**PONTIFICA UNIVERSIDA CATÓLICA DEL ECUADOR**


**FACULTAD DE INGENIERIA**

**MAESTRÍA EN REDES DE COMUNICACIÓN**

# IDENTIFICACIÓN Y VALORACIÓN DE POLÍTICAS DE ACCIÓN MEDIANTE SISTEMAS DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA EVITAR RIESGOS POR FRAUDE TELEFÓNICO EN LAS EMPRESAS QUE UTILIZAN EL SERVICIO DE TELEFONÍA IP

**AUTOR: VALENZUELA GARZÓN GABRIEL SANTIAGO**

**DIRECTOR: ING. DAVID EDUARDO RAMÍREZ ESPONOSA**

**QUITO, NOVIEMBRE 2015**

## DECLARACIÓN DE AUTORÍA

Yo, GABRIEL SANTIAGO VALENZUELA GARZON, portador de la cédula de ciudadanía No. 1712334521, declaro bajo juramento que el trabajo aquí descrito es de mi total autoría; que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondiente a este trabajo, a la Pontificia Universidad Católica del Ecuador, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

GABRIEL SANTIAGO VALENZUELA GARZON

C.I. 1712334521

## CERTIFICACIÓN DE AUTORÍA

Yo, DAVID EDUARDO RAMÍREZ ESPINOSA, en calidad de Maestrante y Director del presente trabajo de investigación, certifico Esta investigación no contiene plagio y es resultado de un trabajo serio desarrollado en su totalidad por GABRIEL SANTIAGO VALENZUELA GARZÓN.

DAVID EDUARDO RAMÍREZ ESPINOSA
DIRECTOR DE TESIS

## AGRADECIMIENTO

La paciencia, apoyo y fortaleza solo pueden venir de la familia, de aquellas personas que de corazón están ante todo tipo de adversidad, la esposa, los hijos, los hermanos, los padres, los tíos, los abuelitos… A todos ellos que día a día están pendientes del cumplimiento de las metas y objetivos de sus seres queridos y en especial del cumplimiento de este trabajo final un infinito Dios les pague por su fuerza y cariño.

## DEDICATORIA

Para mi Ale, mi Mathi, mi Leo, por su paciencia, sonrisas, y demás locuras que hacemos día a día en este pequeño espacio de tiempo y mágica luz que nos rodea.

# INDICE DE CONTENIDO

## INDICE DE FIGURAS



## INDICE DE TABLAS

# CAPÍTULO 1.

## 1.1 Introducción.

El tema de investigación del presente trabajo pretende establecer los parámetros y lineamientos necesarios que deben cumplirse dentro de una organización para mantener la seguridad en sus sistemas de información y sobre todo minimizar los riesgos de seguridad por fraude en el servicio de telefonía IP aplicando normas e indicadores de control de orden internacional para el control y aplicación de Sistemas de Gestión de Seguridad de la Información *SGSI*. La optimización de recursos tecnológicos dentro de una Empresa actualmente es el paradigma a nivel mundial, en donde se pueda integrar de manera unificada todos y cada uno de los servicios tecnológicos de hoy en día como video, voz, datos y movilidad en una misma aplicación.

Desde los sistemas de conmutación de circuitos a los sistemas de conmutación de paquetes se ha determinado y aplicados todas las normas y recursos necesarios para aplicar la seguridad y confidencialidad de las comunicaciones entre emisores y receptores, sin embargo los problemas de seguridad y vulnerabilidad cada día son más recurrentes y determinan un alto índice de impacto sobre el recurso más importante; la información.

Durante el desarrollo del presente tema de investigación se analizarán y tratarán los diferentes protocolos y arquitecturas de comunicación utilizadas para los sistemas de voz sobre el protocolo IP, las funcionalidades y tipos de soluciones para el servicio de telefonía IP, los diferentes tipos de ataques y vulnerabilidades tanto para

la tecnología de VoIP así como para el servicio de telefonía IP y su respectivo tratamiento de seguridad con políticas y modelos de esquemas de matrices de análisis, evaluación y tratamientos de riesgos, y finalmente las políticas de acción de un Sistema de Gestión de la Seguridad de la Información que deben aplicarse en las empresas para evitar fraudes en los sistemas de telefonía.

## 1.2 Justificación.

Debido a que los sistemas de comunicación son de gran importancia para todo tipo de organización se ven continuamente amenazados y afectados en su seguridad desde una variedad de fuentes que incluyen fraudes, vandalismo y espionaje. Cada vez se vuelve más común encontrar complejos y sofisticados sistemas de ataques e intrusión a la información digital provocando importantes pérdidas económicas para las organizaciones. Una de las plataformas con más afectación de ataques de intrusión o denegación de servicios es la telefonía sobre protocolos IP.

En razón de que día a día crecen las comunicaciones y sus diferentes aplicaciones, ha sido necesario determinar normas y modelos de Sistemas de Gestión de la Seguridad de la Información. Los mismos que están determinados por las necesidades del negocio, tamaño y estructura de una organización, permitiendo garantizar la confidencialidad, integridad y disponibilidad de la información. Una de las normas que tiene mayor uso para el desarrollo de SGSI bajo el sistema de análisis, diseño e implementación del proceso global de seguridad es la ISO/IEC

27001, en donde se definen procesos y procedimientos para el manejo y tratamiento integral de la seguridad de la información.

A través de la elaboración de una matriz de riesgos con la metodología SGSI, se pueden identificar y tratar las diferentes categorías de amenazas y ataques a los que se ven expuestas las organizaciones en sus plataformas de comunicaciones de telefonía IP, para lo cual se analizan los factores internos y externos relacionados con los riesgos y las diferentes estrategias a seguir para mitigar y enfrentar los riesgos de seguridad, tomando en cuenta la valoración y categorización de los mismos.

Con el desarrollo de este proceso de investigación se pretende determinar una propuesta técnica que permita evaluar y controlar los riesgos de seguridad por fraudes en el servicio de telefonía IP, minimizando el impacto de afectación del funcionamiento de este servicio para el giro de negocio dentro de una organización.

## 1.3 Antecedentes.

La información es el activo intangible más importante de toda empresa, y por lo tanto requiere del tratamiento y protección adecuados para garantizar la continuidad del negocio. La seguridad de la información se caracteriza por; confidencialidad, integridad, disponibilidad y no repudio, factores que a su vez permiten asegurar el cumplimiento de un sistema de gestión de seguridad de la información. Por ende todos los sistemas de información y aplicaciones específicas para el tratamiento y manejo de información han sido diseñados para ser seguros, sin embargo es indispensable la administración de la misma a través del esfuerzo conjunto tanto de

normas y políticas, así como del compromiso de empleados, proveedores y organizaciones externas para determinar la seguridad de la información como un ente consolidado de la organización.

