UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: " Estudio de la seguridad informática en el sector de telefonía móvil en Ecuador para la creación de medidas de protección de la información"

.

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor(a): Ingeniero, Cristian Eduardo Lozada Toasa

Director(a): Ingeniero, Luis Fabián Hurtado Vargas, Mg.

Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera, Elsa Pilar Urrutia Urrutia, Mg., e integrado por los señores Ingeniero, Franklin Oswaldo Mayorga Mayorga, Mg., Ingeniero, Hernán Fabricio Naranjo Ávalos, Mg., designados por la Unidad Académica de Titulación de Posgrado de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "Estudio de la Seguridad Informática en el sector de la Telefonía Móvil en Ecuador para la creación de medidas de protección de la información", elaborado y presentado por el señor Ingeniero Cristian Eduardo Lozada Toasa, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia, Mg.,

Presidente del Tribunal

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.,

Miembro del Tribunal

Ing. Hernán Fabricio Naranjo Ávalos, Mg.

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "Estudio de la Seguridad Informática en el sector de la Telefonía Móvil en Ecuador para la creación de medidas de protección de la información", le corresponde exclusivamente a: Ingeniero, Cristian Eduardo Lozada Toasa, Autor; bajo la dirección de Ingeniero, Luis Fabián Hurtado Vargas, Mg., Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero, Cristian Eduardo Lozada Toasa

C.C.: 2100471628

AUTOR

Ingeniero Luis Fabián Hurtado Vargas, Mg.

C.C.: 0913563326

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción del mismo, dentro de las regulaciones de la Universidad.

Ingeniero, Cristian Eduardo Lozada Toasa

C.C.: 2100471628

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

AGRADECIMIENTO

A mi madre por haber inculcado en mí la importancia del estudio, preparación y esfuerzo para conseguir las metas que uno se propone.

Al director de mi trabajo de investigación, por estar pendiente y presto para ayudarme con las cuestiones de la misma.

DEDICATORIA

Con cariño, este trabajo dedico a mi madre, a mi familia y en general, para todas aquellas personas que me han apoyado y que de una u otra manera han contribuido a formarme y poder cumplir mis metas.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"Estudio de la seguridad informática en el sector de telefonía móvil en ecuador para la creación de medidas de protección de la información"

AUTOR: Ingeniero, Cristian Eduardo Lozada Toasa
DIRECTOR: Ingeniero, Luis Fabián Hurtado Vargas, Mg.
FECHA: 04 de enero de 2019

RESUMEN EJECUTIVO

Con el continuo avance tecnológico, las empresas de telefonía móvil se enfrentan a varios desafíos relacionados con la seguridad y la protección de la información de sus clientes, el éxito de estas empresas depende mucho de la protección de los datos, los cuales deben mostrarse al usuario de forma confiable sin que existan errores o mucho menos problemas en el tratamiento de los mismos, la seguridad de la información es una característica que le hace a una empresa ser más competitiva en comparación a otras que brindan el mismo servicio. Si la información que maneja una empresa se ve afectada, por ende, va afectar a la reputación de la misma.

En la actualidad la información se ve amenazada por múltiples vulnerabilidades y amenazas que ocurren cuando un usuario utiliza el internet de forma inadecuada, provocando que la información proporcionada se utilice con fines ilícitos. Por otro lado, los usuarios exigen que la información esté disponible todo el tiempo, por ende, las empresas están obligadas a cumplir con ello. La información siempre estará disponible para los usuarios, pero no en su totalidad, debido a que cierta información es confidencial, además existen sistemas de protección y defensa de los peligros informáticos como crackers, correos no deseados, virus, entre otros los cuales generan un riesgo en las empresas telefónicas que brindan el servicio de comunicación a los usuarios y administran grandes cantidades de información. En la presente

investigación se propone realizar un estudio sobre el tratamiento de la información que se lleva a cabo en las empresas telefónicas activas del Ecuador con la finalidad de implementar políticas de seguridad que se ajusten a la realidad y a las necesidades, haciendo uso de la norma ISO 27001:2013, la cual establece un estándar para sistemas de seguridad de la información. Además, se plantea implementar un Service Desk para gestionar los incidentes por parte de los usuarios, el cual se apoya en una base de conocimiento bien definida para tratar de dar solución a los mismos, de esta manera las empresas conseguirán éxito en su funcionamiento.

Descriptores: Telefonía móvil, seguridad de la información, políticas de seguridad, vulnerabilidades, antivirus, crakers, correo no deseado, Service Desk, gestión de incidentes, base de conocimiento.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"Study of computer security in the mobile telephone sector in Ecuador for the creation of information protection measures"

AUTHOR: Engineer, Cristian Eduardo Lozada Toasa
DIRECTED BY: Engineer, Luis Fabián Hurtado Vargas, Mg.
DATE: 04 of January 2019

EXECUTIVE SUMMARY

With the continuous technological advance, the mobile phone companies face several challenges related to the security and protection of their clients' information, the success of these companies depends a lot on the protection of the data, which must be shown to the user in a reliable way without errors or much less problems in the treatment of them, the security of information is a feature that makes a company more competitive compared to others that provide the same service. If the information handled by a company is affected, therefore, it will affect the reputation of it.

Currently, information is threatened by multiple vulnerabilities and threats that occur when a user uses the Internet in an inappropriate manner, causing the information provided to be used for illicit purposes. On the other hand, the users demand that the information be available all the time, therefore the companies are obliged to comply with it. The information will always be available to users but not in its entirety, because certain information is confidential, in addition there are systems for protection and defense of computer hazards such as crackers, unwanted emails, viruses, among others which generate a risk in the telephone companies that provide the communication service to users and manage large amounts of information. In the present investigation it is proposed to carry out a study on the treatment of the information that is carried out in the active telephone companies of Ecuador with the purpose of implementing

security policies that adjust to the reality and the needs, making use of the norm ISO 27001: 2013, which establishes a standard for information security systems. In addition, it is proposed to implement a Service Desk to manage incidents by users, which is based on a well-defined knowledge base to try to solve them, in this way companies will succeed in its operation.

Keywords: Mobile telephony, information security, security policies, vulnerabilities, antivirus, crakers, spam, Service Desk, incident management, knowledge base.

INTRODUCCIÓN

El continuo crecimiento de la red telefónica y la disponibilidad del Protocolo de Voz sobre Internet (VoIP) han contribuido tanto a la disponibilidad de artefactos flexibles y fáciles de usar para los usuarios, como a un aumento significativo de la actividad cibernética. Los delincuentes utilizan tecnologías emergentes para realizar actividades ilegales y sospechosas.

En la actualidad, se utilizan las redes telefónicas para abusar y estafar a las víctimas, por lo que es necesario proteger los datos que se almacena en un sistema de información y contar con políticas de seguridad de información bien definidas. Los datos de los usuarios muchas de las veces son usados con fines delictivos, por ejemplo, cuando se desea obtener información secreta, de manera privilegiada y confidencial como una estrategia para la ventaja en la guerra, negocios, en la industrialización de los campos e incluso en las ciudades (Copete, 2018).

La seguridad en los dispositivos según (Arias, 2014) se define como: "La disciplina que se ocupa para diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema seguro y confiable" (p. 25). A partir de este concepto se describen los principales aspectos relacionados con la seguridad: tipos de seguridad, propiedades de un sistema de información.

En la actualidad los dispositivos móviles representan una herramienta ideal de comunicación para las personas, debido a que se ajustan a las necesidades de cada usuario. Los dispositivos tecnológicos poseen una gran capacidad de procesamiento de datos, además de velocidades altas de comunicación. Con estas características el usuario puede transmitir voz y datos a cualquier parte del mundo.

En efecto, estos dispositivos móviles incursionan y están en constante evolución. Estos dispositivos pueden ser simples agendas electrónicas o PDA (Personal Digital Assistants), dispositivos refinados con modelos compactos, casi como computadores personales. Los dispositivos actuales suelen tener una excelente conexión y una amplia variedad de redes, como el Internet, este proporciona un intercambio de infinita

información entre ambos, por lo tanto, se han creado, nuevos canales que conllevan a ataques contra la seguridad de todos sus usuarios (Carrera, 2017).

El método convencional del manejo de datos constaba de documentos físicos, estos eran transportados de un lugar a otro según su destino. La persona que transportaba los documentos era un emisario, los llevaba en cilindros metálicos que solo podían ser abiertos con una clave otorgada por el emisor del mensaje. En el caso de no ser la clave correcta se activaba un mecanismo que liberaba un líquido, dañando el mensaje. A diferencia del método convencional en la actualidad se intercambia información por medios digitales. Por ejemplo, los mensajes de voz viajan por dispositivos electrónicos, como computadoras, tabletas, móviles, entre otros. Estos dispositivos usan switchs, routers, módems mediante un canal de transmisión como el internet, conectados a una antena para la transmisión. Pero al igual que los métodos del manejo de datos han cambiado, así mismo han evolucionado los métodos para violentar la seguridad como las claves y la codificación del mensaje, con la finalidad de conocer el contenido de los datos enviados y divulgar la información o hacer estafas.

El desarrollo de esta investigación pretende obtener información oportuna sobre la seguridad informática aplicada en las operadoras móviles en el Ecuador; teniendo en cuenta que las empresas tienen políticas de telecomunicaciones implementadas para prestar óptimos servicios de comunicación a los usuarios. Además, en este estudio se define un modelo conceptual para el uso de componentes, medidas de protección de la información que sirva como una fuente de consulta para cualquier organización o persona que desee implementar como parte de un proceso de seguridad informática en el sector de telefonía móvil en Ecuador.

CAPÍTULO 1. EL PROBLEMA

1.1 Tema

"Estudio de la seguridad informática en el sector de telefonía móvil en el Ecuador para la creación de medidas de protección de la información".

1.2 Planteamiento del Problema

1.2.1 Contextualización

La gestión de la seguridad de la información en todas las organizaciones pertenecientes al sector de las telecomunicaciones es un ámbito de alta importancia que surge a partir de la necesidad de crear métodos y procedimientos que aseguren la protección de la información. En el sector de telecomunicaciones, específicamente, el sector móvil está estrechamente vinculado con la existencia de factores de riesgo, que en dependencia del tipo de actividad y de las condiciones de trabajo, presentan una mayor o menor probabilidad que se origine un hecho peligroso que repercuta en un perjuicio a la integridad de los seres humanos.

Para encontrar los problemas existentes dentro de una entidad se realizan diferentes pruebas, las cuales están diseñadas específicamente para probar que las vulnerabilidades existen, son reales y peligrosas, por lo cual un diseño de procesos correctivos es imperativo. (Sánchez, 2017).

La vulnerabilidad humana, ya sea por ignorancia o por negligencia, los delincuentes cibernéticos con técnicas sencillas pueden engañar a las víctimas, con la sustracción de credenciales de acceso o habilitación de permisos.

Actualmente, las amenazas a la seguridad en internet representan un problema global, cada día éstas se incrementan a la par de los avances de las nuevas tecnologías, causando pérdidas económicas y al no contar con huellas tecnológicas para analizar los delitos informáticos, para los expertos informáticos, se vuelve muy difícil de

detectar desde donde se produjo el ataque o quien es el responsable del daño.

El 13 de mayo del año 2017 se registró el mayor ciberataque en 99 países, según el reporte de la Consultora Informática Avast, que rastreó 75.000 ataques de ransomware, un virus maligno y extorsivo. En Ecuador, cuatro compañías (tres empresas privadas, en áreas de comunicación, salud y una área no especificada y en una empresa pública) fueron afectadas en su información (Boscán, 2017). Este suceso denota la debilidad en cuestiones de seguridad informática en la mayoría de las empresas en el Ecuador, organizaciones grandes o pequeñas han tomado pocas precauciones hacia el tema de seguridad de la información, poniendo en riesgo la información y a su vez el prestigio de alguna institución.

Según el estudio realizado por la Policía Nacional, Interpol y el centro de respuesta a Incidentes Informáticos de Ecuador, con el soporte de entidades afines de América Latina, indica que el 85% de los ataques a los programas informáticos son causados por errores de los usuarios; el 58% de personas deja sus teléfonos móviles que contienen información sensible en sus vehículos o lugares de trabajo; el 60% utiliza la misma contraseña en dispositivos de trabajo y de uso diario; el 35% ha ingresado a los correos recibidos por curiosidad por falta de conocimiento del tema; el 59% almacena sus datos de trabajo en la nube; y el 80% de intimidaciones en las redes sociales" (Telégrafo, 2016).

En Ecuador, los ataques o delitos informáticos también suceden dentro del campo de la telefonía móvil. Ante este reto, es necesario fortalecer la seguridad en las empresas con políticas y estrategias de seguridad destinadas a garantizar que toda implantación de nueva tecnología vaya acompañada de un adecuado entrenamiento y capacitación profesional y de un procedimiento de evaluación de los riesgos de seguridad para detectar vulnerabilidades y posibles amenazas de ataques.

1.2.2 Análisis Crítico

1.2.2.1 Árbol de Problemas

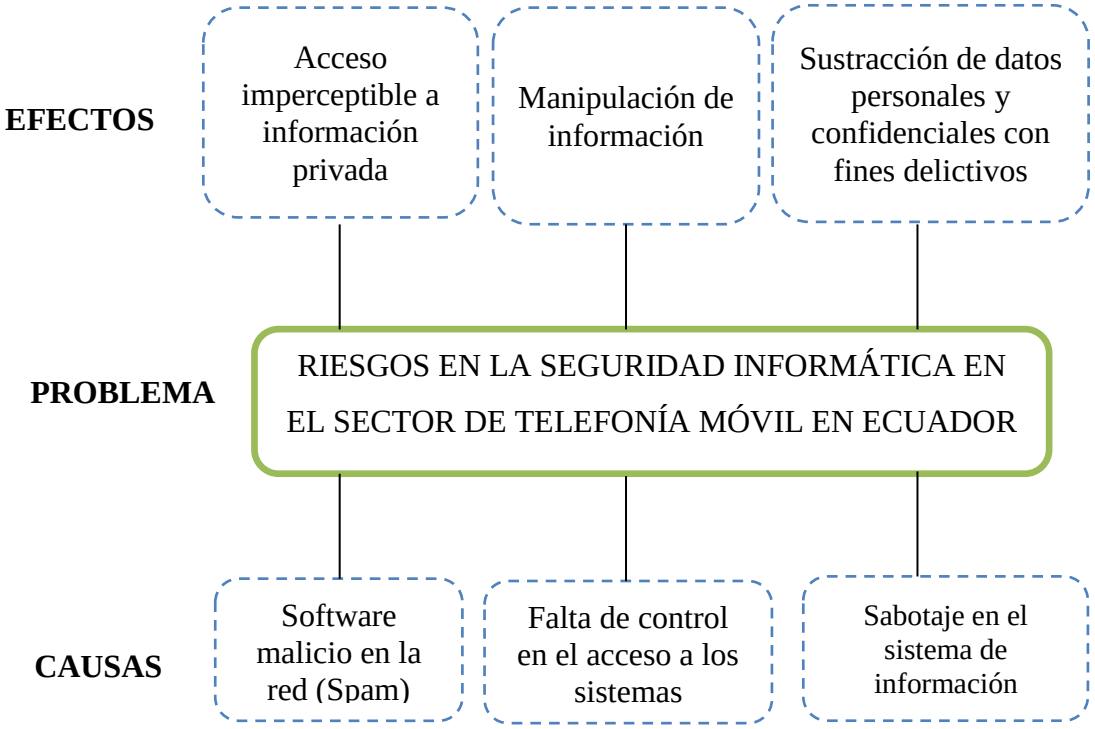

Gráfico 1. Árbol de problemas

Elaborado por: Lozada (2018)

Actualmente, son más y mejores las posibilidades que poseen los seres humanos para comunicarse e interconectarse a través de redes, internet o mediante un dispositivo móvil. Nuevos espacios se han configurado para que empresas y organizaciones, disputen los más sofisticados equipos tecnológicos, ágiles y óptimos sistemas para mejorar el rendimiento y almacenamiento, sin embargo, a la par han surgido amenazas para estos sistemas de información. Por ejemplo, riesgos externos, la falta control en el acceso a los sistemas y un deficiente sistema de cifrado de datos han ocasionado múltiples problemas asociados directamente con los elementos que integran un sistema informático.

Cuando ocurre un incidente o riesgo en la seguridad del sistema informático, la

confidencial e integridad de datos se ve comprometida, dejando expuesto el equipo.

La información y su gestión han pasado a formar parte de la actividad cotidiana de las empresas. Los ordenadores almacenan información, la procesan y la transmiten a través de redes abriendo nuevas posibilidades, por ello cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

Las constantes amenazas informáticas provenientes del internet atacan a la información de las empresas, debido a esto los usuarios están sufriendo graves problemas en cuanto a la seguridad de sus datos, por lo que se hace necesario buscar fortalecer las políticas de seguridad informática y la atención de incidentes; con la finalidad de mantener de confidencialidad, integridad y disponibilidad de la información (CID), puesto que la falta del cumplimiento de estos objetivos pondría a la organización en riesgo y por ende a su información.

1.2.3 Prognosis

En la actualidad, cada día se incrementa el uso de dispositivos móviles y ordenadores con acceso a Internet, lo cual atrae cada vez más a diferentes atacantes para lograr obtener información privilegiada conllevando perjuicios y convirtiéndose en riesgo eminente.

El panorama no es alentador, sin embargo, las soluciones a este problema se basan en la Norma Técnica Ecuatoriana NTE INEN–ISO/IEC 27000, a partir de este conocimiento se puede trabajar esta realidad y brindar una seguridad integral a los datos de los usuarios.

En este contexto, es importante fortalecer el uso de estrategias, políticas, procedimientos, normas y estándares que garanticen la Seguridad de la Información, crear o mejorar la respuesta a incidentes, lo cual facilitara el cumplimiento de los objetivos de negocio de las entidades de telefonía de Ecuador.

1.2.4 Formulación del Problema

¿Cuáles son las medidas de protección con las que cuentan las empresas telefónicas del país para resguardar la información de los usuarios?

1.2.5 Interrogantes (Subproblemas)

- ¿Las empresas de telefonía móvil han realizado estudios sobre la seguridad y protección de la información?
- ¿Qué tipo de información se tiene actualmente sobre la seguridad de la información dentro de las empresas del sector de telefonía móvil, enfocado a las más grandes empresas de antivirus como es el caso de Kaspersky, Symantec, McAfee y ESET?
- ¿Cuáles son las métricas aplicables al control y protección de la información que salvaguarden la información dentro de las empresas de telecomunicaciones?

1.2.6 Delimitación del Objeto de Investigación

Campo: Desarrollo empresarial.
Área: Innovación basada en tecnología.
Aspecto: Seguridad de la información enfocados en las operadoras de telefonía móvil.

Delimitación Espacial
Cualquier entorno de seguridad de la información.

Delimitación Temporal
El período en el que se desarrollará el estudio de la seguridad de la información corresponde a los últimos dos años.

Unidades de Observación
Ninguna.

1.3 Justificación

Una de las interrogantes más importantes que existen como empresa de telecomunicación Móvil es ¿realmente se está garantizando la seguridad de la información con los servicios ofertados?, también debe cuestionar ¿Se tiene políticas implantadas, que garanticen la seguridad de la información?, debido a que si se cumple con el objetivo de seguridad de la información se mejorará la imagen de la compañía y la confiabilidad por parte de los usuarios hacia la misma.

En la actualidad existe un desarrollo tecnológico importante, donde las tecnologías como móviles, computadores, PDA, entre otros, se han convertido en una estrategia para el mercado de las telecomunicaciones. Las empresas de telecomunicación usan los medios tecnológicos para captar un mayor nivel de aceptación por parte de los usuarios, debido a que los dispositivos inteligentes potencian el uso de internet en todo momento.

Ante esta realidad es esencial poseer una perspectiva dinámica y visionaria, con el afán de identificar los factores de riesgo de la seguridad de la información, para proponer políticas que disminuyen los factores de riesgo y aumentan la seguridad de la información.

Lo que pretende alcanzar el presente proyecto es fortalecer las políticas que se emplean para la seguridad de la información de las empresas de telefonía, en el caso del Ecuador, con esto es posible mejorar las políticas empleadas actualmente en las telefónicas en cuanto a la seguridad de la información, para crear nuevas políticas que abarquen de una manera amplia las falencias encontradas en la seguridad de la información. Las nuevas políticas creadas son útiles para aplicarlas en las empresas mencionadas.

El alcance de este proyecto está orientado a la creación de medidas de seguridad de la información, estableciendo una serie de pautas que permitan mejorar la seguridad de los sistemas de información existentes tanto de forma proactiva como reactiva frente a las amenazas tanto externas como las internas en el sector de las telecomunicaciones.

1.4 Objetivos

1.4.1 Objetivo General

- Estudiar el sistema de seguridad de la información para proponer medidas de protección para las empresas del sector de telefonía móvil en el Ecuador.

1.4.2 Objetivos Específicos

- Analizar la perspectiva de la información en torno a la protección de la información en las empresas del sector de telefonía móvil.
- Analizar la seguridad de la información, basados en los informes emitidos anualmente por las más grandes empresas de antivirus, Kaspersky, Symantec, McAfee y ESET, enfocados a las actuales operadoras de telefonía móvil en Ecuador.
- Generar políticas de protección de la información que salvaguarden la información dentro de las empresas de telecomunicaciones.

CAPÍTULO 2. MARCO TEÓRICO

2.1 Antecedentes Investigativos

De acuerdo con la Superintendencia de Telecomunicaciones el Ecuador cuenta con más de 16.9 millones de usuarios de telefonía móvil, de los cuales 10 millones cuentan con servicio de internet. Considerando que la población del Ecuador es aproximadamente de 15 millones, implica que el número de líneas móviles supera la cantidad de habitantes en el Ecuador. (Ecuador, 2018)

En muchos sentidos esto representa un alto crecimiento del acceso a internet en el Ecuador, además de mostrar una marcada tendencia al aumento en los siguientes años. Esto se debe a las facilidades de acceso a dispositivos tecnológicos como móviles, computadores, PDA, entre otros.

El crecimiento es evidente y si a esto le adicionamos la proliferación de redes inalámbricas que brindan acceso a internet a través de tecnología Wi-Fi, siendo muy comunes encontrarlas en empresas, universidades, domicilios, parques, entre otros. Es un indicador claro que en la actualidad no resulta difícil estar conectados a internet para el intercambio de voz y datos en cualquier momento.

Las empresas de telecomunicación en el Ecuador tienen que abastecer esta demanda, pero aseguran el acceso a la red desde cualquier lugar; En el último reporte sobre ciberseguridad en el país, desarrollado en el 2018 por la Corporación Nacional de Telecomunicaciones (CNT), identifica los desafíos que tiene el país. Por ejemplo, hay escasa legislación para frenar la violencia digital y proteger datos.

En el estudio realizado por (Deloitte, 2017) sobre la “Seguridad de la Información - Ecuador 2017” los ataques y amenazas están siempre presentes en las redes informáticas de las cuales el 79% de las empresas cuentan con un responsable de seguridad de la información, mientras que un 21% no lo tiene.

Estado del arte

Autor: (Peñuela, 2018)

Tema: "Análisis e identificación del estado actual de la seguridad Informática, dirigido a las organizaciones en Colombia, que Brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información".

El estudio de la situación de seguridad del sistema informático de una organización, el análisis de riesgos en una empresa ofrece una valoración de los recursos informáticos y las amenazas a las que están expuestos, con el fin de establecer acciones, métodos y procedimientos que se ejecutarán en función de las exigencias presentadas para establecer medidas y políticas para gestionar los riesgos y mejorar la seguridad informática (Oficina de Seguridad para las Redes Informáticas, 2013).

En este sentido también se puede hablar de una auditoría informática, Piattini & Del Peso (2001) afirma que es el proceso de acopiar, agrupar y valorar evidencias para comprobar si un sistema informático protege los activos, mantiene la integridad de los datos personales y utiliza todos los recursos disponibles de forma eficiente. Analiza un determinado momento en la seguridad informática de la organización.

Objetivos:

- Identificar los elementos básicos acerca de la importancia de la seguridad informática en las organizaciones.
- Indagar la Importancia de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.
- Analizar el estado de la seguridad informática de las organizaciones mediante un test de aplicación de seguridad informática.

Conclusiones:

- El proyecto de grado presentó algunas medidas para proteger el activo de información tomando en cuenta los avances de la tecnología.
- Se identificó que cualquier organización puede implementar su SGSI (Sistema de Gestión de Seguridad Informática), lo que debe hacer o por donde debe empezar una empresa, inicialmente se realiza un análisis del estado actual, se identifica con qué recursos cuenta y que recursos necesita, luego, debe definir el alcance y esto exclusivamente depende de cada organización.

Las empresas a escala mundial se enfrentan todos los días al aparecimiento de nuevas e innovadoras tecnologías, sin duda que éstas han aportado al desarrollo de sus actividades dentro de la empresa, sin embargo, también están expuestas a peligros cibernéticos. En este sentido, es necesario que las organizaciones adopten medidas de seguridad para disminuir esas inseguridades, por ende la importancia de la implementación del SGSI, software de protección de datos, capacitación del personal operativo, control de acceso y seguridad de los dispositivos (Peñuela, 2018).

Autor: (Acosta, 2018).
Tema: "Protocolo de Seguridad Informática para usuarios en la Universidad Regional Autónoma de los Andes UNIANDES"
Se denomina plan de seguridad al conjunto de medidas que definen las gestiones futuras y los medios que se van a utilizar para prevenir y evaluar las vulnerabilidades en los sistemas informáticos, dentro de este proceso se obtienen registros y evidencias que posibilitan la búsqueda, control y supervisión de funcionamiento de un sistema informático. Para elaborar un plan de seguridad informática según (Universidad Internacional de Valencia, 2018) existen algunos pasos como: Identificar los activos de la organización como personal, software, hardware y datos del sistema informático; evaluar los riesgos para conocer las amenazas y vulnerabilidades y el alcance del daño; priorizar la protección de la tecnología de la información; tomar las precauciones adecuadas, es decir, decidir qué pasos, políticas y medidas se tomarán en cuenta para proteger la información

Objetivos:

- Fundamentar científicamente los conceptos de Seguridad Informática, las herramientas que explotan vulnerabilidades.
- Establecer el nivel de seguridad informática de los usuarios en la Universidad Regional Autónoma de Los Andes UNIANDES.
- Preparar un conjunto de políticas que permita mejorar el grado de seguridad informática en los usuarios de UNIANDES.

Conclusiones:

- Se determinó las vulnerabilidades de los usuarios y de esa manera proponer un protocolo de seguridad informática para usuarios con la finalidad de mejorar los niveles de seguridad en la Universidad Regional Autónoma de los Andes UNIANDES.
- Se realizó un análisis de la situación problemática, en la cual se pudo observar que la mayoría de los usuarios desconocen aspectos básicos acerca de la seguridad de sus contraseñas, la navegación por internet y los problemas que conllevan a la falta de actualización de sus programas.
- Se capacitó a los usuarios para que estos puedan aplicar el conocimiento adquirido en las diversas actividades que estén realizando dentro y fuera de la Universidad Regional Autónoma de los Andes UNIANDES con la intención de proteger de una forma correcta su información.

Este trabajo determinó las debilidades en los sistemas de seguridad informática y de los usuarios en el protocolo de seguridad informática de la Universidad Regional Autónoma de los Andes UNIANDES. Se realizó un análisis acerca del conocimiento y conducta que tienen los usuarios al navegar por internet y se estableció que los usuarios necesitan capacitarse acerca de los métodos y técnicas para la protección de su información dentro y fuera de la Universidad (Acosta, 2018).

Autor: (Avilés & Silva, 2017)**.**
Tema: "Implementación de un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético, en la empresa BLENASTOR".

El test de seguridad de la información evalúa las seguridades, políticas y componentes internos de una empresa, además según (Avilés & Silva, 2017) permite identificar los siguientes riesgos: vulnerabilidades, debilidades, filtrado de información, elementos desconocidos, entre otros.
Existen mecanismos de detección en seguridad informática, son algo complejos y es necesario tener un conocimiento técnico previo para utilizarlo, sin embargo, estas herramientas de detección son útiles para conocer si el sistema informático ha sufrido violaciones en el tema de seguridad y si existió una intrusión total o parcial a un determinado recurso por parte de terceros infractores (Romero, et al., 2018).

Objetivos:

- Implementar un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético y seleccionado la herramienta que más se ajuste a la empresa Blenastor.
- Investigar las herramientas de hacking ético indicadas, sus beneficios y utilidad.
- Desarrollar el modelo o metodología de seguridad para ver debilidades en la red.

Conclusiones:

- Es necesario tener un ambiente cerrado con ordenadores específicos, para poder saber a detalle los ataques que sufre cada uno de éstos, y, sobre todo, poder comprobar si las recomendaciones que se hace a cada ordenador sean los que, de verdad, mejore la seguridad de estos.
- Mediante la investigación del origen, funcionamiento y las funcionalidades de las herramientas de Hacking Ético investigadas se puede ver como su uso puede llegar a ser útil para encontrar vulnerabilidades en los sistemas y de esta manera se pueda tomar cartas en el asusto y mejorar la protección de la organización.
- La seguridad de datos privilegiados en una empresa es de vital importancia para las mismas, por lo que la seguridad informática cumple un rol importante, que consiste en la protección de datos, en los tiempos actuales en donde toda información se traslada a través de Internet, por lo que es primordial proteger el flujo de datos, con esto se da a entender el lugar tan importante que ocupa la seguridad informática.

Existen herramientas informáticas útiles como el Hacking Ético para encontrar vulnerabilidades en los sistemas informáticos y para establecer acciones futuras en cuanto a la protección de datos de una empresa. Cuando se analiza la situación de seguridad informática se puede implementar planes, políticas y medidas que permitan para actuar y prevenir ataques cibernéticos en los dispositivos o en los datos de los usuarios (Avilés & Silva, 2017).

