uso del protocolo TLP (ARCOTEL, 2019), son normativas creadas por el organismo de control a nivel nacional, en las cuales se registra las reformas y el control que se deben tener para la seguridad e integridad de la información.

CAPITULO III

METODOLOGÍA

Para establecer el diseño de la metodología planteada, se realizó una investigación experimental, utilizando herramientas de laboratorio y de campo, en el cual se ejecutará un análisis de la situación actual y las diferentes soluciones para una empresa de telecomunicaciones.

3.1. Descripción del área de estudio

La metodología que se propone es el diseño y análisis organizacional, en la cual se muestra avances e impactos de las soluciones que se realizan a lo largo de la implementación de la guía, además de los resultados obtenidos mismos que deben de ser validados.

El uso de esta metodología aporta y genera conocimientos en la creación de equipos de trabajo que se pueden adaptar para ayudar a la orquestación de los recursos de un Internet Service Provider – ISP, por sus siglas en inglés, con la finalidad de salvaguardar la integridad de la información de la empresa y sus usuarios.

3.2. Enfoque y tipo de investigación

La necesidad de establecer un sistema de gestión de la seguridad de la información para una empresa de telecomunicaciones y las exigencias de los organismos de control como ARCOTEL, permite el planteamiento de una metodología que otorgue a los ISP la debida confiabilidad de los usuarios sobre el transporte de la información y la disponibilidad de la misma.

3.3. Diseño de Guía Metodológica

El establecimiento de un equipo de respuesta CSIRT para las empresas proveedoras del servicio de Internet es muy importante, casi indispensable en la actualidad, los ISP están obligados a cumplir con algunos parámetros de calidad y disponibilidad del servicio según las exigencias del organismo de regulación y control de las telecomunicaciones como es la ARCOTEL, además de preservar la confidencialidad e integridad de la información de sus clientes y del negocio (0652, 2015b).

Un CSIRT es responsable de responder a incidentes de seguridad de manera técnica para solucionar el incidente como también generando recomendaciones para la prevención de incidentes futuros. Se puede encontrar varias acciones que no son técnicas en una respuesta de un determinado evento, como la comunicación entre empleados o con personas ubicadas en el lugar. (Mendoza, 2015)

Este trabajo se centra en generar una guía por la cual los ISP podrían implementar equipos de respuesta a incidentes CSIRT, teniendo en cuenta las diferentes normativas y leyes que rigen al sector de las telecomunicaciones en el Ecuador, con el objeto de ayudar a mitigar el impacto de las amenazas de seguridad e integridad de la información en la organización.

3.3.1. Definición de Política

La norma NTE INEN-ISO/IEC 27001 está vigente desde el año 2013, se enfoca en Sistemas de Gestión de la Seguridad de la Información (SGSI), en la cual se determinan 130 requisitos, básicamente esta norma plantea dos etapas para la elaboración de las políticas de seguridad

a. Evaluación y tratamiento de riesgos

b. Implementación de Medidas de seguridad

En la norma se define como organizar la seguridad de la información en cualquier tipo de organización, en general se basa en cumplir con el SGSI, es decir ofrecer confidencialidad, integridad y disponibilidad de la información, el documento referencia es:

"tecnologías de la información — técnicas de seguridad — sistemas de gestión de seguridad de la información – requisitos (ISO/IEC 27001:2013+Cor.1:2014+ Cor. 2:2015, IDT)" (27001:2013, 2015)

Tabla 4

Contenido Norma ISO/IEC 27001:2013,2015

	ISO/IEC 27001:2013, 2015
Dominios de Anexo A	14
Objetivos de Control	35
Controles	114

Nota: Se indica cuantos dominios, objetivos de control y controles tiene la norma ISO/IEC 27001

En la **tabla 4** se puede observar los diferentes parámetros de la norma ISO/IEC 27001 que se deben analizar, de acuerdo a las necesidades de cada organización, en este estudio se indica los ítems mínimos de la norma que se debe de tener en cuenta para la seguridad e integridad de la información.

Para realizar la selección de controles de la normativa ISO/IEC 27001, hay que hacer un levantamiento de información de los recursos con los que cuenta el ISP, además de

revisar las necesidades del negocio y las obligaciones a las que se está sujeto como prestador del servicio de Internet.

3.3.2. Levantamiento de Información

El punto de partida para la implementación de un CSIRT es la recopilación de toda la información disponible acerca de la organización con la finalidad de identificar los recursos disponibles y las necesidades del negocio, así como también conocer las ordenanzas vigentes para el funcionamiento como prestador de servicios, en la figura 2 se puede observar algunos de los datos que se deben de recolectar:

Figura. 2

Ejemplos de Información relevante

Nota: Basado en la metodología NIST 800-61 Revisión 2 (Cichonski et al., 2012)

3.3.3. Alcance y objetivos

ALCANCE

Esta guía pretende ayudar a las empresas proveedoras de servicios de Internet (ISP), formar equipos de respuesta a incidentes, con la finalidad de minimizar las afectaciones en cuanto a la seguridad de la información.

Objetivo General - Planear y organizar las actividades para mantener y garantizar la integridad de la información, así como resguardar los activos de la empresa.

Objetivos Específicos

- Revisión de la resolución ARCOTEL-2018-0652, la normativa técnica NTE INEN-ISO/IEC 27001 y la Guía de manejo de incidentes NIST, identificando cuales son las exigencias del organismo de control nacional y cuáles son las recomendaciones y mejores prácticas para la identificación y solución de incidentes.
- Seleccionar los controles y dominios de la norma técnica NTE INEN-ISO/IEC 27001 que inciden en la seguridad de la información, con la finalidad de identificar las amenazas y vulnerabilidades que esta presentes en los ISP.
- Establecer un esquema de sistema de seguridad de la información considerando las recomendaciones de la guía de manejo de incidentes NIST claro bajo la responsabilidad de los proveedores del servicio de Internet.

3.3.4. Selección de Dominios, objetivos de control y controles

La selección de los controles[9] es importante, ya que serán los indicadores del progreso del sistema de gestión de la información dentro de la organización, están basados en el análisis previo al levantamiento de información acerca del estado actual del ISP como empresa.[10]

9 El objetivo de los controles es brindar parámetros de medición sobre el cumplimiento de las medidas adoptadas por la empresa para la seguridad de la información

10 En esta guía metodológica se presenta una selección de controles que se deben de cumplir basados en el análisis del caso de estudio

Tabla 5

Identificadores para clasificación de controles

	No aplica/ sin implementar: cada control que este marcado en blanco no será tomado en cuenta
	Aplica/ implementado: Cada control marcado en verde, será tomado en cuenta y ya está previamente implementado.
	Aplica/ en desarrollo: Cada control marcado en amarillo, se tendrá en cuenta, pero se está generando en la empresa
	Aplica/ sin implementar: Cada control marcado en rojo, se tendrá en cuenta, pero aún no existe ningún procedimiento o desarrollo del mismo.

Nota: descripción a que corresponde cada selección de los controles de la normativa ISO/IEC 27001

En la **tabla 6** se selecciona los controles de cada dominio que presenta la normativa NTE INEN-ISO/IEC 27001 según lo especificado en la **tabla 5**.

Tabla 6

Clasificación de dominios y controles(27001:2013, 2015)

A.5	Política de seguridad de la información			
A.5.1	Dirección de gestión de seguridad de la información			
		Existente	Estado	Aplica/No Aplica
A.5.1.1	Políticas para la seguridad de la información	No	No Cumple	Aplica
A.5.1.2	Revisión de las políticas para la seguridad de la información	No	No Cumple	Aplica
A.6	Organización de la seguridad de la información			

A.6.1	Organización interna			
A.6.1.1	Roles y responsabilidades de seguridad de la información	No	No Cumple	Aplica
A.6.1.2	Separación de funciones	No	No Cumple	No Aplica
A.6.1.3	Contacto con las autoridades	No	No Cumple	Aplica
A.6.1.4	Contacto con los grupos de interés especial	No	No Cumple	No Aplica
A.6.1.5	Gestión de proyectos de seguridad de la información	No	No Cumple	No Aplica
A.6.2	Dispositivos móviles y teletrabajo			
A.6.2.1	Política de dispositivo móvil	No	No Cumple	No Aplica
A.6.2.2	Teletrabajo	No	No Cumple	No Aplica
A.7	Seguridad de los RRHH			
A.7.1	Antes del empleo			
A.7.1.1	Investigación de antecedentes	No	No Cumple	No Aplica
A.7.1.2	Términos y condiciones del empleo	No	No Cumple	No Aplica
A.7.2	Durante el empleo			
A.7.2.1	Responsabilidades de la dirección	No	No Cumple	Aplica
A.7.2.2	Concienciación, educación y formación en seguridad de la información	No	No Cumple	Aplica
A.7.2.3	Proceso disciplinario	No	No Cumple	Aplica
A.7.3	Finalización y cambio de empleo			
A.7.3.1	Responsabilidades ante la finalización o cambio de empleo	No	No Cumple	Aplica

A.8	Gestión de Activos			
A.8.1	Responsabilidad de los activos			
A.8.1.1	Inventario de activos	No	Si Cumple	Aplica
A.8.1.2	Propiedad de los activos	No	Si Cumple	Aplica
A.8.1.3	Uso aceptable de los activos	No	No Cumple	Aplica
A.8.1.4	Devolución de activos	No	Si Cumple	Aplica
A.8.2	Clasificación de la información			
A.8.2.1	Clasificación de la información	No	No Cumple	Aplica
A.8.2.2	Etiquetado de la información	No	No Cumple	No Aplica
A.8.3	Manejo de los medios			
A.8.3.1	Gestión de medios extraíbles	No	No Cumple	No Aplica
A.8.3.2	Eliminación de los medios	No	No Cumple	No Aplica
A.8.3.3	Transferencia de medios físicos	No	No Cumple	Si Aplica

A.9	Control de Acceso			
A.9.1	Requisitos de negocio para el control de acceso			
A.9.1.1	Política de control de acceso	No	No Cumple	Si Aplica
A.9.1.2	Acceso a redes y servicios de red	No	No Cumple	Si Aplica
A.9.2	Gestión de acceso de los usuarios			
A.9.2.1	Registro y retiro de usuario	No	No Cumple	Si Aplica
A.9.2.2	Provisión de accesos a usuarios	No	No Cumple	Si Aplica
A.9.2.3	Gestión de privilegios de derechos de acceso	No	No Cumple	Si Aplica
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	No	No Cumple	Si Aplica
A.9.2.5	Revisión de los derechos de acceso de usuario	No	No Cumple	No Aplica
A.9.2.6	Retirada y ajuste de los derechos de acceso	No	No Cumple	No Aplica
A.9.3	Responsabilidades del usuario			
A.9.3.1	Uso de la información secreta de autenticación	No	No Cumple	Si Aplica
A.9.4	Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción del acceso a la información	No	No Cumple	Si Aplica
A.9.4.2	Procedimientos seguros de inicio de sesión	No	No Cumple	Si Aplica
A.9.4.3	Sistema de gestión de contraseñas	No	No Cumple	Si Aplica
A.9.4.4	Uso de programas utilitarios privilegiados	No	No Cumple	No Aplica
A.9.4.5	Control de acceso al código fuente del programa	No	No Cumple	No Aplica

A.10	Criptografía			
A.10.1	Controles criptográficos			
A.10.1.1	Política de uso de los controles criptográficos	No	No Cumple	No Aplica
A.10.1.2	Gestión de llaves	No	No Cumple	No Aplica

A.11	Seguridad física y del entorno			
A.11.1	Áreas seguras			
A.11.1.1	Perímetro de seguridad física	No	No Cumple	No Aplica
A.11.1.2	Controles físicos de entrada	No	No Cumple	No Aplica

A.11.1.3	Seguridad de oficinas, despachos e instalaciones	No	No Cumple	No Aplica
A.11.1.4	Protección contra las amenazas externas y ambientales	No	No Cumple	No Aplica
A.11.1.5	Trabajo en áreas seguras	No	No Cumple	No Aplica
A.11.1.6	Áreas de carga y entrega	No	No Cumple	No Aplica