Dentro del análisis y planteamiento de los esquemas de seguridad para el monitoreo y búsqueda de vulnerabilidades para el servicio de telefonía IP, se han desarrollado herramientas tecnológicas y procesos de evaluación mediante sistemas de gestión de seguridad de la información a través de varias normas, una de las más utilizadas es la norma internacional ISO/IEC 27001 la cual se encuentra abierta para cada país que desee adoptarla según sus necesidades, es así como a nivel de Latinoamérica se establece el uso e implementación de varias normas, entre ellas: la norma colombiana (NTC-BS-7799-2), la norma ecuatoriana (NTE INEN-IDO/IEC 27001:2011 o 27001:2013), la norma peruana (NTP-ISO/IEC 27001:2014), entre otras.

En cuanto al uso y aplicación de las diferentes herramientas tecnológicas para la evaluación de vulnerabilidades en el servicio de telefonía IP se han desarrollado aplicaciones de análisis de tráfico de paquetes, control de tráfico, conexión de red, análisis de riesgos y auditorías como: *Wireshark, Netscantools, Languard, Acunetix, Nessus, Assaint,* entre otros. Así también existen diferentes tipos de organizaciones a nivel mundial que prestan sus servicios con especialistas certificados para la identificación y tratamiento de riesgos de seguridad por fraudes en esta especialidad, enfocando metodologías con tecnologías, entre ellas destacan: *Level_3, Cisco Systems, Avaya, Fica Consulting, 3CX Innovation Communications para Asterisk.*

La identificación y análisis de riesgos de seguridad a través de la implementación de herramientas tecnológicas y de políticas de control y prevención, permiten determinar la definición y evaluación del impacto causado en las organizaciones y el tipo de afectación que se da a la información de la organización; clasificando a los riesgos según su impacto en: mitigados, transferidos, eludidos y aceptados.

La aplicación de la norma para determinar los Sistema de Gestión de la Seguridad de la Información (SGSI), permitirá enmarcar en un solo contexto los riesgos tecnológicos que enfrentan las organizaciones, asegurando y determinando los controles de seguridad adecuados. Es así como para el presente trabajo de investigación se consolidará tanto las herramientas como el tipo de metodología para determinar los procesos de control y prevención para enfrentar los riesgos de seguridad por fraudes en el servicio de telefonía IP.

## 1.4 Objetivos.

### 1.4.1 Objetivo general.

Identificar a través de las matrices de análisis, evaluación y tratamientos de riesgos, las políticas de acción de un Sistema de Gestión de la Seguridad de la Información que deben aplicarse en las empresas para evitar fraudes en los sistemas de telefonía basados en la tecnología de comunicación de VoIP.

### 1.4.2 Objetivos específicos.

- Identificar y clasificar los diferentes riesgos de seguridad que afectan a los sistemas de comunicación de VoIP.
- Formular políticas de acción para el tratamiento de riesgos por afectación de servicio.
- Establecer controles y lineamientos para la evaluación sobre la disponibilidad y continuidad del servicio de comunicaciones de telefonía IP en una organización.
- Proponer una solución técnica que permita identificar, evaluar y mitigar los riesgos de seguridad por fraude para el servicio de telefonía IP.

# CAPÍTULO 2. ESTADO DEL ARTE

La era de las comunicaciones tecnológicas, data desde la década de los 50 y los 60, a partir del cual se han desarrollado variedad de plataformas y aplicaciones de Hardware y Software que han permitido evolucionar constantemente en el modo de transmitir y recibir información en diferentes lugares del planeta y hasta fuera de él.

En la continua evolución de las redes de comunicación se han creado todo tipo de tecnologías y aplicaciones para el servicio de voz, video y datos, los cuales han implicado costos de mantenimiento y actualización elevados para las empresas a nivel mundial en periodos de medianos y corto plazo. Es así como a partir del año 2006 varias empresas proveedoras de tecnología de la información, definieron el uso de las Comunicaciones Unificadas como plataforma de aplicaciones para mejorar la productividad individual, grupal de las organizaciones, integrando diferentes canales y componentes de comunicación, como: mensajería instantánea, correo electrónico, conferencias web, comunicaciones móviles, entre otros, permitiendo así que las personas y equipos geográficamente dispersos puedan trabajar juntos de manera eficiente a través de una interfaz uniforme en diferentes tipos de medios.

Según el estudio de mercado realizado por la Empresa *Frost & Sullivan*[1]en el primer semestre del año 2014, se revela que para el segundo semestre del año 2015 existirán aproximadamente 49,5 millones de personas a nivel mundial que se beneficiarán con el uso de las comunicaciones unificadas, teniendo un crecimiento anual promedio del 68.72 %, tal como se muestra en la **Figura 1**.

[1] Frost & Sullivan. (2010). Unified Communications: What does the Future Hold for Vendors? Recuperado de: http://www.frost.com/reg/blog-personal-index.do?pageSize=12&userId=479763&page=3

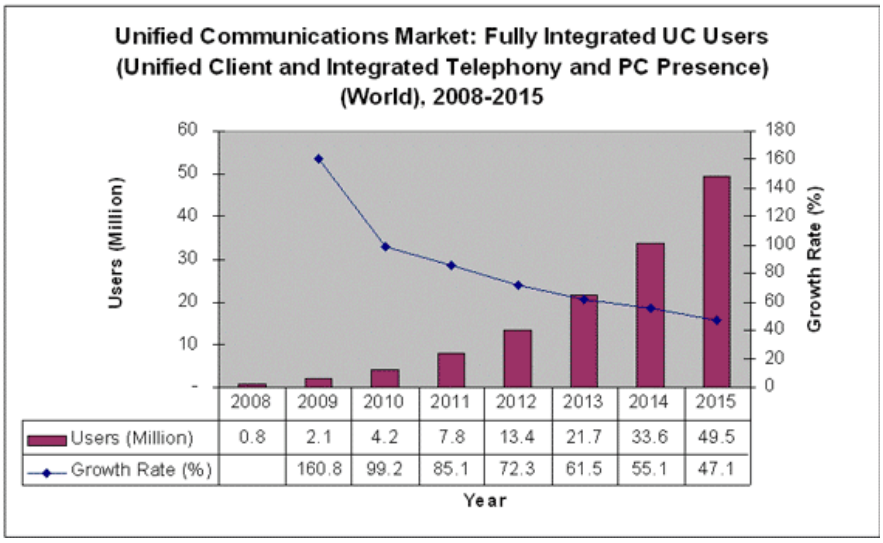


*Figura 1:* **Usuarios de Comunicaciones Unificadas por año (Frost & Sullivan 2014).**

Los principales factores que han motivado la migración a soluciones de comunicaciones unificadas se identifican en: el servicio de mensajería unificada (correo electrónico, chat y videoconferencia), movilidad de comunicaciones, mejora en la eficiencia de las comunicaciones, reducción de costos por llamadas de voz sobre protocolo IP y sobre todo la tele presencia. Por tal motivo, las comunicaciones unificadas han llegado a ser una de las herramientas esenciales para la integración profesional y tecnológica de las organizaciones a nivel mundial, agilizando los procesos de negocio y productividad de los empleados, manejando la comunicación tecnológica con eficiencia, eficacia y en tiempo real.