2.2 Fundamentación Teórica

2.2.1 Categorías Fundamentales

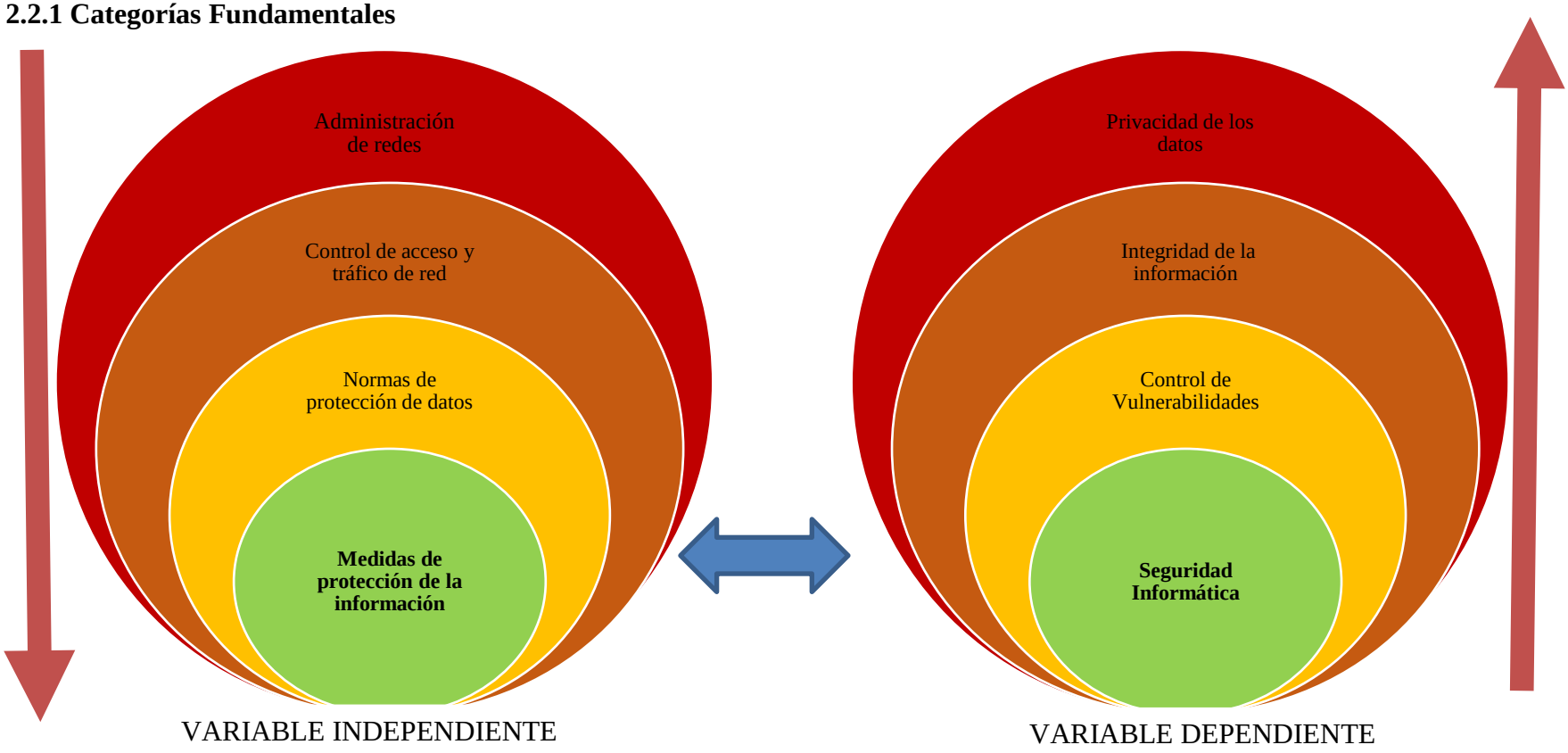

Gráfico 2. Inclusiones conceptuales

Elaborado por: Lozada Cristian (2018)

2.2.2 Supra-Ordenación de Variables

Gráfico 3. Inclusiones conceptuales
Elaborado por: Lozada Cristian (2018)

2.3 Variable Independiente

2.3.1 Administración de Redes

Cuando se habla de seguridad informática, este concepto refiere a la protección de datos acumulados en sistemas de información o, aquellos que son transmitidos a través de una red. La exposición de datos, los riesgos asociados al acceso, el empleo de sistemas no autorizados, hackers cibernéticos, delitos por internet, entre otros, son algunos de los riesgos para la seguridad informática y las empresas que cada día luchan por controlar.

La administración de redes informáticas especifica las numerosas tareas que realizan los expertos en tecnologías de la información en un sistema una red informática, con el fin de ofrecer óptimos servicios de red, de tal forma que se garantice a los usuarios una red activa, segura, eficaz, útil, con control y vigilancia permanente y de excelente calidad (BITS- Desarrollo e Ingeniería, 2016).

Este proceso comprende el trabajo de individuos, software y hardware. Existen numerosas actividades que conllevan al buen funcionamiento de la información y datos de una empresa u organización. Este servicio utiliza múltiples herramientas, servicios y mecanismos de gestión de redes que forman parte del software, en el hardware tenemos los dispositivos en los que administradores de red, profesionales informáticos garantizan el servicio de red de forma continua (BITS- Desarrollo e Ingeniería, 2016).

Las funciones y objetivos de la administración de redes son:

- Diseño, innovación y desarrollo de la red para mejorar las operaciones de red con mecanismos apropiados de control y seguimiento y métodos para resolver inconvenientes informáticos.
- Configuración de sistemas operativos y aplicaciones para mejorar el uso de red los recursos informáticos.
- Garantizar la disponibilidad, la integridad y la confidencialidad de la información para protegerla del acceso no autorizado, de esta forma, se refuerza la protección de la información almacenada de los usuarios.

- Suministrar servicio de soporte técnico para controlar las variaciones y actualizaciones en red de forma que no produzcan interrupciones en el servicio.
- Corregir problemas de la red (BITS- Desarrollo e Ingeniería, 2016).

2.3.2 Control de Acceso y Tráfico de Red

Un sistema de seguridad informática contiene un grupo de elementos que deben funcionar de manera correcta, para prevenir riesgos como pérdida, alteración o revelación de datos y el funcionamiento de sistemas informáticos, por esta razón, se han desarrollado herramientas aptas para el control de acceso de seguridad informática.

Los controles de acceso son mecanismos que funcionan como un filtro para permitir o negar el acceso a un sistema informático o prevenir estafas al momento de autenticar a una persona que desea ingresar a un sistema, a través de autorizaciones, códigos o contraseñas, para identificar a un usuario de manera segura, constituyen un elemento importante para la protección de sistemas operativos, para mantener la integridad, disponibilidad y confidencialidad de los datos y resguardar la información privada de accesos que no sean autorizados.

El control de acceso "funcionan como una suerte de compuerta capaz de filtrar quién entra a un sistema informático y quién no, valiéndose de permisos, códigos o contraseñas, que identifican de manera efectiva a un usuario o grupo de usuarios" (USS- Seguridad Integral, 2018)

Los sistemas de control de acceso a la seguridad informática tienen muchas ventajas para las empresas y usuarios porque previenen estafas o riesgos de manera inesperada, pueden identificar amenazas a la información o sistemas de una empresa a través de la identificación o autenticación de una persona que intenta ingresar al sistema de manera arbitraria (USS- Seguridad Integral, 2018).

Se pueden distinguir dos tipos de control de acceso para la protección de datos del usuario, así tenemos:

- Control de acceso autónomo, mecanismo que permite, restringe o administra de

modo seguro el acceso físico a una instalación, mediante una clave de acceso, tarjeta magnética o patrón biométrico.

- Control de acceso en red, mecanismo que está integrado por medio de un equipo tecnológico, cuenta con un software de control que lleva un registro de todas las acciones que susciten y permiten también la identificación del usuario en red. (USS- Seguridad Integral, 2018).

El concepto de tráfico de red se refiere fundamentalmente a la circulación y flujo de datos detallados, procesables, aplicaciones y protocolos que son transportados en la red. En este sentido, constituye las estadísticas de las tramas que han sido generadas por cada protocolo que convive en la red, por lo cual, se estima necesario su evaluación para la tasación y control adecuado de estos paquetes de protocolos y el uso de ancho de banda de los dispositivos habilitados.

2.3.3 Normas de Protección de Datos

En la seguridad informática se habla de protección de datos, el objetivo del resguardo no lo constituyen los datos sino el contenido de la información que se acopie sobre personas o instituciones con el fin de evitar consecuencias negativas en contra de los propios usuarios como: divulgación de información, alteración sin autorización o de forma accidental de información fundamental, pérdida de información y la negación de acceder a la información.

El motivo principal para establecer normas de protección de parte de entidades privadas o gubernamentales es garantizar la seguridad de estos datos, asegurando que el tratamiento de estos se efectúa respetando las reservas legales existentes. El usuario, además, debería conocer su derecho a saber de qué forma y por qué se están utilizando o almacenando su información y también ayudaría a determinar algunos criterios cuando el usuario exija anular o transferir esos datos, suspenderlos o modificarlos si son incorrectos (Gestión de Riesgo en la Seguridad Informática, 2019)

En la mayoría de los estados existen normas jurídicas que regulan el tratamiento de información y datos personales, en el Ecuador no existe una Ley Orgánica para Proteger Datos Personales, sin embargo, la Constitución del Ecuador (2008) afirma:

En el Art. 66, numeral 19, estipula el derecho a la protección de los datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley. (p. 49)

Aunque esta ley no está regulada, existe el esfuerzo de algunas empresas privadas, por establecer normas y medidas de protección de datos de los usuarios.

En algunos países de la Unión Europea se cuenta con una ley para garantizar la protección de los datos personales, por ejemplo, en España o en Estados Unidos de América. Un nuevo reglamento que se ejecutó en el mes de abril del año pasado en España, el tema de protección de datos y su aplicación en entidades públicas y privadas es el que trata sobre:

El derecho al olvido, es decir, a limitar la difusión de datos personales si ya no se usan para el fin con el que se recogieron, si el interesado ya no quiere que se conserven y no hay otro motivo más legítimo para mantenerlos o si se han usado de manera ilícita. (Rodella, 2018)

Esta novedosa norma de protección bien podría ser tema de análisis y estudio en las empresas privadas y gubernamentales en el Ecuador y no sólo de telefonía móvil, sino que podría aplicarse con el objetivo de frenar la inseguridad en los sistemas de información y proteger la información de los usuarios.

Para que se empleen medidas o normas de protección de datos deben aplicarse controles, estos serían procesos, programas de software o hardware, mecanismos que favorezcan el resguardo de datos de usuarios en el mundo.

Tarazona señala que además de las medidas o normas que instauren las empresas privadas o públicas de telecomunicaciones, otra forma de protección de los datos de los usuarios es el cumplimiento y la observación de los estándares ISO 17799 e ISO 27001, debido a que le proporcionan a una organización las bases justas para desarrollar una verdadera y efectiva gestión de seguridad de la información, que brinde protección de sus activos, información, reducción de riesgos y vulnerabilidades y un óptimo servicio de

telecomunicaciones (Tarazona, 2018).

2.3.4 Medidas de Protección de la Información

Ecuador no cuenta con medidas de protección de información, aunque existe en la Constitución un artículo que plantea el derecho a la protección de los datos, no existe una Ley de Protección de Datos Personales (LPDP) que regule y proteja los datos personales y tampoco existe un enfoque ágil del empleo de esos datos.

En materia de legislación de protección de datos, expertos legales aseguran que hay que guardar un equilibrio entre la protección de derechos y el desarrollo comercial, es necesario recordar que los usuarios se encuentran en un entorno digital, están el Internet, la virtualidad, pero también existen factores como el humano y empresas que deben respetar la información, la disponibilidad y la integridad de los datos.

"Desde octubre de 2017, la Dirección Nacional de Registro de Datos Públicos (Dinardap) inició la construcción de los contenidos del Anteproyecto de Ley de Protección de Datos Personales juntamente con varios sectores públicos y privados alineados a la temática" (Dirección Nacional de Registro de Datos Públicos, 2017)

El contexto actual favorece el estudio de este trabajo de investigación, el que servirá para establecer un contexto general acerca de la situación de la seguridad informática en el sector de la telefonía móvil en el país.

2.4 Variable Dependiente

2.4.1 Seguridad Informática

El constante y amplio desarrollo de las nuevas tecnologías, los acelerados cambios a nivel mundial, la globalización de la economía y el exceso de información de los múltiples sistemas que almacenan nuestros datos, han provocado que el índice de vulnerabilidades y amenazas aumente propiciando el escenario ideal para incurrir en delitos. Los usuarios de teléfonos móviles desconocen la dimensión exacta de este problema que trae consigo: amenazas cibernéticas, hurto de información, acceso indebido a la información de los

usuarios y hasta el deterioro de los dispositivos móviles, de ahí que, sea importante reflexionar sobre esta problemática que desencadena muchas veces en acciones deshonestas (Suárez & Ávila, 2015).

La seguridad informática resguarda los recursos de los sistemas de información de las organizaciones o empresas, el uso que se les suministre a los mismos, el acceso a la información acopiada y si existe alguna modificación al sistema solo puedan acceder las personas que se encuentren acreditadas y autorizadas (González, 2014).

La seguridad informática garantiza las condiciones, protege los datos y la información, minimiza el riesgo de vulnerabilidad y riesgos en los sistemas de información.

La seguridad informática comprende software como las bases de datos, metadatos y archivos, hardware como sus partes físicas, la información privada y todo lo que la empresa estime que debe resguardarse si llega a manos de terceros, convirtiéndose, por ejemplo, en información privilegiada que puede ser utilizada con fines delictivos (González, 2014).

Para aplicar medidas de seguridad hay que hacerlo de modo planificado y racional, para evitar esfuerzos innecesarios y para invertir recursos en áreas que realmente lo requieran, para que estas medidas y elementos de protección resulten eficientes, adecuados y efectivos, deben integrarse y gestionarse dentro de un sistema más amplio de seguridad informática (Gil & Gil, 2017)

Cuando se habla de seguridad informática y de seguridad de la información, aunque son conceptos muy similares guardan algunas diferencias en cuanto su aplicación y en el énfasis de acción que cada uno posee. La seguridad informática se encarga del aspecto técnico tradicional de seguridad, es decir, todo lo relacionado con la IT (tecnología informática) como aplicaciones de software, dispositivos o equipos de hardware que evitan imperfecciones en los sistemas de computación, apoyándose en acciones especialmente técnicas para garantizar la seguridad. La seguridad de la información, por otro lado, se ocupa mucho más de la parte administrativa de la información, es decir, es un compromiso de la gerencia y la parte administrativa de una organización en cuanto a la seguridad (Ormella, 2019).

En este sentido, en el tema de seguridad de la información de una empresa es importante observar los riesgos técnicos y también los riesgos de operación, organización y materiales (Ormella, 2019).

La seguridad de la información no es solamente un problema de seguridad en los ordenadores, tener un óptimo sistema de seguridad de la información debe estar encaminado a resguardar los activos de propiedad intelectual, los datos y la información almacenada sustancial de las organizaciones y de las personas (Tarazona, 2018).

2.4.2 Control de vulnerabilidades

Una vulnerabilidad es una debilidad que se presenta en un sistema operativo, software o sistema que ocasiona el mayor daño posible a la información almacenada en los sistemas, permite el fácil acceso violando la privacidad, integridad, disponibilidad de los datos y produce fallas en el control de acceso y consistencia sobre los elementos de un sistema o de sus datos, y en el caso de los dispositivos móviles sobre los componentes relacionados con la información y el propio dispositivo (Informática & Tecnología, 2013).

Se pueden considerar dos conceptos al momento de enfrentarse al entorno informático actual, las vulnerabilidades y amenazas están ligadas intrínsecamente y actúan juntas cuando se afecta el entorno interno y externo de empresas y, además a las personas.

Las vulnerabilidades son debilidades que tienen la tecnología o los procesos relacionados con la información, es decir, son particularidades propias de los sistemas de información o de los equipos que la contiene. Una amenaza es cualquier entorno o suceso que puede perjudicar el buen funcionamiento de las organizaciones y personas, por ende, afecta directamente las actividades, la información y los sistemas de información (Tarazona, 2018).

En el sistema de los Teléfonos inteligentes o conocidos como Smartphone, existen algunas vías de acceso y contagio que se convierten en amenazas y en vulnerabilidades para equipos, información y sistemas, por ejemplo, a través de ficheros descargados, navegación web, aplicaciones engañosas, consecuencias de Root o Jailbreak y ataques en

internet (García, 2017).

César Tarazona plantea que los tipos de amenazas a la información se dividen en cuatro categorías:

- Factores Humanos (accidentes o fallas).
- Errores en los sistemas de información.
- Catástrofes naturales.
- Actos malintencionados (Tarazona, 2018).

2.4.3 Integridad de la Información

Actualmente el tema de seguridad informática y control deberían ser una prioridad en las empresas públicas y privadas, debido a las amenazas internas y externas que existen, estas instituciones deberían proponer medidas y sistemas más eficientes de protección de datos de los usuarios.

Cuando hablamos de integridad de datos, también debemos hablar de las normas y los procedimientos que hay que aplicar y seguir para evitar los ataques a la seguridad de los datos. La seguridad de la información sirve para resguardar los datos que almacena, maneja y dispone una empresa que deberá "gestionar de forma eficaz el almacenamiento, procesamiento y transmisión de la información" (Sistemas de Gestión de Seguridad en la información, 2018).

Para mantener un sistema informático en buen estado, seguro, preventivo, auténtico, responsable y fiable, los datos o información deben considerar tres aspectos: confidencialidad, integridad y disponibilidad (Sistemas de Gestión de Seguridad en la información, 2018).

Hablar sobre la integridad de la información significa que los datos se mantengan inalterados ante ataques malignos de terceras personas para prevenir modificaciones no autorizadas de los datos almacenados o información y, si se requiere en algún momento alterar la información, deberá ser bajo previa autorización (Sistemas de Gestión de Seguridad en la información, 2018).

Para mantener el control de acceso e integridad de los datos, debe contarse con mejores prácticas de autenticación; óptimas políticas internas en las empresas que protejan y se responsabilicen por los datos de los usuarios; mayor control de acceso; responsabilidad y un óptimo mantenimiento de los equipos tecnológicos y un sistema de control de acceso de usuario que defina los permisos que determinan quién puede acceder a qué datos (Zambrano, 2015).

2.4.4 Privacidad de los Datos

En los medios de comunicación, escuchamos y observamos informes que alarman a los usuarios de telefónicas en Ecuador y en el mundo entero. Detrás del hurto de móviles, problemática que está en aumento, se encuentra oculto un contexto preocupante, ya que la cantidad de información que los usuarios almacenan en sus dispositivos es muy alta.

En este sentido, la seguridad del usuario se ve amenazada, debido a que, si extravía o le substraen su equipo, un tercero podría acceder fácilmente a sitios web, mensajes de texto o información privada desde el teléfono móvil.

El usuario también se enfrenta a los ataques al sistema de los celulares o a través de mensajes de texto, lo que puede propiciar un posible robo.

Acceder a un sistema de seguridad informática resulta necesario y obligatorio para resguardar los datos, contraseñas e información que almacene el dispositivo móvil.

La protección de datos, también llamada privacidad de información es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartido con terceros (Rouse, 2014).

La privacidad de los datos de los usuarios desde una perspectiva social es un derecho que garantizaría al beneficiario de cualquier servicio tener el control sobre el uso y empleo de sus propios datos, esto, con el fin de frenar el manejo ilícito y ofensivo de los mismos por terceros y, además, su decisión sobre qué información quiere compartir y qué no en el

mundo informático.

2.5 Hipótesis

El estudio de la seguridad informática de la telefonía móvil para la implementación de medidas de protección de la información aumenta positivamente la seguridad informática en dicho sector.

2.6 Señalamiento de las Variables

2.6.1 Variable Independiente

Medidas de protección de la información

2.6.2 Variable Dependiente

Seguridad Informática

2.7 Marco Legal de las Telecomunicaciones en el Ecuador

2.7.1 Introducción

Las telecomunicaciones son el medio o instrumento muy importante para la transformación de los países alrededor del mundo, debido a esto es realmente necesario delimitar un marco normativo, adecuado dentro del cual el sector pueda desarrollarse con legitimidad.

De acuerdo a los diferentes puntos de vista es inevitable administrar a los servicios de telecomunicaciones del marco legal que respete la importancia, complejidad, magnitud y especialidad de este servicio, contando con que el mismo pueda tomarse en cuenta en actividades como: gestión empresarial y beneficio social, para ello se presentara a continuación una tabla con las leyes que resguardan las telecomunicaciones en Ecuador:

Tabla 1. Leyes de comunicación en Ecuador

Tipo de Norma	Norma Jurídica	Publicación Registro Oficial	Fecha publicación	Referencias bibliográficas.
Normas Constitucionales	CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR 2008	Registro Oficial N°. 449 2	20/10/2008	(Constitución de la República del Ecuador, 2008)
Normas Primarias del Sector	CONVENIO DE CONSTITUCIÓN DE LA UIT	Registro Oficial N°. 781	14/09/1995	(Convenio de Constitución de la UIT.)
Normas Primarias del Sector	LEY ORGÁNICA DE TELECOMUNICACIONES	Registro Oficial N°. 439	18/02/2015	(Ley de la Propiedad Intelectual, 2016)
Normas Primarias del Sector	REGLAMENTO GENERAL A LA LEY ORGÁNICA DE TELECOMUNICACIONES	Registro Oficial Suplemento N°. 676	25/01/2016	(Reglamento General a la Ley Especial de Telecomunicaciones, 2015)
Normas Primarias del Sector	REGLAMENTO PARA LA PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES Y SERVICIOS DE RADIODIFUSIÓN POR SUSCRIPCIÓN	Registro Oficial N°. 749	06/05/2016	(Ley de la Propiedad Intelectual, 2016)
Normas de Creación	EMPRESAS PÚBLICAS DEBEN CONTRATAR TELECOMUNICACIONES DEL ESTADO	Registro Oficial N°. 459	31/05/2011	(Empresas Públicas Deben Contratar Telecomunicaciones del Estado, 2011)
Leyes conexas	LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS	Registro Oficial N°. 557	17/04/2002	(Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002)
Leyes conexas	LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA	Registro Oficial Suplemento N°. 337	18/05/2004	(Ley Orgánica de Transparencia y Acceso a la Información Pública, 2004)

Fuente: Investigación propia
Elaborado por: Lozada, Cristian (2018)

2.7.2 Leyes que Rigen la Seguridad Informática

En el Ecuador, las leyes que rigen la seguridad informática se encuentran inscritas en la Constitución del 2008. Existen leyes que afirman que la información es un bien jurídico

que debe ser tutelado y protegido, también existen ciertas leyes y reglamentos que hacen alusión especial hacia la tecnología y su información. Para conocimiento y efecto de estas se mencionan a continuación:

- Ley Orgánica de transparencia y Acceso a la Información Pública,
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes Datos,
- Ley de Propiedad Intelectual,
- Ley Especial de Telecomunicaciones,
- Ley de Control Constitucional (Reglamento Habeas Data).

2.7.2.1 Ley Orgánica de Transparencia y Acceso a la Información Pública

La (LOTAIP) fue publicada el 18 de mayo del 2004, bajo el Registro Oficial suplemento 337, este documento se publicó con la finalidad de llevar a la práctica la disposición basada en el Art. 81 de la Constitución de Política del año 1998 en el Ecuador, la misma que afirmaba que la "información es un derecho de las personas que garantiza el Estado", esta ley hace referencia a que todas las instituciones del sector público ponen a disposición de la ciudadanía el libre acceso a la información institucional, compuesta por la estructura orgánica, bases legales, regulaciones metas, objetivos, presupuestos, resultados de auditorías, entre otros.

2.7.2.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes Datos

La (LCELEC) se publicó el 17 de abril del 2002, bajo el Registro oficial N°.557, donde manifiesta que los mensajes de datos tendrían igual valor jurídico que los documentos escritos. Contienen principios jurídicos que hacen especial mención a la información dentro del contenido general, protegiendo la confidencialidad de los mensajes de datos en sus diversas formas. Se establece que el documento escrito se equipara en conjunto con el documento electrónico, para que en los casos donde amerite la presentación de un documento escrito este pueda proceder con la misma legalidad del documento electrónico, para evitar que su conservación no sea alterada.

A su vez la firma electrónica tendrá total validez aún cuanto esta conste como un requisito

fundamental de legalidad documental, protegiendo las bases de datos creadas u obtenidas por una transmisión electrónica de un mensaje de datos, otorgando al titular correspondiente la disposición de su información, ya sea que los mismos hayan sido resultado por ser usuario del servicio o por el intercambio de mensajes de datos, ratificándose la defensa legal mediante el derecho Constitucional de Habeas Data.

2.7.2.3 Ley de Propiedad Intelectual

Esta ley se publicó en el Registro Oficial Nro. 426 el 28 de diciembre de 2006, fue creada con el objetivo de ofrecer por parte del Estado una correcta protección de los derechos intelectuales y asumir la defensa de los mismos, caracterizándole como un factor imprescindible para el desarrollo tecnológico y por ende económico del país. El Instituto Ecuatoriano de Propiedad Intelectual (IEPI) está a cargo de la aplicación de leyes y reconoce la importancia que guarda la propiedad intelectual en Ecuador y su correcta aplicación a los sectores económicos, industriales y de investigación.

La ley incluye dentro de su ordenamiento la codificación de la protección de bases de datos, que tenga formato impreso u otros formatos, así también, como los programas de ordenador como software, ya que son considerados como obras literarias. Su principal objetivo se basa en la piratería que se ha acrecentado en los últimos días y por lo tanto resulta imprescindible, el derecho a la propiedad intelectual.

2.7.2.4 Ley Especial de Telecomunicaciones

La Ley Especial de Telecomunicaciones fue publicada el 10 de agosto del 1992, con el Registro Oficial, N°. 996, donde se manifiesta expresamente que es necesario proveer los servicios de telecomunicaciones dentro de lineamientos en la normativa legal, esta tiene como objeto general poder regir con leyes referentes a las telecomunicaciones, lo concerniente a emisión o recepción de signos señales, imágenes, sonidos e información de cualquier naturaleza por un hilo de radioelectricidad, medios ópticos entre otros electromagnéticos.

2.7.2.5 Ley de Control Constitucional (Reglamento Habeas Data)

Esta ley se publicó bajo el Registro Oficial N°. 99 del 2 de Julio de 1997, la misma se le calificó con la jerarquía y con el carácter de Ley Orgánica, por medio de una resolución legislativa con publicación del 8 de Marzo del 2001, con el Registro Oficial 280, en su capítulo II del Habeas Data, hace especial mención que "las personas naturales o jurídicas, nacionales o extranjeras, que tengan el deseo a tener el acceso a documentos, bancos de datos e informes que sobre si misma o sus bienes que estén al poder de entidades públicas, o personas naturales o jurídicas privadas, y es así como conocer el uso y finalidad que se les haya dado o se les otorgue, podrán interponer el recursos de Habeas Data".

2.7.3 Ministerio de Telecomunicaciones y de la Sociedad de la Información

El Ministerio de Telecomunicaciones se creó ante la necesidad de coordinar acciones de apoyo y asesoría para garantizar el acceso equitativo a los servicios que tienen que ver con el área para apoyar el avance del progreso hacia la Sociedad de la Información y del Conocimiento y las Tecnologías de la Información y Comunicación y así poder alcanzar el buen vivir de la población ecuatoriana.

Esta cartera de Estado tiene varios objetivos como: establecer y coordinar la política del sector de telecomunicaciones, desarrollar planes con la Agencia de Regulación y Control de Telecomunicaciones, diseñar y ejecutar proyectos ligados al desarrollo del sector, realizar investigaciones y estudios del sector de telecomunicaciones, entre otros (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019).

Este Ministerio como órgano público dependiente de la Función Ejecutiva administrará de forma integral las tecnologías de la información, las telecomunicaciones y el espectro radioeléctrico a través de la planificación y diseño de Políticas Públicas que permitan la inserción de los ciudadanos a la sociedad de la información y, además, éstos puedan generar y acceder al conocimiento e información (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019).

Bajo el Ministerio de Telecomunicaciones se adscriben la Dirección Nacional de Registro Civil, la Agencia Nacional Postal, Correos del Ecuador, la Corporación Nacional de Telecomunicaciones. El Ministro de Telecomunicaciones preside el Consejo Nacional de Telecomunicaciones (CONATEL), al que se fusionó el Consejo Nacional de Radio y

Televisión (CONARTEL). El Ministro de Telecomunicaciones también será presidente del CONATEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019).

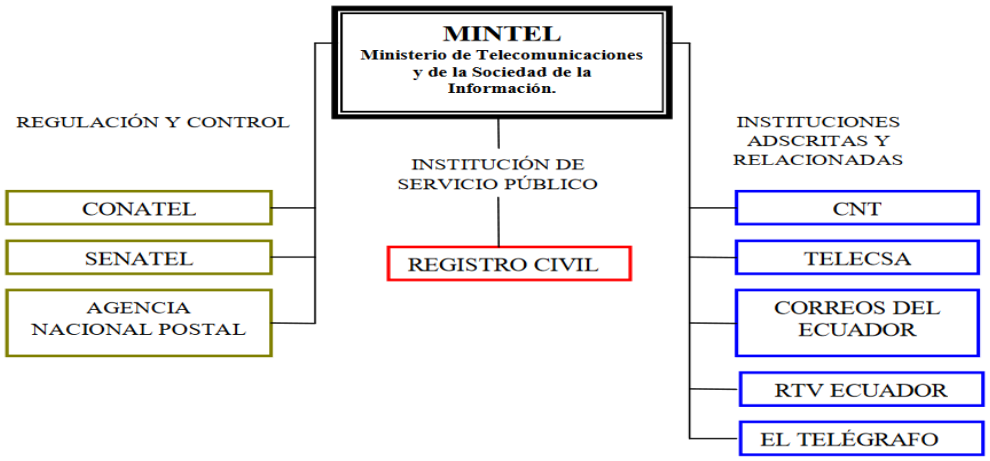

Figura 1. Estructura Actual del Ministerio de Telecomunicaciones
Elaborado por: Lozada Cristian (2018)

Las predisposiciones sobre seguridad informática para Ecuador se enmarcan en el Consejo Nacional de Telecomunicaciones, CONATEL, que es un cuerpo colegiado conformado por 6 miembros, presidido por el delegado del Jefe de Estado y tiene la representación del gobierno para ejercer la administración y regulación de los servicios de telecomunicaciones del Ecuador ante la Unión Internacional de Telecomunicaciones (UIT).

El 13 de agosto del año 2009 en el Decreto Ejecutivo No. 8, se establece en el:
Artículo 13.- Fusiónese el Consejo Nacional de Radio y Televisión CONARTEL al Consejo Nacional de Telecomunicaciones CONATEL. (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019)

Se menciona además y de acuerdo con el Artículo 14, del mismo Decreto se dispone que: Las competencias, atribuciones, funciones, representaciones y delegaciones constantes en leyes, reglamentos y demás instrumentos normativos y atribuidas al CONATEL serán desarrolladas, cumplidas y ejercidas por el CONATEL, en los mismos términos constantes en la Ley de Radiodifusión y Televisión y demás normas secundarias. Exclusivamente las funciones administrativas que ejercía el presidente del CONATEL, las realizará el Secretario Nacional de Telecomunicaciones, en los mismos términos

constantes en la Ley de Radio y Televisión y demás normas secundarias. (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019)

Entre las competencias del Ministerio de Telecomunicaciones están por ejemplo, designar de manera técnica el espectro radioeléctrico denominado como un recurso natural con el fin de que todas las operadoras del sector de las telecomunicaciones lleven a cabo sus actividades en óptimas y eficientes condiciones; expedir normas que cumplan con las reglas establecidas de acuerdo a las prácticas que impidan la leal competencia; determinar las obligaciones que los operadores deben cumplir en el marco que asigne la Ley y los reglamentos respectivos y defender los derechos de los ciudadanos en todo momento para que satisfagan su necesidad de comunicación (Ministerio de Telecomunicaciones y de la Sociedad de la Información , 2019).

CAPÍTULO 3. METODOLOGÍA

En el presente capítulo, se presenta un conjunto de métodos e instrumentos que se emplearon en la investigación planteada, desde el enfoque, el tipo de estudio, el diseño, población, muestra y técnicas de recolección de datos, los cuales aportan las herramientas para la verificación de hipótesis y el cumplimiento de los objetivos.

3.1 Enfoque

El enfoque de esta investigación posee un enfoque cualitativo y cuantitativo, se realiza un estudio dentro del sector de las telecomunicaciones móviles, además de una cuidadosa recolección, análisis e interpretación de los datos obtenidos, basándose en un marco teórico cuidadosamente preparado que recoge muchos conocimientos previos obtenidos de la investigación bibliográfica realizada.

En este sentido, se utilizó entrevistas no estructuradas que permitieran la obtención de datos de las distintas empresas objetos de estudio con lo que se pudo analizar los resultados y hacer una explicación según el resultado obtenido por cada ítem. Permitiendo deducir conclusiones generales a partir de primicias particulares.

3.2 Modalidad Básica de la Investigación

Se realizó una investigación bibliográfica haciendo uso de libros, documentos técnicos, revistas, artículos y leyes existentes para la elaboración del marco teórico sobre la Seguridad de la Información, la Vulnerabilidad y las Medidas de Protección dentro de la industria de las telecomunicaciones a nivel nacional, enfocándose básicamente en las empresas de telefonía móvil del Ecuador.