A.11.2	Equipos			
A.11.2.1	Ubicación y protección de equipos	No	No Cumple	Si Aplica
A.11.2.2	Instalaciones de suministro	No	Si Cumple	Si Aplica
A.11.2.3	Seguridad del cableado	No	No Cumple	Si Aplica
A.11.2.4	Mantenimiento de los equipos	No	No Cumple	Si Aplica
A.11.2.5	Eliminación de activos	No	No Cumple	Si Aplica
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	No	Si Cumple	Si Aplica
A.11.2.7	Reutilización o eliminación segura de equipos	No	Si Cumple	Si Aplica
A.11.2.8	Equipo de usuario desatendido	No	No Cumple	No Aplica
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	No	No Cumple	Si Aplica

A.12	Seguridad de las operaciones			
A.12.1	Procedimientos y responsabilidades operacionales			
A.12.1.1	Documentación de procedimientos de operación	No	No Cumple	Si Aplica
A.12.1.2	Gestión de cambios	No	No Cumple	Si Aplica
A.12.1.3	Gestión de capacidades	No	No Cumple	Si Aplica
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	No	No Cumple	No Aplica
A.12.2	Protección contra un malware			
A.12.2.1	Controles contra un malware	No	No Cumple	No aplica
A.12.3	Copia de seguridad			
A.12.3.1	Copias de seguridad de la información	No	No Cumple	Si aplica
A.12.4	Registro y monitoreo			
A.12.4.1	Registro de eventos	No	No Cumple	Si aplica
A.12.4.2	Protección de la información de registro	No	Si Cumple	Si aplica
A.12.4.3	Registros de administración y operación	No	Si Cumple	Si aplica

A.12.4.4	Sincronización del reloj	No	Si Cumple	Si aplica
A.12.5	Control de software operacional			
A.12.5.1	Instalación del software en los sistemas operativos	No	Si Cumple	Si aplica
A.12.6	Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de vulnerabilidades técnicas	No	No Cumple	Si aplica
A.12.6.2	Restricciones en la instalación del software	No	No Cumple	Si aplica
A.12.7	Consideraciones de auditoría de sistemas de información			
A.12.7.1	Controles de auditoría en los sistemas de información	No	No Cumple	Si aplica

A.13	Seguridad de las Comunicaciones			
A.13.1	Gestión de seguridad de la red			
A.13.1	Controles de red	No	No Cumple	Si aplica
A.13.1.2	Seguridad de los servicios de red	No	No Cumple	Si aplica
A.13.1.3	Separación en las redes	No	No Cumple	Si aplica
A.13.2	Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información	No	No Cumple	Si aplica
A.13.2.2	Acuerdos de transferencia de información	No	No Cumple	Si aplica
A.13.2.3	Mensajería electrónica	No	Si Cumple	Si aplica
A.13.2.4	Acuerdos de confidencialidad o no revelación	Si	Si Cumple	Si aplica
A.14	Adquisición, desarrollo y mantenimiento del sistema			
A.14.1	Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No	No Cumple	Si aplica
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	No	No Cumple	Si aplica
A.14.2	Seguridad en el desarrollo y en los procesos de soporte			
A.14.2.1	Política de desarrollo seguro	No	No Cumple	Si Aplica
A.14.2.2	Procedimientos de control de cambios en sistemas	No	No Cumple	Si Aplica
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No	No Cumple	Si Aplica
A.14.2.4	Restricciones a los cambios en los paquetes de software	No	No Cumple	No Aplica

A.14.2.5	Principios de ingeniería de sistemas seguros	No	No Cumple	Si aplica
A.14.2.6	Ambiente de desarrollo seguro	No	No Cumple	Si aplica
A.14.2.7	Desarrollo externalizado	No	No Cumple	No Aplica
A.14.2.8	Pruebas de seguridad del sistema	No	No Cumple	Si aplica
A.14.2.9	Pruebas de aceptación de sistemas	No	No Cumple	Si aplica
A.14.3	Datos de prueba			
A.14.3.1	Protección de los datos de prueba	No	No Cumple	No Aplica
A.15	Relaciones con proveedores			
A.15.1	Seguridad de la información en relación con los proveedores			
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No	No Cumple	No Aplica
A.15.1.2	Requisitos de seguridad en contratos con terceros	No	No Cumple	No Aplica
A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	No	No Cumple	No Aplica
A.15.2	Gestión de la provisión de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de los servicios de proveedores	No	No Cumple	No Aplica
A.15.2.2	Gestión de cambios en los servicios de proveedores	No	No Cumple	No Aplica
A.16	Gestión de incidentes de seguridad de la información			
A.16.1	Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	No	Si Cumple	Si aplica
A.16.1.2	Informe de los eventos de seguridad de la información	No	Si Cumple	Si aplica
A.16.1.3	Informe de debilidades de seguridad de la información	No	No Cumple	Si aplica
A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	No	No Cumple	Si aplica
A.16.1.5	Respuesta a incidentes de seguridad de la información	No	No Cumple	Si aplica
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	No	No Cumple	Si aplica
A.16.1.7	Recopilación de evidencias	No	No Cumple	Si aplica

A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio
A.17.1	Continuidad de seguridad de la información

A.17.1.1	Planificación de la continuidad de la seguridad de la información	No	No Cumple	Si aplica
A.17.1.2	Implementación de la continuidad de seguridad de la información	No	No Cumple	Si aplica
A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información	No	No Cumple	Si aplica
A.17.2	Redundancias			
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	No	Si Cumple	Si aplica

A.18	Cumplimiento			
A.18.1	Cumplimiento de los requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	No	Si Cumple	Si aplica
A.18.1.2	Derechos de propiedad intelectual	No	No Cumple	Si aplica
A.18.1.3	Protección de los registros	No	No Cumple	Si aplica
A.18.1.4	Protección y privacidad de la información de carácter personal	No	No Cumple	Si aplica
A.18.1.5	Reglamentos de controles criptográficos	No	No Cumple	Si aplica
A.18.2	Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de seguridad de la información	No	No Cumple	Si aplica
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	No	Si Cumple	Si aplica
A.18.2.3	Comprobación del cumplimiento técnico	No	No Cumple	Si aplica

Nota: Se presenta los dominios y controles de la normativa IEC/ISO 27001 y cuales si aplican o ya existen en la empresa.

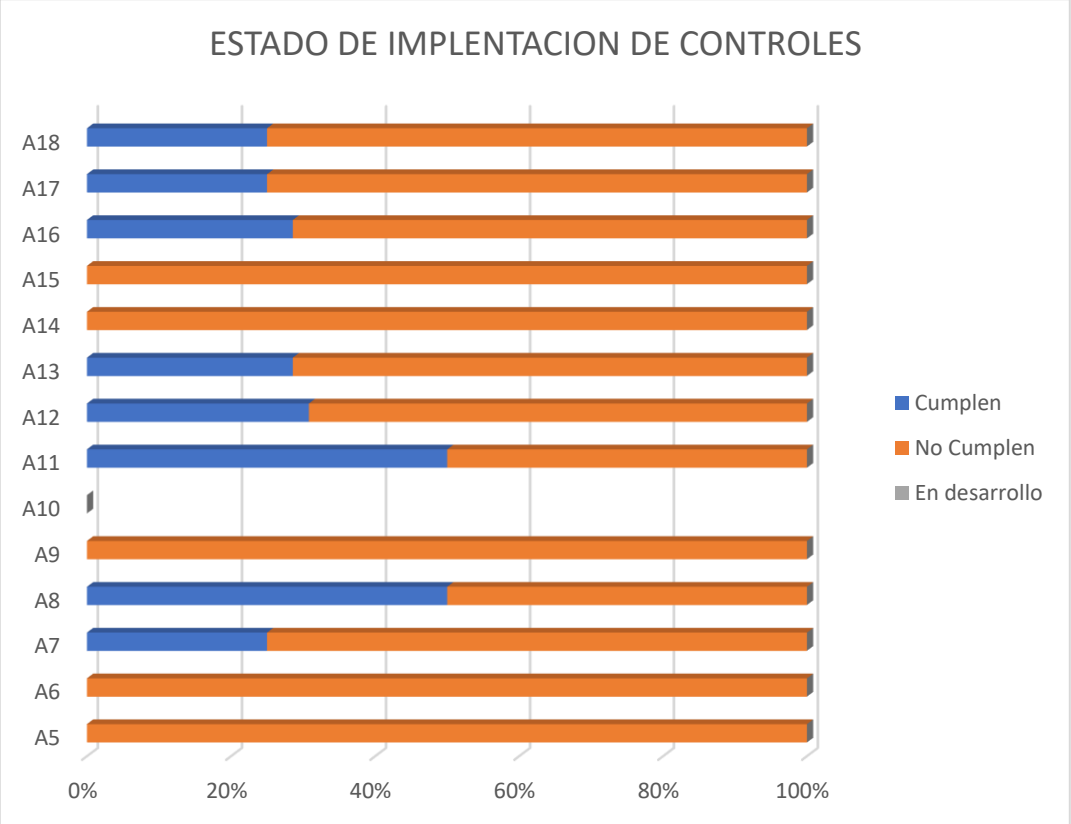
Mediante el levantamiento de información previo y el análisis de cada dominio, se realiza la selección de controles, obteniendo en primera instancia cuál de estos se aplican y cuales no deben considerarse para la organización, además de identificar si existen algunos procedimientos ya establecidos como se muestra en la tabla 6; en algunas ocasiones puede

darse que, se mantenga un determinado control sobre cierta actividad, pero no hay un registro o documento que sirva para verificar y constatar el proceso.

En la **figura 3** se puede ver la relación de cumplimiento de los controles considerados de la normativa IEC/ISO 27001 en el ISP, en el que se puede notar el porcentaje según cuales si existen o se cumple un proceso en la empresa y cuáles no.

Figura. 3

Relación de controles implementados y no implementados



Nota: Muestra la relación de los controles ya implementados, en desarrollo y los que faltan en la empresa.

En la **tabla 7** se detalla un resumen del análisis diferencial de los controles seleccionados por cada dominio y cuantos están implementados en el ISP

Tabla 7

Resumen de Análisis diferencial

Dominio	Total controles seleccionados	Cumple
A.5	2	0
A.6	2	0
A.7	4	1
A.8	6	3
A.9	10	0
A.10	--	--
A.11	8	4
A.12	13	4
A.13	7	2
A.14	7	0
A.15	4	0
A.16	7	2
A.17	4	1
A.18	8	2

Nota: la normativa IEC/ISO 27001 contiene 14 dominios de los cuales se analiza los controles que se gestionan dentro de la empresa y su cumplimiento.

3.3.5. Valoración de activos

La valoración de los activos se realiza teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información, este documento se basa en la metodología NIST-800, en la cual se recomienda que se realice en tres escalas, asignando un valor cualitativo (alto, medio, bajo), pero también es posible hacer una un análisis cuantitativo en el que se asigna un valor que se pueda cuantificar como se muestra en la **tabla 8** y así obtener cifras exactas o muy aproximadas del valor de activo dentro de la empresa. (Henares, 2018)

Tabla 8

Valores calificativos y cuantitativos

	Valor cualitativo	Valor cuantitativo
	Alto	3
	Medio	2
	Bajo	1

Nota: Asignación de valeres cuantitativos con respecto a los valores cualitativos de los activos.

3.3.5.1. Identificación de activos Hardware

Todos los activos se deben manejar bajo el mismo concepto de valoración con la finalidad de saber cuáles son los elementos más críticos en la organización, en la **tabla 9** se indica algunos ejemplos de los que se puede considerar activos en hardware (Mejía et al., 2016):

Tabla 9

Ejemplos de Activos en Hardware

Activo	**Ubicación**
Computador de escritorio	Oficinas
Computador Portátil	Oficina/Campo
Celular	Oficina/Campo
Teléfonos	Oficinas
Antenas de distribución	Nodos de distribución y control
Antenas de Acceso	Acceso cliente
Servidores	Cuarto de equipos
Enrutadores	Cuarto de equipos
Switchs	Nodos de distribución y control
OLT	Nodos de distribución y control
ONT	Acceso cliente

Batería líquida	Nodos de distribución
Batería Seca	Nodos de distribución y control
Batería de gel	Nodos de distribución
Inversor 12V/100 AH	Nodos de distribución y control
Regulador de Voltaje	Nodos de control y distribución
breaker monofásico	Nodos de distribución y control
Aire acondicionado	Cuarto de equipos

Nota: Lista de activos que se encuentran en el ISP correspondientes al hardware.

3.3.5.2. Identificación de activos Software

La valoración de los equipos activos se realiza teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información (Ortiz-Lazo & Vizñay-Duran, 2019), en la **tabla 10** se considera algunos ejemplos y parámetros que se deben de tener en cuenta.