Según *Gartner*, "el éxito de una solución de comunicaciones unificadas depende de características como: movilidad, interoperabilidad, uso de la nube y funcionamiento atractivo de la solución para el proceso de toma de decisiones de uso por parte de los usuarios de una organización". En el reporte de cuadrante mágico de

comunicaciones unificadas de agosto del 2014[2], **Figura 2** se anuncia a Microsoft como líder en el ámbito de las comunicaciones unificadas por una de sus productos insignes del mercado; Office 365 y sus herramientas: *Skype, Offfice, Cortana y Lync Server*.


*Figura 2:* **Cuadrante Mágico Comunicaciones Unificados, (Gartner Agosto 2014).**

En el presente capítulo se denotan las características, normas y estándares de la tecnología de voz sobre IP *VoIP*. Su aplicación en el uso de sus diferentes servicios para el tratamiento de la gestión de información, así como también las normas y estándares de seguridad para el manejo de la información tecnológica que se ha determinado a través de la evolución de los sistemas de gestión de la seguridad de la

[2] Gartner, Inc. (Agosto 2014). Magic Cuadrant for Unified Communications. Recuperado de: http://www.gartner.com/technology/reprints.do?id=1-1YWQWK0&ct=140806&st=sb

información para beneficio de las organizaciones públicas y privadas a nivel mundial que utilizan la tecnología IP.

## 2.1. Arquitectura de VoIP.

El servicio de telefonía bajo el protocolo de voz sobre IP se encuentra determinado por tres elementos fundamentales dentro de su arquitectura:

- **Terminales:** Son los terminales físicos (teléfonos IP) o programas informáticos (*softphones)* que sustituyen a los teléfonos tradicionales, los teléfonos físicos utilizan conectores RJ45 para la conexión a una red IP e implementan funciones de multi-switch, optimizando recursos de conexiones de red. Las aplicaciones de software que son utilizadas para el servicio de telefonía IP pueden funcionar bajo cualquier tipo de plataforma y pueden tener las siguientes características:
    - Validación de usuarios a través de servidores de directorio activo (LDAP).
    - Importación y exportación de libretas de directorios.
    - Soporte multi conferencia y tele presencia.

  Existen además los adaptadores *ATA* que permiten conectar un teléfono analógico dentro de una red digital, transformando la señal analógica en protocolos de VoIP.

- **Gatekeepers:** Proporcionan y desarrollan servicios para los terminales, estos elementos permiten realizar; traslación de direcciones, autorización de llamadas, control de admisión, control de zonas, gestión de ancho de banda, gestión de llamadas, reserva de ancho de banda, servicios de directorio, entre otros.
- **Gateways:** Son los dispositivos que permiten enlazar con la red telefónica tradicional y la red IP, gestionan la interconexión de redes y protocolos diferentes en todo nivel de comunicación, convierte la señal analógica en una señal de paquetes IP y viceversa.

## 2.2. Protocolos de señalización para VoIP.

A través del uso de los protocolos de comunicación se determina la conexión entre los diferentes dispositivos que permiten el uso del servicio de telefonía IP, de estos protocolos depende la calidad, eficiencia y seguridad de la comunicación. Los protocolos más utilizados para este servicio son: SIP, H.323, IAX, MGCP, Skinny Client Control Protocol (Cisco), CorNet-IP (Siemens), entre otros. Todos ellos normados y certificados por instituciones y organismos reguladoras como la ITU-T, IETF, IEC, ETSI, EIA-TIA.

Actualmente en el mercado de las comunicaciones de VoIP y específicamente para el servicio de telefonía IP como tal existen variedad de productos que funcionan bajo los diferentes protocolos de VoIP, sin embargo es necesario mencionar que los más conocidos son los protocolos SIP y H.323.

### 2.2.1. Protocolo SIP.

SIP es el protocolo de inicio de sesión que permite a los usuarios participar en sesiones de intercambio de información multimedia, estructurando mecanismos de; establecimiento, modificación y finalización de llamada. Este protocolo es considerado un mecanismo genérico de señalización del servicio de telefonía IP, el cual soporta 5 elementos funcionales para el inicio y terminación de una comunicación multimedia:

- Localización de usuarios.
- Intercambio y negociación de capacidades de los terminales.
- Disponibilidad de usuarios.
- Establecimiento de llamada.
- Mantenimiento de llamada.
- Terminación de llamada.

El protocolo SIP es basado en el modelo cliente servidor y permite la comunicación entre dispositivos multimedia a través de los protocolos de transporte RTP/RTCP que posteriormente serán analizados. Por lo cual cada cliente debe establecer las peticiones de "*Request Messages*" hacia el servidor, el mismo que devuelve una respuesta "*Response Messages*", este proceso es proporcional al número de llamadas y procesos de comunicación sean realizados. Los terminales pueden realizar llamadas directas sin intervención de elementos intermedios, mediante los procedimientos de peticiones "*Invite Request*" para inicio de llamada o "*Bye Request*" para la finalización. Las direcciones de los usuarios llamadas URI

"*Uniform Resource Identifiers*" se determina bajo el estándar **user@host; user:** utilizado para el nombre, alias o número telefónico y **host:** para el dominio.

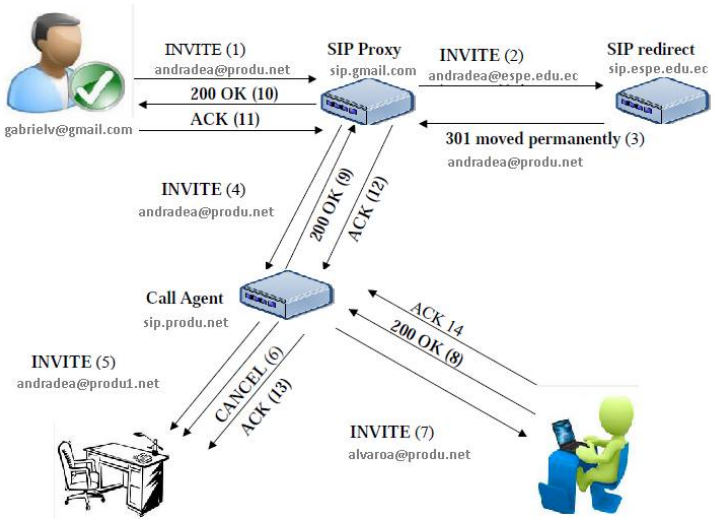


*Figura 3:* **Modelo Protocolo de Inicio de Sesión. Elaborado por el Autor.**

## 2.2.2. Arquitectura SIP.

La arquitectura del protocolo de señalización SIP, requiere la definición de cuatro funciones para su proceso de comunicación tal como se detalla en la **Figura 4.**

- **Servidor Proxy:** Determina el camino de las peticiones y respuestas desde el origen al destino, determinado por el número de saltos de nodos que pueda establecer, utiliza el parámetro "Via" que permite determinar el mismo camino o ruta tanto para la petición como para la respuesta de la comunicación.