Asimismo, se realizó una investigación de campo pues la información primaria fue recogida directamente de los involucrados a través de entrevistas no estructuradas, por medios digitales.

3.3 Nivel o tipo de Investigación

La investigación es Aplicada de tipo Descriptivo la cual de acuerdo con Catacora (2018) tiene como finalidad la solución de un problema mediante la aplicación de conocimientos científicos tecnológicos para resolver un problema práctico. Además, se realizó la descripción e interpretación de la naturaleza actual del sistema de las telecomunicaciones, bajo estudio, trabajando sobre la realidad de los hechos.

Adicionalmente, exploratoria ya que se obtiene la información inicial para continuar con una investigación más rigurosa, y permite formular la hipótesis que se podrá retomar para nuevas investigaciones.

Por otro lado, se ha tomado la investigación como asociativa y correlacional lo que permite medir la relación existente entre la variable independiente, correspondiente a las medidas de protección y su influencia en el aumento de la seguridad informática en el sector de la telefonía móvil.

3.4 Población y muestra

La población y muestra dentro de la investigación puede considerarse relevante, pues se conoce las tres operadoras a las cuales se les ha dedicado las preguntas de la encuesta para identificar los criterios de Seguridad Informática y de Medidas de Protección bajos los cuales dirigen cada una de sus corporaciones.

Esta investigación se ha desarrollado utilizando una muestra de las empresas de telefonía móviles más comerciales en el Ecuador, cada una de estas empresas podrían beneficiarse directamente del estudio en la creación de medidas de la protección de la información, tomando a personal del Departamento de IT de las empresas seleccionadas para el estudio.

3.5 Operacionalización de las Variables

Variable Independiente: Medidas de protección de la Información.

Tabla 2. Variable Independiente

Conceptualización	Dimensiones	Indicadores	Ítems básicos	Técnicas	Instrumentos
Son prácticas de seguridad informática que ayudan a proteger los datos de una empresa. Implica el proceso de proteger contra intrusos el uso de recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.	Normas de seguridad	Nivel de exigencia de acceso	Identificación de estándares en los sistemas	Investigación bibliográfica y Entrevista	Entrevista, y documentos relacionados al tema de investigación.
	Políticas de seguridad	Nivel de resguardo de la información	Disposiciones		

Fuente: Investigación propia
Elaborado por: Lozada, Cristian (2018)

Variable Dependiente: Seguridad Informática.

Tabla 3. Variable Dependiente

Conceptualización	Dimensiones	Indicadores	Ítems básicos	Técnicas	Instrumentos
El proceso de prevenir y detectar el uso no autorizado de un sistema informático. La seguridad informática es una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos	Protección	Grado de Integridad de la información	Disposición de un sistema fiable	Investigación bibliográfica y aplicación de entrevistas	Entrevistas y documentos relacionados al tema de investigación.
	Control		Infraestructura de los sistemas		
	Manejo	Vulnerabilidades	Personal involucrado		
		Nivel de Accesibilidad			

Fuente: Investigación propia
Elaborado por: Lozada, Cristian (2018)

3.6 Plan de Recolección de Información

La recolección de la información se hizo posible mediante la aplicación de entrevistas no estructuradas, lo que ayudó a la obtención más concreta de la información que queremos obtener sobre las variables de estudio, con el objetivo de demostrar la hipótesis planteada.

Consta de las siguientes preguntas básicas:

Tabla 4. Preguntas básicas para la entrevista

PREGUNTAS BÁSICAS	EXPLICACIÓN
1. ¿Para qué?	Con la finalidad de alcanzar los objetivos de la investigación
2. ¿De qué personas u objetos?	Individuos encargados del sistema informático dentro de la empresa.
3. ¿Sobre qué aspectos?	Medidas de seguridad informática.
4. ¿Quién, ¿quiénes?	Investigador
5. ¿Cuándo?	2018
6. ¿Dónde?	Empresas del sector de telecomunicaciones seleccionadas.
7. ¿Cuántas veces?	Una
8. ¿Qué técnicas de recolección?	Entrevistas Datos estadísticos
9. ¿Con qué?	Registros digitales
10. ¿En qué situación?	Correo Electrónico

Fuente: Investigación propia

Elaborado por: Lozada, Cristian (2018)

3.7 Plan de Procesamiento y Análisis de la Información

Para procesar la información recolectada, se siguieron los pasos a continuación descritos:

- Revisión crítica de la información recogida.
- Repetición de la recolección, en ciertos casos individuales para corregir errores de contestación.
- Tabulación de la información obtenida.
- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).
- Estudio estadístico de datos para presentación de resultados.
- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados con apoyo del marco teórico en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPÍTULO 4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 La seguridad de información en las organizaciones de telefonía móvil

Las empresas de telefonía móvil enfrentan el permanente desafío de brindar a los usuarios una experiencia móvil segura, cumpliendo al mismo tiempo con las obligaciones de proteger la seguridad pública. Mientas se desarrollan servicios más avanzados y complejos, de la misma manera aumenta la lista de posibles amenazas y la trascendencia de los daños que pueden causar. Las estafas y los ataques son cada vez más sofisticados, por ello deben existir soluciones de seguridad de información más integrales. (GSMA, 2018)

Las empresas de telefonía móvil del Ecuador mantienen políticas de seguridad de la información, con las cuales tratan de proteger a las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Sin embargo, mantienen ciertas vulnerabilidades en la seguridad de la información debido al incremento de ataques maliciosos y amenazas existentes en las redes informáticas. Parad exterminar estas vulnerabilidades se realizó entrevistas a los operadores móviles y consultores y/o integradores de las compañías. Las preguntas presentadas en las entrevistas realizadas se encuentran en el Anexo 1 del presente documento y los resultados obtenidos se muestran a continuación:

4.1.1 Compañía Claro

El Consorcio Ecuatoriano de Telecomunicaciones (CONECEL) está operando en el Ecuador desde el año 1993, en el año 2000 pasó a ser parte de América Móvil. Claro es denominada una empresa de información, comunicación y entretenimiento que proporciona acceso al servicio móvil al 96% de la población ecuatoriana con productos y servicios de tecnología avanzada, y además es la primera operadora privada que provee a sus usuarios tecnología digital, GSM, 3G, HSPA +, y 4G LTE en las cuatro regiones del país y recientemente 4.5G. (Claro, 2019)

4.1.1.1 Información obtenida

Tabla 5. Consolidado de respuestas y aporte Claro

INVESTIGACIÓN EXPLORATORIA **NUEVAS TENDENCIAS EN SEGURIDAD INFORMÁTICA EN REDES MÓVILES EN ECUADOR** **ANÁLISIS DE INFORMACIÓN**				
Institución y/o Experto	**Tipo de Institución y/o Experto**	**Fecha de solicitud**	**Medio de solicitud de información/respuesta**	**Tipo de archivo solicitado**
CLARO	Operador Móvil	24/09/2018	Correo Electrónico	.doc, .docx, .xls, .xlsx, .ppt, .pptx , .pdf, .gpeg
Información solicitada	**ÍTEM**	**Aporte a la investigación**		
La cabalidad en la aplicación de políticas o estándares de cifrado de la información para su clasificación. (Pública, privada, confidencial, etc.). Normas de manejo de datos.	1 -4	La empresa Claro cuenta con gran portafolio robusto de soluciones informáticas que le permiten tener la información segura, permiten alojar aplicaciones e información en un centro de datos (Data Center) que es un medio de almacenamiento y backup disponibles para la seguridad de la información (activo más valioso) de su empresa. Algunas de las aplicaciones de Claro son las siguientes: - Internet seguro - Control de servicios SAP - Videos de seguridad Las herramientas más utilizadas en la empresa como medio de protección de la información son: Spam Killer, monitoreo y Firewall, las cuales crean un bloque de la información no		
Respuesta aportada				
La operadora manifiesta que disponen de todas las medidas posibles y altos estándares de cifrado, por lo que la información es netamente confidencial de acuerdo a las leyes plasmadas también en sus contratos de adquisición de servicio.				
Información solicitada	5-7			

Situación actual de acuerdos de confidencialidad en la construcción y despliegue de protocolos de seguridad informática implantada en sus diferentes redes de datos móviles en el país.		deseada y del acceso a aquella información que pudiese perjudicar a los usuarios. La finalidad de la compañía Claro es ofrecer a los clientes internos y externos estándares altos de servicio y satisfacción permanente de sus necesidades, además CONECEL establece como compromisos orientados a garantizar el Sistema de Gestión de Calidad de Información, cuyos lineamientos están enmarcados en las Normas Internacionales ISO. Claro como todas las empresas no se pueden asegurar en su totalidad que el usuario que accede a los servicios web de claro sea el Titular de la Cuenta. (Dueño de la cuenta)
Respuesta aportada		
Afirman que la seguridad implantada en las redes informáticas está basada en los organismos internacionales, sin embargo han existido fallos en la confidencialidad de datos de los usuarios.		
Información solicitada	8	
Contexto de riesgo de la infraestructura con respecto a ataques, delitos e incidentes informáticos en sus diferentes redes de datos móviles en el país, proporción de registros en los últimos 2 años.		
Respuesta aportada		
Durante los 2 últimos años la brecha de fuga de información ha tenido una importante reducción, debido a la administración simplificada de la información, la protección y monitoreo aplicado en las diferentes redes informáticas.		

Información solicitada	9	
Control de roles y privilegios en las aplicaciones de servicio, monitoreo y difusión de los usuarios.		
Respuesta aportada		
Expresan que cuentan Spam Killer que evita el uso indiscriminado y la asignación arbitraros de roles y privilegios de los usuarios, además resulta complicado asegurar si el usuario que está utilizando la cuenta sea el propio dueño, ya que pude ser otra persona.		

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.1.2 Seguridad de la información

Dentro del portal web de Claro (2019), se encueran ciertas políticas de privacidad y seguridad que permiten determinar el tratamiento de información de sus usuarios al momento de adquirir un servicio de la compañía.

Tabla 6. Seguridad de la información

Característica	Descripción
Certificación de Seguridad	La Gestión de Seguridad de la Información de la compañía Claro está enmarcada en las Normas Internacionales ISO.
Política de Privacidad	Los lineamientos de seguridad de Claro se encuentran respaldados por las políticas de seguridad de la información que fueron construidas bajo los

	estándares de seguridad existentes y dando cumplimiento a las normas internacionales vigentes. Estas políticas son de estricto cumplimiento por los funcionarios directos o indirectos que desempeñan alguna labor u actividad al interior de Claro.
Revelación de Información	La información de los usuarios debe ser veraz, completa, actualizada, exacta, comprobable y comprensible. Claro prohíbe el trato de datos parciales, incompletos o que induzcan a error.
Protección de la información personal	Claro respeta la privacidad de la información personal de los usuarios y garantiza la confidencialidad en el tratamiento de los datos de carácter personal que se solicitan a través de los distintos servicios, así como la implementación de las debidas medidas de índole técnica y organizativa.

Fuente: (Claro, 2019)
Elaborado por: Lozada Cristian (2018)

4.1.1.3 Vulnerabilidades en la seguridad de la información

Tabla 7. Vulnerabilidad en la seguridad de la información

Vulnerabilidad	Descripción
Software malicioso o virus	Se utiliza Spam Killer, monitoreo y Firewall para la seguridad de información que crean un bloque de la información no deseada y del acceso a aquella información que pudiese perjudicar a los usuarios.
Cuentas de usuario	No se puede asegurar que el que accede a los servicios de claro sea el Titular. (Persona dueño de la cuenta)
Tiempos de acceso a la información	Debido a la alta latencia en la red del proveedor de servicios, congestión del canal de internet del proveedor, congestión de las redes troncales y redes de acceso.

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.2 Compañía Movistar

La compañía Movistar Ecuador (Telefónica) provee de servicios inalámbricos de comunicaciones incluyendo servicios de voz, roaming internacional, internet inalámbrico, características mejoradas de llamadas, servicios de datos, intranets inalámbricas y otros servicios.

Para la seguridad de la información se apoya en normativas corporativas de seguridad de la información y en el reglamento corporativo de controles mínimos de seguridad, además cuenta con una certificación de seguridad de información proporcionada por la norma internacional ISO.

De acuerdo a lo expuesto en el informe anual de (Movistar, 2017), millones de datos de clientes de Movistar han estado expuestos debido a un error de programación, entre los datos afectados se identifican como nombres, domicilios, direcciones de correos electrónicos, números de teléfono y desgloses de llamadas.

Facua (2018) considera el incidente como "la mayor brecha de seguridad en la historia de las telecomunicaciones en España". De acuerdo a este informe cualquier persona podía acceder a la información de los clientes tan solo con ingresar a una cuenta en el portal de Movistar, los datos eran obtenidos mediante la consulta de facturación propia, por lo cual, dicho código alfanumérico equivalente al número de recibo, al modificarse, conducía directamente a las facturas de otros clientes de la compañía y así al cambiar de referencia, un usuario podía ir de un recibo ajeno en otro consultando los datos personales que en ellos aparecían.

Con respecto a esta gran brecha informática Facua (2018) declaró en un comunicado que la empresa optó por inhabilitar funcionalidades de su página oficial para evitar la visualización de datos ajenos.

4.1.2.1 Información obtenida

Tabla 8. Consolidado de respuestas y aporte Movistar

INVESTIGACIÓN EXPLORATORIA **NUEVAS TENDENCIAS EN SEGURIDAD INFORMÁTICA EN REDES MÓVILES EN ECUADOR** **ANÁLISIS DE INFORMACIÓN**				
Institución y/o Experto	**Tipo de Institución y/o Experto**	**Fecha de solicitud**	**Medio de solicitud de información/respuesta**	**Tipo de archivo solicitado**
Movistar	Operador Móvil	24/09/2018	Correo Electrónico	.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg

Información solicitada	**ÍTEM**	**Aporte a la investigación**
La cabalidad en la aplicación de políticas o estándares de cifrado de la información para su clasificación de la información. (Pública, privada, confidencial, etc.). Normas de manejo de datos.	1-4	Movistar protege y respeta la confidencialidad, así como también proporciona una correcta utilización de los datos accesibles por la empresa Otecel en la aplicación APP Mi Movistar. La compañía Movistar en el año recibió de la Asociación Española de Normalización y Certificación AENOR la certificación del Sistema de Gestión de Seguridad de la Información bajo la norma ISO 27001:2013.
Respuesta aportada		
La empresa estima que maneja los reglamentos pero está en constante crecimiento y agregación de estándares.		
Información solicitada	5-7	En el año 2017, la compañía Movistar sufrió un ataque informático que afecto a los equipos informáticos a nivel mundial. Estos hechos afectaron a las páginas web en la que la exposición de los datos de los clientes fue evidente por lo cual las
Situación actual de acuerdos de confidencialidad en la construcción y despliegue de protocolos de seguridad informática implantada en sus diferentes redes de datos móviles en		

el país.		medidas a tomar fueron inmediatas. Además, Movistar presenta la opción para acceder a datos de los usuarios, pero es información básica ya que indican que solo el titular de la línea puede acceder a información como registros de llamadas o actividad de la línea.
Respuesta aportada		
Expresa que han existido faltas internas a nivel de confidencialidad en cuanto al sistema de seguridad pues, se han registrado importantes pérdidas de información.		
Información solicitada	8	
Contexto de riesgo de la infraestructura con respecto a ataques, delitos e incidentes informáticos en sus diferentes redes de datos móviles en el país, proporción de registros en los últimos 2 años		
Respuesta aportada		
La vulnerabilidad en la página web de la empresa se registra en el acceso en cuanto a facturación, por lo cual estiman un nivel importante de riesgo e incidentes.		
Información solicitada	9	
Control de roles y privilegios en las aplicaciones de servicio, monitoreo y difusión de los usuarios.		
Respuesta aportada		
La mayoría de servicios que ofrece cuentan con los controles y privilegios, sin embargo los ataques informáticos causan que los datos de los usuarios queden expuestos.		

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.2.2 Seguridad de la información

Tabla 9. Seguridad de la información

Característica	Descripción
Certificación de Seguridad	Según la Norma Internacional ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información
Política de Privacidad	La compañía Movistar se compromete a proteger y respetar la confidencialidad de los datos, así como también dar un correcto uso de los datos accesibles por OTECEL en el sitio web www.movistar.com.ec.
Revelación de información	Protege los datos y las claves asociadas a las cuentas de correo electrónico, almacenándolas en servidores seguros y evitando su divulgación a terceras personas, solo se muestra información básica al público.
Protección de la información personal	El cliente es el único responsable de mantener su palabra clave (password) y la información de su cuenta.

Fuente: (Movistar, 2018)
Elaborado por: Lozada Cristian (2018)

4.1.2.3 Vulnerabilidades en la seguridad de la información

Tabla 10. Vulnerabilidad en la seguridad de la información

Vulnerabilidad	Descripción
Software malicioso o virus	La compañía Movistar fue víctima de un Software malicioso "ransomware" que afectó a las redes informáticas y a los sistemas Windows.
Cuentas de usuario	Cualquier persona tenía acceso a la información de los clientes con solo ingresar a una cuenta en el portal de Movistar.
Tiempos de acceso a la información	A veces las páginas se vuelven lentas lo que perjudica el acceso a la obtención de los datos.

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.3 Compañía CNT

La Corporación Nacional de Telecomunicaciones de (CNT, 2017) es un operador del estado que ofrece servicios de telefonía de línea fija y móvil, televisión satelital e internet. Los servicios y productos abarcan la instalación de nuevas líneas telefónicas, identificador y transferencia de llamadas, además planes de llamadas de larga distancia nacional e internacional.

Según los datos recolectados de esta compañía, fundamenta sus productos y servicios en el control para confidencialidad, integridad y disponibilidad del su sistema según la ISO 27001:2013 con capacidad de organización para conocer sus riesgos, identificar sus amenazas y reducirlas y, aun así, han recibido multitud de ataques de índole externa. La seguridad informática con respecto a esta compañía tuvo un alto nivel de ataques mitigados en la telefonía móvil e internet el año pasado en su último reporte de seguridad en el rubro. (CNT, 2017).

Por esto, se dispone que los planes de seguridad y las políticas generadas en la empresa presentan faltas en su implementación. Por esta razón la gestión de seguridad debe mantenerse al tanto de cualquier evento ocurrido sobre la infraestructura de red que ocasione un cambio significativo.

4.1.3.1 Información obtenida

Tabla 11. Consolidado de respuestas y aporte CNT

INVESTIGACIÓN EXPLORATORIA **NUEVAS TENDENCIAS EN SEGURIDAD INFORMÁTICA EN REDES MÓVILES EN ECUADOR** **ANÁLISIS DE INFORMACIÓN**				
Institución y/o Experto	**Tipo de Institución y/o Experto**	**Fecha de solicitud**	**Medio de solicitud de información/respuesta**	**Tipo de archivo solicitado**

CNT	Operador Móvil	24/09/2018	Correo Electrónico	.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg

Información solicitada	**ÍTEM**	**Aporte a la investigación**
La cabalidad en la aplicación de políticas o estándares de cifrado de la información para su clasificación de la información. (Pública, privada, confidencial, etc.). Normas de manejo de datos.	1-4	La Corporación Nacional de Telecomunicaciones tiene una política de seguridad y privacidad de información que permite el manejo y la recopilación delos datos personales mediante el acceso a la página Web. CNT recibió la Certificación ISO 27001: 2013 de la Asociación Española de Normalización y Certificación (AENOR), que la reconoce como una empresa que "dispone de un sistema de Seguridad de la Información conforme a la Norma UNE-ISO/IEC 27001:2014". (www.cnt.gob.ec) Con el propósito de reducir el riesgo de que la información de los usuarios o que se vea comprometida por hackers, la empresa impulsa nuevos proyectos para el año 2020 en la que se percibirá la evolución de las redes móviles y la mayor parte de la información se podrá encontrar en la nube, la misma que contara con niveles altísimos de seguridad ya que esto comprende el compromiso de la empresa. Una de las desventajas de CNT es el tiempo y la capacidad de acceso a los
Respuesta aportada		
Estiman que si cumplen con las leyes correspondientes para el manejo de datos.		
Información solicitada	5-7	
Situación actual de acuerdos de confidencialidad en la construcción y despliegue de protocolos de seguridad informática implantada en sus diferentes redes de datos móviles en el país.		
Respuesta aportada		
Expresan cumplir con los acuerdos de confidencialidad, pero no tienen en menos la mejora continua en vista de los continuos ataques que han intentado a su plataforma.		
Información solicitada	8	
Contexto de riesgo de la infraestructura con respecto a ataques, delitos e incidentes		

informáticos en sus diferentes redes de datos móviles en el país, proporción de registros en los últimos 2 años		datos debido a la falta de cobertura a nivel nacional.
Respuesta aportada		
Consideran que su plataforma está en ascenso, que el contexto de la infraestructura debe mejora a pesar de ser consistente. En los últimos 2 años han recibido numerosos ataques y otro gran número ha sido no exitoso.		
Información solicitada	9	
Control de roles y privilegios en las aplicaciones de servicio, monitoreo y difusión de los usuarios.		
Respuesta aportada		
Se cuenta con privilegios y roles de usuarios en las diferentes aplicaciones informáticas, sin embargo existe vulnerabilidades en el acceso a los datos por falta de cobertura a nivel nacional.		

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.3.2 Seguridad de la información

Tabla 12. Seguridad de la información

Característica	Descripción
Certificación de Seguridad	Norma ISO 27001:2013
Política de Privacidad	El propósito de esta Política de Privacidad es la de

	informar respecto de la recopilación y manejo de la información personal suministrada, mediante el acceso a la página Web ("sitio") de la Corporación Nacional de Telecomunicaciones CNT EP ("CNT EP").
Relevación de la información	CNT EP obtiene, revelará y transfiere la información personal con su conocimiento, que puede ser expreso o implícito, dependiendo de la sensibilidad de la información personal, los requerimientos legales y otros factores. La Corporación CNT precisara de la colaboración de un tercero para el tratamiento de la información que de manera directa o indirecta sea ingresada en el sitio.
Protección de la información personal	CNT EP mantiene salvaguardas moderadas para proteger la confidencialidad, seguridad e integridad de la información personal. Se emplean medidas de seguridad para proteger su información personal contra la revelación no autorizada, el mal uso o la alteración, como es el caso con todas las redes de computadoras vinculadas a Internet.

Fuente: (CNT, 2017)
Elaborado por: Lozada Cristian (2018)

4.1.3.3 Vulnerabilidades en la seguridad de la información

Tabla 13. Vulnerabilidad en la seguridad de la información

Vulnerabilidad	Descripción
Software malicioso o virus	Al igual que las grandes empresas, las redes informáticas de CNT están expuestas aplicaciones maliciosas como Fraude de IP-PBX, es un delito informático en el que las personas no autorizadas utilizan el servicio de llamadas locales y celulares a destinos internacionales costosos a expensas del propietario del sistema telefónico que fue comprometido, explotando alguna vulnerabilidad.

Cuentas de usuario	Las personas que son víctimas de IP-PBX pueden verificar el registro de llamadas internacionales caso contrario, debe solicitar el bloqueo a nivel de CNT E.P.
Tiempos de acceso a la información	Principalmente el tiempo de acceso a los datos se da debido a la falta de cobertura a nivel nacional.

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

4.1.4 Comparación de la seguridad de la información en las compañías de telefonía móvil

Para realizar la comparación se tomó como aspecto importante la seguridad de la información de las compañías, así como también las vulnerabilidades encontradas en los últimos años en lo referente la seguridad de información.

Para calificar a cada aspecto referente a la seguridad de la información se tomó como base la escala de rango determinado por Muy de acuerdo (5), De acuerdo (4), Ni de acuerdo ni en desacuerdo (3), En desacuerdo (2) y Muy en desacuerdo (1), como se detalla a continuación:

Tabla 14. Cuadro comparativo de la seguridad de la información en las compañías móviles

Característica	Claro	P.	Movistar	P.	CNT	P.
Certificación de Seguridad	Muy de acuerdo	5	Muy de acuerdo	5	Muy de acuerdo	5
Política de Privacidad	De acuerdo	4	De acuerdo	4	De acuerdo	4
Relevación de la información	De acuerdo	4	De acuerdo	4	De acuerdo	4
Protección de la información personal	De acuerdo	4	En desacuerdo	2	De acuerdo	4

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

Con la información anterior se puede determinar que las empresas de telefonía móvil tienen políticas de seguridad para el tratamiento de información de los usuarios, además Movistar y CNT cuentan con certificación de Gestión de Seguridad de la información ISO 27001, sin embargo, Movistar registra problemas en lo referente a protección de la información personal debido a los constantes ataques informáticos que sufrió la compañía.

Tabla 15. Cuadro comparativo de las vulnerabilidades de seguridad de la información en las compañías móviles

Vulnerabilidad	Claro	P.	Movistar	P.	CNT	P.
Software malicioso o virus	De acuerdo	4	Muy de acuerdo	5	De acuerdo	4
Cuentas de usuario	De acuerdo	4	Muy de acuerdo	5	De acuerdo	4
Tiempos de acceso a la información	De acuerdo	4	De acuerdo	4	De acuerdo	4

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

De la tabla anterior se puede concluir que las que en las empresas de telefonía móvil a pesar de estar certificadas presentan ciertas vulnerabilidades en el momento del acceso a los datos, siendo la principal característica vulnerable el software malicioso o virus que día a día atacan a las redes informáticas en todo el mundo.

4.2 Vulnerabilidades identificadas en las empresas de telefonía móvil

Según el estudio realizado la mayoría de las vulnerabilidades encontradas en las organizaciones de telefonía móvil son: los constantes ataques informáticos a las redes informáticas por software maliciosos, provocando el robo de identidad o robo de datos.

4.3 Ataques informáticos y Antivirus

Para este estudio se tomó como base de investigación las empresas de antivirus a nivel mundial como son: Kaspersky, Symantec, McAfee y ESET, los cuales día a día

reconocen el mayor número de ataques informáticos o virus, y realizan análisis regularmente de todo el sistema.

4.3.1 ESET

Con base en el informe de seguridad que realizó (ESET, 2018) donde describe un análisis estadístico acerca del panorama de la seguridad actual en las empresas de América latina con el objetivo de reflejar cuáles eran los problemas, desafíos actuales y futuros, el alcance de las soluciones y la inversión y costos involucrados en su implementación, advirtió una serie de preocupaciones que engloban al conjunto de las compañías entrevistados.

Entre las temáticas analizadas y reflejadas en su Security Report, se destacan las amenazas a la seguridad de la empresa donde la pérdida de datos apareció como la principal inquietud, al ser seleccionada por el 65,96% de las entrevistas. Los ataques de malware y las vulnerabilidades del software ocupan el segundo y tercer lugar respectivamente, con el 58,30% y el 55,32% (ESET, 2018).

En Latinoamérica, ESET mencionó que existe una serie de preocupaciones de sus encuestados, el 56,32% consideró que es esencial la implementación de planes de concientización en materia de seguridad que, sumados a aquellos que asignaron una importancia muy alta a la cuestión se concluye que más del 85% de los profesionales concuerdan en la importancia de la capacitación y educación del personal para prevenir problemas de seguridad informática, pero sólo el 34,18% de los interrogados afirmó que en su empresa se llevan a cabo planes de concientización con periodicidad. (ESET, 2018).

Por otra parte, en cuanto al presupuesto, más de la mitad de los encuestados (52,37%) afirmó que menos del 5% del presupuesto de IT es utilizado para tal fin y tan sólo un 18,11% de las organizaciones declaró que asigna más del 10% del presupuesto del departamento de informática y sistemas (ESET, 2018).

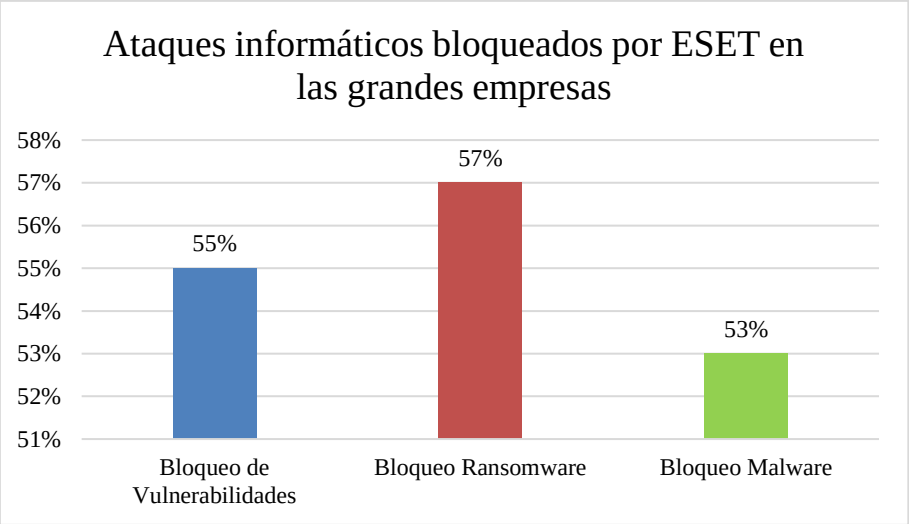

Gráfico 4. Ataques informáticos bloqueados por ESET en las grandes empresas
Fuente: (ESET, 2018)
Elaborado por: Lozada (2018)

El gráfico anterior muestra los principales ataques informáticos identificados por ESET son las vulnerabilidades, los programas maliciosos como el rasomware y malware. En el año 2017, ESET bloqueo vulnerabilidades en un 55%, el software malicioso ransomware en un 57 % y realizó bloqueos malware en un 53% en las grandes empresas, entre estas las empresas de telefonía móvil.

4.3.2 Symantec

En base a lo expuesto por el informe anual de seguridad brindado por (Symantec, 2018) las amenazas a la seguridad digital pueden provenir de fuentes nuevas e inesperadas y cada año que pasa, además del aumento del volumen absoluto de amenazas, el escenario de amenazas se ha tornado más diversificado, con un trabajo más arduo de los grupos de ataque para descubrir nuevos caminos de ataques y cubrir sus rastros.

En el año 2017, Symantec detecto y bloqueo nuevas amenazas a los datos, es así que detecto un 92 % de nuevas amenazas de variantes de descargas, 80 % de amenazas a Mac, esto se relaciona frecuentemente al desempeño y lentitud de los equipos de trabajo de las organizaciones. (Symantec, 2018)

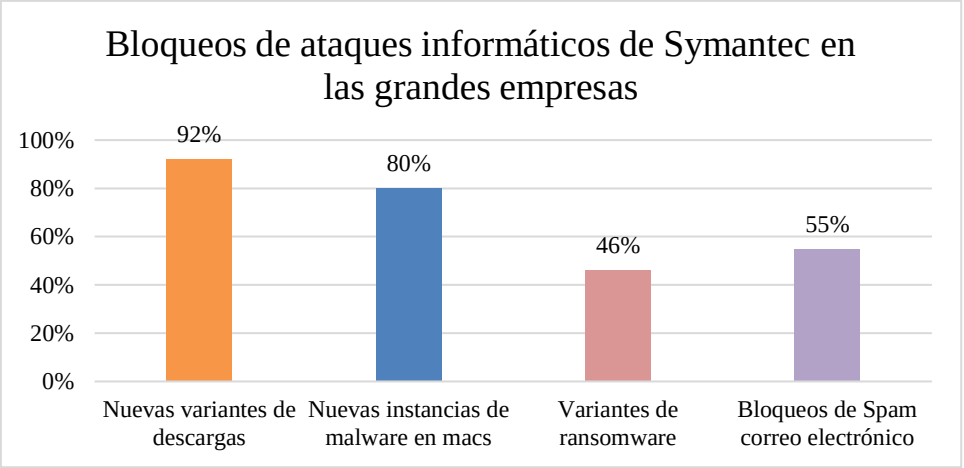

Gráfico 5. Bloqueos de ataques informáticos de Symantec en las grandes empresas
Fuente: (Symantec, 2018)
Elaborado por: Lozada (2018)

Además, la cantidad de variantes de ransomware aumentó un 46%, indicando que los grupos criminales establecidos se mantienen bastante productivos, bajó la cantidad de familias de ransomware. (Symantec, 2018)

Finalmente, se puede indicar que Symantec bloqueó un 55 % de correos no deseados o spams que atacan a las grandes empresas a nivel mundial.