Tabla 10

Activos en Software considerados en el ISP

Activo	**Sistema Operativo**	**Ubicación**	**Sistema de Propietario**	**Licenciado/No Licenciado**
Computador de escritorio	Windows 8	Oficina	Si	Si
Computador de escritorio	Windows 10	Oficina	Si	SI
Computador Portátil	Windows 10	Campo	Si	SI
Computador Portátil	GNU/Linux	Campo	Si	No

Servidor Dude	Windows 8	Nodo Matriz Ibarra	Si	Si
Servidor Sistema Integrado	GNU/Centos 7.17.08 64bits	Nodo Matriz Ibarra	Si	No
Teléfono Celular	Android x.	Oficina	Si	No
Teléfono Celular	Android x.	Campo	Si	No

Nota: Lista de software en los activos que se encuentran en el ISP.

3.3.5.3. Identificación de otros activos

En las empresas de telecomunicaciones y en especial en los ISP se puede encontrar otro tipo de activos como son los componentes pasivos de red, los cuales forman parte esencial del funcionamiento de negocio, por tal razón es indispensable conocer cuáles son y la criticidad que desempeñan en la continuidad de los servicios que presta la empresa, como se puede observar en la **tabla 11.**(Ortiz-Lazo & Vizñay-Duran, 2019)

Tabla 11

elementos pasivos de red

ELEMENTOS PASIVOS
Segmento de Torre
Gabinete metálico de piso
Gabinete metálico de poste
Gabinete metálico para medidor
Barra Tensora
Rack de Piso
Rack de pared

Organizadores horizontales
Alambre Tensor
Cable Sucre 2x10 AWG
Soporte Antena
Splitter óptico 1x4
Splitter óptico 1x8
Splitter óptico 1x16
NAP
ODF
Mangas
Conectores (SC, LC)
Cable de Fibra óptica (2h, 4h, 12h, 24h, 48h)

Nota: Lista de activos pasivos que se utilizan en el ISP para brindar el servicio de Internet.

Otros de los activos que se deben tener en cuenta es la cantidad de trabajadores que tiene la empresa, razón por la cual se deben considerar todos aquellos que realizan un trabajo constante[11] y tienen un acuerdo directamente con la organización, por ejemplo, la lista de la **tabla 12.**

Tabla 12

Ejemplos de personal como activo

PERSONAL		
Nombre	Cantidad	Sucursal
Empleados	45	Matriz
Empleados	20	UNO
Empleados	5	DOS
Empleados	10	TRES
Socios Directivos	3	Matriz

[11] Cantidad de empleados con un contrato de pertenencia a la empresa en cada sucursal y trabajadores ocasionales que no pertenecen a la empresa, pero realizan un trabajo para la misma.

Planta Externa	5	Matriz

Nota: En la tabla se muestra cómo se debe identificar al personal que trabaja para el ISP teniendo en cuenta la dependencia cantidad y sucursal en caso de haber diferentes.

3.3.6. Análisis de Riesgos

Una amenaza se puede definir como cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. los valores porcentuales del impacto y la probabilidad se tomarán en cuenta según el nivel de riesgo (Cichonski, 2012) de la siguiente manera:

Impacto: 0% si la amenaza no produce ningún daño
50% si el daño es considerable
100% si el daño es muy crítico para la empresa

Probabilidad: 0% si la probabilidad de que la amenaza se materialice es baja
50% si la probabilidad es considerable
100% si la probabilidad es muy alta

En relación a lo mencionado en la tabla 8 se realiza la asignación de valores cuantitativos, con la finalidad de identificar el impacto y la probabilidad de que suceda un incidente, como se muestra en la **tabla 13.**

Tabla 13

Ejemplo de calificación de impacto y probabilidad

Clasificación de Impacto y probabilidad		
Valoración	**Rango**	**Identificador**
Alto	100%	3
Medio	50%	2
Bajo	0%	1

Nota: Detalles correspondientes a la valoración, rango e identificador para la clasificación de impacto y probabilidad de incidentes.

Entre los riesgos con mayor frecuencia que se pueden identificar en un ISP y por los cuales pueden generar suspensión del servicio y falta de disponibilidad de la información se muestran en la **tabla 14**, además se realiza un análisis de impacto y probabilidad en la afectación de la red de un proveedor de Internet. (Ortiz-Lazo & Vizñay-Duran, 2019)

Tabla 14

Riesgos de suspensión de servicio general

Riesgo	Valor	Impacto	Probabilidad
Ataques informáticos externos	2	2	2
Infecciones con malware	2	3	2
Inundaciones	2	2	1
Robo de equipos	3	3	2
Incendio o cortes de fluido eléctrico	3	3	3
Cortes de Fibra Óptica cable troncal	3	3	2
Cortes de Fibra Óptica cables de distribución	3	3	2
Cortes de fibra Óptica en última milla	3	2	3
Fallas de equipos de backbone	3	3	2
Fallas de equipos de distribución	2	2	3
Fallas de equipos de última milla	2	2	3
Falta de definición de responsabilidades a personal capacitado	3	3	3
Fallas en elementos pasivos	2	1	2

Nota: Se indica cual es el valor, impacto y la probabilidad de ocurrencia de los riesgos identificados en el ISP durante un periodo de tiempo y un registro de eventos por parte del área técnica de la empresa.

3.3.7. Clasificación y tratamiento de la Información

Cada uno de los departamentos tienen diferentes niveles de injerencia sobre la información, la clasificación de la misma se realiza en diferentes niveles, bajo, medio, alto y muy alto (Cichonski et al., 2012); según Traffic Light Protocol (TLP) el etiquetado de la información se deber realizar en los distintos estados del semáforo, donde el color blanco no tiene un valor de criticidad considerable, por tanto en la **tabla 15** se considera:

Tabla 15

Igualación de valores cuantitativos a estados del TLP

		TLP blanco, sin restricción
1. Bajo		TLP verde, divulgación limitada
2. Medio		TLP Ámbar, difusión limitada
3. Alto		TLP rojo, difusión restringida

Nota: Asignación de valores de acuerdo al protocolo TLP basado en (ARCOTEL, 2019)

La ARCOTEL ha dispuesto el protocolo TLP para la clasificación y acceso a la información (ARCOTEL, 2019), el tipo de tratamiento que se genera para la integridad de la información comprende las áreas de conocimiento para realizar las medidas de prevención requeridas en cada dependencia, tales como:

1. Socialización de Procedimientos
2. Capacitación técnica
3. Generación de políticas de seguridad
4. Implementación de reglas de seguridad

5. Toma de decisiones sobre procedimientos técnicos
6. Toma de decisiones en el área contable
7. Autorización de procedimientos Técnicos y administrativos
8. Acceso a la información de difusión restringida (TLP: Rojo)
9. Acceso a la información de difusión limitada (TLP: Ámbar)
10. Acceso a la información de divulgación limitada dentro de la comunidad (TLP: verde)
11. Acceso a la información de divulgación sin restricción (TLP: blanco)

3.3.7.1. Tratamiento de información por dependencias

El propósito de clasificar la información es para poder etiquetar según la criticidad de la misma, además de conocer quién puede acceder y quien no tiene los permisos suficientes, por ejemplo, se puede realizar según las áreas o dependencias en el ISP como se muestra en la **tabla 16.**

Tabla 16

Categorización y Tratamiento de información por dependencias

Dependencias	Prioridad	Tratamiento
Gerencia	3	1,4,5,6,7,8,9,10,11
Subgerencia	2	1,4,6,7,9,10,11
Presidencia	2	1,4,6,7,10,11
Departamento jurídico	3	1,9,10
Departamento de TI	2	1,2,3,9,10
Departamento Financiero	2	1,3,9,10
Área de Pagaduría	2	1,6,10
Departamento Comercial	1	1,10
Departamento de Seguridad Industrial	1	1,10
Jefe Técnico	3	1,2,4,5,9,10

Área de Regulación	3	1,3,4,9,10
Área técnica administrativa	2	1,2,4,9,10
Área técnica de campo	2	1,2,4,9,10

Nota: lista de etiquetado según la clasificación y tratamiento de la información de las dependencias del ISP.

Cada dependencia tiene acceso a información dentro del ISP, por tal razón es importante saber cuál es la criticidad de la misma según el área en la que se encuentra y el tratamiento que se debe tener en cuenta como mediadas de prevención tratadas anteriormente.

3.3.8. Identificación de amenazas y vulnerabilidades

Mediante la investigación actual se pretende identificar y analizar las vulnerabilidades y causas de ausencia del servicio; así como el acceso a la red por parte de los usuarios internos y externos de un ISP, con la finalidad de minimizar el impacto de amenazas y ausencias de los recursos que brindan las empresas proveedoras de servicios de Internet.

Mediante el monitoreo y registros de alertas que generan los agentes[12], se logra identificar cuáles son los eventos con mayor frecuencia, así como también por medio de visita a los sitios, en donde suceden los cortes o problemas del servicio de Internet. (Ortiz-Lazo & Vizñay-Duran, 2019)

[12] Un agente es una pequeña parte de software que se instalan en los equipos que se desea monitorear, el cual sirve para la extracción de información y ser enviada al servidor de monitoreo.

En la **tabla 17** se encuentran los riesgos estudiados y mediante el monitoreo y registro de eventos según las alertas generadas se debe de identificar cual es el incidente y los controles para la solución, en la siguiente tabla se propone los controles para los riesgos establecidos anteriormente (Ortiz-Lazo & Vizñay-Duran, 2019)

Tabla 17

Control de riesgos a riesgos estudiados

Riesgo	Control Propuesto
Ataques informáticos externos	Monitoreo de tráfico para la identificación de ataques de denegación de servicio, políticas de seguridad del uso adecuado de correo electrónico y páginas de acceso seguro.
Infecciones con malware	Generación de procesos y políticas de respaldo de la información.
Inundaciones	Implementación de procesos y políticas de seguridad físicas de los sitios en riesgo de inundaciones.
Robo de equipos	Monitoreo de agentes, generación de políticas de seguridad y procesos de acción.
Incendio o cortes de fluido eléctrico	Monitoreo de equipos mediante equipos dedicados al estado del fluido eléctrico, generación de políticas de seguridad para el respaldo de energía
Cortes de Fibra Óptica cable troncal	Monitoreo de Equipos (agentes) de puntos de conexión en extremos, equipo de respuesta a incidentes.
Cortes de Fibra Óptica cables de distribución	Monitoreo de Equipos (agentes) de puntos de conexión en extremos, equipo de respuesta a incidentes.
Cortes de fibra Óptica en última milla	Monitoreo de Equipos (agentes) de puntos de conexión en extremos, equipo de respuesta a incidentes.
Fallas de equipos de backbone	Elaboración de inventario de activos en caso de cambio de equipos, implementación de políticas de seguridad y procesos de respuesta, Realizar capacitaciones del uso de equipos al equipo de respuestas a incidentes.
Fallas de equipos de distribución	Elaboración de inventario de activos en caso de cambio de equipos, implementación de políticas de seguridad y procesos de respuesta. Realizar capacitaciones del uso de equipos al equipo de respuestas a incidentes.
Fallas de equipos de última milla	Elaboración de inventario de activos en caso de cambio de equipos, implementación de políticas de seguridad y procesos de respuesta
Falta de definición de responsabilidades a personal capacitado	Realizar proceso de asignación de responsabilidades y un plan de contingencia.
Fallas en elementos pasivos	Elaboración de inventario de elementos pasivos para tener actualizado la disponibilidad de los mismos.