- **Servidor de Redirección:** Determina la misma función que el servidor Proxy, con la diferencia de que procesa la petición de un "*Invite*" con un mensaje de redirección con las indicaciones para contactar al destino.
- **Servidor de Registro:** Permite mantener la localización de un usuario, este servidor facilita la característica de movilidad de los usuarios.
- **Agente de Llamada:** Además de realizar las funciones de los servidores anteriores determina la ejecución de las siguientes acciones:
    - Almacena información de llamadas**.**
    - Determina el filtrado de llamadas por tiempo y origen
    - Implementa el servicio de localización, reenvío y redirección de llamadas

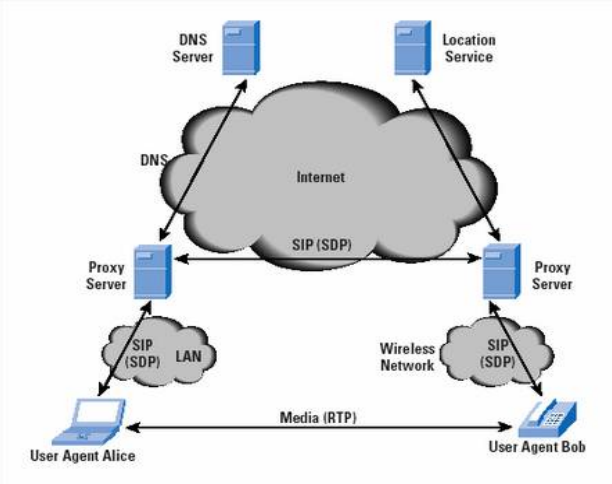


*Figura 4:* **Modelo Arquitectura de Protocolo de Inicio de Sesión (Cisco 2015).**

Dentro del proceso de una llamada a través del servicio de telefonía IP mediante protocolo SIP, existen varios tipos de métodos para peticiones y respuestas.

- **Solicitudes SIP:**

Hay seis tipos de métodos / solicitudes:

  - INVITE = Establece una sesión
  - ACK = Confirma una solicitud INVITE
  - BYE = Finaliza una sesión
  - CANCEL = Cancela el establecimiento de una sesión
  - REGISTER = Comunica la localización de usuario (nombre de equipo, IP).
  - OPTIONS = Comunica la información acerca de las capacidades de envío y recepción de teléfonos SIP

- **Respuestas SIP:**

Las solicitudes SIP son atendidas con respuestas SIP, de las cuales hay 6 clases:

  - 1xx = respuestas informativas, tal como 180, la cual significa teléfono sonando.
  - 2xx = respuestas de éxito.
  - 3xx = respuestas de redirección.
  - 4xx = errores de solicitud
  - 5xx = errores de servidor
  - 6xx = errores globales

### 2.2.3. Protocolo H.323.

H.323 es un protocolo que define la forma de establecer sesiones de comunicaciones para aplicaciones audiovisuales sobre paquetes de red, es utilizado para el servicio de telefonía y videoconferencias sobre IP, este tipo de protocolo no garantiza la calidad del servicio sin embargo fue diseñado para proveer al servicio de comunicación de voz capacidad de envío y recepción de video y datos sobre redes de conmutación de paquetes para reducir costos y aumentar el desempeño de las comunicaciones para el usuario final.

Este protocolo consta de una serie de protocolos como H.225 para el control de llamadas, el cual incluye señalización, registro y admisión, H.235 para el cifrado y seguridad, H.245 para el control de canales multimedia, T.120 para conferencia multimedia. Así también emplea una serie de codecs de audio como: G.711, G.722, G.723, G.728 y G.729 y video como: H.261, H.263 y H.264.

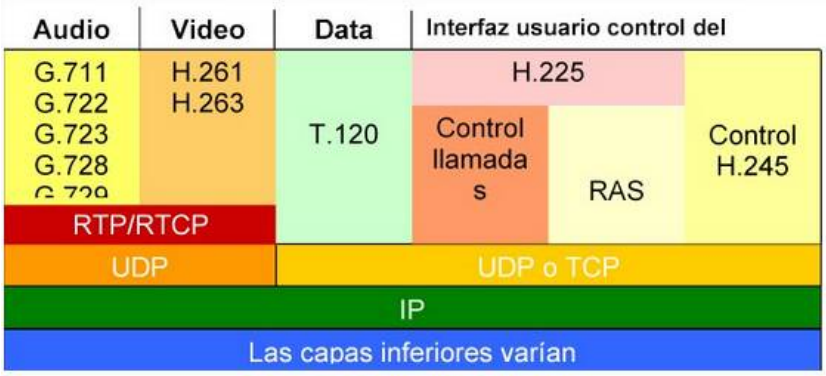


*Figura 5:* **Modelo de Protocolo H.323 (Comisión Interamericana de Telecomunicaciones 2008).**

### 2.2.4. Arquitectura H.323.

Debido a su estándar y componentes, H.323 permite el control de tráfico de la red, lo cual asegura que no existan caídas en su desempeño, además, de la independencia de hardware o tipo de red para su aplicación., además es un estándar que comprende un conjunto de protocolos de señalización que permiten controlar el establecimiento, mantenimiento y liberación de conexiones de multimedia (audio, vídeo y datos) sobre redes de paquetes, actualmente se encuentra en la versión 4 desde el año 2000. Y es comúnmente conocida como *"Packet based multimedia communications systems"*, Está determinado según el modelo por 4 elementos funcionales tal como se aprecia en la **Figura 3**.

- **Terminal H.323:** Es un terminal que establece comunicación bidireccional en tiempo real con otro terminal, pasarela o unidades de control multipunto (MCU), soportando la trasmisión de voz, datos, video, o al menos una de ellas.
- **Pasarela H.323 (GW)**: es un elemento que permite inter-operar terminales H.323 entre redes de circuitos, provee acceso permanente a la red IP conectándose con otros terminales H.323 u otras pasarelas, necesariamente debe tener dos interfaces para adaptación y convergencia entre ambas. Las llamadas de voz se digitalizan, codifican, comprimen, descomprimen, decodifican y rearman tanto en el Gateway de origen como de destino. El

Gateway es un elemento esencial en la mayoría de las redes, su misión es la de enlazar la red VoIP con la red telefónica analógica PSTN[3].

- **Unidad de Control Multipunto (MCU):** Es el elemento de la red H.323 que permite establecer comunicaciones multipunto, está compuesta por el controlador multipunto (MC) que se encarga de la negociación y control de miembros del grupo, y el procesamiento multipunto (MP) que se encarga de realizar la mezcla de medios (audio, voz, video). Esta funcionalidad de la MCU puede ser integrada en un terminal H.323.
- **GateKeeper (GK):** Proporciona y desarrolla servicios para al resto de elementos anteriormente mencionados, a pesar de ser un elemento opcional, este elemento permite realizar traslación de direcciones, autorización de llamadas, control de admisión, control de zonas, gestión de ancho de banda, gestión de llamadas, reserva de ancho de banda, servicios de directorio, entre otros.