4.3.3 McAfee

De acuerdo a los análisis y estadísticas de esta empresa, se concluye que existe un crecimiento de números en el amenazante crimen de seguridad teniendo el objetivo de rentabilizar dicha actividad con un mínimo esfuerzo, así mismo empleando un número bajo de intermediarios y reproducir delito tras delito con mayor rapidez y menor riesgo. (McAfee, 2018)

La dificultad para acceder a determinados servicios es una de los principales motivos por los cuales la información es vulnerable a ser sustraída y una solución que se plantea en la actualidad es el denominado “paquetizado” que puede ser gestionado por parte del propio cliente de forma simple integrando los productos de seguridad a los equipos

de sobremesa y dispositivos móviles con el objetivo de ayudar a los usuarios a mantenerse protegidos contra las últimas amenazas.

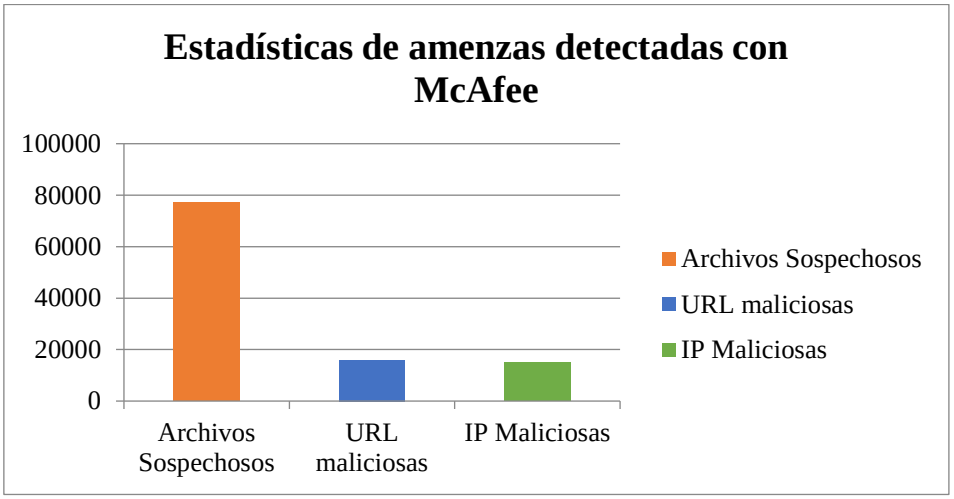

Gráfico 6. Estadísticas de amenazas detectadas con McAfee
Elaborado por: Lozada (2018)

De acuerdo lo señalado con (McAfee, 2018).

- Analizó 77 000 millones de archivos sospechosos y calificó 73 millones (0,01) como peligrosos.
- Analizó 16 000 millones de URL maliciosas y calificó 63 millones (0,4 %) como peligrosas.
- Analizó 15 000 millones de direcciones IP maliciosas y calificó 66 millones (0,4 %) como peligrosas.

4.3.4 Kaspersky

De acuerdo con lo señalado por (KASPERSKY LAB, 2019):

- El 29,4% de los equipos de los usuarios sufrieron al menos un ataque de programas maliciosos a través de Internet en el año.
- Las soluciones de Kaspersky Lab neutralizaron 1 188 728 338 ataques lanzados desde recursos en Internet distribuidos por todo el mundo.

- Los componentes antivirus web reconocieron 199 455 606 URLs únicas como maliciosas.
- La antivirus web de Kaspersky Lab detectaron 15 714 700 objetos maliciosos únicos.
- 939 722 equipos de usuarios únicos fueron atacados por programas maliciosos cifradores.
- Las soluciones de Kaspersky Lab bloquearon 1 126 701 intentos de ataques de malware diseñado para robar dinero mediante la banca online.

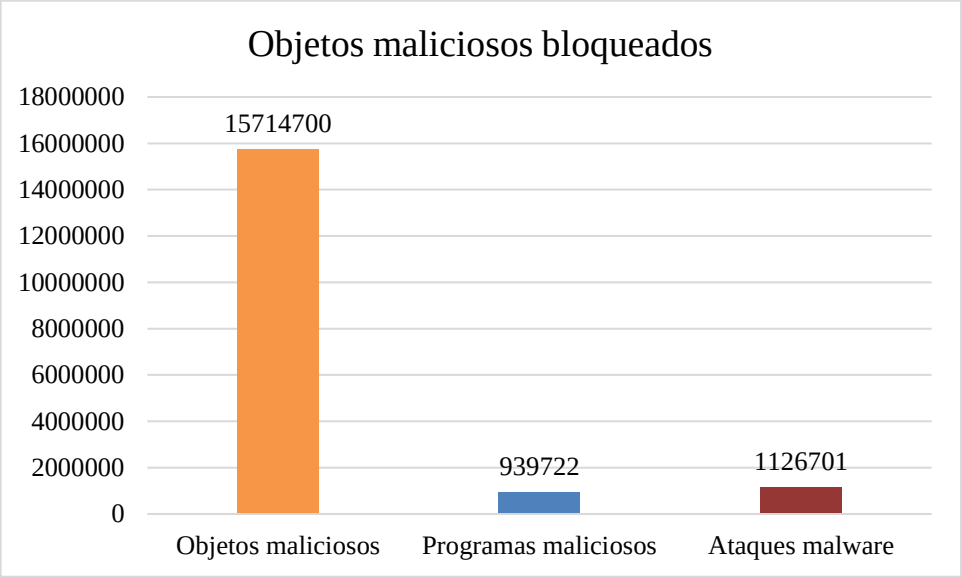

Gráfico 7. Objetos maliciosos bloqueados
Elaborado por: Lozada (2018)

Los ataques por programas maliciosos son frecuentes y se registran en una gran cantidad por ello las acciones por parte de las empresas de servicio de telefonía móvil sugieren que sus usuarios de manera independiente adquieren unos programas que clasifique la información que recibe de tal manera que la información que se identifique como dudosa sea inmediatamente bloqueada para evitar que la información sea robada y utilizada para actos delincuenciales.

En síntesis, a pesar de contar con leyes adecuadas para los delitos informáticos, las infraestructuras críticas y la protección de datos resultan vulneradas de manera frecuente, por lo que, a nivel estadístico, estas amenazas que han afectado la seguridad interna y externa de las compañías han estado ligadas directamente a la no

profundización o a las faltas de aplicación de estas medidas. Por otra parte, si bien es cierto que las normas son adecuadas, con el avance tecnológico también surgen riesgos de última tecnología que muchas veces mitigan las leyes, en este orden de ideas, la responsabilidad no recae en un 100% en las políticas de seguridad de las compañías sino en la misma tecnología que construye tanto sus avances como sus riesgos.

4.3.5 Cuadro comparativo de análisis de los Antivirus

Para realizar el análisis de los antivirus se tomó en cuenta lo siguiente aspectos:

- Rendimiento del PC
- Protección de contraseñas
- Contrafuegos
- Seguridad de datos en la Red
- Ataque al software malicioso

Tabla 16. Estudio comparativo de las empresas de antivirus

Característica	ESET	P.	Symantec	P.	McAfee	P.	Kaspersky	P.
No disminuye el Rendimiento PC	De acuerdo	4	Muy de acuerdo	5	Muy de acuerdo	5	De acuerdo	4
Protección de Contraseñas	Muy de acuerdo	5	Muy de acuerdo	5	Muy de acuerdo	5	Muy de acuerdo	5
Cortafuegos	Muy de acuerdo	5	Muy de acuerdo	5	De acuerdo	4	Muy de acuerdo	5
Seguridad de Datos en las redes	Muy de acuerdo	5	De acuerdo	4	De acuerdo	4	Muy de acuerdo	5
Ataca al Software Malicioso	Muy de acuerdo	5	De acuerdo	4	De acuerdo	4	Muy de acuerdo	5

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

Con la tabla anterior se puede determinar que todos los antivirus presentan ventajas al

momento de utilizar las redes informáticas, ESET y Kaspersky son las empresas que ofrece mayores más ventajas ofrece sobre las demás lo que permite la eliminación del software malicio o virus y permite una mejor protección en los datos de los usuarios cuando utilicen las redes informáticas, sin embargo, se reduce el nivel de rendimiento de los equipos informáticos.

4.4 Verificación de hipótesis

Para verificar la hipótesis se utilizó la pregunta 2 de la entrevista aplicada a las empresas de este estudio, pues permite evaluar directamente el impacto de la solución propuesta implementada en seguridad informática del proceso de servicio que brinda la institución, y cómo ellos califican las medidas de protección que utilizan con el propósito de acometer la vulnerabilidad y seguridad de los sistemas informáticos.

4.5 Planteamiento de la hipótesis Modelo lógico

Hipótesis Nula (H0): El estudio de la seguridad informática de la telefonía móvil para la implementación de medidas de protección de la información NO aumenta positivamente la seguridad informática en dicho sector.

Hipótesis Alternativa (H1): El estudio de la seguridad informática de la telefonía móvil para la implementación de medidas de protección de la información SI aumenta positivamente la seguridad informática en dicho sector.

Relación entre los medios de protección y las operadoras

Se realiza un ensayo de un Análisis de Componentes Principales para conocer la relación existente entre los Medios para la Protección que se han revisado en la bibliografía y las Compañías de Telefonía que se han analizado también en la revisión, y se observa que existe una asociación entre las características de los antivirus McAfee y Symantec con las compañías Claro y CNT. Por otro lado, los antivirus Kaspersky y ESET, se asocian con Movistar.

Gráfico 8. Asociación entre las compañías de telecomunicaciones con los medios de protección informática
Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

Las características de los antivirus que sirven como medios de protección para garantizar la seguridad informática que buscan las compañías Movistar, Claro y CNT. En base a una determinación de características podría expandirse el número de antivirus candidatos para las empresas que lo requieran y recolectar información necesaria para relacionar las parejas de antivirus-operadora más acorde a las características de cada uno.

Modelo estadístico

Se utilizó una prueba estadística no paramétrica de correlación para medir la asociación existente entre las medidas de protección y la seguridad informática. La prueba de correlación utilizada fue la correlación no paramétrica de Spearman, los resultados se presentan con una confianza del 95%.

Mediante el siguiente esquema matemático, se plantea el coeficiente de correlación

$$r_k = \frac{\sum(u_i - \bar{u})(v_i - \bar{v})}{(\sum(u_i - \bar{u})^2 \sum(v_i - \bar{v})^2)^{1/2}},$$

Donde u_i y v_i son los rangos de X_i e Y_i, las variables involucradas en el estudio (Taylor, p. 411).

Mediante el uso del programa estadístico SPSS versión 22, se procede a calcular las correlaciones existentes entre Seguridad de los sistemas informáticos de las compañías de telecomunicaciones que se analizan; la Vulnerabilidad de estos sistemas y los Medios de Protección, en este caso los antivirus.

Se puede ver que existe una correlación negativa total entre la Vulnerabilidad y la Seguridad, esto es totalmente comprensible, pues mientras más aumente la seguridad, la vulnerabilidad disminuirá directamente. De igual manera, se puede ver que existe una correlación de 0.314 entre las medidas de protección y la seguridad informática. Por otro lado, se tiene una correlación de -0.314, entre las medidas de protección y la vulnerabilidad de los sistemas informáticos (ver Tabla 16).

Se puede entonces aseverar que la vulnerabilidad disminuye aproximadamente un 31% y la seguridad aumente en un 31% cuando las medidas de protección son estudiadas y tomadas en cuenta dentro de las compañías de telecomunicaciones, por lo que se rechaza la hipótesis nula estadísticamente se puede proferir que el estudio de la seguridad informática de la telefonía móvil para la implementación de medidas de protección de la información aumenta positivamente la seguridad informática en dicho sector.

Tabla 17. Correlaciones (no paramétricas) entre las medidas de protección y la vulnerabilidad y seguridad de los sistemas informáticos de las compañías de

telecomunicaciones

CORRELACIONES			Vulnerabilidad	Seguridad	Protección
Rho de Spearman	Vulnerabilidad	Coeficiente de correlación	1,000	-1,000**	-,314*
		Sig. (bilateral)			,0319
	Seguridad	Coeficiente de correlación	-1,000**	1,000	,314*
		Sig. (bilateral)			,0319
	Protección	Coeficiente de correlación	-,314*	,314*	1,000
		Sig. (bilateral)	,0319	,0319	

****. La correlación es significativa en el nivel 0,01 (2 colas).**

***. La correlación es significativa en el nivel 0,05 (2 colas).**

Fuente: Investigación propia
Elaborado por: Lozada Cristian (2018)

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La seguridad informática en las empresas del sector de telefonía móvil en el Ecuador en la actualidad, ha presentado nodos de vulnerabilidad de acuerdo a los focos de ataques principales de robo información en todas sus formas y estados en vista de su altísimo valor, por lo cual, la garantía de manutención de la integridad y confidencialidad de datos, entre otros servicios de seguridad ofrecidos por éstas empresas se han visto quebrantados, a pesar de la disposición de canales estandarizados de distribución de aplicaciones implementados por los fabricantes y desarrolladores de las plataformas.

- Las empresas de telefonía móvil en el Ecuador conocen la necesidad de mantener la usabilidad y confidencialidad de la información que soportan sus sistemas, en base a la implementación íntegra de los métodos de seguridad soportados en los estándares vigentes que protejan las redes ante eventuales amenazas.

- Las estadísticas de ataques recibidos por las empresas de telefonía móvil en el Ecuador han expuesto la necesidad de capacitación constante de las organizaciones en su conjunto, a fin de manejar a cabalidad normas, procedimientos, y herramientas vigentes que faciliten la administración de la seguridad en el activo principal de este tipo de empresas, como lo es la información de sus usuarios.

- Los informes actuales emanados por las empresas de antivirus que fueron objeto en este estudio de investigación mostraron la amplia gama de ataques a los que las compañías de telefonía móvil en el Ecuador se han vistos expuestos en los últimos años, a consecuencia de la naturaleza de sus datos y la corriente actual de movilidad a la que está sujeta la información. Por lo cual, se ha derivado en incidentes con impactos negativos para las mismas a nivel económico, legal y de confiabilidad de sus usuarios.

- La adecuada implementación de políticas de seguridad informática en el sector de las telecomunicaciones preserva y administra los activos de estas compañías, además de dar solución, prevenir, controlar, así como subyugar los daños de estos incidentes asociados a la seguridad informática.

5.2 Recomendaciones

- Promover el conocimiento de las políticas de seguridad de la información que posee las empresas de telecomunicaciones hacia los usuarios, para que estos conozcan y puedan usar los dispositivos de forma adecuada en cuanto a la seguridad de la información.

- Explorar nuevas metodologías de protección de la información, que pueda servir de complemento para las políticas propuestas en el presente estudio. Es muy útil para obtener un nivel alto de la seguridad de la información.

- Es necesario la evaluación de las leyes y políticas de seguridad de la información implementadas en las empresas de telecomunicación cada determinado tiempo, debido a que continuamente existen avances tecnológicos en cuanto a software y hardware. Para garantizar la seguridad informática y la seguridad de la información.

- Se recomienda hacer un análisis evolutivo de las políticas propuestas, una vez implementadas. Puesto que este tipo de análisis permite conocer el nivel de efectividad de las políticas propuestas, para seguir tomando medidas correctivas y ajustar las políticas a las necesidades de cada empresa.

CAPÍTULO 6. PROPUESTA

6.1 Tema

Diseño de Políticas Informáticas de Seguridad Informática en el sector de Telefonía Móvil en el Ecuador.

6.2 Datos Informativos

Institución: Telefonía Móvil del Ecuador (Claro, Movistar, CNT)
Beneficiarios: Usuarios de la Telefonía Móvil del Ecuador
Responsable: Ing. Cristián Lozada
Director: Ing. Fabián Hurtado V., MGS.

6.3 Antecedentes de la propuesta

Tomando en cuenta las vulnerabilidades en la seguridad de la información planteo crear un Diseño de Políticas Informáticas de Seguridad Informática en el sector de Telefonía Móvil del Ecuador basadas en la Certificación ISO/IEC 27001:2013, misma que facilitará los requisitos que se deben adoptar las instituciones para poder implementar un Sistema de Gestión de Seguridad de la Información, con lo que se podrá mantener la información de la organización de una forma segura ante cualquier posible amenaza, además para atender los requerimientos de los usuarios planteo diseñar una estructura de Service Desk basado en la "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de redes y servicios de telecomunicaciones" que están establecidas por la ARCOTEL.

La gestión de la información debe estar amparada en tres pilares que son, ***confidencialidad, integridad y disponibilidad***, la cual aplica barreras y procedimientos que aseguran el acceso a la información y sólo permite acceder a las personas autorizadas. Las grandes empresas manejan un enorme volumen de datos que son procesados, almacenados y transmitidos y consideran que la información es un bien muy importante y se considera como prioritario.

6.4 Justificación

Se considera que es importante el diseño de Políticas Informáticas de Seguridad Informática en el sector de Telefonía Móvil en Ecuador con la implementación de un Service Desk puesto que la información es uno de los activos más importantes de una institución, constituyéndose en un factor crítico para la supervivencia de las organizaciones. El diseño permitirá proteger de mejor manera la integridad y la privacidad de la información almacenada en el sistema informático de las instituciones, además se ocupa de establecer los procedimientos, métodos y técnicas, orientados a proveer condiciones seguras de acceso a los datos.

6.5 Objetivos

6.5.1 Objetivo General

Establecer Políticas Informáticas de Seguridad de la información en el sector de Telefonía Móvil en Ecuador.

6.5.2 Objetivo Específicos

- Analizar la seguridad de la información implementada en los servicios informáticos que prestan las instituciones de la telefonía móvil del Ecuador.
- Determinar las soluciones tecnológicas para brindar la seguridad en la información en las diferentes telefonías móviles del Ecuador.
- Diseñar un modelo de políticas informáticas de seguridad de la información para el sector de Telefonía Móvil en el Ecuador basado en la certificación ISO/IEC 27001:2013 y realizar un Service Desk basado en la “Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de redes y servicios de telecomunicaciones” que están establecidas por la ARCOTEL.

6.6 Análisis de Factibilidad

6.6.1 Factibilidad operativa

La propuesta tecnológica es factible puesto que se cuenta con la información necesaria referente al tema de investigación y con la colaboración del personal que labora en las instituciones de la Telefonía Móvil del Ecuador.

6.6.2 Factibilidad económica

La propuesta tecnológica es totalmente factible económicamente hablando, ya que no representa un gasto adicional respecto al implementar un diseño de políticas informáticas y propuesta al diseñar una estructura de Service Desk. Sin embargo, aplicar el diseño propuesta, si representa un beneficio ya que se implementa políticas de seguridad de información.

6.6.3 Factibilidad legal

La propuesta tecnológica es factible legalmente ya que se enmarca en lo establecido en la Ley Orgánica de Telecomunicaciones, la cual regula el uso y explotación del espectro radioeléctrico en el Ecuador. (Ley Orgánica de Telecomunicaciones, 2015)

6.6.4 Fundamentación

SEGU.INFO (2017) afirma que el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

La Seguridad Informática permite compartir los sistemas de información de la empresa entre sus empleados, e incluso con terceros, pero garantizando su protección.

6.7 Metodología, modelo operativo

6.7.1 Estudio de los sistemas informáticos de las telefonías móviles del Ecuador

Las empresas de telefonía móvil en el Ecuador tienen sus propias políticas de seguridad de la información por parte de los usuarios basadas en la certificación ISO/IEC 27001:2013. En las páginas web oficiales www.miclaro.com.ec, www.movistar.com.ec, www.cnt.gob.ec se describen las políticas de seguridad y privacidad con respecto al acceso, disponibilidad y tratamiento de información de los diferentes servicios que ofrecen las compañías. Un aspecto importante es que los usuarios pueden acceder a los servicios informáticos de cada compañía siempre y cuando este bien registrados siguiendo filtros adecuados y contraseñas cifradas.

Por otra, según el estudio realizado en este proyecto se pudo determinar que las compañías utilizan paquetes informáticos de software que permiten eliminar el software malicioso, amenazas del internet y permiten la protección contra hackers o fallo en algunas páginas web, sin embargo, a pesar de esto existen vulnerabilidades en la seguridad de información, es por es que como se plantea ciertas políticas de seguridad que permitirá mejorar la seguridad informática en los medios tecnológicos de estas compañías.

6.7.2 Soluciones informáticas para la seguridad de la información

La norma ISO/IEC 27001:2013 presenta medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza o código malicioso, de forma que se garantice en todo momento la continuidad de las actividades de la empresa. El objetivo del Sistema de Gestión de Seguridad de la Información (SGSI) es preservar la información en cuanto a la confidencialidad, integridad y la disponibilidad de la información. (ISO, 2019)

La metodología que presenta la norma ISO /IEC 27001:1300 es la siguiente:

1. Identificar los activos de información y sus responsables

2. Identificar las vulnerabilidades de cada activo
3. Identificar las amenazas
4. Identificar los requisitos legales y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores
5. Identificar los riesgos
6. Cálculo del riesgo
7. Plan de tratamiento del riesgo

6.7.3 Políticas informáticas de seguridad de la información para las empresas de telefonía móvil

Para el diseño de las políticas de seguridad se tomó en cuenta las vulnerabilidades y los riesgos existes en el tratamiento de la información de las compañías móviles del país.

Tabla 18. Vulnerabilidades más importantes identificadas en las empresas de telecomunicaciones

Vulnerabilidades	Descripción
Software malicioso o virus	Software malicioso "ransomware" que afecta a las redes informáticas y a los sistemas operativos. Fraude de IP-PBX, es un delito informático en el que las personas no autorizadas utilizan el servicio de llamadas locales y celulares
Fallas en las cuentas de usuario	Las empresas de telecomunicaciones no pueden asegurar en su totalidad que el usuario que accede a los servicios sea el titular de la cuenta.
Largos tiempos en el acceso a los datos	Principalmente el tiempo de acceso a los datos se da debido a la falta de cobertura a nivel nacional. Debido a la alta latencia en la red del proveedor de servicios, congestión del canal de internet.

Fuente: Investigación propia (Empresas de telecomunicaciones)
Elaborado por: Lozada Cristian (2018)

6.7.3.1 Administrar la seguridad de las Tecnologías de Información (TI)

- Desarrollar una independencia total del entorno de las TI, lo que podría en ciertas circunstancias delimitar su accionar para conseguir los objetivos de seguridad se cumplan dentro de las organizaciones de telefonía en el país.

- Realizar una alineación de los objetivos de negocio, objetivos de la Gerencia Nacional de TI y con los objetivos de seguridad, en la cual permite guiar las acciones de las tareas y labores del plan de seguridad.

- Realizar un análisis de riesgo tecnológico y organizacional para medir el riesgo y poderlo mejorar.

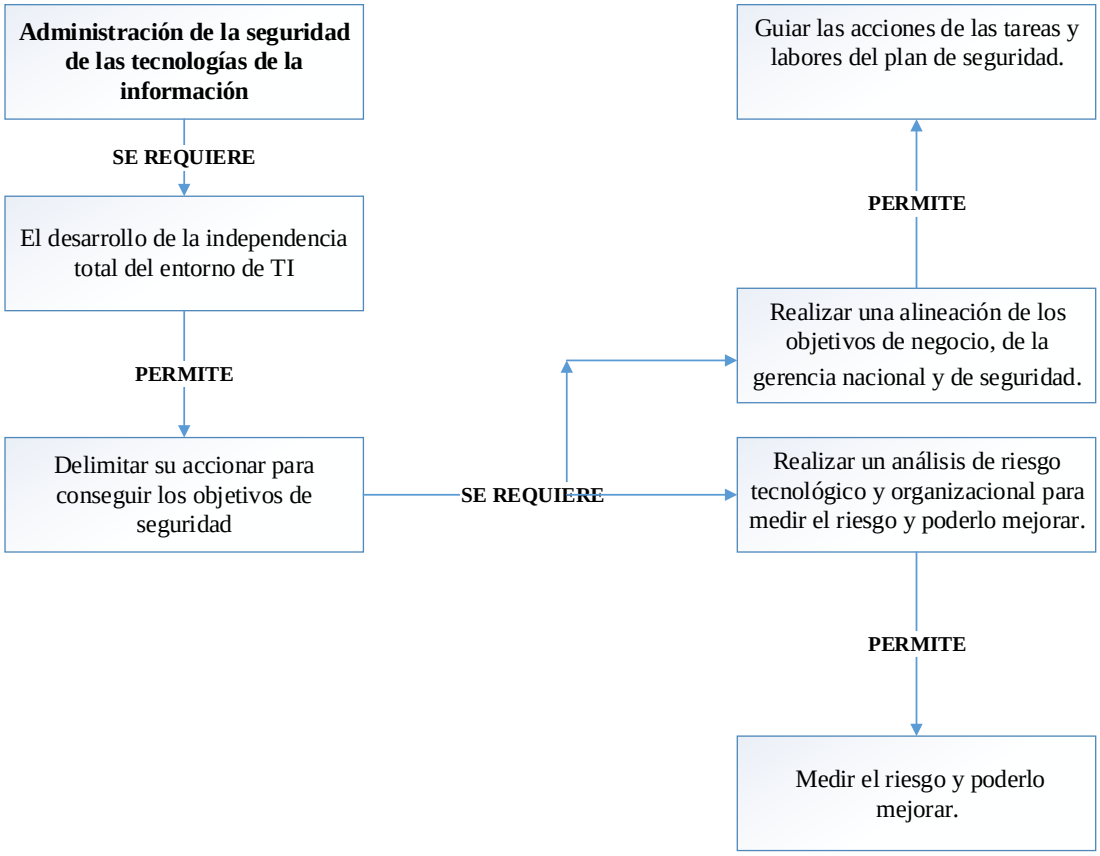

Figura 2. Flujograma de Administración de la seguridad de las Tecnologías de la Información (TI)
Elaborado por: Lozada Cristian (2018)

6.7.3.2 Plan de seguridad de las Tecnologías de Información (TI)

- Mejorar las políticas de seguridad informática para las organizaciones de telefonía.
- Implementar levantamientos de procesos en cuanto a la gerencia nacional de TI para fomentar una adecuada segregación de funciones y establecimientos de roles para cada empleado, mejorando los controles en los procedimientos, así como la mejora en la falta de revisión periódica.
- Difundir los procedimientos y políticas mediante correo electrónico para mejorar la seguridad de la información enviada.

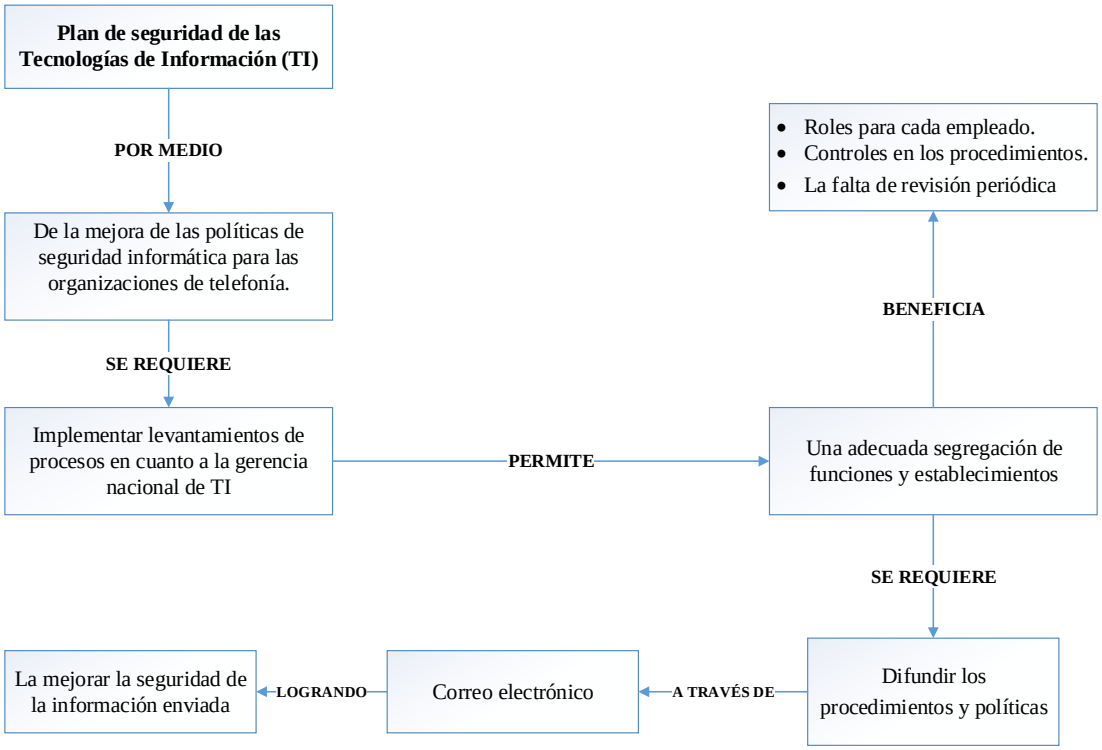

Figura 3. Flujograma plan de seguridad de las Tecnologías de Información TI
Elaborado por: Lozada Cristian (2018)

6.7.3.3 Administración de identidades

- Mejorar la estandarización de nombres de usuario con las aplicaciones organizacionales.
- Generar aportaciones formales de permisos de acceso a cada trabajador
- Socializar documentación de evidencia con las responsabilidades específicas.

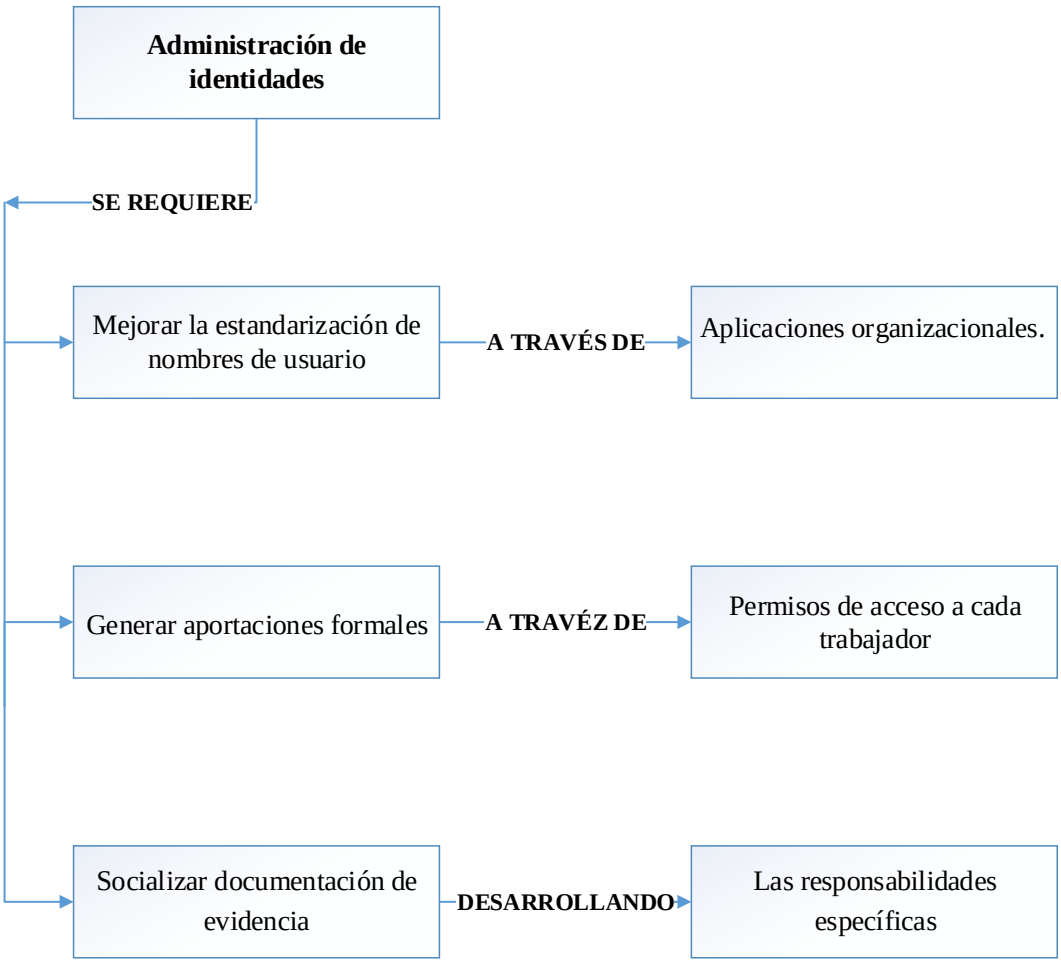

Figura 4. Flujograma de administración de identidades
Elaborado por: Lozada Cristian (2018)

6.7.3.4 Administración de las cuentas de usuario

- Continuar utilizando cuentas de usuario de manera individual y no compartida dentro de las organizaciones de telefonía.
- Desarrollar un estándar de nombres de usuario para evitar réplicas de usuarios y fomentar el uso individual de la persona.
- Para el uso de aplicaciones de las instituciones de telefonía se debe tener en cuenta las siguientes características de seguridad
    - Autenticación para red y sistemas
    - Autenticación por tablas de base de datos
    - Sistema autenticación para el acceso Wireless.