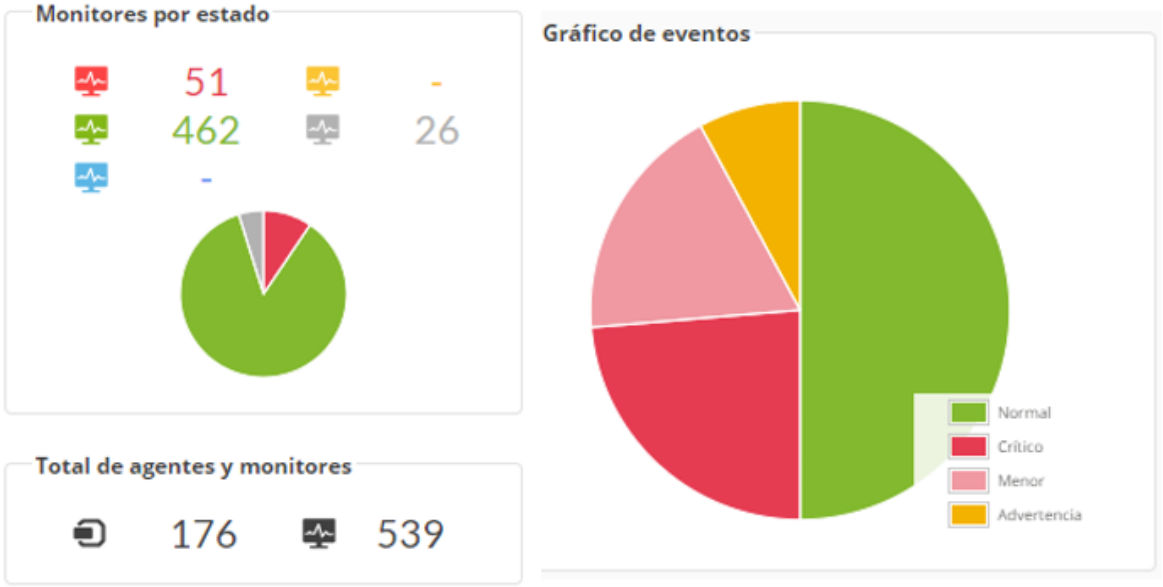
Nota: Lista de riesgos encontrados en el ISP y los controles propuestos para la mitigación o solución

En este trabajo se utiliza como software de monitoreo pandora ya que es una opción que brinda obtener gráficas y estadísticas de eventos en su versión gratuita, en el Anexo 1 se puede revisar a más detalle de la elección de Pandora FMS como servidor de monitoreo.

En la **figura 4** se puede observar las gráficas de los eventos actuales, en los cuales se puede identificar el tipo de alerta y el estado de los equipos o nodos en monitoreo, entre los detalles se resalta el estado y el tipo de evento, es decir, si esta todo normal, si es un evento de menor incidencia o de alta criticidad.

Figura. 4

Monitoreo de eventos



Nota: Resultado del comportamiento de la red observado en el software Pandora.

En la figura 4 se puede identificar el comportamiento de una subred funcionando normalmente cuando todo está de color verde, quiere decir que no ha sufrido o recibido algún tipo de alertas, a diferencia de las zonas en rojo, que son las que indican eventos críticos o en gris cuando son agentes con un largo tiempo de desconexión.

Figura. 5

Notificaciones o alertas de eventos

Nota: Estado de la actividad en la red de un dispositivo monitoreado en el software Pandora.

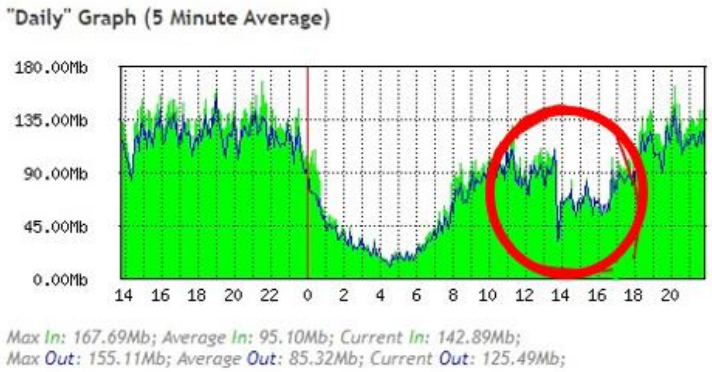
En la figura 5 se muestra el estado de un agente y las alertas que se generan cuando sucede algún incidente en el funcionamiento del equipo, en este caso se observa un evento crítico, ya que transcurre un tiempo de falta de respuesta hacia el servidor de monitoreo, en el cual se encontró que era un corte del cable de fibra óptica que conecta al dispositivo final, de acuerdo al reporte del personal que acude al sitio del daño.

No todas las incidencias son físicas, también hay lógicas en las cuales se pueden generar diferentes situaciones, en la figura 6 se puede identificar una disminución de tráfico en el nodo monitoreado, en la que se puede observar la cantidad de Megabits por segundo

que pasan a través del equipo en cada hora, notando el cambio de un instante de tiempo a otro.

Figura. 6

Monitoreo de tráfico en Mbph



Nota: Monitoreo de tráfico en un punto especifico de la red mediante la herramienta de los equipos Mikrotik

Al tener un monitoreo constante sobre los dispositivos o infraestructura de red, ayuda a tener una respuesta rápida de algún incidente, además de generar reportes que permitan realizar un diagnóstico y mitigar el problema para que no se repita de ser posible, por tal razón dentro del personal que conforma un CSIRT debe de incluirse a quien esté en el área de monitoreo de red. (Cichonski, 2012)

Al generarse alertas o notificaciones de algún problema o incidente que comprometan la continuidad del servicio o la integridad de la información, se puede generar estadísticas y mitigar las amenazas identificadas. En la tabla 18 se listan algunas de las amenazas que se pueden suscitar para un ISP (C., 2019).

Tabla 18

Lista de Amenazas clasificadas en categorías(C., 2019)

Desastres Naturales (N)	Origen Industrial (I)	Errores y Fallos no intencionados (E)	Ataques Intencionados (A)
N.1. Fuego	I.1. Fuego	E.1. Errores de usuarios	A.1. Manipulación de los registros de Actividad
N.2. Daños por agua	I.2. Daños por Agua	E.2. Errores de Administrador	A.2. Manipulación de la configuración
N.3. Otros desastres Naturales	I.3. Daños Industriales	E.3. Errores de monitorización	A.3. Suplantación de la identidad del usuario
	I.4. Contaminación Mecánica	E.4. Errores de Configuración	A.4. Abuso de privilegios de Acceso
	I.5. Avería de origen físico o lógico	E.5. Difusión de software Dañino	A.5. Uso no previsto
	I.6. Corte del suministro eléctrico	E.6. Errores de enrutamiento	A.6.Difusión de software dañino
	I.7. Condiciones inadecuadas de temperatura o humedad	E.7. Errores de Mantenimiento/actualización de software	A.7. Acceso no Autorizado
	I.8. Fallo de servicios de comunicaciones	E.8. Pérdida de equipos	A.8. Modificación deliberada de la Información
	I.9. Interrupción de otros servicios y suministros esenciales	E.9. Indisponibilidad de personal	A.9. Divulgación de la información
		E.10. Fugas de Información	A.10. Manipulación de Equipos
		E.11. Vulnerabilidad de los programas (software)	A.11. Denegación de servicio
			A.12. Robo
			A.13. Indisposición de personal
			A.14. Ingeniería Social

3.3.8.1. Análisis de amenazas por Activos

Las vulnerabilidades más comunes y puntos de acceso utilizados por intrusos se evalúan según el impacto que tienen en el funcionamiento de la red y el grado de afectación

a la integridad de la información, se clasifican con el mismo concepto que la valoración de activos ya planteado en la tabla 8, de la siguiente manera:

1. Bajo
2. Medio
3. Alto

La escala de valoración de impacto y probabilidad se toma como máximo 100%, que corresponde a que impacta a la totalidad de activos de la empresa.

3.3.8.2. Cálculo de Nivel de Riesgo

El cálculo de nivel aceptable de riesgos se basará en los siguientes parámetros:

Tabla 19

Escala de Impacto

Escala de Impacto	
Alto	
Medio	
Bajo	

Nota: en la tabla se muestra los colores según la escala de impacto

El nivel de riesgo es la relación que existe entre el nivel de impacto y el nivel de probabilidad de ocurrencia de las incidencias que afectan a la continuidad de los servicios prestados por el ISP, en la **tabla 20** se muestra los valores correspondientes en porcentaje, obteniendo como el valor máximo 100% (ROJO) y el mínimo del 0% (VERDE) (Henares, 2018)

Tabla 20

Niveles de evaluación de Riesgo

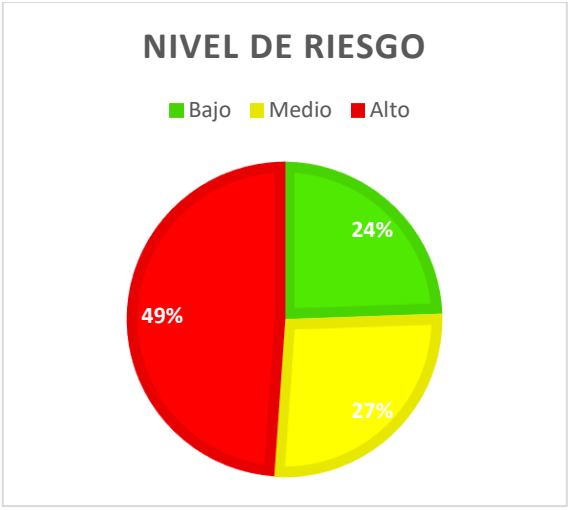
Nivel de Impacto	1	0%	50%	100%
	0.5	0%	25%	50%
	0	0%	0%	0%
		0	0.5	1
		Nivel de Probabilidad de Ocurrencia		

Nota: De acuerdo a la tabla 20 se determina el nivel de riesgo a la que está expuesta la información en el ISP, de acuerdo al valor, impacto y probabilidad de ocurrencia, determinando el grado de afectación al negocio. (Henares, 2018)

En la **figura 7** se muestra el resultado del análisis de las amenazas y vulnerabilidades ya detalladas en las tablas l8 y 17 obteniendo lo siguiente:

Figura. 7

Nivel de riesgo actual del ISP



Nota: Se indica el nivel después del riesgo del análisis de las amenazas y vulnerabilidades basado en (Henares, 2018)

En la **figura 7** se nota que el nivel de riesgo es alto un 49% por tal razón la confidencialidad, integridad y disponibilidad de la información pueden tener una afectación considerable para la continuidad del negocio. (C., 2019)

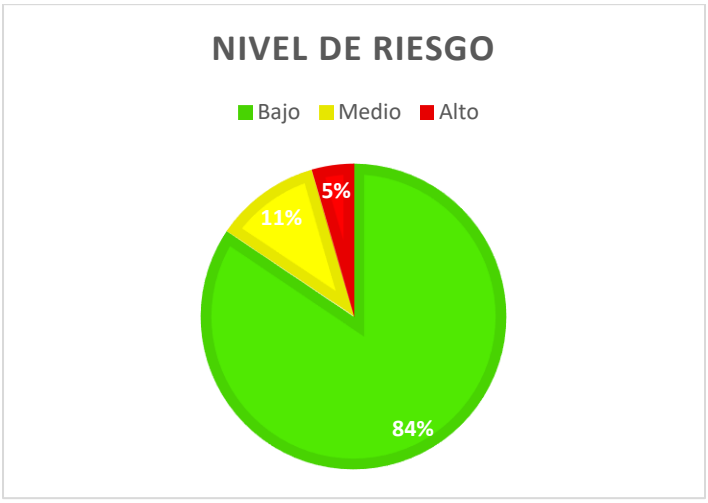
3.3.9. Plan de Tratamiento de reducción de riesgos

La gestión de amenazas y vulnerabilidades se realiza una vez se complete cada uno de los anteriores ítems, ya que se debe tener conocimiento de cuáles son las incidencias de mayor criticidad, el nivel de impacto de cada riesgo y la frecuencia con la que se presentan.

Al tener identificado cada uno de los riesgos más frecuentes que afectan la continuidad del negocio y del estado actual del ISP, se puede decir que la misión es “Contar con un plan estratégico en el que se pueda establecer una guía para la prevención, reducción, mitigación y solución de los diferentes daños que se pueden presentar lógica y físicamente en el transporte, disponibilidad de la información y servicios que brinda la empresa”, no todos los riesgos se pueden eliminar completamente, pero si se puede minimizar el impacto de afectación al negocio, con lo cual se espera un obtener un resultado como se indica en la **figura 8.**

Figura. 8

Nivel de riesgo estimado del ISP



Nota: Nivel de riesgo esperado después de realizar la mitigación de incidentes identificados en la empresa. (Henares, 2018)

3.3.9.1. ¿Cuáles son los objetivos del CSIRT?