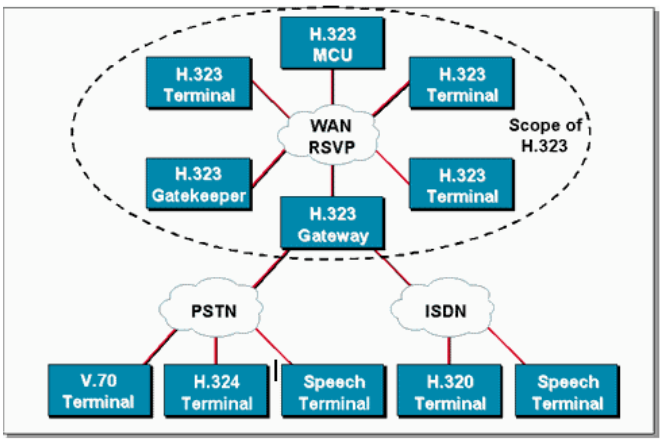


*Figura 6: Modelo* **Estándar *H.323 (***Seminaria Entorno Educativo2010).

[3] Pearson Education Inform IT. (2015). Capítulo 5. La Red Telefónica Pública **PSTN**. Recuperado de: http://www.informit.com/library/content.aspx?b=Signaling_System_No_7&seqNum=29

### 2.2.5. Otros Protocolos de comunicación para telefonía IP.

- **IAX:** El protocolo IAX (*Inter-Asterisk Exchange*) es un protocolo abierto y fue desarrollado para conexiones de VoIP entres servidores Asterisk. Es utilizado como protocolo de transporte a través de puertos UDP y RTP, las características principales son:
    - Empaquetar múltiples funciones dentro de un flujo de datos consumiendo menos ancho de banda y permitiendo mayor número de canales de comunicación entre terminales.
    - Permite la autenticación entre terminales.
    - La versión IAX2, permite trabajar con equipo que utilizan el enmascaramiento de direcciones IP (NAT).

Este protocolo es uno de los más utilizados por Asterisk en el manejo de conexiones entrantes entre equipos servidores de telefonía. Actualmente este protocolo no se utiliza debido a que ha sido suplantado por el protocolo IAX2. IAX provee control y flujo de datos multimedia sobre redes IP, incluyendo estándares de transmisión de datos tipo SIP.

- **IAX2:** Permite manejar diferentes tipos de codecs de audio como G.729, G.723, G.711 (codecs de audio, especialmente utilizados en centrales Asterisk), es utilizado para el servicio de conferencia o *streaming*, el mayor uso de este protocolo es a nivel interno debido a su seguridad y señalización de datos, además del soporte de *trunking* con lo cual se puede enviar datos de señalización por múltiples canales. El principal objetivo de IAX e IAX2 es reducir el uso del canal de ancho de banda.

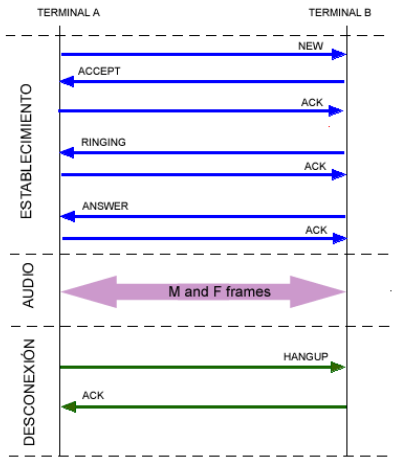


*Figura 7:* **Funcionamiento de Protocolos IAX e IAX2 (Seminaria Entorno Educativo2010).**

- **MGCP:** A diferencia de los protocolos SIP y H.323 basados en conexiones punto a punto, este protocolo está orientado en la conexión cliente / servidor, utiliza el protocolo de descripción de sesión (SDP) para describir y negociar la comunicación.

  MGCP es un protocolo de la capa de aplicación, se basa en la arquitectura de control de llamadas tipo maestro-esclavo, manteniendo la inteligencia del control de llamadas

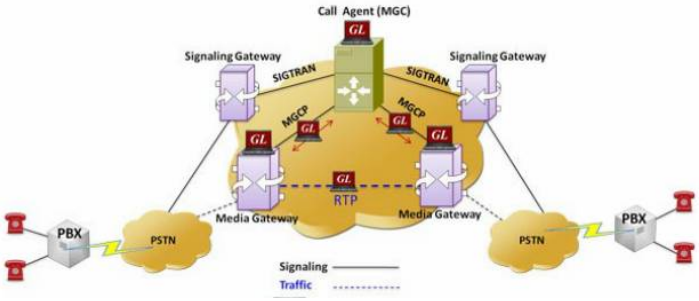


*Figura 8:* **Funcionamiento de Protocolos MGCP (GL Communications Inc. 2013)**

- **SCCP (skinny client control protocol):** Protocolo propietario de Cisco, basado en el modelo cliente servidor, toda la carga de procesamiento, control, señalización, establecimiento y transmisión de la comunicación se encarga el servidor de telefonía IP.

  SCCP define un conjunto de mensajes entre un teléfono IP con un cliente *skinny* y un servidor de llamadas (Call Manager). Es el protocolo de señalización para la comunicación con el servidor utilizando TCP/IP. Y está diseñado como protocolo de comunicaciones para clientes con hardware limitado tanto para CPU como memoria.

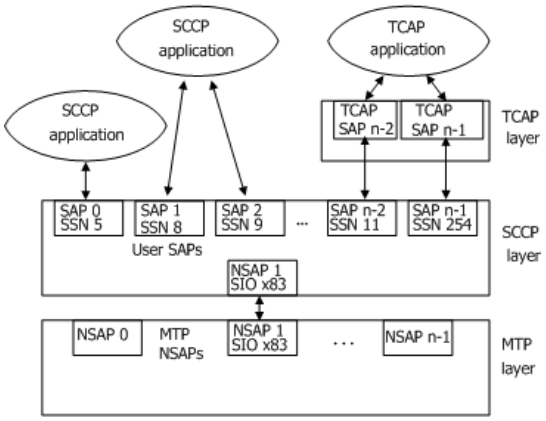


*Figura 9:* **Funcionamiento de Protocolos SCCP (NMS Communications 2013).**

## 2.3. Protocolos de transporte de voz sobre redes IP.

Los protocolos de transporte se encargan de asegurar que los datos de una comunicación lleguen intactos del origen al destino y viceversa, determinando los requerimientos necesarios de calidad de servicio *QoS* y ancho de banda adecuados. Los protocolos más utilizados para las comunicaciones de voz y datos son RTP y

RTCP. Estos protocolos fueron diseñados específicamente para la comunicación en tiempo real, con base a los protocolos de señalización y las comunicaciones de voz y video. Entre los protocolos de transporte más utilizados se determinan RTP y RTCP.