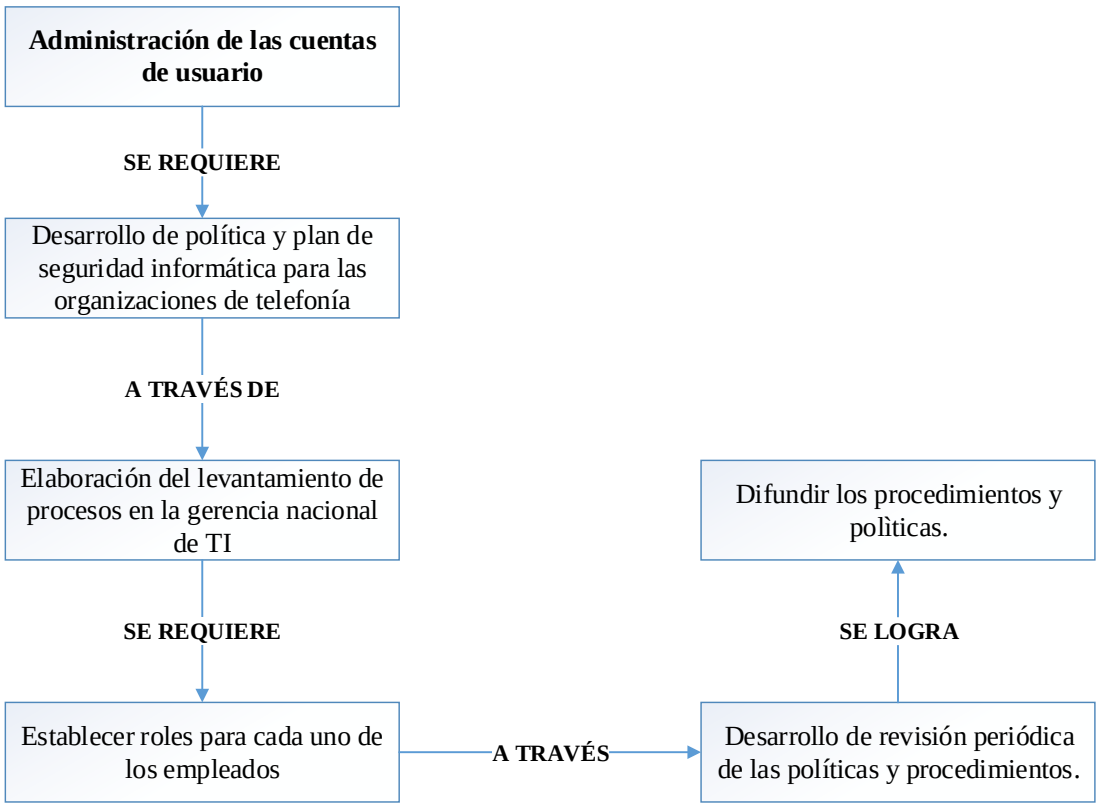

Figura 5. Flujograma de Administración de las cuentas de usuario
Elaborado por: Lozada Cristian (2018)

6.7.3.5 Pruebas, vigilancia y monitoreo de la seguridad

- Desarrollar pruebas continuas de funcionamiento de los sistemas implantados en las organizaciones.
- Desarrollar controles de seguridad, que permitan la detección temprana de eventos con anomalías de los cuales se reconozca con facilidad y evitar hackeos de información en la organización.
- Monitorear la seguridad implantada en las organizaciones.

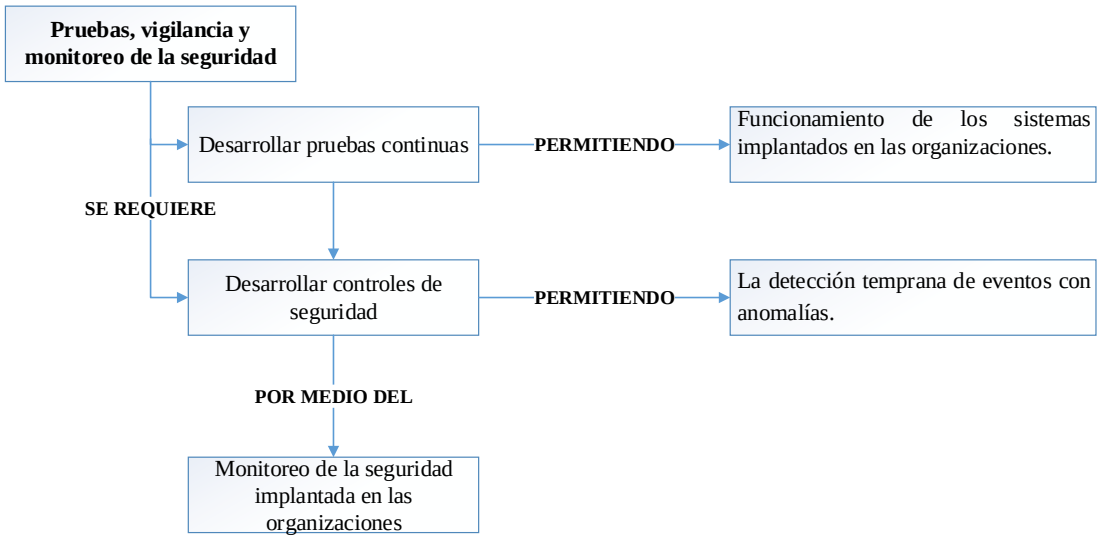

Figura 6. Flujograma de pruebas, vigilancia y monitoreo de la seguridad
Elaborado por: Lozada Cristian (2018)

6.7.3.6 Definición de incidente de seguridad

- Desarrollar de un procedimiento de manejo de incidentes de seguridad donde se determinen los criterios bajo los cuales se establecen o clasifican los incidentes de seguridad
- Elaborar políticas y guías que permitan manejar los incidentes suscitados.

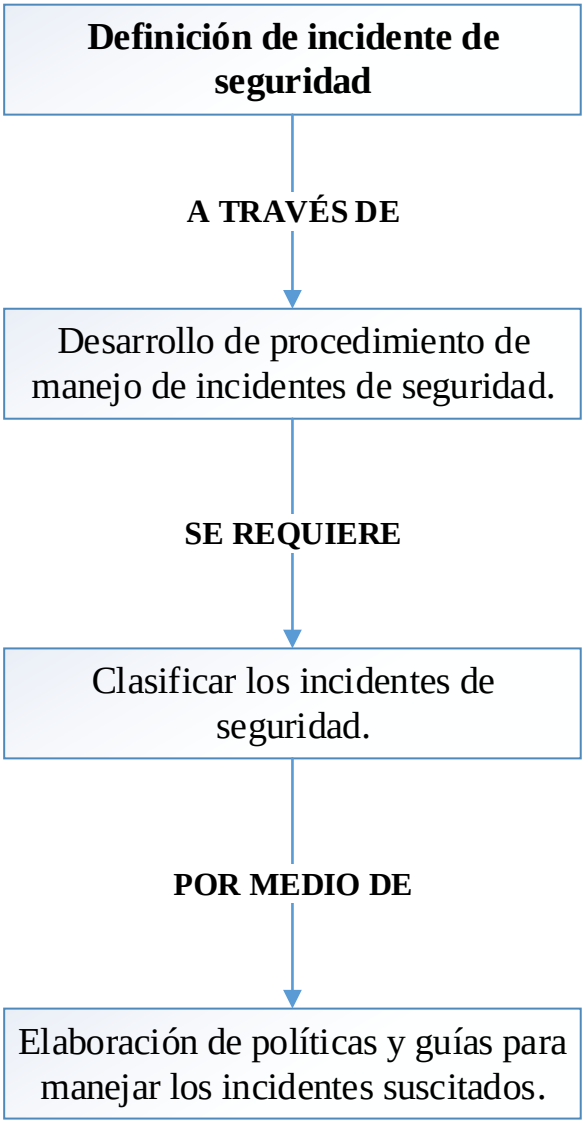

Figura 7. Flujograma para incidentes de seguridad
Elaborado por: Lozada Cristian (2018)

6.7.3.7 Protección de la tecnología de seguridad

- Se debe realizar una recopilación de información documentada con fines de seguridad de equipos en la red como firewalls y el IPS.
- Desarrollo de un sistema de tecnologías de información.

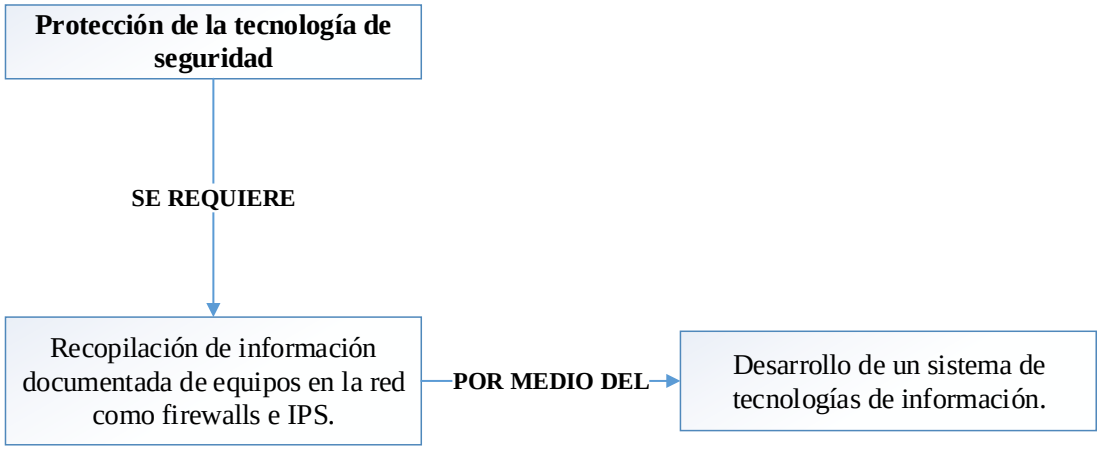

Figura 8. Flujograma para protección de la tecnología de seguridad
Elaborado por: Lozada Cristian (2018)

6.7.3.8 Administración de llaves criptográficas

- Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.
- En este aspecto, no es de gran importancia consideran los aspectos tecnológicos y que las organizaciones de análisis no se enfocan en llaves criptográficas.

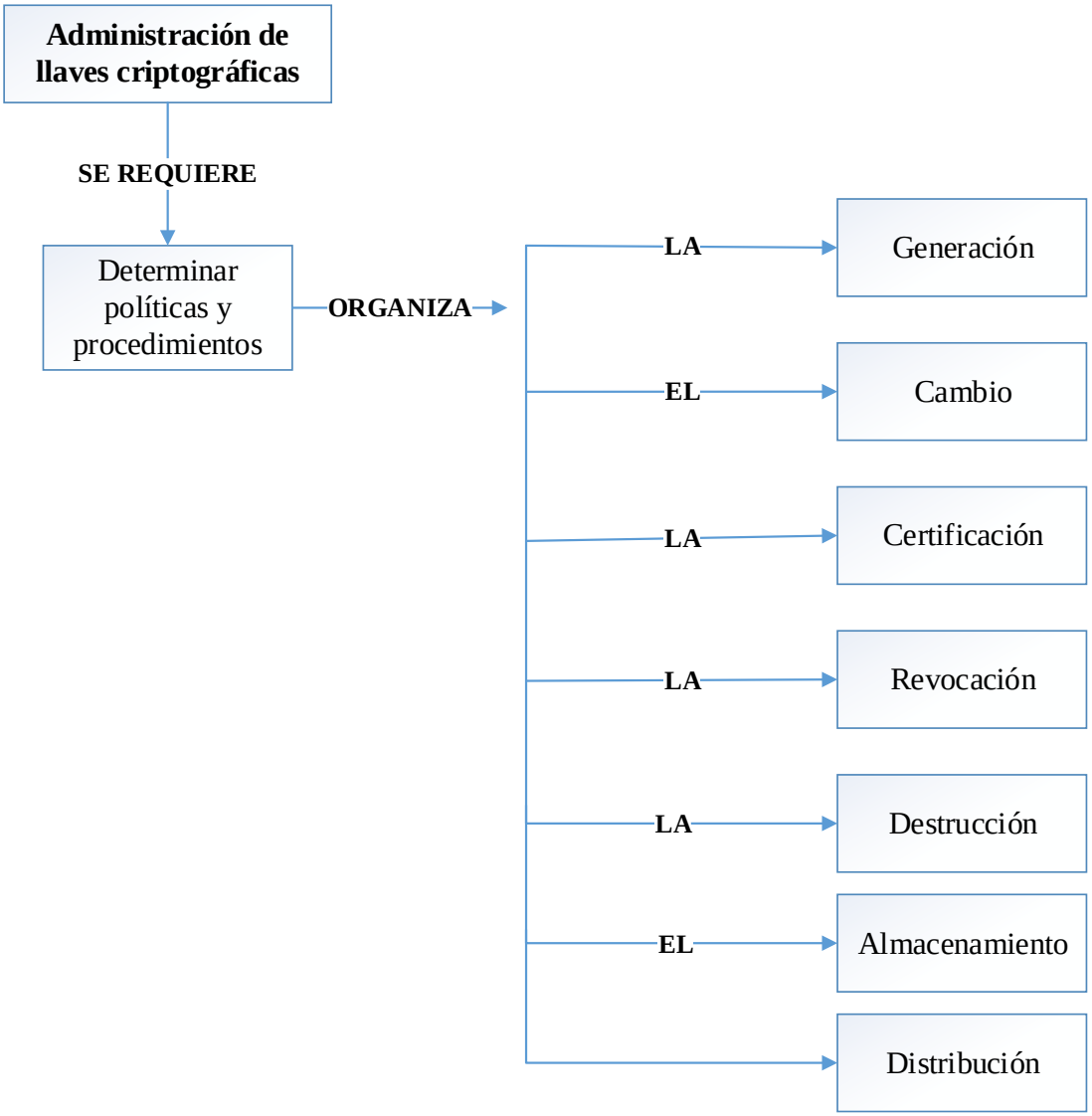

Figura 9. Flujograma para Administración de llaves criptográficas
Elaborado por: Lozada Cristian (2018)

6.7.3.9 Prevención, detección y corrección de software malicioso

- Tener un antivirus actualizado, para evitar el ingreso de malware que puede hackear información de las organizaciones de telefonía, ya que representan situaciones de difícil desarrollo.
- Implementar una revisión de software cada cierto tiempo.
- Desarrollo de políticas de parches de seguridad para establecer controles y niveles de riesgo óptimos para cada servidor de la organización.

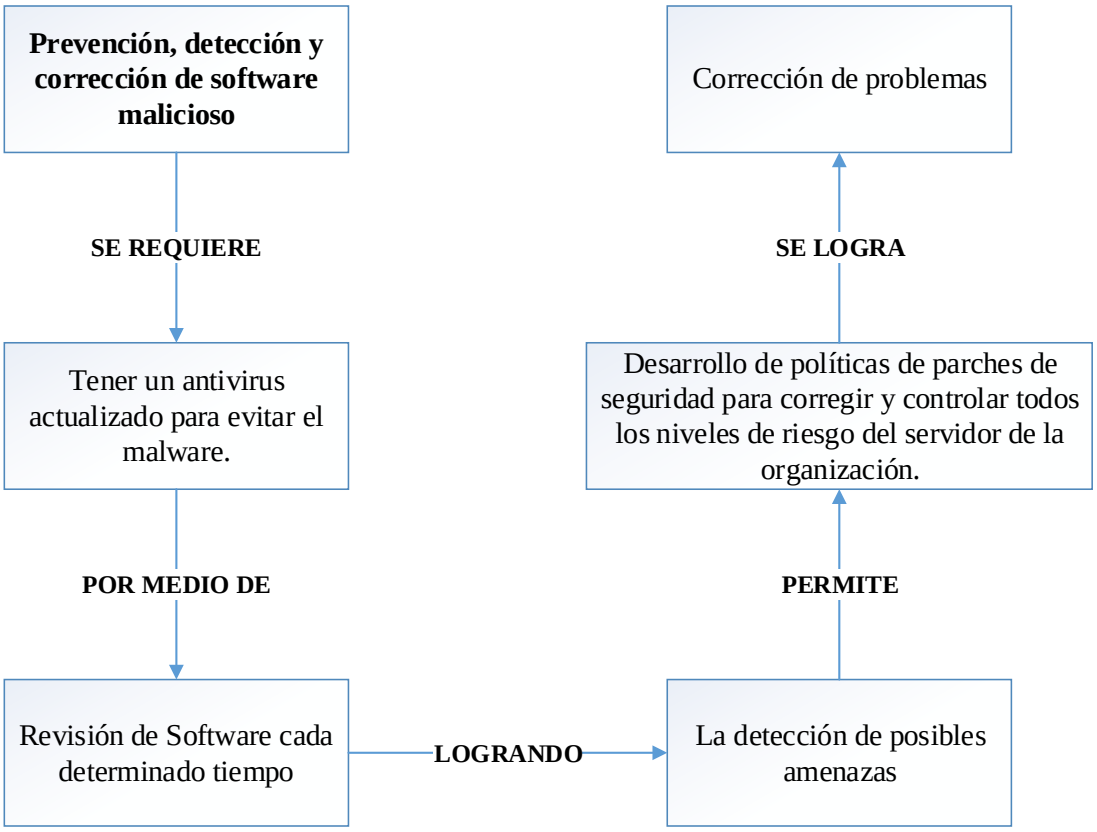

Figura 10. Flujograma Prevención, detección y corrección de software malicioso
Elaborado por: Lozada Cristian (2018)

6.7.3.10 Seguridad de la red garantizada

- Llevar a cabo un diseño de la red con un enfoque en desempeño más que con un enfoque de la seguridad.

- Desarrollar políticas de control de acceso a la red.
- Implementar herramientas que restrinjan el acceso a la red de compañías autorizadas.

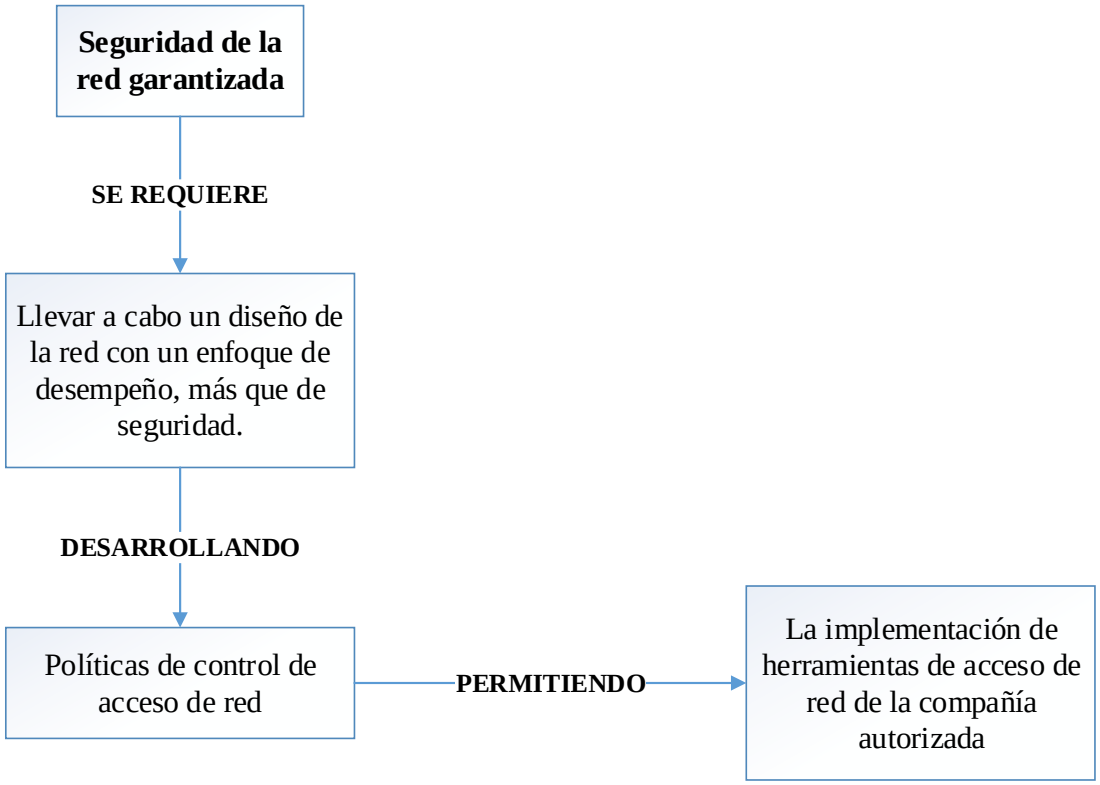

Figura 11. Flujograma Seguridad de la red Garantizada
Elaborado por: Lozada Cristian (2018)

6.7.3.11 Intercambio de datos sensibles

- Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción.
- Se debe realizar una clasificación de criticidad a nivel gerencial de las transacciones e intercambio sensible.

En base a todas las directrices tomadas en cuenta para el desarrollo de esta propuesta está basado en la socialización de los elementos dentro de las organizaciones de telefonía.

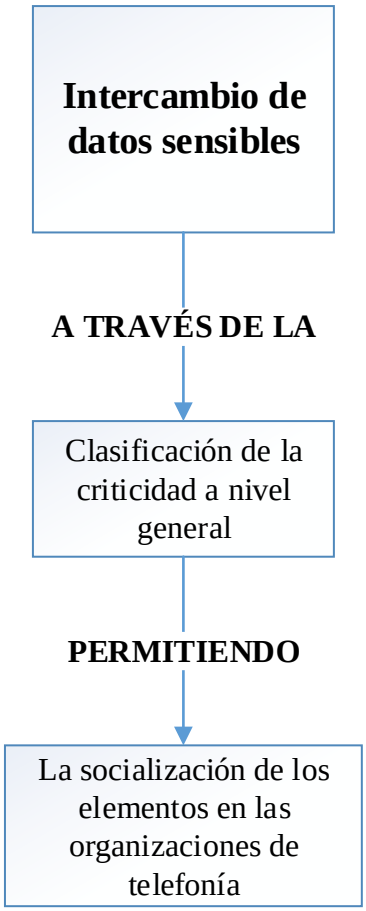

Figura 12. Flujograma intercambio de datos sensitivos
Elaborado por: Lozada Cristian (2018)

6.7.4 Diseño de un Service Desk

El diseño de una estructura de Service Desk o mesa de servicios en las empresas de telefonía móvil permitirá crear un punto principal de contacto del Departamento de Tecnología y Comunicación (TI) y los usuarios para la entrega de servicios, dicho punto permitirá brindar el servicio en el menor tiempo posible, y se facilitará el registro de todas las actividades realizadas, controlar el catálogo de servicios mediante la actualización y mejoramiento de los mismos, además permitirá la creación de informes de desempeño.

El Service Desk estará enmarcado en el informe emitido por Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL, 2017), que pone de manifiesto la

“Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicio de telecomunicaciones”, la cual establece medidas de seguridad de información enmarcadas en la Ley orgánica de las telecomunicaciones y protección de datos, Título VIII “Secreto de las comunicaciones y protección de datos” y en el Reglamento General a la Ley Orgánica de Telecomunicaciones, Título XV “Secreto de la comunicación y protección de Datos”.

Por medio del Service Desk se adoptarán medidas técnicas y de gestión, adecuadas para preservar la seguridad de los servicios y la invulnerabilidad de la red, de esta manera garantizar el secreto de las comunicaciones y de la información que es transmitida por las redes de telecomunicaciones. Estas medidas garantizarán un nivel de seguridad adecuado a un determinado riesgo.

Las empresas de telefonía móvil deben proporcionar medidas técnicas de seguridad e invulnerabilidad para preservar la seguridad de sus servicios y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes.

6.7.4.1 Aplicación del Service Desk

6.7.4.1.1 Introducción

Para las empresas telefónicas se propone la implementación de un Service Desk Distribuido, debido a que estas empresas son muy grandes y mantienen grandes cantidades de usuarios, por esta razón se ha limitado a un estudio general que abarque solamente la ciudad de Quito con una matriz para lo cual se determina las características del Service Desk Distribuido que será el objetivo a cumplir con la presente investigación.

6.7.4.1.2 Objetivos

- Diseñar un modelo de service desk que permita la recepción, clasificación y registro de incidentes, con la finalidad de gestionarlos de manera eficiente.
- Determinar el personal idóneo para resolver incidentes puntuales, de forma rápida.
- Crear FAQs (preguntas frecuentes) de acceso a la información de los incidentes para dar soluciones definitivas.
- Ubicar como punto principal una oficina matriz, para el ingreso del servidor del Service Desk Virtual y para la base de conocimiento.
- Mantener SLAs para la atención a los clientes y usuarios.
- Administrar un Service Desk en las oficinas matrices de las telefónicas que puedan atender los requerimientos de los clientes.

6.7.4.2 Service Desk Distribuido

En la siguiente figura se describe los elementos que conformarán el Service Desk Distribuido, el cual tendrá la mesa de apoyo (con los operarios) y el Service Desk Virtual, todos estos ubicados en la matriz de cada compañía telefónica.

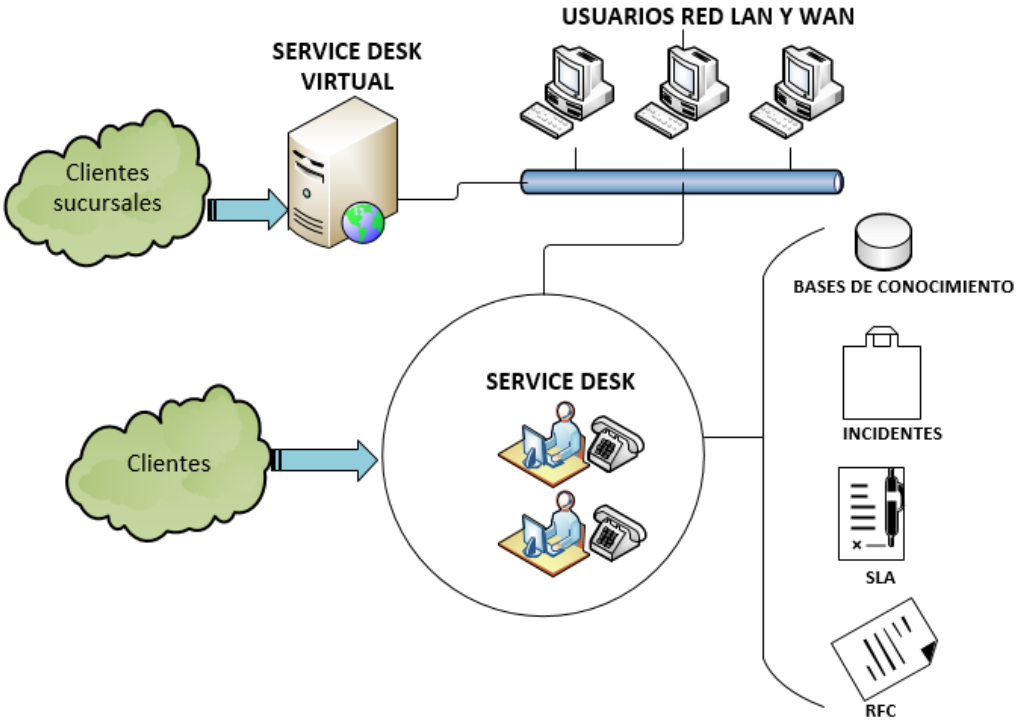

Figura 13. Descripción física del Service Desk Distribuido
Elaborado por: Lozada Cristian (2018)

Como se puede observar en la figura anterior el Service Desk Distribuido constará de un Service Desk Virtual que mantendrá un acceso fácil por parte de la Red LAN y WAN respectivamente, el Service Desk Físico que constará con dos mesas de apoyo, con acceso telefónico, el cuál manejará las KB (Bases de Conocimiento), atenderá y dará solución a los incidentes reportadas por teléfono o vía Web, además dará a conocer servicios SLA.

A continuación, se describen detalladamente cada uno de los elementos que interviene en el Service Desk Distribuido:

Service Desk Físico: Estará compuesto con dos mesas de apoyo, el cual tendrá bases de conocimiento, atenderá y dará soluciones a los incidentes solicitados por los clientes y usuarios ya sea por vía web o telefónica.

Service Desk Virtual: Receptará las inquietudes de los clientes de las diferentes sucursales de las compañías y todos los requerimientos se centralizará en el Service Desk físico a través de la red LAN y WAN para buscar las soluciones respectivas.

Bases de conocimiento (KB): Es una base de datos donde se encuentra almacenada la información referente a los incidentes, problemas y a las posibles soluciones a los mismos, así como también las preguntas frecuentes realizadas por los clientes.

Incidentes: Está constituido por todos los incidentes, problemas o fallos que identificados por los clientes o usuarios en las aplicaciones de escritorio o en los servicios prestados por las compañías telefónicas.

Acuerdos de Niveles de Servicio (SLA): Son los acuerdos contractuales entre las empresas telefónicas que ofrecen los servicios y los clientes, aquí se define los tipos de servicios prestados y los compromisos de calidad.

Preguntas Frecuentes (RFC): Es un registro de las preguntas y opiniones realizadas por los clientes cuando tiene algún incidente en la información.

6.7.4.3 Plan Capacitación

A través de un plan de capacitación, como primera instancia se debe involucrar, a los usuarios internos, al personal responsable de service desk y líderes de procesos, en los siguientes contenidos: contenidos en ITIL v4, manejo de service desk, y sobre todo en el manejo de conflictos.

Tabla 19. Plan Capacitación

Contenido	Objetivos	Asiste
ITIL Foundation v4.0	• Adquirir formación acerca de las mejores prácticas de ITIL v4.0	• Personal de Soporte • Personal de Service Desk • Personal de Seguridad Informática • Líderes de Proceso

Gestión de Incidentes	• Conocer proceso de gestión Service Desk • Asumir responsabilidades	• Personal de Soporte • Personal de Service Desk • Personal de Seguridad Informática • Líderes de Proceso
Manejo de Conflictos	• Desarrollar habilidades en la solución de problemas	• Personal de Service Desk

Fuente: Propia
Elaborado por: Lozada Cristian (2018)

6.7.4.4 Levantamiento de Información

La base para que el proceso funcione correctamente, el cual recopila datos e información de tecnología, con el propósito de identificar con que se cuenta. Se lleva a cabo mediante el uso de instrumentos y técnicas como: entrevista, encuesta, inspecciones; previo permiso de las instancias correspondientes, otras fuentes de información como: informes, reportes de auditoria, organigramas, manuales y procedimientos.