El equipo de prevención y respuesta a incidentes debe trazar el plan de acción para minorizar las incidencias que afecten a la integridad de la información y la continuidad del negocio(Csirt, 2015), por tanto, deben:

- Identificar las posibles eventualidades que se pueden presentar en la interrupción del servicio y seguridad de la información
- Poner a disposición, herramientas, mecanismos y estrategias que apoyen las medidas de seguridad del ISP
- Concientizar de la importancia del manejo de la información

3.3.9.2. Asignación de responsabilidades

La selección del personal responsable de para ejecutar los diferentes controles es muy importante en el CSIRT, se debe de asignar las responsabilidades al personal capacitado para desempeñar las diferentes actividades para la prevención de riesgos y la solución de incidentes. (C., 2019)

No es simplemente realizar la asignación, también es delegar las responsabilidades para obtener datos técnicos acerca de las incidencias y la solución, obtener registros con la finalidad de tener información que permita mitigar y mejorar los tiempos de respuestas a las problemáticas que se afrontan cada día en los ISP. (C., 2019)

Se puede dividir grupos por áreas o por capacidades, pero siempre debe de haber una designación del encargado de la seguridad, el cual debe de realizar la revisión y medición del CSIRT, así como de sensibilizar al personal de la importancia de la seguridad e

integridad de la información, pero no es el único responsable, en la **tabla 21** se puede observar una distribución de responsabilidades.(Csirt, 2015)

Tabla 21

Asignación de responsabilidades

Asignación	Área/departamento	Responsable
Responsabilidades Generales	Todos a quienes sean afectados por el SGSI	Gerente General
Gestión de cumplimiento de normativa	Todos a quienes sean afectados por el SGSI	Gerente General, jefes de área
Gestión de riesgos	Todos a quienes sean afectados por el CSIRT	Responsable de seguridad de la información
Revisión y medición del CSIRT	Todos a quienes sean afectados por el SGSI	Responsable de seguridad de la información
Gestión de Activos	Departamento de Sistemas, departamento técnico	Jefes de áreas
Gestión de incidencias	Departamento Técnico y de regulación	Jefes de áreas y responsable de la seguridad de la información
Gestión de comunicación	Departamento de regulación y departamento técnico	Jefes de áreas y responsable de la seguridad de la información

Nota: Asignación de responsabilidades por áreas/departamentos al personal del ISP.

3.3.9.3. Procedimientos Operacionales

El objetivo del CSIRT es minimizar la afectación a los servicios del ISP y preservar la disponibilidad e integridad de la información, por esta razón todos los procedimientos deben de ser documentados, revisados y aprobados por las autoridades respectivas; después

de haber analizado cada control de la normativa ISO/IEC 27001 y la guía NIST, se determina que los prestadores de servicios de internet al menos deben constar los siguientes procedimientos:

- Procedimientos de la gestión de activos
- Procedimientos de la gestión de vulnerabilidades y suspensión de servicio
- Procedimiento para el tratamiento de la gestión de riesgos
- Procedimientos de revelación de información privada o limitada
- Procedimientos de retiro y desinstalación de equipos por termino de contrato
- Procedimiento del respaldo de información sensible de la empresa
- Procedimiento de suspensión del servicio de internet
- Procedimiento de registro de afectaciones al servicio de internet mediante la gestión de tickets
- Procedimiento de gestión y clasificación de información según el protocolo TLP
- Procedimiento de comunicación de incidencias a ente regulatorio ARCOTEL

3.3.9.4.Formulación de políticas de Seguridad

La formulación de las políticas de seguridad sirve para generar guías sobre la conducta de los trabajadores en la empresa y para concientizar la importancia del manejo de la información, lo primero que se debe identificar es el alcance que se desea que tengan las Políticas de seguridad (Mejía et al., 2016), por ejemplo

Alcance- las políticas de seguridad se elaboran de acuerdo al análisis de riesgos y vulnerabilidades que se presentan para la red del ISP, por lo cual las políticas que se establece son solo para la empresa.

Después de saber cuál es el alcance es importante plantear los objetivos de las políticas de seguridad, sin olvidarse hasta donde se pretende llegar, hay que tomar como referencia la misión y visión de la empresa.

El planteamiento de las políticas de la seguridad del ISP regirá cual debe ser el comportamiento con respecto a la seguridad e integridad de la información y el actuar del CSIRT (Mejía et al., 2016), por tanto, se debe de tener en cuenta todo el análisis anteriormente desarrollado, en cada uno de los literales de este capítulo, en resumen, para la formulación de políticas de seguridad hay que tener en consideración los siguientes puntos:

- Políticas de Seguridad Generales
- Políticas Generales Para Administradores
- Políticas de Gestión de Activos
- Políticas de Seguridad de las Operaciones
- Políticas de Control de Acceso
- Políticas de Seguridad para la Infraestructura
- Políticas de seguridad para los Recursos Humanos (R.R.H.H.)

CAPITULO IV

ANÁLISIS DE RESULTADOS

La realización de este proyecto se ejecutó sobre la red en producción de un ISP que funciona actualmente sobre las regiones Norte y Centro del Ecuador, por tanto, se utilizará los equipos y trabajadores de la empresa que formará el objeto de estudio.

4.1. Parámetros de evaluación

Para los ISP existen varias normativas que se deben cumplir a parte de la ley orgánica de telecomunicaciones, entre las cuales se puede identificar diferentes parámetros o requisitos que los prestadores de servicios de Internet están sujetos para el funcionamiento de la empresa de acuerdo con el ente regulatorio ARCOTEL.

Con el establecimiento del CSIRT para el ISP se considera el comunicado de la ARCOTEL a los prestadores de servicios de telecomunicaciones, en el que menciona "***Articulo 85.- obligaciones adicionales*:** *la Agencia de Regulación y control de las telecomunicaciones establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las telecomunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculadas para las y los prestadores de servicios… las obligaciones de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad*…", para lo cual los prestadores deberán ejecutar planes de acción sobre las vulnerabilidades y garantizar el secreto de las telecomunicaciones y de la información transmitida en la red del proveedor de servicios de internet. (0652, 2015a)

Además se considerar la " Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones", en el titulo IX, Seguridad de redes y servicios, se establece en el ***Articulo 36,*** *-que "la*

ARCOTEL, podrá disponer a los prestadores de servicios de telecomunicaciones, la realización, a costo del prestador de una auditoría de seguridad, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de la red y los servicios que se brindan… estas auditorias deben de incluir al menos pruebas de vulnerabilidad y penetración a su propia red".(0652, 2015a)

La auditoría según la circular *Nro. ARCOTEL-DEDA-2018-008-C*, debe cumplir con al menos con las pruebas de vulnerabilidad y penetración a la propia red del ISP, en la que se incluya:

- La evaluación de la aplicación de las políticas de seguridad
- La evaluación de la aplicación de procesos y procedimientos de seguridad

Tabla 22

Parámetros de evaluación según las normativas de ARCOTEL

Normativas	Descripción	Parámetros destacados
RESOLUCIÓN No. 216-09-CONATEL-2009		Disponibilidad de servicio mínimo del 98%
RESOLUCÓN-2018-0652	Norma técnica para coordinar la gestión de incidentes y vulnerabilidad que afecten la seguridad de las redes y servicios de telecomunicaciones	Seguridad de redes y servicios, identificación de activos, identificación y detección de incidentes de seguridad, posible generación de riesgos y vulnerabilidades, comunicación hacia el ente regulatorio
NTE INEN-ISO/IEC 27001	Tecnologías de la información - técnicas de seguridad - sistemas	Norma nacional que se ha preparado para

	de gestión de seguridad de la información - requisitos (ISO/IEC 27001:2013+Cor.1:2014+ Cor. 2:2015, IDT)	proporcionar los requisitos para establecer, implementar y mantener el mejoramiento continuo en un sistema de gestión de seguridad de la información.
TLP (Traffic Light Protocol o Protocolo de Semáforos)	Guía de uso del protocolo TLP	Clasificación de la información según la criticidad para el negocio

Nota: Lista de algunas normativas y guías reconocidas por el ente de regulación nacional ARCOTEL

En la **tabla 22** se indica las normativas, guías y protocolos que se analizaron en cuanto a la legislación nacional, además de incluir la guía metodológica NIST 802 como procedimiento para el establecimiento de un CSIRT, con la finalidad de cumplir las obligaciones de los ISP con el organismo nacional de control ARCOTEL.

4.2. Establecimiento de CSIRT

Al no existir un cálculo exacto de la cantidad de trabajadores que se necesitan para la formación de un CSIRT, ya que cada empresa tiene diferentes ambientes y objetivos que cubrir, sin embargo, partiendo de la información brindada por diferentes estudios (Gil-Osle, 2019), para un ISP que debe tener una gran disponibilidad del servicio de Internet diariamente se puede decir que un CSIRT debe cumplir con lo que se muerta en la **tabla 23**.

Tabla 23

Establecimiento de CSIRT en un ISP

Misión	Contar con un plan estratégico en el que se pueda establecer una guía para la prevención, reducción, mitigación y solución de los diferentes daños que se pueden presentar lógica y físicamente en el transporte, disponibilidad de la información y servicios que brinda la empresa		
Autoridad	Se limita al análisis, mitigación y solución de incidentes en el área técnica donde se involucre la seguridad e integridad de la información		
Servicios	Alertas y advertencias	Tratamiento y manejo de incidentes	Tratamiento y manejo de vulnerabilidades
Modelo de funcionamiento	Reactivo: reacción en consecuencia a un incidente o requerimiento	Proactivo: Brindar información con la finalidad de prevenir y reducir incidentes	
Tipo: Interno	Proporciona los servicios de manejo a incidentes para el ISP		
Integrantes del CSIRT	Encargado de la seguridad	Personal de monitoreo	Personal técnico

Nota: Detalles para el establecimiento de un CSIRT en un ISP

Los integrantes del CSIRT deben tener diferentes actitudes y conocimientos, en los cuales se pueden destacar la capacidad de análisis, habilidades organizacionales, liderazgo, gran conocimiento de tecnología de Internet y protocolos, conocimientos en el manejo de sistemas operativos y diferentes equipos de los que se maneja en el ISP, conocimientos de aplicaciones de Internet y amenazas de seguridad, además de disponibilidad de trabajos prolongados y en diferentes horarios. (Gil-Osle, 2019). A continuación una breve descripción de estos integrantes:

El **Encargado de seguridad** de acuerdo al ***Artículo 21*** literal 3 de la *resolución ARCOTEL 2018-0652* detalla que es *"el responsable de receptar, analizar, gestionar y dar seguimiento al trámite de las vulnerabilidades e incidentes de seguridad de la información que le sean notificadas…"*(0652, 2015b).

Figura. 9

Encargado de la seguridad

El **Personal de monitoreo** es el que tiene que estar en constante revisión de los puntos críticos donde se pude dar la interrupción del servicio de Internet de forma puntual o general, como se puede observar en la **figura 10** siempre deben de estar alerta, además de crear los reportes o tickets para la gestión de los eventos que se presenten. (Lanfranco, 2017)

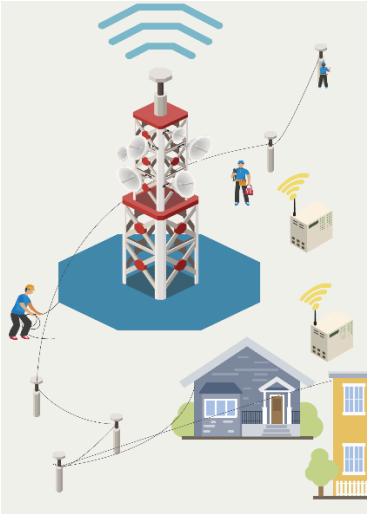
Figura. 10

Personal de monitoreo

El **Personal técnico** que pertenece al CSIRT como se muestra en la **figura 11** es el que asiste a la solución de los incidentes que reporta el área de monitoreo, el equipo de trabajo tiene como objetivo mitigar y solucionar el problema, recoger información con la finalidad de prevenir o minimizar el impacto de un nuevo incidente de la misma procedencia. (Cichonski et al., 2012)

Figura. 11

Personal técnico



4.3. Recopilación de resultados

Entre las obligaciones de los prestadores de servicios de Internet esta realizar una auditoría de las vulnerabilidades (ver Anexo II) que se presenta en el ISP, como resalta en el artículo 36 de la resolución ARCOTEL 2018-0652, en los cuales se debe evaluar el cumplimiento de las políticas de seguridad y aplicación de procesos y procedimientos de seguridad. (0652, 2015b)