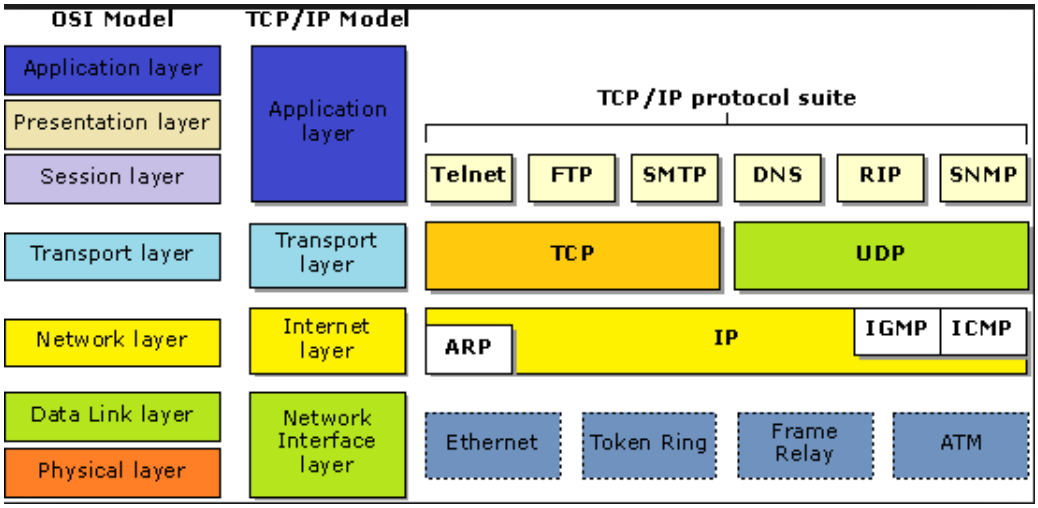


*Figura 10:* **Protocolos de transporte IP en el modelo OSI. Elaborado por el Autor.**

## 2.3.1. Protocolos RTP Y RTCP.

El protocolo de Transporte en Tiempo Real (RTP) fue diseñado con la finalidad de soportar la creciente demanda de recursos y servicios en línea como música, video, telefonía transmitidos a través de Internet. Es así como también se determina el uso del protocolo RTCP, que a diferencia de su predecesor utiliza mecanismos de control (CP) para su retroalimentación y determinar así de manera continua la calidad de la transmisión de datos en el canal de comunicación.

RTP y RTCP se ejecutan sobre el protocolo UDP, lo cual significa asegurar un menor retardo y mayor velocidad en la entrega del paquete, multiplexando varios flujos de datos en tiempo real en un solo flujo de paquetes UDP ya sea a uno o varios

destinos, teniendo así la característica de ser (*unicast*) o (*multicast*). Adicionalmente este protocolo integra un marcador de tiempo denominado (*time-stamping*) el cual se encarga de establecer los tiempos de inicio y fin de transmisión entre origen y destinatario de comunicación, encontrando la capacidad de almacenar un buffer en el receptor de una comunicación para reducir los efectos de fluctuación de la comunicación.

En la actualidad los protocolos RTP y RTCP son utilizados en el servicio de transmisión multimedia en tiempo real sobre protocolo IP, ofreciendo calidad de servicio y soporte para variedad de algoritmos de codificación de audio y video. Así también es necesario mencionar el estricto esquema de seguridad que se debe cumplir y garantizar para el uso de este protocolo debido a su vulnerabilidad de ser alterado o modificado.

### 2.3.2. Protocolo RTSP.

RTSP a diferencia que sus predecesores RTP y RTCP es un protocolo no orientado a conexión, que establece y controla uno o varios flujos sincronizados de datos, sin embargo puede determinarse a través del uso de paquetes sobre TCP para el control del reproductor de transmisión de comunicación y paquetes UDP para el proceso de *streaming* de voz y video en tiempo real, utiliza 3 tipos de operaciones para su funcionamiento:

- **Recupera contenidos multimedia del servidor:** solicitar la descripción de un método de comunicación, *unicast* y *multicast*, puertos y direcciones de acceso.

- **Invitación de un servidor multimedia a una conferencia:** Permitir el acceso a métodos de conferencia distribuido.
- **Adición multimedia a una presentación existente:** permite establecer presentaciones en vivo.

Las principales características de este protocolo es ser: seguro a través de mecanismos de seguridad como TLS, extensible en métodos y parámetros, con capacidad multiservidor, independiente del protocolo de transporte sea con en UDP o TCP y capacidad multi-servidor con el manejo y administración de flujos multimedia en diferentes servidores, en la **Figura 5** se determina la estructura de componentes del protocolo RTSP.

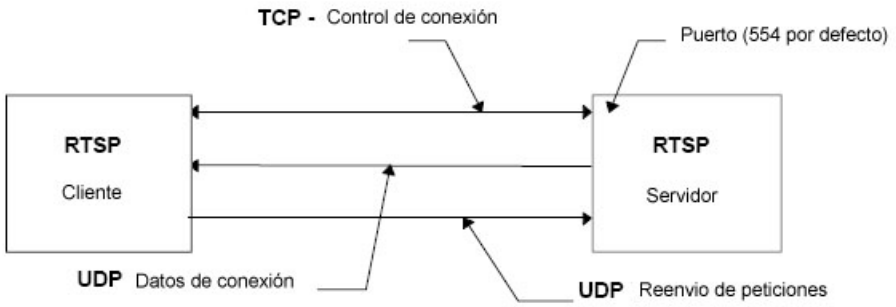


*Figura 11:* **Modelo de Protocolo RTSP (Cisco 2008).**

## 2.4. Funcionalidades del servicio de telefonía de voz sobre IP

La telefonía de voz sobre el protocolo IP ha sido determinada como un servicio vital para el beneficio y uso de las personas en su entorno grupal y organizacional, obteniendo varios beneficios para su negocio como: mejorar el panorama de

continuidad de negocios, reducir costos de administración y operación, permitir que las compañías reaccionen para cambiar con eficacia, mejorar el servicio al cliente, entre otras[4]. Es así como se han determinado diferentes tipos de soluciones, de las cuales se enmarcan las principales características; convergencia, presencia, colaboración y movilidad.

### 2.4.1. Convergencia.

La convergencia es la principal funcionalidad del servicio de telefonía IP dentro de las organizaciones, donde se integran las telecomunicaciones y las aplicaciones, la tendencia actual en los sistemas de comunicación sobre redes IP es determinar estándares de aplicaciones de software que permitan orientar a las organizaciones hacia una nueva forma de comunicación. El servicio de telefonía IP puede ser utilizado de manera conjunta, el objetivo principal es reducir el tiempo que toma la comunicación entre individuos separados geográficamente.