El acceso a la información es primordial por lo cual se debe emplear plantillas para el levantamiento de información como podemos revisar en el formato de inventario de hardware (Anexo 2), formato de inventario de software (Anexo 3).

Es necesario entender las actividades y roles requeridos para mantener el catálogo de servicios, entender las opciones que tecnología dispone para crear, implementar y mantener la organización, por lo mencionado es necesario establecer el catálogo de servicios (Anexo 4).

Cuando se brinda un servicio entre una empresa y un proveedor, se establecen los niveles de calidad (Anexo 5) o el alcance de servicio acorde a los requerimientos solicitados, los acuerdos de servicio también pueden ser establecidos entre procesos internos, importante definir métricas, para luego verificar si se está cumpliendo con lo establecido. El catálogo de servicio sin duda alguna es el punto de partida para el

service desk, pudiendo hacer los ajustes necesarios que permitan evidenciar mejoras.

6.7.4.5 Medios Solicitud de Servicio

El acceso a la atención del Service Desk se realizará a través de: Vía Telefónica, vía web por medio de las FAQs (Preguntas Frecuentes), vía email, trámite documentario y vía chat para reportar el incidente, y obtener una solución.

6.7.4.5.1 Vía Telefónica

- Existirá un número de teléfono a disposición de los usuarios al cual podrán acceder de forma permanente en el horario laboral previamente establecido.
- El operario deberá atender el reporte de una incidencia o requerimiento y deberá ingresar la información en el Service Desk, para abrir el caso respectivo
- Para resolver el incidente primero se deberá buscar FAQs (preguntas frecuentes), la existencia de un caso similar reportado anteriormente y resolverlo.
- Si no existe el incidente en la Base de Conocimientos de las FAQs el operario deberá proceder con la resolución inmediata del caso abierto, posteriormente, registrará, el incidente con la solución del mismo de forma rápida.
- Si el operario no puede resolver el caso tendrá la obligación de realizar el proceso de escalado al siguiente nivel y determinar los recursos que se asignarán al mismo.
- Posteriormente deberá registrar, monitorear el incidente e informar al usuario que la solución está dada, y posteriormente cerrar el caso.
- El operario mantendrá herramientas de Gestión Remota para resolver incidentes de ser necesario el acceder al equipo del usuario para dar una solución al requerimiento presentado.

6.7.4.5.2 Vía WEB

- El Service Desk Virtual mantendrá un acceso mediante la Web para la Matriz o cualquiera de sus sucursales.

- El Service Desk puede ser accedido por cualquier usuario desde la matriz o desde las sucursales las 24 horas del día.
- El usuario tendrá un acceso rápido y sencillo a resolver cualquier incidente que se encuentre en las FAQs.
- Al no poder resolver el incidente, el usuario deberá ingresar el incidente con las características del mismo.
- Los operarios tendrán la obligación de revisar los incidentes que le reporten por este medio.
- Se mantendrá diferentes formularios dependiendo de la aplicación o requerimiento de los clientes, usuarios y proveedores.

6.7.4.5.2.1 FAQs

Cuando los incidentes son reportados por vía Web o vía Telefónica, el acceso a las FAQs (Anexo 6) es uno de los principales aspectos a tomar en cuenta, por tal razón los usuarios deberán encontrar información a sus requerimientos con un lenguaje fácil que ellos puedan comprender sin necesidad de tener mucho conocimiento en informática, su metodología deberá ayudarlo a resolver fácilmente los incidentes, el operario que tiene un mayor conocimiento deberá manejar una FAQ más completa, con metodologías.

6.7.4.5.3 Vía email

- Existirá un correo a disposición de los usuarios al cual podrán enviar la descripción del incidente de forma permanente en el horario laboral previamente establecido.
- El operario deberá atender el email o requerimiento y deberá ingresar la información en el Service Desk, para abrir el caso respectivo
- Para resolver el incidente primero se puede responder enlace posible solución FAQs (preguntas frecuentes) y resolverlo.
- Si no existe el incidente en la Base de Conocimientos de las FAQs el operario deberá proceder con la resolución inmediata del caso abierto, posteriormente,

registrará, el incidente con la solución del mismo de forma rápida.

- Si el operario no puede resolver el caso tendrá la obligación de realizar el proceso de escalado al siguiente nivel y determinar los recursos que se asignarán al mismo.
- Posteriormente deberá registrar, monitorear el incidente e informar al usuario que la solución está dada, y posteriormente cerrar el caso.
- El operario mantendrá herramientas de Gestión Remota para resolver incidentes de ser necesario el acceder al equipo del usuario para dar una solución al requerimiento presentado.

6.7.4.5.4 Vía trámite documentario

- A través de un formato (ANEXO 7) a disposición de los usuarios al cual podrán acceder de forma permanente en el horario laboral previamente establecido.
- El operario deberá atender el reporte de una incidencia o requerimiento y deberá ingresar la información en el Service Desk, para abrir el caso respectivo
- Para resolver el incidente primero se deberá buscar FAQs (preguntas frecuentes), la existencia de un caso similar reportado anteriormente y resolverlo.
- Si no existe el incidente en la Base de Conocimientos de las FAQs el operario deberá proceder con la resolución inmediata del caso abierto, posteriormente, registrará, el incidente con la solución del mismo de forma rápida.
- Si el operario no puede resolver el caso tendrá la obligación de realizar el proceso de escalado al siguiente nivel y determinar los recursos que se asignarán al mismo.
- Posteriormente deberá registrar, monitorear el incidente e informar al usuario que la solución está dada, y posteriormente cerrar el caso.
- El operario mantendrá herramientas de Gestión Remota para resolver incidentes de ser necesario el acceder al equipo del usuario para dar una solución al requerimiento presentado.

6.7.4.5.5 Vía chat

- El Service Desk Virtual mantendrá un acceso mediante el chat para la Matriz o cualquiera de sus sucursales.
- El Service Desk puede ser accedido por cualquier usuario desde la matriz o desde las sucursales, sin embargó las respuestas serán realizadas en horas laborables de los operarios.
- Al no poder resolver el incidente, el operario deberá ingresar el incidente con las características del mismo.
- Los operarios tendrán la obligación de revisar los incidentes que le reporten por este medio.
- Se mantendrá diferentes formularios dependiendo de la aplicación o requerimiento de los clientes, usuarios y proveedores.

6.7.4.6 Perfil de operarios

A continuación, se detalla características que deben poseer un perfil TI, para el área de la gestión de incidencias:

- Tener conocimiento en informática.
- Conocer las políticas de seguridad de la información de las empresas telefónicas.
- Seguridad de ingreso a terceros
- Conocimiento en la gestión de outsourcing
- Tener conocimiento en Redes de Computadoras
- Conocimiento en Gestión de riesgos
- Manejo de las partes interesadas o afectadas
- Control y seguimiento
- Trabajo en equipo
- Conocimiento en Gestión del cambio
- Deben conocer los métodos, para el manejo de información sobre las incidencias, o requerimientos que son ingresados a las mesas de apoyo por

cualquiera de los medios.

- Saber el momento en el que se debe realizar un escalado y no hacerlo de forma innecesaria.
- Conocer el uso de las herramientas a ser usadas tanto para el Service Desk.
- Tener dominio en el manejo de conflictos.

Perfil propuesto manejo de Incidencias, Responsable Jefe o Gestor de Incidentes, seguido de personal como analista de incidente, quienes se contactarán con expertos en temas que no puedan solucionar, así mismo, serán quienes se contacten con proveedores, cuando sea necesario.

Figura 14. Organigrama Service Desk
Elaborado por: Lozada Cristian (2018)

6.7.4.6.1 Jefe o Gestor de incidentes

El jefe o gestor de incidentes deberá cumplir con las siguientes actividades:

- Generar reportes mensuales acerca del tratamiento y gestión de incidentes.
- Asistir a reuniones cuando lo requieran.

- Verificar que se cumplan la atención de los incidentes y supervisar el trabajo que se realiza en cada etapa por el personal de soporte.
- Asegurar la eficiencia y eficacia del proceso.
- Recomendar e implementar mejoras para la gestión de incidentes.
- Programar y manejar el soporte de los incidentes.

6.7.4.6.2 Analista de Incidente

Este personal deberá cumplir con las siguientes actividades:

- Dar soporte a los incidentes.
- Registrar los incidentes.
- Guiar al grupo indicado para resolución de los incidentes.
- Proporcionar soporte inicial y clasificación de los incidentes.
- Asignación, supervisión, seguimiento, clasificación y comunicación, con los distintos niveles de servicio.
- Dar resolución a los incidentes asignados.
- Cierre de casos.

6.7.4.6.3 Experto de TI

Este personal deberá cumplir con las siguientes actividades:

- Dar soporte a los incidentes que no pueden ser resueltos en segunda línea del nivel de servicio.
- Investigar y diagnosticar los incidentes asignados.
- Detectar y registrar los posibles problemas.

6.7.4.6.4 Escalar un incidente Proveedor TI

Se deberá escalar un incidente cuando no pueden resolverlo, el cual debe estar basado en parámetros principales como:

- El número de llamadas que ingresa al Service Desk.
- Los tipos de incidentes, que no pueden ser resueltos porque implica el

involucramiento de otros niveles.

- La urgencia y el impacto que tengan los incidentes que puedan influenciar en la compañía.

6.7.4.7 Niveles de solución de los incidentes

El proceso de escalado puede resumirse gráficamente como sigue:

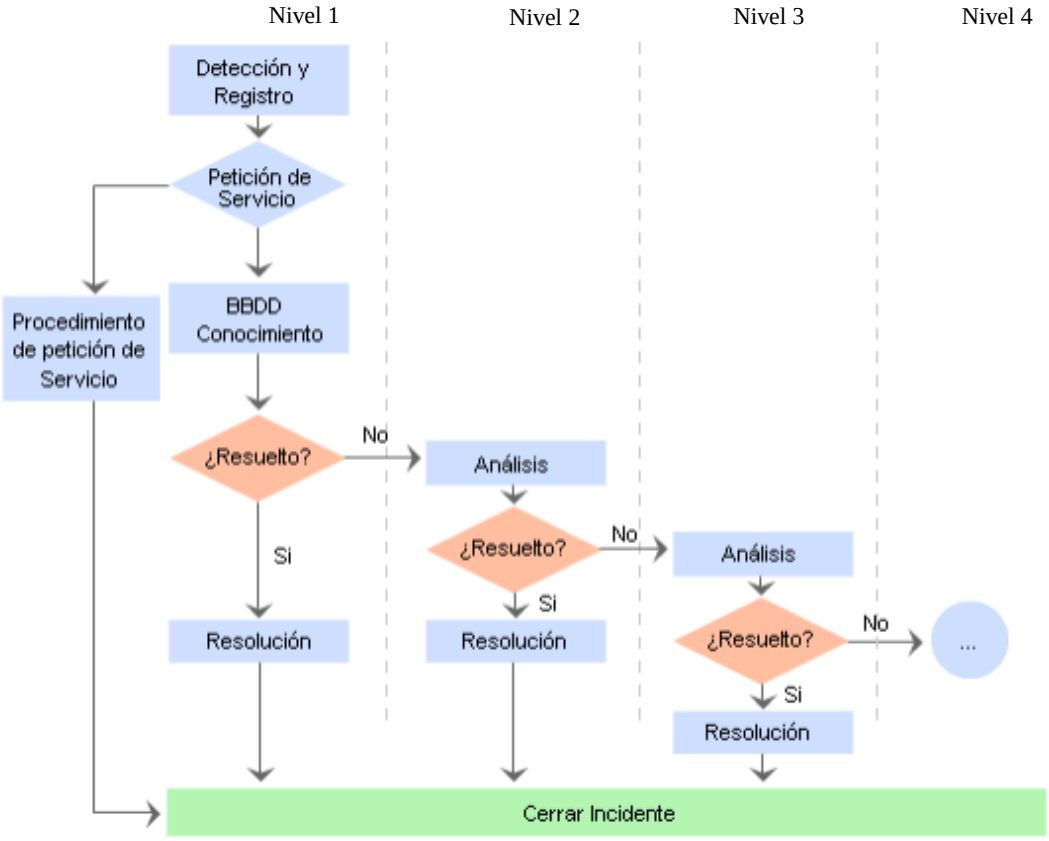

Figura 15. Niveles de Solución de los Incidentes
Elaborado por: **Lozada Cristian (2018)**

Nivel 1: Este nivel estará conformado por los elementos quienes forman el Service Desk, los soportes de incidencias por cualquiera de los medios, ya sean escritos, telefónicos, o mediante la aplicación Service Desk. Este nivel busca dar solución rápida a los incidentes, es importante atender y comprender las necesidades del cliente para ofrecer soluciones para restablecer un servicio de forma rápida y con el menor impacto al negocio.

Nivel 2: Este nivel es conocido como el de mantenimiento en el cuál se da un nivel de servicio parecido al anterior, con mayor respaldo a los incidentes que no pueden ser resueltos en el primer nivel, para las empresas telefónicas se ha visto conveniente ubicar en este nivel a los procesos de soporte de escritorio, soporte de aplicaciones, cuyas funciones estarán determinadas por conocimientos avanzados de hardware y software para la resolución de los problemas, además de dar un soporte básico de red.

Nivel 3: En este nivel se encuentra el personal de especialistas y desarrolladores, (EXPERTOS) aquí se mantendrá el mismo proceso de distribución de problemas y el tiempo de resolución de cada una de ellas, la información que posea este nivel sobre los incidentes no será tan limitada, y cada uno buscará el mejor método para dar una solución lo más pronto posible. Cuando este nivel no puede resolver el incidente o encuentra que no existe una solución, para el mismo se procederá a informar al Gestor de Incidentes para que se determine una solución adecuada.

Nivel 4: En este nivel el Gestor de Incidentes es el responsable de buscar una solución al incidente presentado, que frecuentemente es la de tratar con los proveedores de determinado servicio, para conjuntamente resolver el incidente. Cuando el incidente no pueda ser identificado será obligación de este nivel de determinar sus características para que posteriormente se sigan los procesos de elevarlo a categoría de problema y comenzar los procesos para que sea tratado por la "Gestión de Problemas".

6.7.4.8 Clasificación de los incidentes

Los incidentes se pueden generar dentro y fuera de la empresa, como se detalla a continuación:

Tabla 20. Clasificación de los Incidentes

Categoría	Descripción
Incidentes en el hardware	• En esta categoría se puede encontrar subcategorías de los equipos de cómputo, donde los usuarios

	deberán especificar el área del incidente.
Incidentes en la Software	• Dentro de esta categoría se registra toda información referente al uso de aplicaciones de escrito como procesadores de texto, hojas de cálculo y sistemas que son de uso permanente de todo el personal
Incidentes en la Red y la telefonía	• En esta categoría se registran los incidentes en los distintos dispositivos de red y los teléfonos que son de su uso frecuente de los operarios.
Incidentes en los servicios prestados a los clientes	• Dentro de esta categoría están incluidos los servicios prestados a los clientes según los acuerdos de nivel de servicio (SLA), además se incluye servicios de correo electrónico, aplicaciones externas, internet, entre otros

Fuente: Propia
Elaborado por: Lozada Cristian (2018)

Con frecuencia existen múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas, el nivel de prioridad se basa esencialmente en dos parámetros:

Tabla 21. Prioridad

Prioridad	
Impacto	• Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados, el daño que causa a la empresa.
Urgencia	• Depende del tiempo máximo acordado en el SLA, para la resolución del incidente y/o el nivel de servicio. Es la velocidad con la que la empresa necesita corregir el

	incidente.

Fuente: Propia
Elaborado por: Lozada Cristian (2018)

A través de una grafico podemos apreciar de mejor manera

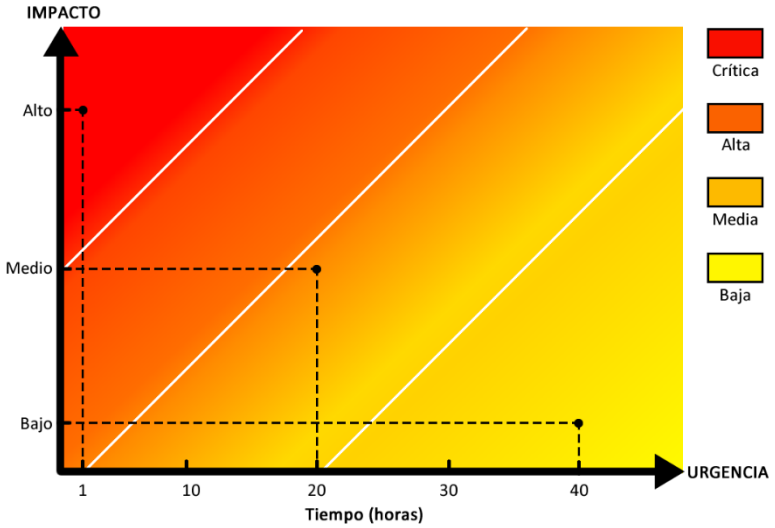

Figura 16. Prioridad del incidente
Elaborado por: Lozada Cristian (2018)

Según la norma iso 27001, la intersección de los parámetros nos permite establecer la prioridad de cada incidente, por lo que de esta forma podemos generar la siguiente tabla de valores:

Impacto / Urgencia	Alto	Medio	Bajo
Alto	1	2	3
Medio	2	3	4
Bajo	3	4	5

Figura 17. Prioridad Tabla de Valores
Elaborado por: Lozada Cristian (2018)

6.7.4.9 Diseño de la base de datos de Conocimiento KB

La base de datos de conocimiento proporciona servicio al cliente, puede contener manuales, documentos, preguntas y respuestas FAQs que permiten resolver los incidentes o problemas reportados.

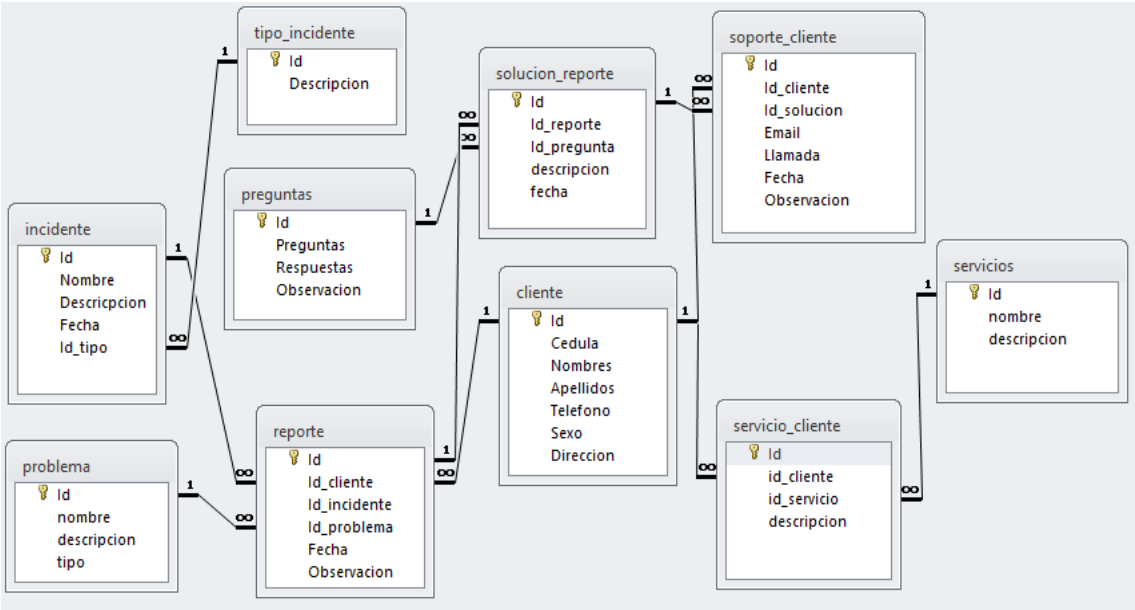

Figura 18. Diseño de la Base de Datos de Conocimiento KB
Elaborado por: Lozada Cristian (2018)

Ejemplo de incidencia "Fallos en la Red"

Una vez reportado el incidente por el usuario, este entra a la base de conocimientos la cual debe tratar de dar una solución adecuada vista que contiene información referente al incidente con un registro de preguntas, respuestas y FAQs. Una vez identificado el incidente le presenta al usuario dos alternativas de solución: conectar adecuadamente los cables de red y reiniciar computadora; si el usuario después de aplicar cualquiera de estas dos alternativas no solucionó el incidente, este se elevaría a un problema y debe ser solucionado por un administrador de sistemas.

Tabla 22. Caso de Uso del Incidente "Fallos en la Red"

Caso de Uso	Incidente “Fallos en la Red”
Actores	Usuario, Administrador de Sistemas
Descripción	1. Usuario reporta el incidente sobre fallos en la red. 2. El reporte ingresa a la base de conocimiento. 3. La base de conocimientos tiene almacenado información referente a fallos en la red y le proporciona dos soluciones: a. Conectar cables correctamente. ▪ Observar que el cable de red que está conectado a la computadora titila, caso contrario conectar y desconectar el cable nuevamente. ▪ Cuando el cable conectado nuevamente titila se tiene internet. b. Reiniciar la computadora. ▪ Reinicie o apague la computadora de manera se restablezcan los servicios de red. 4. Si estas dos alternativas no solucionan el incidente se vuelve un problema y pasa a un administrador de sistemas para que brinde la solución respectiva.

Fuente: Propia
Elaborado por: Lozada Cristian (2018)

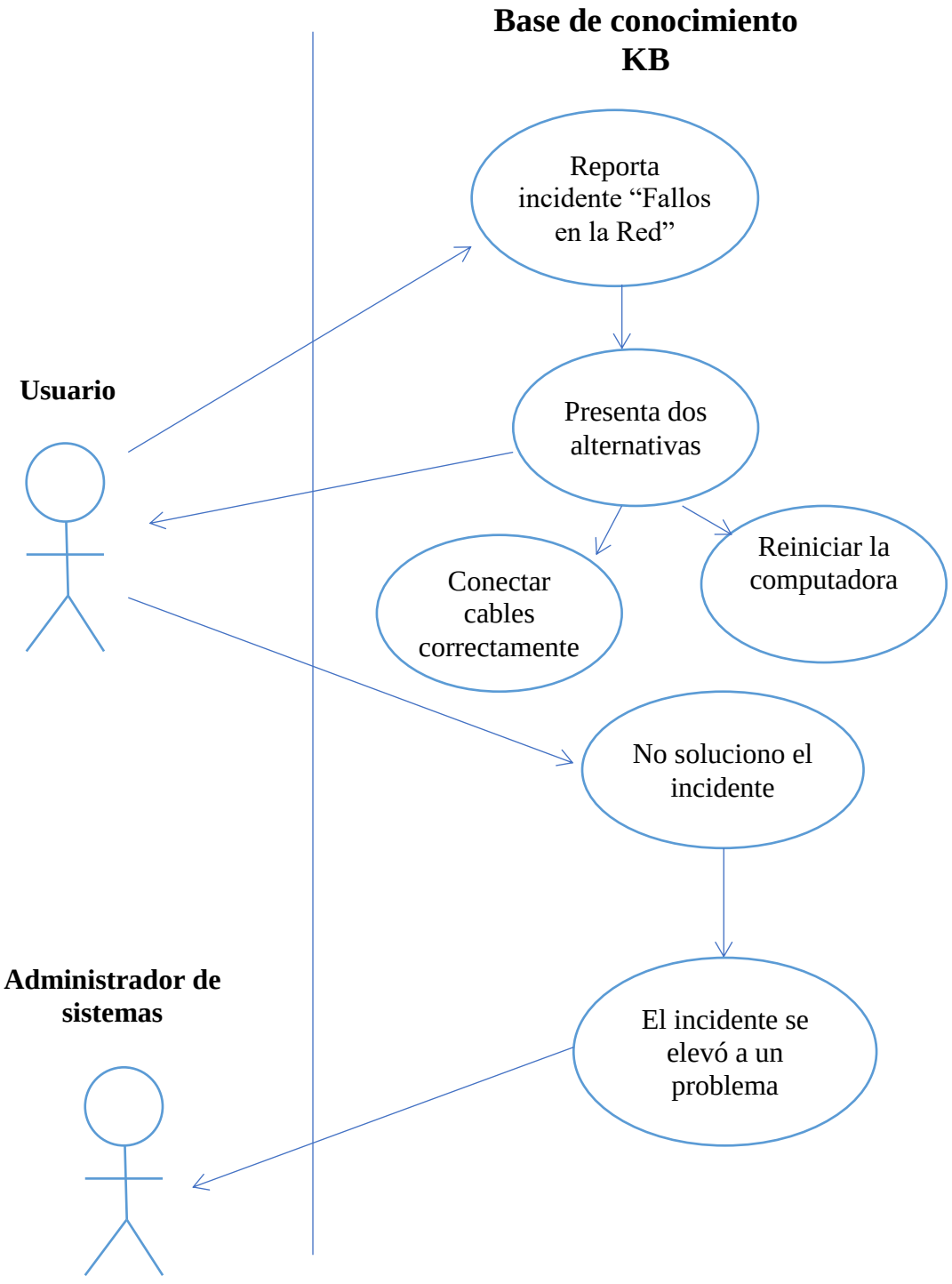

Figura 19. Diagrama de Caso de Uso “Fallos en la Red”
Elaborado por: Lozada Cristian (2018)

6.7.4.10 Diseño de la base de datos de la Gestión de Incidentes

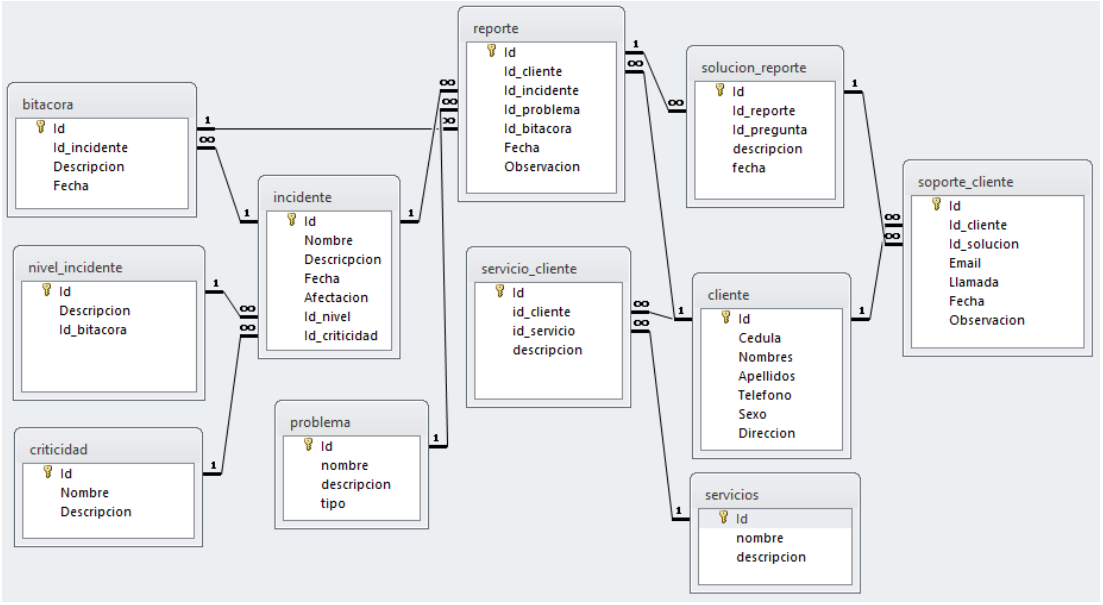

Figura 20. Diseño de la Base de Datos de Conocimiento KB
Elaborado por: Lozada Cristian (2018)

Ejemplo de Incidencia "Error al navegar por internet"

En una empresa de telefonía móvil se encuentra en la primera línea atención al cliente. Un usuario dice que cuando intenta navegar por Internet le da error e, investigando y preguntándole, averigua que las aplicaciones que utilizan Internet, como mensajería instantánea o redes sociales, tampoco funcionan.

Solución

Esto sería una incidencia se clasificaría en el primer nivel o en primera instancia, y se puede intentar resolver ya que puede haber un problema con el terminal del cliente, o a su vez se puede escalarlo por si hay una incidencia con la red en general.

Tabla 23. Caso de Uso del Incidente “Error al navegar por internet”

Caso de Uso	Incidente “Fallos en la Red”
Actores	Usuario, Administrador de Sistemas
Descripción	1. Usuario reporta el incidente sobre fallos en el internet, redes sociales y mensajería. 2. Se identifica el incidente claramente, cuanto más pronto se detecta el incidente, menos tiempo debe tener la falta de servicio, siempre y cuando se actúe inmediatamente. 3. Se clasifica al incidente en primer nivel. 4. Se determina el nivel de criticidad del incidente en las diferentes áreas. 5. Se asegura que cumpla con los servicios SLA (Service Level Agreement). 6. El sistema puede resolver el incidente puesto que idéntica que el problema es en el terminal del cliente. 7. Si no se soluciona el incidente se puede escalarlo a un segundo nivel. 8. Se escala a un segundo nivel vista que se trata de una incidencia de la red en general.

Fuente: Propia
Elaborado por: Lozada Cristian (2018)

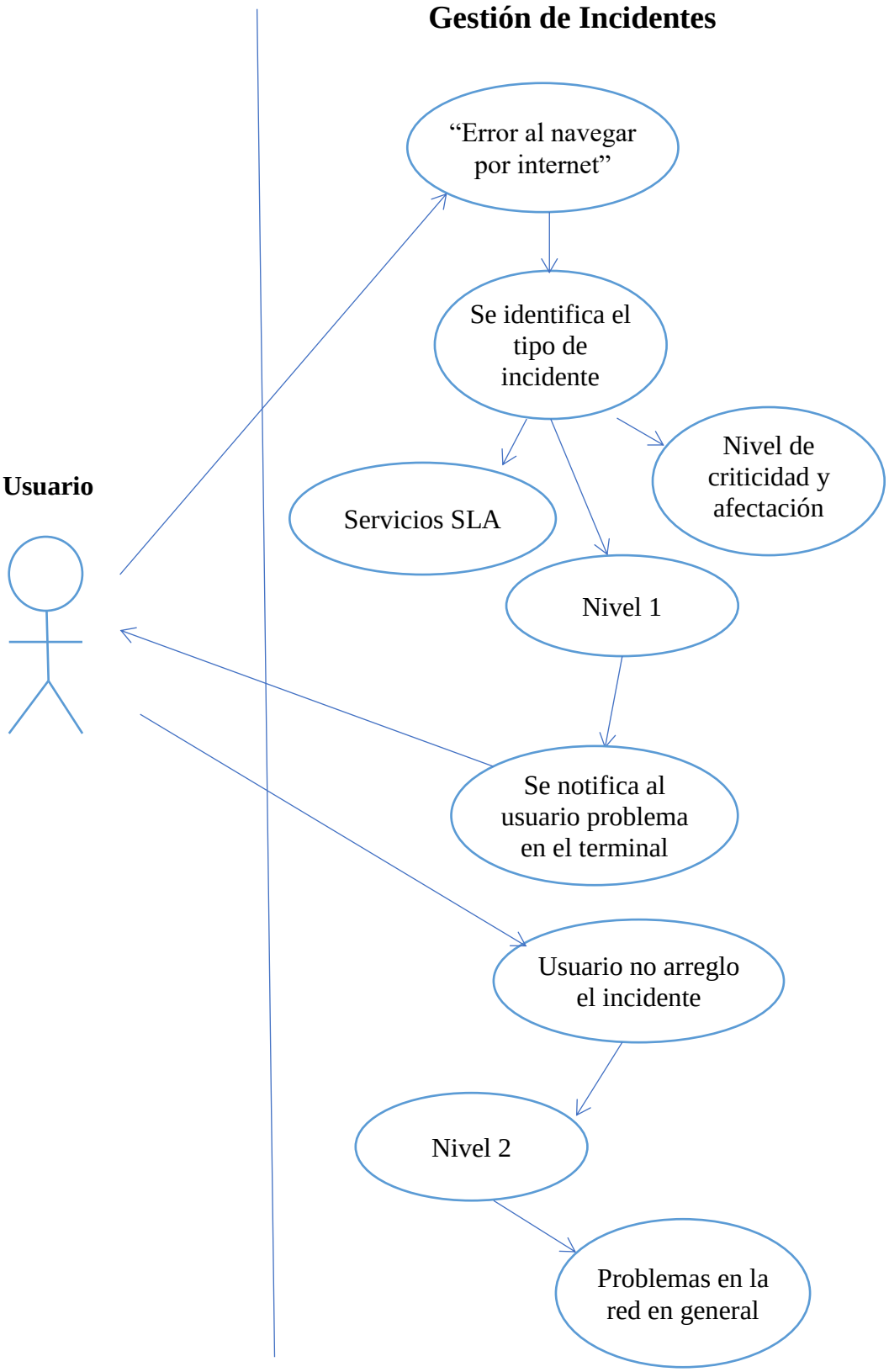

Figura 21. Diagrama de Caso de Uso "Error al navegar por internet"
Elaborado por: Lozada Cristian (2018)

6.7.4.11 Gestión de incidentes

La Gestión de incidentes tiene como objetivo principal de ofrecer una administración del incidente y restaurar a un estado normal los servicios, tan rápido como sea posible procurando que el impacto sea el mínimo sobre las operaciones de las empresas telefónicas, ofreciendo altos niveles de calidad y disponibilidad a los clientes y usuarios.