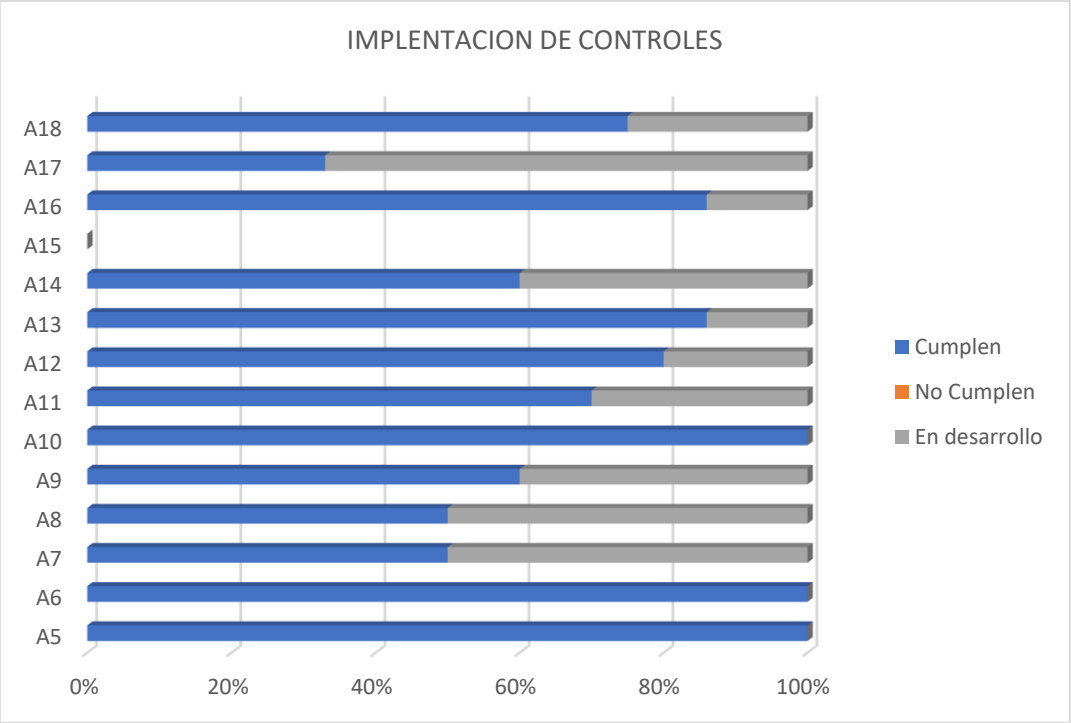
La auditoría inicia con la petición de la documentación de las políticas de seguridad y de todos los procesos que están vigentes en el ISP, con esto se constata si se está realizando

las acciones que garanticen la disponibilidad, integridad y seguridad de la información. (0652, 2015b)

Mediante la implementación de los controles de la normativa ISO/IEC 27001 ya seleccionados Y DESCRITOS previamente, se cumple con la implementación de políticas de seguridad, procesos y procedimientos de seguridad de la información, en la figura 11 se puede observar el cumplimiento y estado de cada uno.

Figura. 12

Estado de controles implementados y en desarrollo



Basados en las figuras 3 (pág. 40) y figura 12 se puede observar que después de realizar la implementación de las políticas de seguridad y los diferentes procedimientos para que estas se cumplan, se tiene un panorama más claro hacia la evaluación que realiza el auditor.

4.3.1. Evaluación de la aplicación de las políticas de seguridad

La evaluación de las políticas de seguridad las realiza un auditor externo a la empresa, ya que es un requisito por parte de la ARCOTEL que se realice una auditoría a la seguridad de la información como se menciona la circular Nro. ARCOTEL-DEDA-2018-008-C.

Realizar auditorías periódicas permiten conocer que los procesos establecidos se cumplan por parte del personal que labora dentro de la empresa. El procedimiento que se debe analizar dentro del ámbito en la auditoría es de políticas de seguridad, el cual fue solicitado por parte del ente regulador (ARCOTEL).

El mecanismo mediante el cual se realiza el análisis es a través de una lista de verificación y entrevistas al personal responsable, todo esto con el objetivo de evaluar los procedimientos establecidos; y por ende que el ISP cumpla con la normativa vigente a la fecha del proyecto, además brinde los resultados solicitados, tomando en cuenta los rangos de la **tabla 24**.

Tabla 24

Rango de Evaluación de políticas de seguridad por el auditor

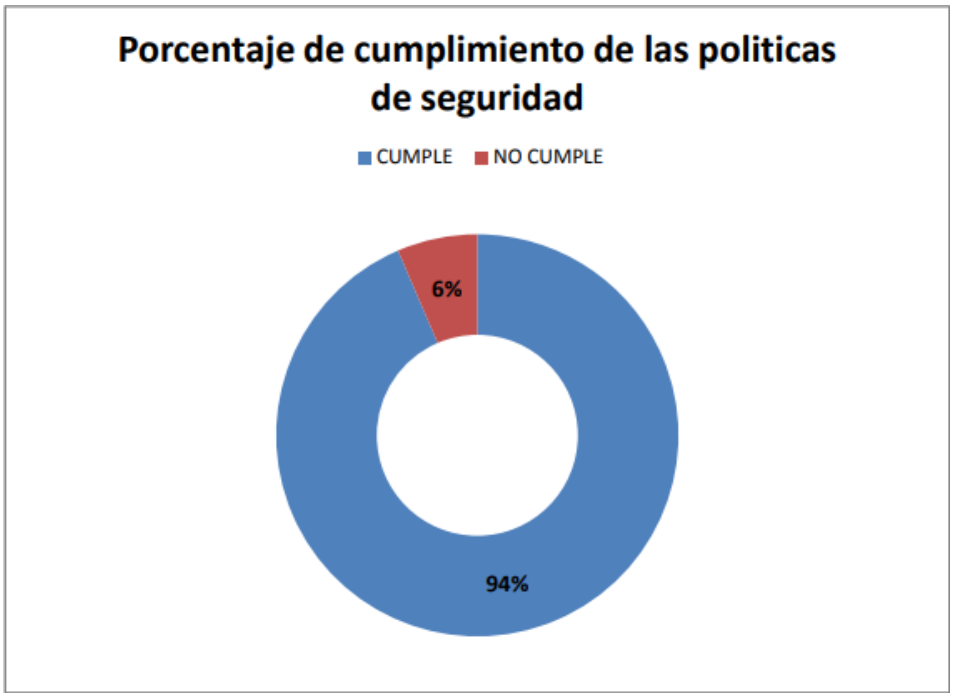
Cumplimiento	Rango
Satisfactorio	> 80%
Aceptable	> 60% < 80%
No Cumple	< 60%

Nota: Se indica el rango de cumplimiento de las políticas de seguridad por parte de la empresa que realiza la auditoría al ISP.

En la **figura 13**, se puede observar el resultado de la evaluación de las políticas de seguridad basados en la lista de procesos y procedimientos de seguridad que el auditor[13] evalúa como se indica en el Anexo II, con la finalidad de realizar el informe ejecutivo.[14]

Figura. 13

Porcentaje de cumplimiento de las políticas de seguridad en la evaluación del auditor



La evaluación registra que "La entidad tuvo una calificación de 94% de cumplimientos durante la auditoría y teniéndose el rango antes indicado la entidad recibe una calificación cualitativa de Satisfactorio."

[13] Es el profesional que brinda el servicio de una revisión detallada de la infraestructura de seguridad de una organización, teniendo en cuenta los requerimientos o estándares de los entes de regulación. (Gil-Osle, 2019)
[14] El informe ejecutivo es un documento que exige la ARCOTEL con la finalidad de conocer el estado actual del ISP en cuanto a la seguridad de la información y la gestión de incidencias.

4.3.2. Resultados de pruebas de vulnerabilidad por software

Teniendo en cuenta los procesos y procedimientos de seguridad establecidos se debe realizar los controles correspondientes, teniendo en cuanta las políticas de acceso y de infraestructura de red (Ver Cap. 3; literales 3.3.9.3. y 3.3.9.4).

El objetivo de las pruebas de vulnerabilidad y pruebas de penetración, solicitadas en el Artículo 36 de la resolución ARCOTEL 2018-0652, es evaluar la seguridad de los activos de la red, para los cuales se realiza ataques autorizados por el ISP a los elementos de la red.

El análisis de vulnerabilidades permite detectar cuales son las deficiencias que presenta la red en la seguridad de los activos que se involucran en la seguridad de la información, utilizando herramientas que permiten realizar el análisis correspondiente, se puede encontrar 3 tipos de pruebas que son:

- **Black box:** No se tiene mucha información de los activos a auditar
- **Gray box:** Se obtiene información parcial de los activos a auditar
- **White box:** Se tiene pleno conocimiento de la información esencial de los activos a auditar.

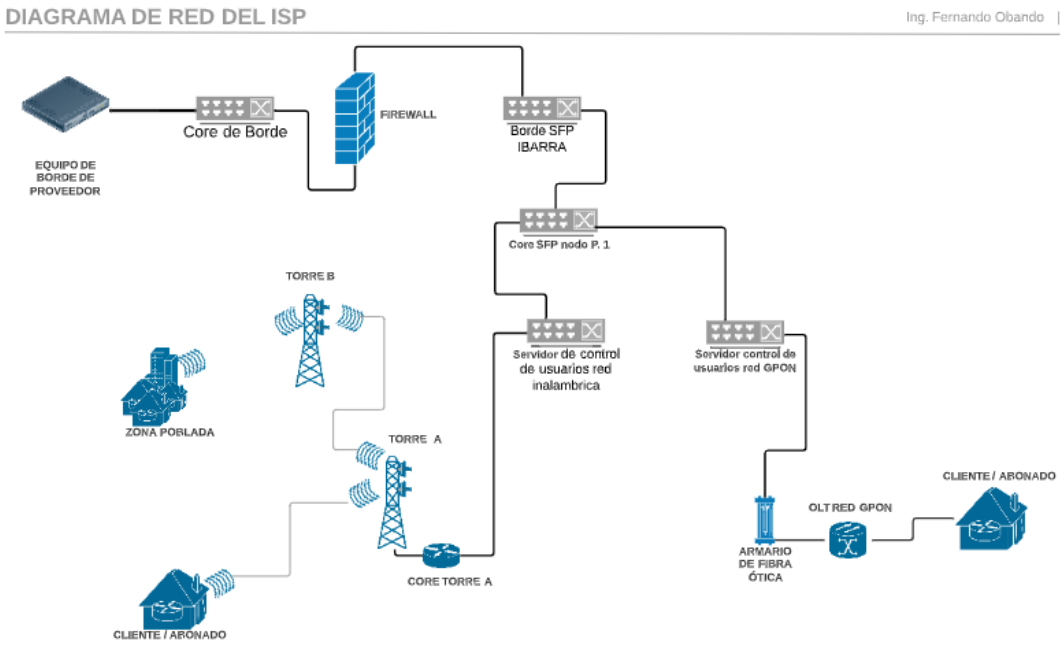
En este proyecto se utiliza el tipo de pruebas de vulnerabilidad “Gray Box”, ya que se entrega información parcial de los activos y elementos de red, que se deben de auditar.

4.3.3. Resultados de vulnerabilidades internas y externas

Con la finalidad de entender los resultados se plantea en la **figura 14** se plantea la topología de red física, donde se puede observar un planteamiento general de la infraestructura de red dentro de un ISP.

Figura. 14

Topología de red física del ISP



Teniendo en cuenta los procesos operacionales y las políticas de seguridad de la información se debe también realizar las respectivas reglas en los equipos de borde o firewall del ISP, en las cuales se pueden destacar:

- Control de acceso
- Control de usuarios de red
- Marcas de tiempo TCP
- Certificados SSL/TLS
- Software/firmware actualizados
- Bloqueo de contenidos
- Bloqueo de puertos

En la **figura 15** se muestran los porcentajes de las **vulnerabilidades externas**[15] encontradas según la severidad[16].