Dentro de la convergencia en el servicio de telefonía IP se determina el uso del sistema de comunicaciones de Internet, donde se integran las interfaces informáticas y telefónicas a través del uso de la tecnología CTI, permitiendo la interacción de llamadas telefónicas a través del computador, un ejemplo de este tipo de aplicaciones es la aplicación *"Microsoft Lync"*, *"Interaction Client"*, entre otras. Así también la convergencia se aplica en la característica de movilidad a través del uso de teléfonos

[4] NEC de México S.A. (2011). Comunicaciones Unificadas, Convergencia de los canales de comunicación. Recuperado de: http://www.necmex.com/nec/soluciones-comunicaciones-unificadas.php

celulares y dispositivos inteligentes móviles, en cuyo campo se ha incrementado el desarrollo y uso de aplicaciones comúnmente denominadas *"app"* las cuales en la actualidad son requeridas por todo tipo de organizaciones, no sin antes manejar dos claras características que deben ser integradas; la seguridad por la confidencialidad de la información tanto de usuarios como de organizaciones, y la interoperabilidad por el funcionamiento de aplicaciones en diferentes tipos de marca y modelos de dispositivos móviles.

### 2.4.2. Presencia.

La presencia muestra el estado de disponibilidad de una persona para comunicarse a través del servicio de telefonía IP con otras personas, ya sea a través de su computador, un dispositivo telefónico, o a su vez con un dispositivo móvil, como una aplicación ícono de esta funcionalidad se puede encontrar los clientes de aplicaciones telefónicas de software *"softphones"*, los cuales alertan la presencia y conexión de un sujeto. Debido al éxito que se tuvo en los años 90 con sistemas de mensajería instantánea a través del Internet, poco a poco se fueron desarrollando herramientas de uso corporativo y laboral que permitirían agilizar la comunicación y por ende los funciones laborales empresariales. La presencia implica fácil acceso y disponibilidad en el servicio para el usuario final y su entorno organizacional.

### 2.4.3. Colaboración.

La colaboración involucra la participación de dos o más sujetos trabajando en conjunto para alcanzar un bien común, es así que para desarrollar esta funcionalidad en el servicio de telefonía IP, se determina el uso de varias herramientas como por ejemplo; vistas y pizarras compartidas, transferencia de archivos, navegación web compartida. La funcionalidad y características avanzadas dependerán de cada aplicación en el tipo de herramienta libre o propietaria para que los usuarios trabajen de manera integrada, independientemente de la ubicación física en la que se encuentren.

### 2.4.4. Movilidad.

El uso de teléfonos celulares y dispositivos móviles a través de los años ha permitido desarrollar y determinar el uso de aplicaciones que permiten brindar la capacidad de conexión y acceso a las diferentes herramientas de comunicación personales y organizacionales a tal punto que hoy por hoy, se establece la tendencia (BYOD) *"Bring your own device"*, tendencia que conlleva el uso de aplicaciones móviles de correo, chat y servicio de voz para los miembros de una organización en un mismo dispositivo, integrando las funcionalidades anteriormente descritas; convergencia, presencia y colaboración para el servicio telefónico de VoIP.

La integración de las comunicaciones personales y sobre todo empresariales conlleva aspectos de seguridad e interoperabilidad que deben ser considerados en el

diseño e implementación de todo tipo de aplicaciones, a fin de evitar daños en la integridad misma de la información.

## 2.5. Objetivos de los servicios de telefonía en una arquitectura de VoIP.

El objetivo del servicio de la telefonía de voz sobre IP es optimizar los procesos y procedimientos laborales en el entorno de la comunicación de una Organización, mejorando y simplificando los procesos que benefician las ganancias del negocio, a través de la integración conjunta de los servicios de telefonía, correo electrónico, mensajería instantánea y conferencias. Adicionalmente el servicio de telefonía IP ofrece una manera de integrar las funciones de comunicación directamente en las aplicaciones de negocio, lo que según Gartner denomina la "CEBP"[5], es decir, "capacidad de comunicación habilitadora para procesos de negocio". El alcance de la integración de las funciones de comunicación directamente aplicadas en los sistemas y el uso de aplicaciones de los individuos es la de incrementar la latencia humana, entendiéndose por "latencia humana" a la mejora de la productividad personal vinculada a los procesos de negocio.

Tomando como referencia el caso de estudio que anualmente realiza Gartner en referencia al análisis del cuadrante mágico para aplicaciones de Comunicaciones Unificadas, se determina tres áreas funcionales como objetivos principales donde se

[5] Gartner Inc. (Abril 2006). **CEBP**: Achieving Agility Through Communication-Enabled Business Processes. Recuperado de: http://lib-resources.unimelb.edu.au/gartner/research/137800/137838/137838.pdf

hace un enfoque especial al servicio de telefonía IP y su integración con la convergencia de servicios de comunicaciones en línea:

- **Servicio de telefonía VoIP con enfoque personal:** Orientado hacia la persona como tal, se centra en los teléfonos y dispositivos inteligentes, incluyendo teléfonos celulares, tablets y computadores portátiles, determina presencia y disponibilidad de estado para las personas o recursos compartidos simplificando la ejecución de tareas diarias en las labores de una organización.
- **Servicio de telefonía VoIP con enfoque a grupos de trabajo:** Orientado a brindar el apoyo necesario para lograr el trabajo grupal con la ayuda de aplicaciones como salas virtuales de conferencia y entornos de trabajo compartidos.
- **Servicio de telefonía VoIP con enfoque corporativo:** Combina las comunicaciones a nivel empresarial incluyendo los procesos de negocio y las diferentes áreas organizacionales de una Empresa. Permitiendo así la toma de decisiones en tiempo real para la ejecución de procesos.

La convergencia de los tres tipos de enfoques asegura la generación de oportunidades de negocio marcando claras tendencias de cambio en el mercado, permitiendo la generación de mayores beneficios como; facilidad de uso de diferentes canales de comunicación con recursos comunes, velocidad en la comunicación telefónica, y experiencia en fidelidad de audio y video para llamadas telefónicas y videoconferencias.

## 2.6. Entorno de las organizaciones y el mercado con el servicio de la telefonía IP.

En el entorno de las organizaciones día a día el volumen de la información es creciente y diversificado por lo cual es necesario asegurar la velocidad, el control y seguridad de la información del negocio, es así como el servicio de telefonía IP es la alternativa ideal para las empresas que desean optimizar gastos de operación y agilizar el proceso de gestión y manejo de información en la operación de sus comunicaciones, resultando en una herramienta de generación de ventaja competitiva.

Dentro de toda organización debe existir la sinergia suficiente entre las áreas de Control de Gestión, el área Informática y el área de Compras, a fin de que puedan establecer los parámetros necesarios para establecer la contratación y puesta en funcionamiento del uso del servicio de telefonía IP. El uso de este servicio es de tipo discrecional por lo cual la definición de una estrategia adecuada de implementación y uso es necesario para un entorno adecuado y controlado de gestión de comunicación.

La integración de servicios virtuales y de movilidad, características propias del servicio de telefonía IP, permiten facilitar el despliegue de trabajo remoto y el acceso a la información a pesar de que los usuarios se encuentren en diferentes ubicaciones físicas a la de su oficina habitual. Actualmente las Empresas a nivel mundial buscan en este servicio la ventaja competitiva que les permita evolucionar tecnológicamente frente a su competencia a fin de abarcar un mercado global, reduciendo los tiempos y costos de operaciones.