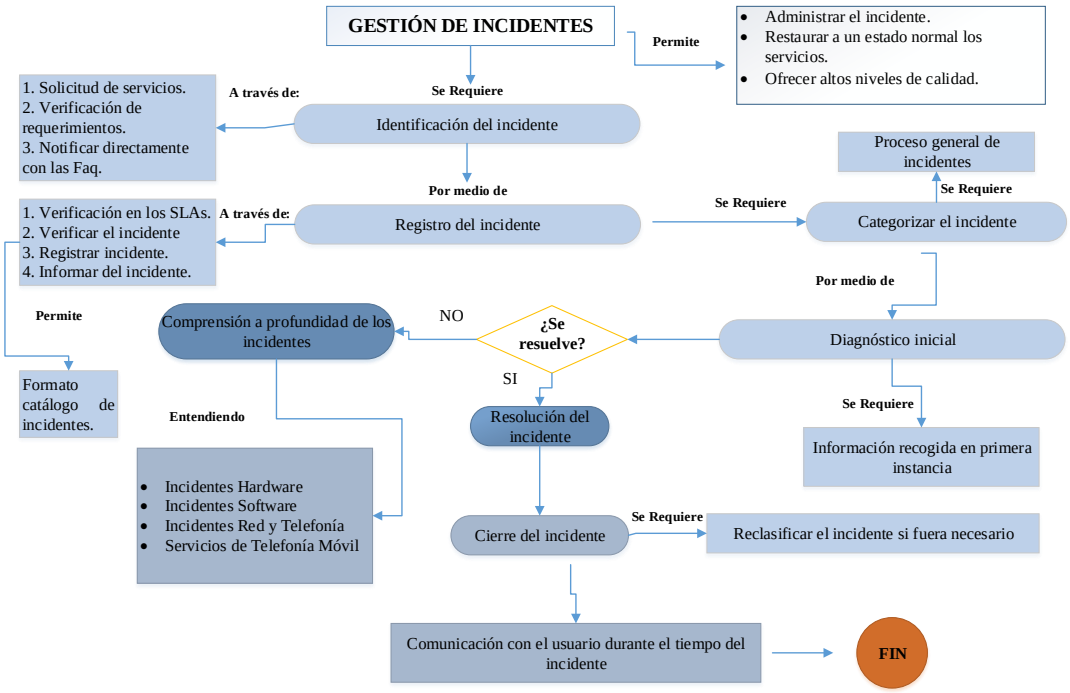

Ilustración 1. Gestión de incidentes
Elaborado por: Realización propia

También se pretende que el personal que trabaja en las TI de las empresas telefónicas tenga una fuente de información sobre el tratamiento de incidentes desde momento en que es detectado, hasta dar una solución definitiva y permita restablecer los servicios a su estado normal y posterior cierre del caso.

Además, se debe crear conciencia en un tratamiento de incidentes proactivo y no reactivo, para buscar posibles incidentes y dar una solución adecuada, y en caso de no ser previstos, sino que forman parte de un tratamiento reactivo, buscar el seguir los procedimientos adecuados durante el ciclo de vida de un incidente.

6.7.4.11.1 Identificación del Incidente

Para la identificación del Incidente se utiliza los medios de solicitud de servicio, descritos en el punto 6.7.4.5, se procede a verificar el requerimiento, se puede notificar directamente con las Faq, y posibles responsables para la solución, también se debe revisar el SLA, así como primer paso debemos identificar el incidente.

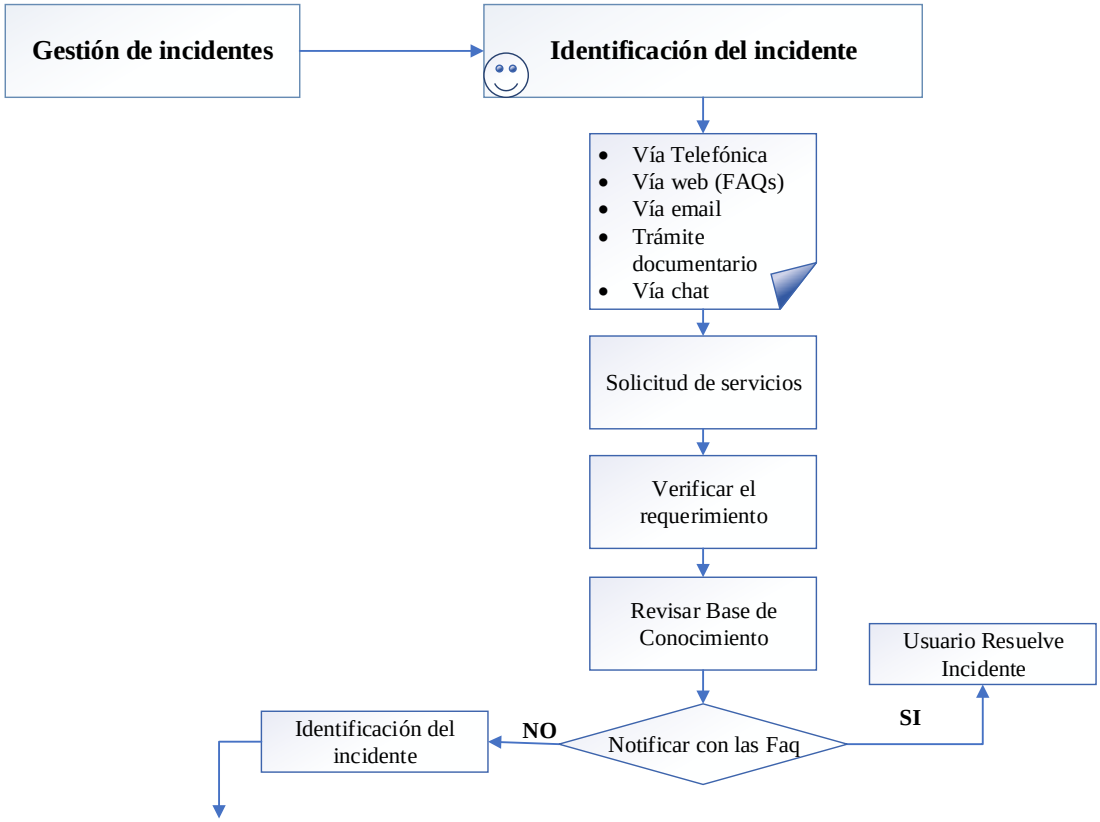

Ilustración 2. Identificación de incidentes
Elaborado por: Realización propia

6.7.4.11.2 Registro del incidente

- Cada pedido realizado por los clientes debe ser verificado en los SLAs, con la finalidad de constatar que los mismos están contemplados.
- Verificar en la base de conocimientos si el Incidente se presentó anteriormente para evitar duplicidad de información por registrar un error conocido.

- Registrar los pasos que se han seguido para resolver el incidente que permitan a los operarios dar una solución rápida
- Informar del incidente cuando sea necesario a los otros usuarios que vayan a ser afectados directamente por la aparición del mismo.

Los incidentes serán registrados de acuerdo al (ANEXO 8), se puede dar solución inmediata a través de FAQs de la página web, también se debe indicar que la prioridad del incidente podría cambiar en su proceso hasta su cierre.

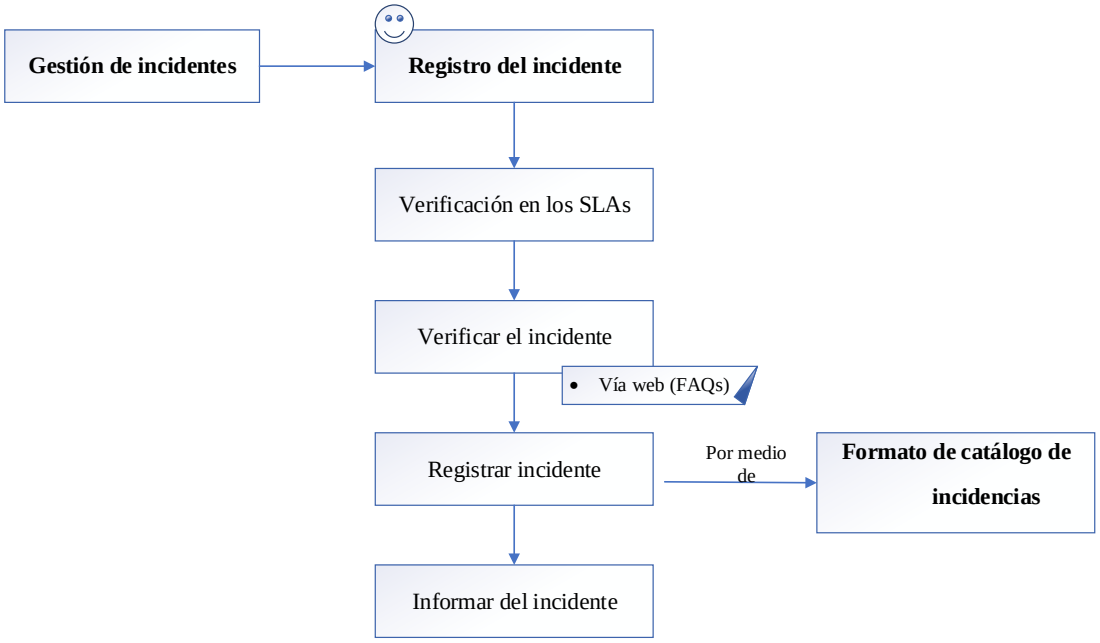

Ilustración 3. Registro de incidente
Elaborado por: Realización propia

6.7.4.11.3 Categorización del incidente

La categorización de incidentes de ITIL es un elemento crítico en el proceso general de gestión de incidentes, ya que el incidente se categoriza se convierte en un elemento de entrada futuro útil para la gestión de problemas, la gestión de proveedores y actúa como un punto de referencia cruzada para la gestión de activos y configuración del servicio.

El registro de incidentes es el tercer paso en el proceso de gestión de incidentes. Se basa en el enunciado 6.7.4.8.

La categorización multinivel es una práctica común y es fácil de explicar a través de un ejemplo. Un incidente se puede categorizar como Hardware, Servidor, CPU incidente. Cuanto mayor sea la granularidad de la categorización del incidente, más beneficiosa será la información para análisis futuros.

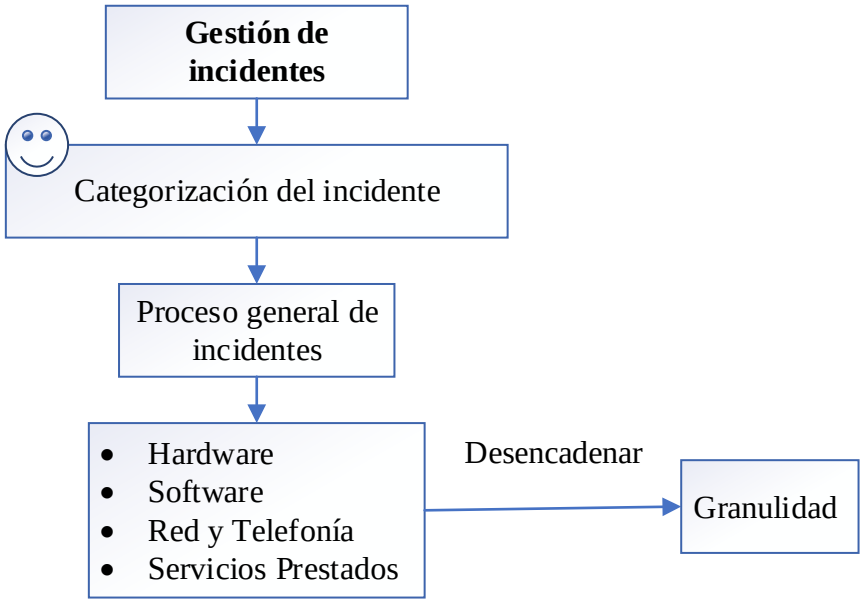

Ilustración 4. Categorización de incidentes
Elaborado por: Realización propia

6.7.4.11.4 Priorización del incidente

Necesario asignar "prioridades a los incidentes", incluida la definición de lo que constituye definir un "incidente importante". Dado que las reglas de escalamiento de la Gestión de incidentes se basan generalmente en las prioridades, la asignación de la prioridad correcta a un Incidente es esencial para desencadenar las "escaladas de

incidentes" apropiadas. En este punto nos basamos en la definición de la prioridad y el impacto. Tabla 21. Prioridad y Figura 16. Prioridad del incidente.

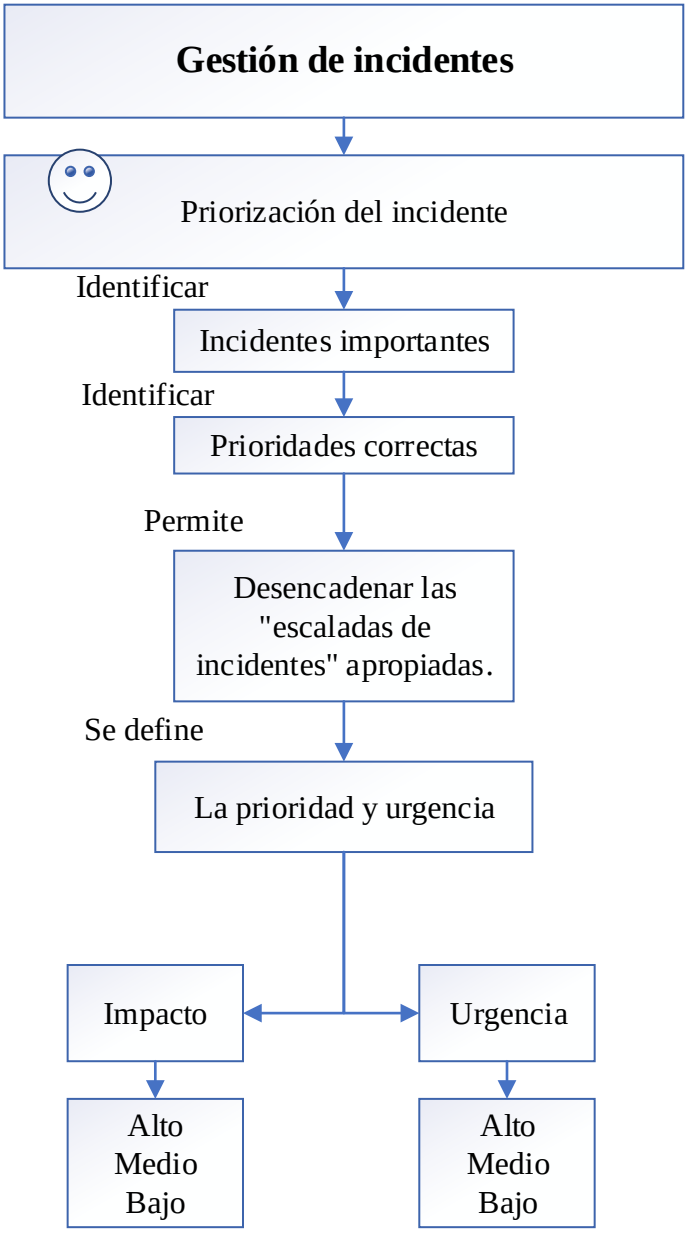

Ilustración 5. Priorización del incidente
Elaborado por: Realización propia

6.7.4.11.5 Diagnóstico inicial

Gracias al avance de la tecnología el incidente reportado podría ser resuelto inmediatamente, gracias a la información recogida en primera instancia, dependiendo

de la magnitud del caso, se podría analizar inmediatamente su escalamiento. Si en caso no puede ser resulto por los grupos internos de la empresa se procederá a escalar al nivel de proveedor de servicios. Toda información registrada servirá para obtener indicadores referentes a los tiempos de investigación y diagnóstico.

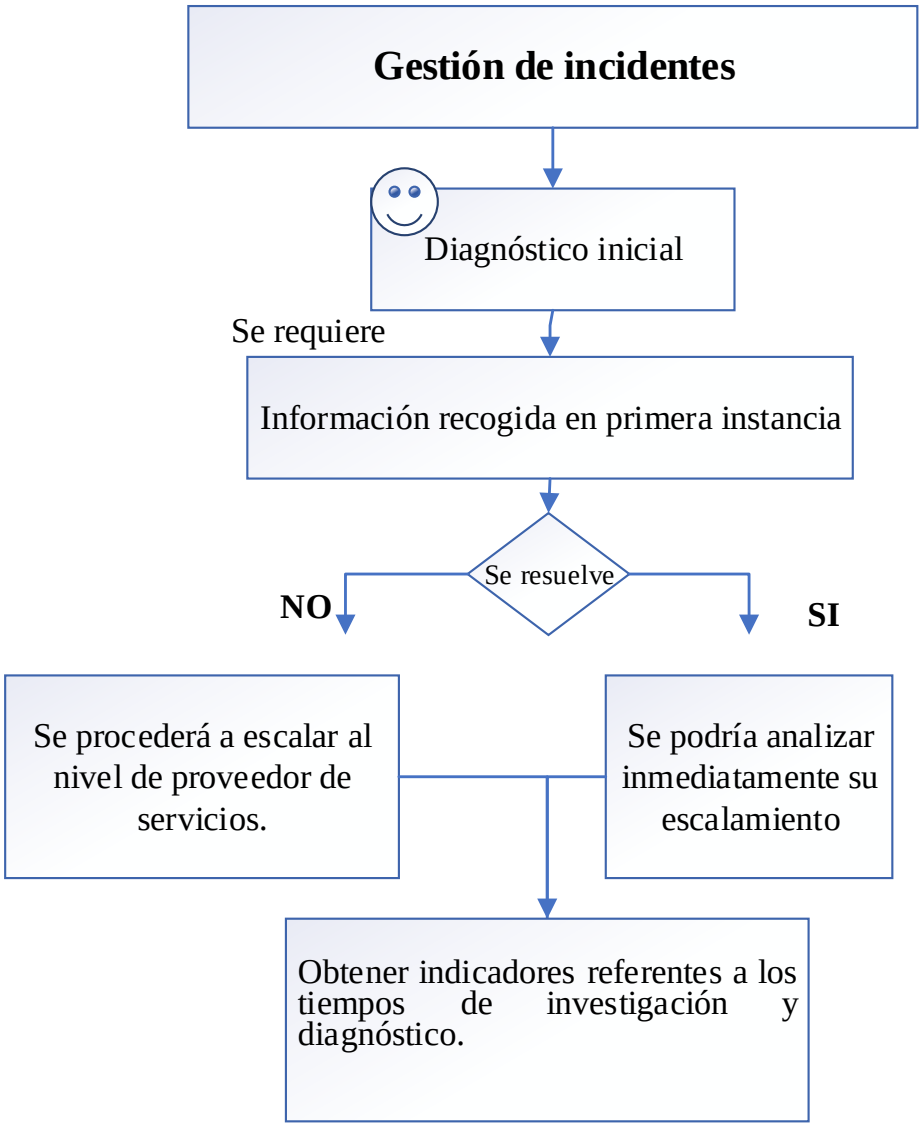

Ilustración 6. Diagnóstico inicial
Elaborado por: Realización propia

6.7.4.11.6 Paso de nivel (si es necesario)

Prácticamente este paso se basa en la complejidad del incidente, por lo cual el nivel de

solución de los incidentes, en la siguiente figura se describe el nivel de solución de los incidentes de acuerdo a su tipo.

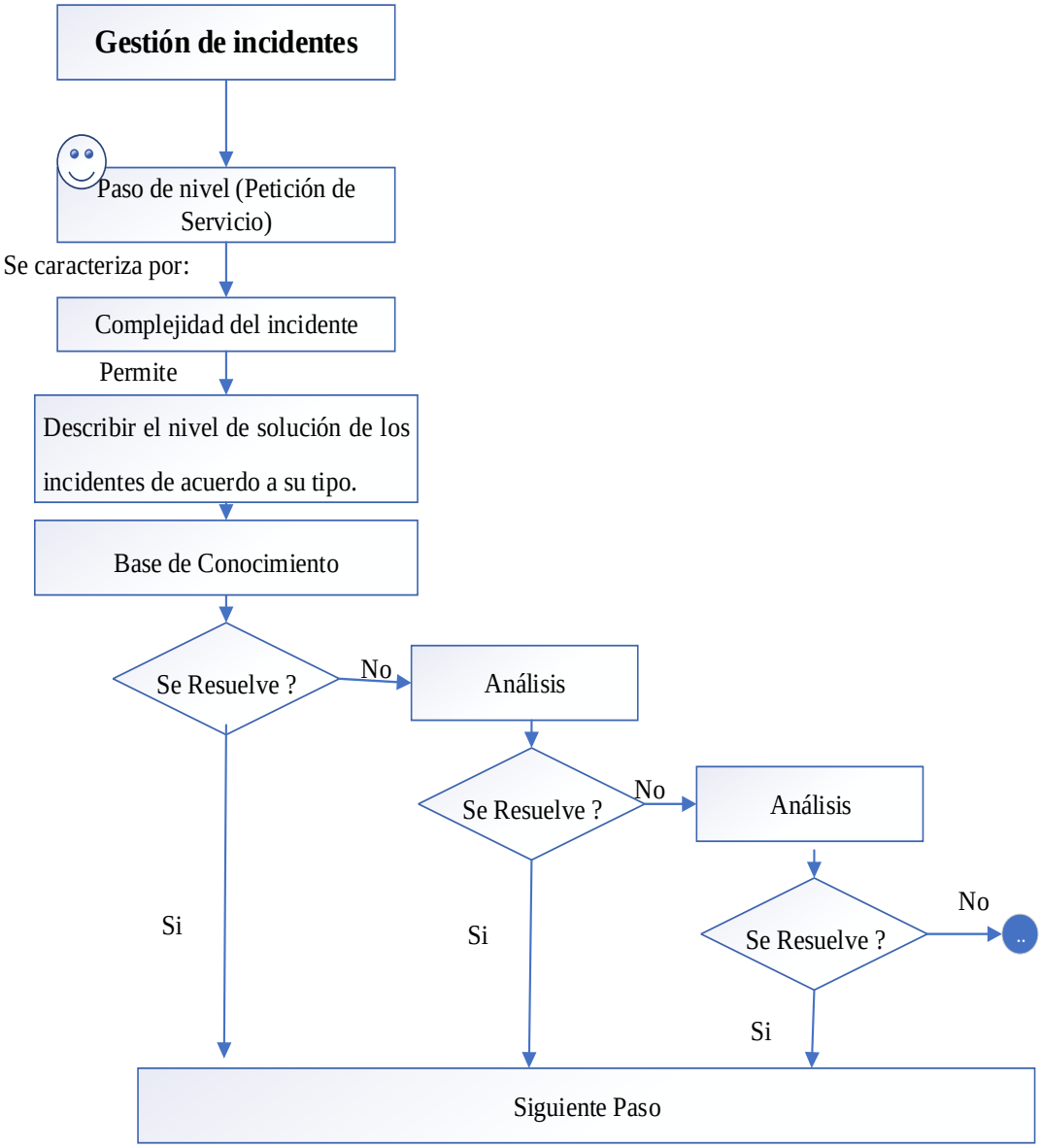

Ilustración 7. Paso de nivel
Elaborado por: Realización propia

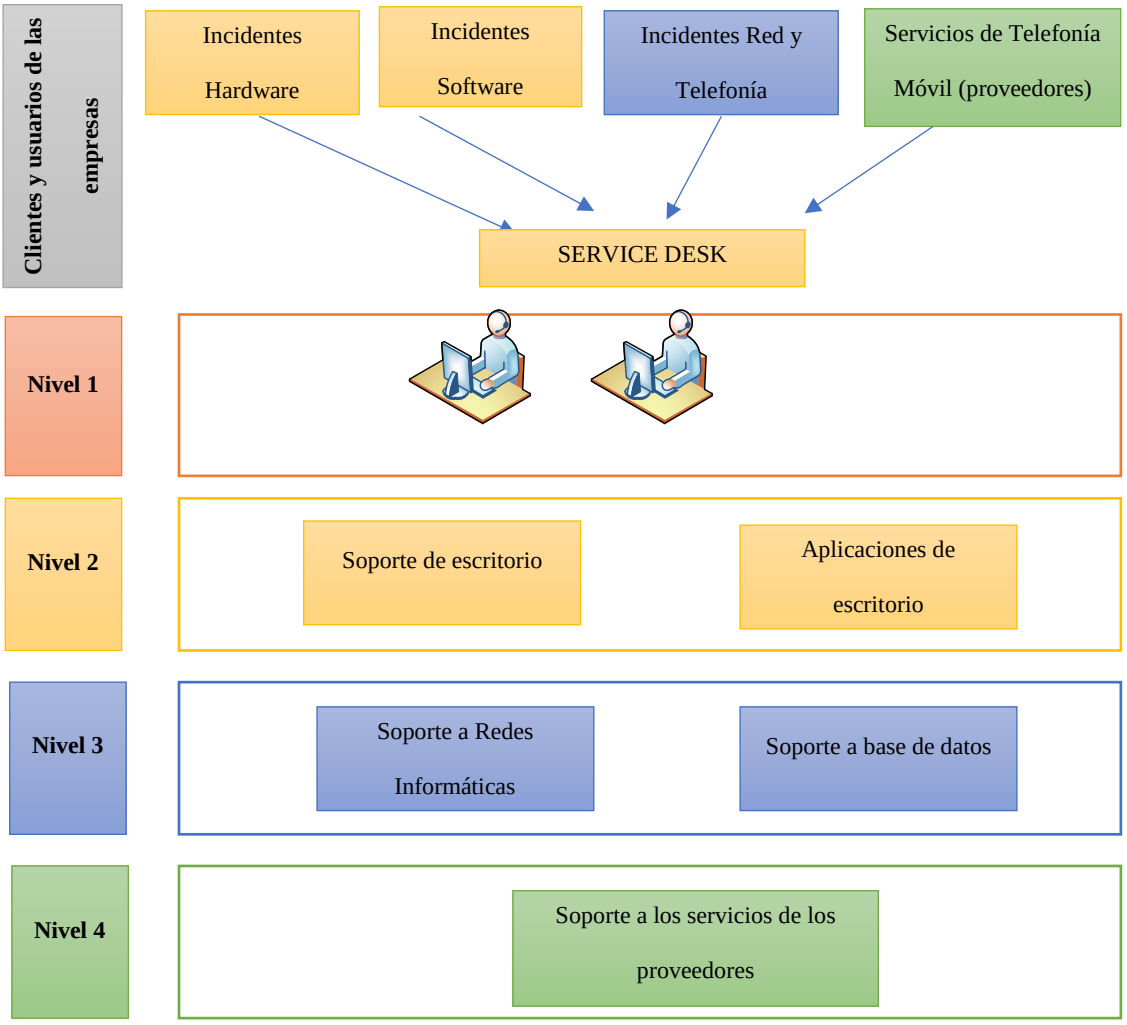

Figura 22. Escalamiento del Incidente
Elaborado por: Lozada Cristian (2018)

6.7.4.11.7 Resolución del incidente

La resolución y recuperación de incidentes de ITIL se realiza una vez que el incidente se comprende por completo. Encontrar una solución a un incidente significa que se ha identificado una forma de corregir el problema. El acto de aplicar la resolución es la fase de recuperación.

La recuperación puede ser realizada por el personal de soporte de TI o proporcionando

al usuario final un conjunto de instrucciones a seguir.

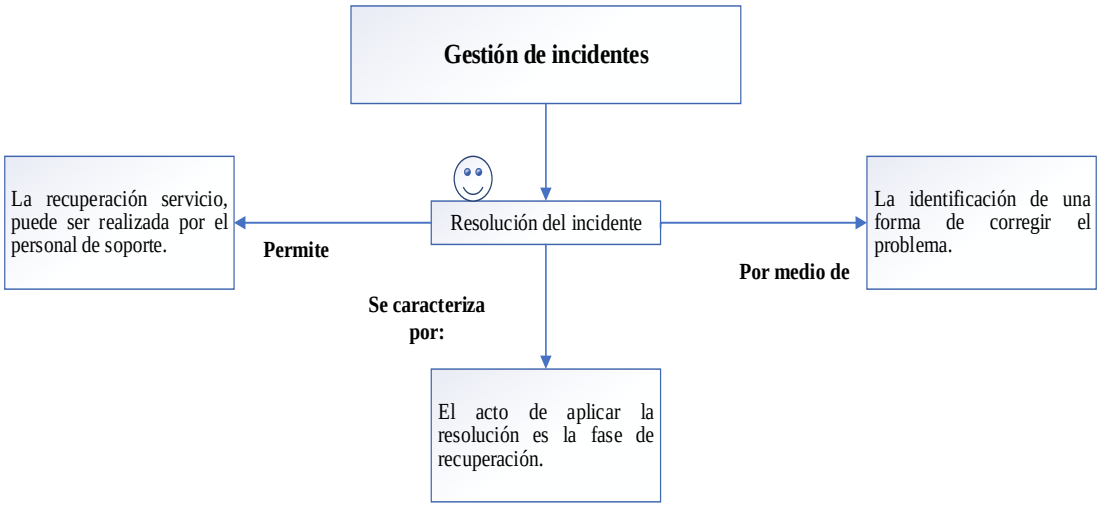

Ilustración 8. Resolución de incidentes
Elaborado por: Lozada Cristian (2018)

6.7.4.11.8 Cierre del incidente

Cuando se haya solucionado el incidente, se procede a:

- Reclasificar el incidente si fuera necesario.
- Actualizar la información en la base de datos de gestión de configuraciones (CMDB) sobre los elementos de configuración implicados en el incidente.
- Medir el grado de satisfacción del usuario. En el caso que no sea satisfactoria la respuesta del usuario se procederá de nuevo con la actividad de Investigación y Diagnóstico hasta encontrar la solución definitiva para el incidente.