Figura. 15

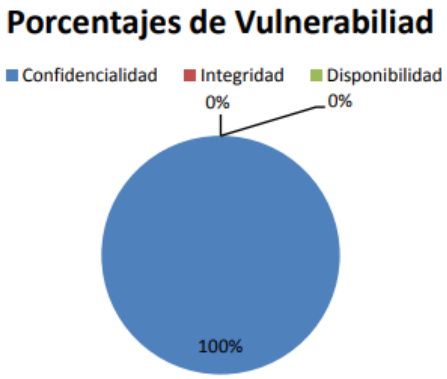
Porcentaje de Vulnerabilidades externas según la severidad

Como se puede observar en la anterior figura el porcentaje de las **vulnerabilidades externas** encontradas es bajo, y de acuerdo a la auditoría realizada se centran como vulnerabilidades que afectan la confidencialidad de la información, como se indica en la **figura 16**.

[15] Se consideran vulnerabilidades externas aquellas que puedan comprometer la disponibilidad, integridad y confidencialidad de la información desde afuera de la red del ISP. (Ortiz-Lazo & Vizñay-Duran, 2019)
[16] La severidad es un parámetro que se utiliza para la clasificación de la gravedad de un incidente con respecto a la afectación de la información (Gil-Osle, 2019)

Figura. 16

Porcentaje de vulnerabilidad externas de la confidencialidad, integridad y disponibilidad de la información

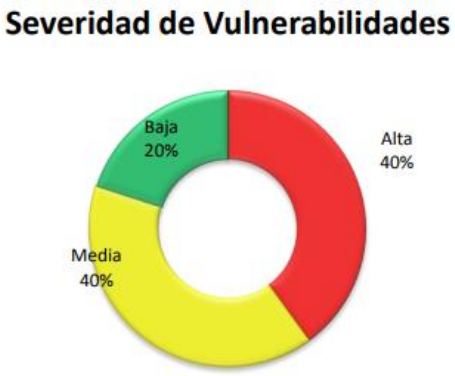


De acuerdo a los resultados esto se da por tener activas las marcas de tiempo TCP (TCP timestamps), además del puerto 81 habilitado para visualizar las gráficas de consumo y el puerto 2000 para realizar test de velocidad desde equipos MikroTik[17].

La **figura 17** muestra los resultados de las **vulnerabilidades internas**[18] encontradas según la severidad.

Figura. 17

Porcentaje de Vulnerabilidades internas según la severidad



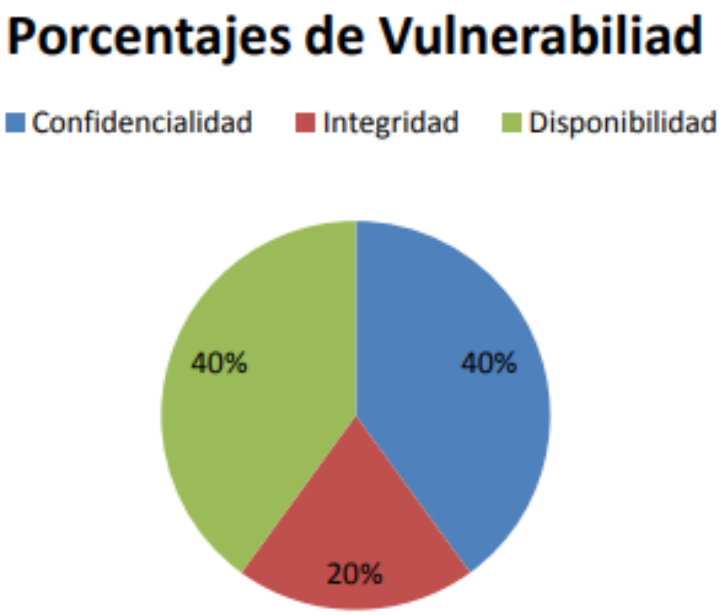
[17] MikroTik es una empresa letona que desarrolla enrutadores y sistemas ISP inalámbricos. MikroTik proporciona hardware y software (RouterOS) para la conectividad a Internet está presente en varios países del mundo. Recuperado de: https://mikrotik.com/aboutus

[18] Se consideran vulnerabilidades internas aquellas que puedan comprometer la disponibilidad, integridad y confidencialidad de la información hacia o desde la red local del ISP (Ortiz-Lazo & Vizñay-Duran, 2019)

Se puede evidenciar que hay diferentes resultados en los porcentajes de las **vulnerabilidades internas** encontradas, estos pueden afectar a la confidencialidad, integridad y disponibilidad de la información en la empresa, como se observa en la **figura 18.**

Figura. 18

Porcentaje de vulnerabilidad internas de la confidencialidad, integridad y disponibilidad de la información



Nota: Se indica los porcentajes de las vulnerabilidades internas encontradas en el proceso de auditoría realizado al ISP.

En los resultados de la auditoría (ver Anexo 3), se puede evidenciar por qué se obtiene dichos porcentajes, con lo que se obtiene la siguiente tabla:

Tabla 25

Vulnerabilidades internas encontradas clasificadas CVSS[19]

IMPACTO	VULNERABILIDAD	ACTIVO	SEVERIDAD (CVSS)
Disponibilidad	HTTP negative Content-Length buffer over flow	Core de borde	CVSS: 10.0
Disponibilidad	HTTP User-Agent overflow		CVSS: 7.5
Confidencialidad	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		CVSS: 5.0
Integridad	SSL/TLS: Certificate Expired		CVSS: 5.0
Confidencialidad	TCP timestamps		CVSS: 2.6

Nota: Se puede observar el resultado de las vulnerabilidades internas correspondientes al impacto y la severidad encontradas en la auditoría realizada al ISP.

Si bien el porcentaje de disponibilidad (40%) y de confidencialidad (40%) son considerables, se deben a servicios que no se están utilizando, pero están activos y sin una gestión adecuada, además de tener las marcas de tiempo TCP habilitadas (TCP timestamps), para lo cual es necesario realizar un plan de acción y mitigar dichas vulnerabilidades.

IMPORTANTE

Para la realización y soporte del presente trabajo de investigación se usaron datos obtenidos de los estudios de auditoría realizados por la empresa objeto del estudio. (Véase Anexo 3); es por este motivo que todos los datos usados y utilizados son reales, mismos que aportan al literal 4.3. Recopilación de resultados.

[19] CVSS es un sistema que permite estimar el impacto de las vulnerabilidades en las tecnologías de la información, se utiliza para cuantificar la severidad de las vulnerabilidades y es un estándar abierto recuperado de https://www.first.org/cvss/

CONCLUSIONES

Este trabajo aporta al área de telecomunicaciones como una guía orientada hacia los Proveedores de Servicios de Internet – ISP, mismos que están regulados bajo un ente nacional como es la ARCOTEL; debido a que el presente trabajo está basado en la norma ISO/IEC 27001 y la NIST-800 R2, todo esto con la finalidad de cumplir la Resolución ARCOTEL-0652 y los diferentes protocolos que exige el ente de regulación en consideración a mantener el secreto de la información.

El establecimiento de un CSIRT para empresas que prestan servicios de alta disponibilidad como es el acceso a Internet, ayuda a minimizar las distintas amenazas y riesgos, debido a que existen diferentes eventos que comprometen la seguridad, disponibilidad e integridad de la información, por tal razón se hace necesario contar con personal adecuado para minimizar el impacto en las diferentes áreas que se maneja en un ISP, donde no solo se pueden presentar incidencias lógicas sino también físicas que puedan comprometer la continuidad del negocio.

Si bien existen diferentes guías y documentos que indican como establecer un CSIRT, en ninguno de los casos están orientados específicamente a satisfacer las exigencias de las normativas y resoluciones que el ente de regulación ARCOTEL establece para las empresas de telecomunicaciones; concretamente con los proveedores de servicios de Internet. Por tanto, este trabajo mediante el uso de guías como la NTE INEN-ISO/IEC 27001 y NIST Computer Security Incident Handling Guide Special Publication 800-61 Revisión 2, ayuda a los ISP a cumplir con lo publicado en la resolución ARCOTEL 2018-0652, establecida para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones.

El establecimiento de políticas de seguridad y procesos para salvaguardar el sigilo de la información sensible, permiten gestionar de mejor manera los recursos que puede ser críticos para la continuidad del negocio, con lo cual es necesario que todos los procesos y

procedimientos estén documentados y aprobados, tanto por las autoridades del ISP como también deben ser avalados por una auditoria.

El manejo de un software adecuado para el monitoreo de incidentes es de gran importancia, ya que forma parte esencial de las herramientas de trabajo para el CSIRT, la capacidad de generar eventos estadísticos ayuda a tener un mejor control sobre los incidentes que se han suscitado en un determinado tiempo, con lo cual se podrá mitigar de mejor manera los riesgos de ausencia de servicio del negocio y minimizar los tiempos de discontinuidad de la disponibilidad de la información de la empresa.

La selección adecuada del personal que conforma el CSIRT ayuda a tener un equipo eficiente, debido a que pueden identificar de manera rápida y directa de daños específicos, generando mejores tiempos de respuesta hacia los incidentes generados en un determinado sector.

La finalidad de la auditoría no es solo para saber cuáles son las vulnerabilidades que presenta el ISP en cuanto a las políticas de seguridad de la información y buenas prácticas, sino también ayuda a la revisión de los procedimientos de detección y tratamiento de incidentes, de tal manera se puede generar un plan de acción para realizar las mejoras que beneficien a la disponibilidad de los servicios prestados por la empresa.

RECOMENDACIONES

Si bien la ISO/IEC 27001 no es un estándar que se debe cumplir tal cual como está el texto, se debe considerar y analizar cada uno de los puntos que se menciona en la normativa ya que son documentos que tienen una investigación previa y comprobada, así como la metodología propuesta por NIST-800 R2, con la finalidad de realizar una guía con procesos ya avalados por los diferentes organismos de regulación de las telecomunicaciones o afines.

La conformación de un CSIRT para un ISP debe tomar en cuenta el dimensionamiento de la empresa y los recursos con los que cuenta, de esta manera se podrá determinar el alcance del equipo de respuesta a incidentes y la delegación de responsabilidades.

Es ideal que después de la una auditoría de procesos y del estado de los activos involucrados en la confidencialidad, integridad y disponibilidad de la información se realice un plan de acción en el que se indique los tiempos, actividades y asignación de responsabilidad de los miembros del CSIRT encargados de la solución a las falencias encontradas por el auditor.

En Ecuador existen algunos CSIRT ya conformados, para los Proveedores de Servicios de Internet y empresas de telecomunicaciones que están reguladas por la ARCOTEL es EcuCERT, se recomienda estar afiliado o en contacto con esta dependencia del ente regulador, ya que según la Resolución ARCOTEL 2018-0652 se debe de brindar los reportes de las incidencias que comprometan el secreto de la información, según los formatos y tiempos establecidos por dicho organismo.

BIBLIOGRAFÍA

0652, Resoluc. A.-2018-. (2015a). RESOLUCiÓN ARCOTEL-2018- 0652. *Dk*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

0652, Resoluc. A.-2018-. (2015b). RESOLUCiÓN ARCOTEL-2018- 0652. *Dk*, *53*(9), 1689–1699. https://www.gob.ec/regulaciones/arcotel-2018-0652-norma-tecnica-coordinar-gestion-incidentes-vulnerabilidad-afecten-seguridad-redes-servicios-telecomunicaciones

27001:2013, I. (2015). *ECUATORIANA NTE INEN-ISO / IEC 27001*. 1–5.

AEPROVI. (2020). *No Title*. https://www.aeprovi.org.ec/es/

Agencia de regulación y Control de las Telecomunicaciones. (n.d.). *RESOLUCION 0584.pdf*.

ARCOTEL. (2002). *RESOLUCiÓN No. 282-11-CONATEL-2002*. *282*, 2002.

ARCOTEL. (2019). *Libre difusión. Sujeto a las normas de protección intelectual, puede distribuirse sin restricciones.* 2–4. https://www.arcotel.gob.ec/wp-content/uploads/2018/11/Guia-de-uso-del-protocolo-TLP.pdf

Asamblea Nacional. (2015). Ley Orgánica De Telecomunicaciones. *Registro Oficial Órgano Del Gobierno Del Ecuador*, *Tercer Sup*, 1–40. http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

C., F. J. (2019). *Plan Director de Seguridad de la Información* [Universitat Oberta de Cataluya]. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/97010/8/fjaracTFM0619presentación.pdf

Cichonski, P. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800–61*, 79. https://doi.org/10.6028/NIST.SP.800-61r2

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-61r2

Csirt, S. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). *ReCIBE. Revista Electrónica de Computación, Informática, Biomédica y Electrónica*, *4*(1), VI.