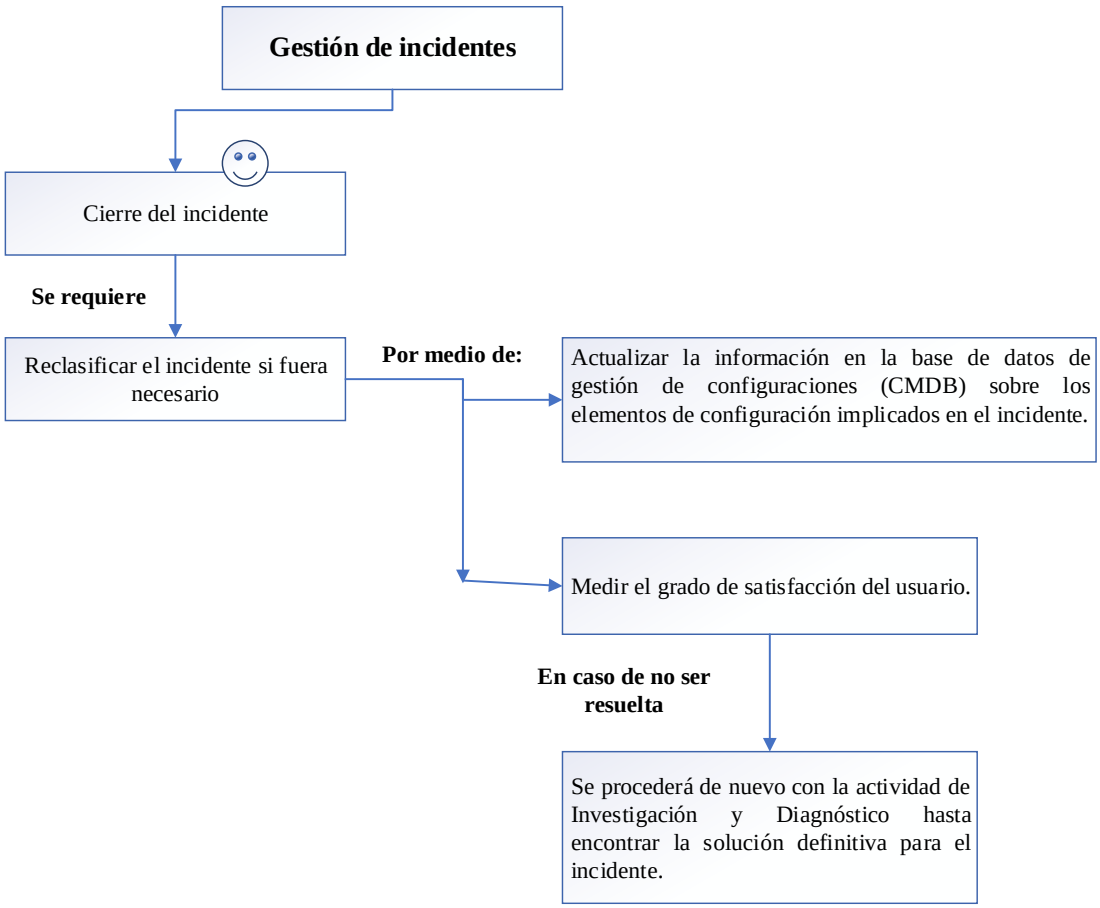

Ilustración 9. Cierre del incidente
Elaborado por: Lozada Cristian (2018)

6.7.4.11.9 Comunicación con el usuario durante el tiempo del incidente

El ciclo de vida de un incidente probablemente incluirá varios puntos de contacto. Done bien, hay una estructura familiar de tres actos para un incidente: primer contacto, actualizaciones durante el incidente, resolución y autopsia.

Parte 1: Primer contacto

La actualización inicial es la más importante. Todo, desde lo que dice hasta cómo y cuándo lo dice, establece el tono de cómo se percibirá su respuesta. Aquí es donde realmente ayuda tener una plantilla configurada antes de tiempo.

Su objetivo debe ser reconocer rápidamente el problema, resumir brevemente el impacto conocido, prometer nuevas actualizaciones y, si es posible, aliviar cualquier inquietud sobre la seguridad o la pérdida de datos. Es importante reconocer que hay un problema, incluso si aún no conoce los detalles exactos.

Parte 2: Actualizaciones regulares durante el incidente.

La comunicación a mitad del incidente es crítica. El analista de incidente es la cara pública del grupo de trabajo de respuesta a incidentes. Sus tareas incluyen definitivamente la publicación de actualizaciones periódicas para el equipo de respuesta a incidentes y las partes interesadas (generalmente a través del correo electrónico), y pueden extenderse a tareas como mantener el documento de incidentes actualizado y preciso. "

Esta persona también estará a cargo de continuar actualizando la página de estado o publicando actualizaciones en otros canales a medida que la situación evolucione. Incluso una actualización que dice "Todavía estamos trabajando en el problema, no hay nada nuevo que informar". Es mejor que no decir nada y dejar a tu público colgado. La gente que se queda en la oscuridad comienza a esperar lo peor.

Parte 3: Resolución

El esquema a manejar debe ser:

Reconocer el problema, empatizar con los afectados y disculparse

Explicar qué salió mal y por qué

Explicar qué se hizo para solucionar el incidente y qué se hizo para evitar que se repitan.

Reconocer, empatizar y disculparse una vez más

No hay necesidad de lenguaje florido ni de afirmaciones grandiosas en una comunicación como esta. Hay que ser directo y confirmar con los usuarios la solución satisfactoria del mismo.

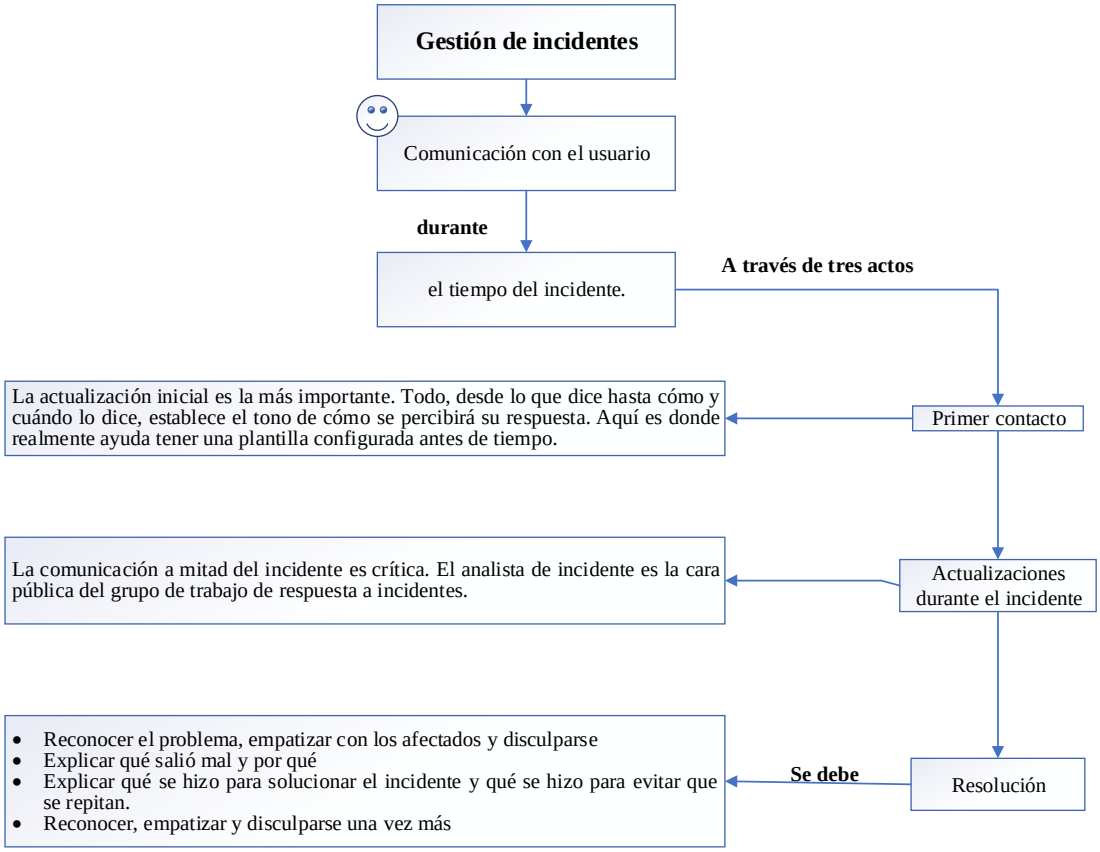

Ilustración 10. Comunicación con el usuario durante el tiempo del incidente
Elaborado por: Lozada Cristian (2018)

6.8 Conclusiones

- La seguridad de la información es una tarea para las medianas y grandes empresas, para proveedor, clientes internos y clientes finales; porque es una actividad compleja, que necesita revisión oportuna.

- El cumplimiento de leyes o regulaciones garantiza la seguridad informática de la empresa, por tanto, es indispensable concienciar al personal de dichas políticas para contribuir al cumplimento de las mismas.

- El presente trabajo ha contribuido con el conocimiento sobre el tema de la buenas practicas que apoyan a la organización a ofrecer servicios de calidad, para mejorar los niveles de protección de la información, a ser utilizadas en las empresas del sector de telefonía móvil del Ecuador.

- La guía de Políticas Informáticas de Seguridad, para el sector de telefonía móvil en Ecuador, al igual que el cumplimiento de las regulaciones, permite el mejoramiento continuo de los diferentes elementos que componen salvaguardar la información y activos.

- La implementación de un Service Desk permitirá adoptar medidas técnicas y preservar la seguridad en los servicios de los usuarios, a través de la gestión adecuada de los problemas, incidentes y vulnerabilidades que puedan existir en las redes informáticas de las organizaciones.

6.9 Recomendaciones

- A medida que las empresas incrementen su estructura tecnológica, su personal, es necesario realizar mayores inversiones en dispositivos de seguridad informática, en planes de socialización, implementación de políticas en todos los niveles de la empresa.

- Según corresponda, es necesario que las leyes y políticas sean revisadas por lo menos una vez al año para mantener la eficacia de lo implementado, ya que la tecnología está en constante evolución y los requerimientos de medidas de prevención en Seguridad Informática, deben ser actualizados.

- Para un correcto desempeño de leyes y políticas implementadas se debe controlar a través de comités o foros, ya dependería de las disposiciones de gerencia, y al no cumplir se debe aplicar sanciones.

- Se recomienda la implementación de planes de capacitación en el

fortalecimiento de las políticas de seguridad de la información, con el propósito de lograr un nivel de especialización mayor en los usuarios internos y externos, que posibilite formar un ambiente en el cual se apliquen las buenas prácticas.

- El personal involucrado como responsable de la mesa de ayuda, debe estar especializado técnicamente y debe tener la habilidad de solucionar conflictos de manera exitosa.

- Se recomienda capacitar al personal responsable de la mesa de ayuda en módulos especializados de cada proceso o involucrarlos para que tengan facilidad de respuesta en la gestión de incidentes y problemas.

BIBLIOGRAFÍA

Acosta, J. (2018). *PROTOCOLO DE SEGURIDAD INFORMÁTICA PARA USUARIOS EN LA UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES.* Ambato: UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES.

ARCOTEL. (2017). *Proyecto de Norma Técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten la seguridad de las redes y de las telecomunicaciones.* Quito.

Arias, M. (2014). *Evaluación de la Seguridad Computacional*. Obtenido de http://centrodecomputoutesa.blogspot.com/2014/04/seguridad-informatica.html

Avilés, R., & Silva, M. (2017). *IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD PARA CONTROL DE ACCESOS A LA RED DE DATOS, EVALUANDO HERRAMIENTAS DE HACKING ÉTICO, EN LA EMPRESA BLENASTOR.* Quito: Pontificia Universidad Católica del Ecuador.

BITS- Desarrollo e Ingeniería. (14 de 10 de 2016). *BITS- Desarrollo e Ingeniería.* Obtenido de BITS- Desarrollo e Ingeniería: http://www.bits.com.mx/como-administracion-de-redes-informaticas/

Boscán, A. (13 de 05 de 2017). Ecuador y casi 100 países sufren ciberataque extorsivo. *Expreso*.

Carrera, E. (2017). *El Costo de la Seguridad en Dispositivos Móviles.* Obtenido de https://revistas.ute.edu.ec/index.php/eidos/article/download/65/61/

Catacora, L. (2018). Protocolo para la presentación de proyecto de investigación e informe final de tesis aplicada. *Trabajo de Grado*. Tacna, Perú: Universidad Privada de Tacna.

Claro. (2019). *¿Quienes somos?* Obtenido de https://www.claro.com.ec

CNT. (2017). *Informe de seguridad.*

Constitución de la República del Ecuador. (2008). CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008. *LEXIS*. Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2016/03/constitucion-de-la-republica-del-ecuador-2008.pdf

Convenio de Constitución de la UIT. (s.f.). CONVENIO DE CONSTITUCION DE LA UIT. *LEXIS*. Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2016/03/convenio-de-constitucion-uit1.pdf

Copete, W. (2018). *NUEVAS TENDENCIAS DE SEGURIDAD INFORMÁTICA EN LAS REDES DE DATOS MÓVILES EN COLOMBIA.*

Deloitte. (2017). *Seguridad de la Información en Ecuador.*

Dirección Nacional de Registro de Datos Públicos. (2017). *DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS*. Obtenido de DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS: http://www.datospublicos.gob.ec/una-ley-de-proteccion-de-datos-personales-es-una-oportunidad-para-el-empresario-ecuatoriano/

Ecuador, S. d. (2018). Estadísticas de Servicios de Telecomunicaciones.

Empresas Públicas Deben Contratar Telecomunicaciones del Estado. (2011). Empresas Públicas Deben Contratar Telecomunicaciones del Estado. *LEXIS*.

ESET. (2018). *Informe Anual de seguridad.*

Facua. (17 de Julio de 2018). *xataka.* Obtenido de https://www.xataka.com/seguridad/brecha-seguridad-web-movistar-expuso-datos-millones-clientes

García, C. (2017). *Seguridad en Smartphones: Análisis de riesgos de vulnerabilidades*

y auditorías de dispositivos. Cataluña: Universidad Oberta de Catalunya.

Gestión de Riesgo en la Seguridad Informática. (2019). *GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA*. Obtenido de GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

Gil, V., & Gil, J. (2017). *Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas.* Bogotá: Universidad Tcenológica de Pereira.

González, D. (2014). *El riesgo y la falta de políticas de seguridad informática: una amenaza en las empresas certificadas BASC.* Bogotá: UNIVERSIDAD MILITAR NUEVA GRANADA, FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD,.

GSMA. (2018). *Seguridad y privacidad en las redes móviles.*

Informática & Tecnología. (2013). *Informática & Tecnología*. Obtenido de Informática & Tecnología: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

ISO. (2019). *Normas ISO*. Obtenido de https://www.normas-iso.com/iso-27001/#section_contacto

KASPERSKY LAB. (2019). *KASPERSKY LAB*. Obtenido de KASPERSKY LAB: https://latam.kaspersky.com/resource-center/definitions/encryption

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2016/03/ley-comercio-electronico-firmas-electronicas-y-mensaje-de-datos.pdf

Ley de la Propiedad Intelectual. (2016). Ley de la Propiedad Intelectual. *LEXIS*.

Ley Orgánica de Telecomunicaciones. (2015). *Ley Orgánica de Telecomunicaciones.* Quito.

Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004). Ley Orgánica de Transparencia y Acceso a la Información Pública. Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2016/03/ley-organica-de-transparencia-y-acceso-a-la-informacion-publica.pdf

McAfee. (2018). *Imforme anual de seguridad.*

Ministerio de Telecomunicaciones y de la Sociedad de la Información . (2019). *Ministerio de Telecomunicaciones y de la Sociedad de la Información* . Obtenido de Ministerio de Telecomunicaciones y de la Sociedad de la Información : https://www.telecomunicaciones.gob.ec

Movistar. (17 de julio de 2018). *Xataka.* Obtenido de https://www.xataka.com/seguridad/brecha-seguridad-web-movistar-expuso-datos-millones-clientes

Oficina de Seguridad para las Redes Informáticas. (08 de 2013). *Infomed.* Obtenido de Infomed: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Ormella, C. (2019). *El portal de ISO 27001 en Español.* Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf

Peñuela, Y. (2018). *ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA*

IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN. Colombia: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.

Piattini, M., & Del Peso, E. (2001). *Auditoría Informática- Un Enfoque Práctico.* México D.F.: AlfaOmega.

Reglamento General a la Ley Especial de Telecomunicaciones. (2015). REGLAMENTO GENERAL A LA LEY ESPECIAL DE TELECOMUNICACIONES. Obtenido de http://www.arcotel.gob.ec/wp-content/uploads/2016/03/reglamento-lot.pdf

Rodella, F. (17 de Abril de 2018). La nueva norma de protección de datos pone a prueba a Administración y empresas. *El País*.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018, 10). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. *3Ciencias*, 118. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Sánchez, J. (2017). *Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.* Ambato: Universidad Técnica de Ambato. Obtenido de http://repo.uta.edu.ec/bitstream/123456789/3128/1/Tesis_t796si.pdf

SEGU.INFO. (2017). *Políticas de Seguridad de la Información.* Obtenido de https://www.segu-info.com.ar/politicas/polseginf.htm

Suárez, D., & Ávila, A. (2015). Una forma de interpretar la seguridad informática. *Journal and Engineering and Technology*, *4*(2), 16-22.

Symantec. (2018). *Informe anual.*

Tarazona, C. (2018). *AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN*. Retrieved from file:///C:/Users/william/Downloads/965-Texto%20del%20art%C3%ADculo-3375-2-10-20180126.pdf

Tarquino, B. (2016). Análisis y Diseño de una estructura de seguridad informática empleando COBIT para ANDINATEL S.A. *ResearchGate*, 20-28.

Telégrafo, E. (2016). *En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario.* Quito: El Telégrafo. Obtenido de https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Universidad Internacional de Valencia. (21 de 03 de 2018). *Universidad Internacional de Valencia*. Obtenido de Universidad Internacional de Valencia: https://www.universidadviu.com/crear-plan-seguridad-informatica-facilmente/

USS- Seguridad Integral. (23 de 07 de 2018). *USS- Seguridad Integral*. Obtenido de USS- Seguridad Integral: https://uss.com.ar/corporativo/tipos-de-control-de-acceso-de-seguridad-informatica/

Zambrano, I. P. (2015). Creación de una empresa de servicios de Seguridad Informática para sitios webs, orientada a PYMES dentro de la ciudad de Guayaquil.

Anexo 1. Encuesta aplicada

UNIVERSIDAD TÉCNICA DE AMBATO
MODELO DE ENTREVISTA A OPERADORAS DE TELECOMUNICACIONES EN ECUADOR SOBRE SEGURIDAD INFORMÁTICA

1.- ¿La operadora dispone de políticas y estándares asociados a la seguridad de la información?

2.- ¿La operadora aplica como medida de seguridad informática el encriptado de información o datos de los clientes o abonados?

3.- ¿La empresa operador dispone de una política de seguridad para la clasificación de los datos o información de los abonados?

4.- ¿Toda la información relacionada a los abonados de la empresa es de tipo confidencial?

5.- ¿En la actualidad existen acuerdos de confidencialidad con respecto a los protocolos de seguridad que se disponen en la empresa?

6.- ¿Los servicios de datos móviles que ofrece a empresa disponen de protocolos de seguridad informática?

7.- ¿En base a que normativa se establece los protocolos de seguridad informática para los servicios que ofrece la empresa?

8.- ¿La empresa registra estadísticas sobre ataques, delitos e incidentes informáticos en sus redes de datos móviles?, por favor aportar estadísticas de los últimos dos años.

9.- ¿Qué herramientas dispone la empresa para el control de roles y privilegios en sus aplicaciones y servicios?

Anexo 2. Formato de inventario hardware

CÓDIGO	SERIAL	EQUIPO	MARCA	MODELO	DESCRIPCIÓN	PROCESO	RESPONSABLE	UBICACION	LICENCIA	FACTURA	GARANTÍA
1701SVR	EMC05DS546	SERVIDOR	DELL	PowerEdge R640	SERVER DELL PowerEdge R640 Intel XeonSilver 4114 16GB 300GB 15K RPM SAS HD iDRAC9 Exp	TECNOLOGIA	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	EXTENDIDA	INTCOMEX 98945	3 AÑOS
1701SW1	FRAS65654	SWITCH	HP	1950	HPE 1950 12XGT 4SFP+ Switch	TECNOLOGIA	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	CADUCADA	MEGAMICRO 903367	1 AÑO
1701COM	ETFA545DS55	CASE	CLON	GENERICO	1 case quasad 4 ram kingstong 1 tb hdd Toshiba 1 placa asus 1 lector dvd	ADMINISTRATIVO	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	OEM PERPETUA	MEGACOM 875465	N/A

Anexo 3. Formato de inventario software

CÓDIGO	SERIAL	PRODUCTO	DESCRIPCIÓN	PROCESO	RESPONSABLE	UBICACION	TIPO LICENCIA	FACTURA	GARANTÍA
1701OOF	ZAQ2W-3SXE4-DC5RF-VT6KB-YBGVT	OFFICE 2013	Office 2013 PROFESIONAL	TECNOLOGIA	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	PERPETUA	INTCOMEX 78456	3 AÑOS
1701SOW	2B87N-8KFHP-DKV6R-Y2C8J-PKCKT	SISTEMA OPERATIVO	WINDOWS 10 64 BITS PROFESIONAL	TECNOLOGIA	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	PERPETUA	CARTIMEX 145645	1 AÑO
1701LICE	EDFG-G125-GFS9-8SDGF-YTIUP	ANTIVIRUS	KASPERSKY	ADMINISTRATIVO	Jefe de Infraestructura Tecnológica	PICHINCHA, QUITO, AMAZONAS, 3ER PISO	ANUAL	CARTIMEX 875465	N/A

Anexo 4. Formato de catálogo de servicios

CÓDIGO	GRUPO DE SERVICIO	SERVICIOS	SUB SERVICIO	DESCRIPCIÓN	DUEÑO DEL SERVICIO	ACUERDOS DE NIVELES DE SERVICIO (SLA)	RESPONSABLE DE LA ATENCIÓN	LÍNEA DE TRABAJO RESPONSABLE
CCB.TI.SS.ST.1.1	Soporte Técnico	Gestión de PCS	Creación de usuarios en directorio activo	Crea un usuario en active directory	Jefe de Infraestructura Tecnológica	2 horas	Analista de Infraestructura Tecnológica	Infraestructura Tecnológica
CCB.CL.SS.1.14	Canales	Tareas operativas	Materiales e insumos	Materiales e insumos	Director de Canales / Operaciones	5 días	Analista de Canales / Operaciones	Canales
CCB.TI.SS.SIREP.1.12	Aplicaciones	Sistema de Facturación	Solicitudes de consulta	Solicitudes de consultas personalizadas	Director de Canales / Operaciones	4 horas	Analista de Solución de Software	Solución de Software
CCB.TI.SS.ST.7.1	Soporte Técnico	Conferencias virtuales	Preparación de conferencias Webex u otras herramientas	Configuración de una videoconferencia con proyector	Jefe de Infraestructura Tecnológica	Principal: 2 horas Sedes: 1 día	Coordinador de Soporte Técnico	Infraestructura Tecnológica

Anexo 5. Formato de acuerdo nivel de servicio (SLA)

Modelo de Acuerdo Nivel de Servicio (SLA)

Entre: Compañía Proveedor & Compañía Prestadora de Servicio

Preparado Por:

Versión

Núm:

Fecha:

PRÓPOSITO Y OBJETIVOS

Proveer al Cliente la disponibilidad de un Servicio de Atención de Incidentes en la Red Edificio Central

La entrega del servicio se iniciará en todos los casos con un requerimiento por parte del Cliente, es decir debe existir un requerimiento formal para que un especialista intervenga. Este documento clarifica las responsabilidades de ambas partes y el procedimiento para asegurar que las necesidades del Cliente son satisfechas de manera oportuna.

PARTES DEL ACUERDO

A continuación, se identifican las partes que suscriben el presente acuerdo:

En calidad de CLIENTE, con RUC xxx RAZON SOCIAL xxx y domicilio en xxx, representado por NOMBRE DEL REPRESENTANTE xxx actuando en nombre y representación de esta entidad en virtud de su condición de CARGO REPRESENTANTE xxx.

Por otra parte, PROVEEDOR como prestador del SERVICIO xxx, con RUC. xxx RAZON SOCIAL xxx y domicilio social en xxx, representado por NOMBRE DEL REPRESENTANTE xxx actuando en nombre y representación de esta entidad en virtud de su condición de CARGO REPRESENTANTE xxx.

FECHA DE INICIO

El presente acuerdo se inicia con fecha efectiva de DD de MM del AAAA, siendo la duración del mismo la establecida hasta la fecha de finalización del contrato.

DEFINICIONES

Es necesaria la claridad en los términos utilizados en el acuerdo a los fines de prevenir confusiones. La terminología deberá ser negociada y acordada entre ambas partes.

REVISIONES PERIÓDICAS

Este acuerdo es válido desde la fecha de firma del contrato y es válido hasta la fecha de expiración o la fecha de terminación prematura del mismo (la más temprana de ambas).

Este acuerdo deberá ser revisado en un mínimo de [una vez] al año; sin embargo, bajo la ausencia o falta de cualquier revisión en cualquier período, este acuerdo deberá permanecer vigente.

El Director General es responsable de facilitar las revisiones regulares a este documento. El contenido de este acuerdo puede ser enmendado o modificado bajo requerimiento y mutuo acuerdo obtenido de todos los signatarios.

Este acuerdo será posteado o publicado en [http://www.xyz.gob.ec/v3/] y será accesible a todos los patrocinadores o partes interesadas.

DESCRIPCIÓN DEL SERVICIO

Esta sección deberá proporcionar una descripción de los servicios proporcionados. Deberá incluir todas las actividades específicas que requerirán de la adecuada implementación del acuerdo, incluyendo el grado de especificidad con que serán

proporcionadas, requerimientos de recursos, adicionándolos al horario definido de actividades.

Referencia	Servicio	Descripción	Especificaciones
1	Gestión Red Inalámbrica	Mantener funcional red inalámbrica	Mantener Firmware actualizado Denegación de Accesos Habilitación Acceso en sitio
2			
3			

RESPONSIBILIDADES

Responsabilidades
Mantener operativo Red Ap sección Cisco
Cambiar equipos inmediatamente en caso de incidencia grave
Mantener Firmware actualizado última versión, incluye revisión periódica.

ADMINISTRACIÓN DEL SERVICIO

DISPONIBILIDAD DEL SERVICIO

Nombre del Servicio	Periodo de Disponibilidad	Mantenimiento	Disponibilidad (%)	Restricciones
Gestión de Red Inalámbrica	24x7	2 horas diarias		Domingos 15:00 a 19:00

RESTRICCIONES DE DISPONIBILIDAD

Las restricciones de Disponibilidad correspondientes al servicio cubierto por este acuerdo son las siguientes:

[Calendario de Feriados, Domingos y Tardes de los sábados]

[Horario Mantenimientos]

[Mantenimientos no calendarizados]

[Backups]

MANTENIMIENTOS DEL SISTEMA

Constituye una buena práctica para cada servicio una tabla que establezca los períodos de mantenimiento. Estos períodos deberán ser especificados en días, semanas o meses. Dependerá del servicio y de la necesidad de mantenimiento.

Tiempos	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Inicio							15:00
Finalización							19:00

MÉTRICAS DEL SERVICIO

Esta sección establece las medidas utilizadas para garantizar la óptima proporción de los servicios. Estas pueden ser definidas en términos de disponibilidad de servicio (tiempos de respuesta) desempeño del servicio, (capacidad de almacenamiento y transmisión de data) y calidad del servicio (frecuencia de no disponibilidad, encuestas a los beneficiarios, entre otros.

	Consulta General	**Incidente**	**Incidente Urgente**	
Horario Soporte	Lunes a viernes 08:00 12:00 13:00 16:00	Lunes a viernes 08:00 12:00 13:00 16:00	24x7	
	Tiempo de respuesta máximo.	**Tiempo de respuesta máximo.**	**Tiempo de respuesta máximo.**	**Tiempo de reparación máximo.**
Balanceador de Carga	12 horas	12 horas	2 horas	8 horas
Nuevo acceso a través de mac	12 horas	6 horas	2 horas	4 horas

SERVICIOS DE REPORTERIA

Esta sección especificará los reportes necesarios.

Reporte	Descripción	Periodo	Remite
Reporte de Monitoreo Red Inalámbrica	Este reporte muestra el número de brechas para el servicio de red inalámbrica	Mensualmente	Responsable de Infraestructura.

PENALIDADES NIVEL SERVICIO

Si los niveles de servicio garantizados no pudiesen ser respetados, el PROVEEDOR computará al CLIENTE, siempre y cuando éste lo haya notificado de forma escrita en el plazo establecido.

La siguiente tabla muestra la compensación en crédito en cuenta que se puede entregar a cada CLIENTE por incumplimiento con los distintos niveles de disponibilidad:

Disponibilidad del Servicio	Compensación
98 % a 99,8 %	10 %
95% a 97,9 %	20 %
90% a 94,9 %	30 %
89,9% o menos	50 %

ADMNISTACIÓN DE LA CONTINUIDAD DEL SERVICIO

Plan	Tiempo
Plan Internet Nodo 2 Proveedor de Internet, Habilitación Internet	3 horas

DOCUMENTACIÓN DE SOPORTE O APOYO

Documentación	Descripción
Contrato	Este es el contrato principal
Diagrama de Red Interno Edificio N	Jefe Área Tecnología

TERMINACIÓN

El acuerdo de nivel de servicio tendrá validez durante todo el periodo de tiempo que dure la prestación del servicio.

DISPOSICIONES GENERALES

(a) Enmienda. Este acuerdo no podrá ser enmendado exceptuando bajo la firma de dos representantes autorizados por ambas partes ADESS y el Centro de Servicio.

CLIENTE PROVEEDOR

Anexo 6. Formato de preguntas frecuentes

Titulo
Test back bond Internet

Palabras Clave
‘Back bond’ ‘Internet Principal’ ‘Internet Matriz’

Categoría
Infraestructura / Redes / Cableado Estructurado

Síntoma
Sin conectividad

Problema
No existe conectividad entre dos pisos oficina central

Solución
Revisar cuarto de maquinas Revisar Inventario de Ip Revisar Diagrama de Red Utilizar Verificador de Señal colocar en ambos extremos Verificar Conectividad

Comentario

Fecha de Creación	Usuario	Versión	Acciones
15-01-2019	James Go	1.0	Creación

Anexo 7. Formato de trámite documentario

Formato Registro de Incidencias

Información Solicitante

Identificación	Nombre	Ubicación	Proceso	Celular	Correo

Problema	Solución

Detalle Incidente

Id Incidente					
Fecha					
Hora					
Categoría					
Prioridad					
Asistido					
Celular					
Correo					

Observaciones y Recomendaciones

FIRMA SOLICITANTE FIRMA ANALISTA INCIDENTE

Anexo 8. Formato de catálogo de incidencias

CÓDIGO	FECHA	HORA	MEDIO SOLICITUD DE SERVICIO	PROCESO SOLICITANTE	IDENTIFICACIÓN USUARIO	NOMBRE DE USUARIO	CELULAR DE USUARIO

EMAIL DE USUARIO	DESCRIPCIÓN DEL INCIDENTE	NIVEL DE SOLUCIÓN INCIDENTE	RESPONSABLE SOLUCIÓN	ESTADO	RELACIÓN CON OTRO INCIDENTE	CLASIFICACIÓN DE LOS INCIDENTES INCIDENTE	PRIORIZACIÓN