EcuCERT. (2018). *EcuCERT*. https://www.arcotel.gob.ec/ecucert/

Gil-Osle, J. P. (2019). Tabla De Contenidos. *Amistades Imperfectas*, 7–8. https://doi.org/10.31819/9783954870875-toc

Henares, A. J. S. (2018). *Sistemas de Gestión de la Seguridad de la Información*. Universidad Oberta de Catalunya. http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Análisis+y+gestión+de+riesgos

Lanfranco, E. (2017). *CSIRTs Motivación*.

Medina, F. (2017a). *El ciberataque global impactó en Ecuador. El Comercio, pp. 2–3.* https://www.elcomercio.com/actualidad/ciberataque-wannacryimpacto-ecuador-hackeo.html

Medina, F. (2017b). El ciberataque global impactó en Ecuador. *El Comercio*, *I*, 2–3. https://www.elcomercio.com/actualidad/ciberataque-wannacry-impacto-ecuador-hackeo.html

Mejía, J., Muñoz, M., & Ramírez, H. (2016). *Propuesta de Marco de Trabajo para la Protección de un CSIRT Proposed Framework for the CSIRT Protection*.

Mendoza, M. Á. (2015). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?* https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Ministerio del trabajo. (2017). *Resolucion_0144.Pdf*.

Naseri, A., & Azmoon, O. (2012). Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Iran. *International Journal of Computer Science Issues (IJCSI), Vol 9*(1), 156–160.

Ortiz-Lazo, J. E., & Vizñay-Duran, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo Del Conocimiento*, *4*(7), 174. https://doi.org/10.23857/pc.v4i7.1029

Reformada, T., Reformada, E. D. T., & Reformada, T. (2006). *CONSEJO NACIONAL DE TELECOMUNICACIONES CONATEL CONSIDERANDO: Que el articulo 313 de la*.

Salamanca, Y. A. (2019). Falla informática en Ecuador: los datos de casi toda la población quedaron expuestos. *France 24*, 2. https://www.france24.com/es/20190917-ecuador-datos-expuestos-informacion-filtracion

Telecomunicaciones, A. de regulación y C. de las. (n.d.). *RESOLUCION 0807*.

Valladares, P., Fuertes, W., Tapia, F., Toulkeridis, T., & Perez, E. (2017). *Dimensional data model for early alerts of malicious activities in a CSIRT*. *63*, 1–8. https://doi.org/10.23919/spects.2017.8046771

ANEXO I – ELECCIÓN DE SOFTWAR DE ADMINISTRACIÓN DE MONITOREO

La finalidad de tener un software para monitorear la red es supervisar los componentes de la misma, como enrutadores, firewall, Olts, así como también los dispositivos finales de entrega de servicio a abonados/cliente.

En la actualidad existe diferente software de monitoreo de red, que brindan diferentes herramientas para el aviso o alerta de eventos e incidencias que se presenten, el proceso se desarrolla en los siguientes pasos

1. Ping – herramienta básica que se usa para probar la conectividad de los dispositivos de la red
2. SNMP (Simple Network Management Protocol) – es un protocolo de administración de red utilizado por los programas o sistemas de monitoreo.
3. Scrips – se utilizan para optimizar las funciones de las herramientas de monitoreo

El propósito de un monitoreo en el CSIRT no es solo de recibir alertas o notificaciones de un evento puntual o general, sino también de brindar información sobre los incidentes que se presentan a lo largo del tiempo y determinar cuáles son los de más ocurrencia para así tratar de mitigarlos.

De tal manera el software que se escoja para realizar las tareas de monitoreo debe considerar lo antes ya mencionado, el programa o sistema debe ser capaz de brindar las alertas oportunas para la identificación de alertas, pero también sería bueno considerar la generación de graficas o información que permita realizar el análisis correspondiente a los eventos presentados en un determinado tiempo.

Entre los diferentes Software de monitoreo se ha considerado, que tengan versiones gratuitas y que brinden la oportunidad de generar graficas que permitan el análisis de eventos y no solo generen logs de información, entre los que se destaca:

- Nagios
- Pandora FMS
- PRTG
- The DUDE (software que usa el caso de estudio)

Requisitos	Nagios	Pandora FMS	PRTG	The DUDE
Disco de almacenamiento	20 GB	10GB	250GB	1GB
Memoria RAM	2GB	1GB	3GB	1GB
Sistema Operativo	Centos/RedHat 6 o 7	Centos/RedHat 7 o 8	Windows server 12/16 o Windows 10	Windows 7/8/10
CPU	Dual Core, 2.4GHz	1 núcleo 2GHz	3GHz	Dual Core 2.7GHz
Base de datos	MySQL/MariaDB	MySQL estándar/ Percona XTraDB	N/A	N/A

Debido a las limitaciones de los recursos asignados para el equipo de monitoreo por parte de la empresa se tiene lo siguiente:

- 20GB almacenamiento de disco
- 1GB de memoria RAM
- CPU xenón 2.7 Ghz 4 núcleos
- Virtualización sobre proxmox

Por tanto, después de analizar los requisitos de instalación las opciones de elección son The Dude y Pandora FMS, por lo cual se decide usar la segunda Opción ya que presenta entre las herramientas un sistema de estadísticas de eventos por medio de gráficas, en lo cual

The dude no tiene dicha prestación y para el este trabajo es necesario contar con este tipo de resultados.

Toda la información para este anexo 1 fue tomada de los sitios web de propietario de los sistemas o software de monitoreo.

ANEXO II - LISTA DE VERIFICACION DE APLICACIÓN DE POLITICAS DE SEGURIDAD

La lista que se indica a continuación es proporcionada y verificada por el auditor que realiza el proceso de análisis de las políticas de seguridad del ISP.

LISTA DE VERIFICACION DE APLICACIÓN DE POLITICAS DE SEGURIDAD				
		CUMPLE	**NO CUMPLE**	**OBSERVACION**
EV.1	¿Existe personal responsable de la confidencialidad de los datos personales de los clientes?	X		El área de sistemas se encarga de la información de los clientes
EV.2	¿Existen procedimientos que aseguren la confidencialidad de los datos personales de los clientes?	X		Existe un procedimiento para la no revelación de datos de clientes
EV.3	¿Existen registros del direccionamiento IPv4/IPv6 tanto público como privado con detalle de asignación de clientes?	X		Si, cada IP asignada a los clientes se encuentra registrada y almacenada en el sistema integrado del ISP
EV.4	¿Los registros de direccionamiento IPv4/IPv6 se encuentran disponibles?	X		Si, la información se puede revisar mediante los usuarios asignados del sistema integrado
EV.5	¿Los registros de direccionamiento IPv4/IPv6 se encuentran seguros de acuerdo a las políticas de seguridad de la entidad?	X		Los registros del direccionamiento IP se encuentra en el sistema integrado del ISP
EV.6	¿El personal que labora para la entidad posee acuerdos de confidencialidad firmados?	X		En cada contrato de los trabajadores del ISP se encuentra un acuerdo de confidencialidad

EV.7	¿El formato de acuerdo de confidencialidad de la entidad se encuentra estableció de acuerdo al modelo indicado en el anexo 2 de Resolución Arcotel-2018-0652	X		Los contratos firmados por los trabajadores siguen el modelo propuesto por la ARCOTEL
EV.8	¿Los acuerdos de confidencialidad firmados se encuentran almacenados y/o asegurados de acuerdo a las políticas de seguridad de la entidad?	X		Los acuerdos firmados se encuentran almacenados en el área jurídica de la empresa
EV.9	¿Se tienen establecidos procedimientos para el bloqueo de servicios o contenido solicitados por los abonados de la entidad?		X	No hay un proceso establecido
EV.10	¿La información digital confidencial y sensible se encuentra debidamente cifrada?	X		La información solo se encuentra almacenada en los servidores
EV.11	¿La información digital confidencial y sensible se encuentra debidamente almacenada?	X		Se encuentra en el Cuarto de equipos de la Matriz de la empresa
EV.12	¿Se tiene control de acceso para la información confidencial y/o sensible dentro de la entidad?	X		El acceso a la información está restringido el acceso en las instalaciones y en sistema integrado
EV.13	¿La información digital confidencial y sensible se encuentra almacenada en dispositivos personales tales como pendrives, discos duros externos y/o CD's?	X		La información se encuentra almacenada en Servidores, Principal y dos de Backup
EV.14	¿Existe información digital confidencial y sensible almacenada en la "Nube"?	X		Si, solo direccionamiento de infraestructura de red
EV.15	¿El responsable de la seguridad posee una llave publica?	X		

EV.16	¿La información física confidencial y sensible se encuentra debidamente almacenada de acuerdo a las políticas de seguridad de la entidad?	X		Si, el acceso a la información física es solo para el personal autorizado
EV.17	¿Se tiene algún tipo de mecanismo para la gestión de la red de forma remota?	X		Se posee acceso a equipos por IPs públicas y enlaces desde puntos con personal autorizado
EV.18	¿El acceso remoto es de uso exclusivo del personal interno de la entidad?	X		Si, solo personal interno y autorizado puede acceder remotamente a la red
EV.19	¿Se tiene acceso remoto de la red para personal tercero o ajeno a la entidad tales como proveedores?	X		Únicamente personal de la entidad tiene acceso a la red del ISP
EV.20	¿Se tiene procedimientos para la asignación de recursos para acceso remoto a personal tanto interno como externo a la entidad?		X	No existe ningún procedimiento para la asignación de recursos de acceso remoto
EV.21	¿Se tiene sistemas de control de acceso?	X		No, solo en el nodo principal y para el control del ingreso de los trabajadores por medio de registro biométrico
EV.22	¿Se tiene sistemas de control y vigilancia?	X		Se cuenta con sistema de vigilancia con cámaras IP tiempo real, pero NO existe un servidor para tener un registro de eventos (grabaciones)
EV.23	¿Se tiene sistemas de monitoreo de red?	X		Si, se utiliza THE DUDE, para el monitoreo de los equipos de red
EV.24	¿Se tiene sistemas de aprovisionamiento de servicios?	X		Proveedor de servicio Centurylink
EV.25	¿Se tienen procedimientos para asegurar que el software o sistemas para la ejecución del negocio sean seguros?	X		Se adjunta procedimiento del software que se utiliza para que la ejecución del negocio sea segura

EV.26	¿Se tiene procedimientos para la gestión de incidentes?	X		Si, existen procedimientos para la gestión de incidentes debidamente documentados
EV.27	¿Se tiene repuestos de hardware de los elementos de la RED	X		Si, existen los repuestos de igual o similares características para remplazar los equipos en la Red
EV.28	¿Se tienen sistemas de protección de energía para los nodos?	X		Se cuenta con los dispositivos de redundancia de energía mediante un banco de baterías
EV.29	¿Se tiene una adecuada climatización del sitio donde se encuentran los equipos críticos de la RED?	X		El nodo principal cuenta con aire acondicionado para mantener a una temperatura adecuada los equipos, Se adjunta fotografías
EV.30	¿Se tiene seguridad física de acceso al sitio donde se encuentran los equipos críticos de la RED?	X		El ingreso al nodo se encuentra restringido con puertas y Rejas con llave
EV.31	¿Las condiciones del sitio donde se encuentran los quipos críticos de la red son adecuadas?	X		Existe vías de acceso, la superficie es plana y la edificación está cerrada
		CUMPLE	**NO CUMPLE**	
	TOTAL SCORE	29	2	

ANEXO III – DECLARATORIA DE VERACIDAD

De acuerdo al ***artículo 36*** de la resolución *ARCOTEL 2018-0652*, la norma técnica señala -que *"la ARCOTEL, podrá disponer a los prestadores de servicios de telecomunicaciones, la realización, a costo del prestador de una auditoría de seguridad, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de la red y los servicios que se brindan… estas auditorias deben de incluir al menos pruebas de vulnerabilidad y penetración a su propia red"*

Por lo ya mencionado todos los resultados indicados en el literal 4.3 de este trabajo de grado, son reales y obtenidos del estudio de auditoría realizado por la empresa, mismo que por acuerdos de seguridad y confidencialidad no se pueden mostrar de forma pública, pero a su vez se destaca que son datos necesarios para realizar el estudio actual, de esta manera evitar basarse en supuestos y sea de información real.

Si se desea corroborar, surge alguna inquietud o duda acerca de los resultados planteados puede contactar con el autor del trabajo de investigación por el correo electrónico siguiente: cmobandov2@utn.edu.ec