En cuanto al aspecto económico, la implementación del servicio de telefonía IP en las Empresas implica una importante inversión, lo cual se convierte en un activo estratégico, a su vez la ejecución de convergencia que se den a los servicios de voz, datos y video implicarán una reducción de gastos de operación[6] *"OPEX"* que a mediano plazo, aproximadamente 18 meses, se manifestarán claramente a través de un análisis del Retorno de Inversión *"ROI"*. La convergencia de las Tecnologías de la Información y Comunicación aprovechan las ventajas de esta servicio como herramienta esencial para obtener mayores ventajas de la nueva economía digital establecida en el mercado mundial y la facilitación de la relación entre clientes, empleados y proveedores de las Empresas

En cuanto al aspecto tecnológico, enmarca la interoperabilidad entre las diferentes marcas y soluciones que se tienen hoy en día, a través del uso de protocolos y estándares abiertos se determina la operación de aplicaciones y servicios, sin embargo el uso de protocolos y aplicaciones propietarias aún compiten por ganar espacio en el mercado mundial.

## 2.7. Soluciones de telefonía IP para empresas.

Invertir en el servicio de telefonía IP dentro de una empresa determina el incremento de la productividad y la capacidad de respuesta en las funciones operativas, así como el desarrollo efectivo de los procesos organizacionales a través de las herramientas actuales de tecnología, complementando la infraestructura de TI,

[6] Diffen Comparition, (2012). Capex vs Opex. Recuperado de: http://www.diffen.com/difference/Capex_vs_Opex

la seguridad, el manejo de medios, aplicaciones de comunicación, e interoperabilidad de redes. Dentro de este contexto es necesario puntualizar características necesarias para una eficaz aplicación de las soluciones de Comunicaciones Unificadas en las Organizaciones, estas son:

**Protección de la inversión**: Es necesario determinar planes de protección de la inversión establecida tanto en hardware como en software, asegurando la continuidad de la funcionalidad a través de contratos de SLA[7] y soportes técnicos proactivos con tiempos de solución inferiores a 2 horas con los fabricantes o canales especializados para las soluciones implementadas.

**Conectividad y presencia integral**: Implementar aplicaciones y herramientas que permitan mantener la mayor parte del tiempo conectados a los usuarios móviles y fijos de una organización a través del servicio de telefonía IP, accediendo al servicio de voz con características de alta calidad.

### 2.7.1. Esquema de red para soluciones de telefonía de VoIP en las organizaciones.

Uno de los objetivos primordiales a la hora de diseñar e implementar sistemas de VoIP en una red organizacional es definir su esquema de red, en el cual se definan todos los equipos necesarios para garantizar tanto el funcionamiento del servicio, así como la seguridad de la información que en ella se maneje. Es así que es necesario

[7] TechTarget. (2015). Service Level Agreement **(SLA)**. Recuperado de: http://searchitchannel.techtarget.com/definition/service-level-agreement

integrar en un solo diseño, la red a nivel tanto de área local LAN, como de área extendida WAN y acceso al servicio de Internet.

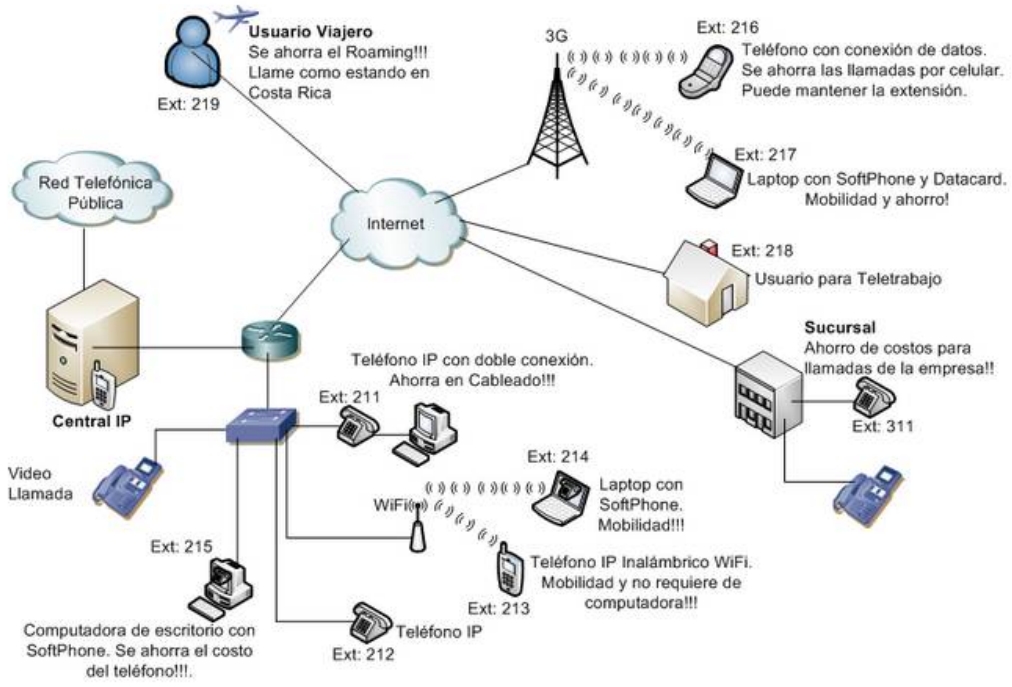


*Figura 12:* **Diagrama Integral de servicio de telefonía IP para una organización (Telefonía IP Chile 2013).**

Se describe a continuación el diagrama integral de esquema de red funcional para el servicio de telefonía IP dentro de una organización, el mismo es aplicable para cualquier tipo de plataforma; privada o de código abierto, en ella se contempla un diseño de red LAN tipo estrella para el uso de los diferentes terminales de telefonía IP físicos o de software para la oficina principal y sus sucursales. Así también se denota el uso y conexión de la telefonía IP con otros tipos de tecnología de comunicación como la telefonía móvil a través del uso de paquetes de datos o la red de telefonía pública *PSTN.* Para determinar la conexión del servicio de telefonía IP

con otras sucursales, dispositivos móviles con servicio de datos y *roaming* se determina mediante el uso del servicio de *Internet*, permitiendo así enmarcar una de las características principales de la telefonía IP (presencia y movilidad).

Principales aplicaciones líderes para el servicio de telefonía IP sobre plataformas propietarias y de código abierto.

### 2.7.2. Solución de telefonía IP CISCO.

Cisco integra dos tipos de soluciones para telefonía IP a nivel empresarial; SBCS (*Cisco Smart Bussines Comunication System*) y CUCME (*Cisco Unified Comunication Manager Express*), las cuales pueden ser adaptadas a cualquier tipo de empresa. Ambos sistemas permiten el tratamiento del servicio de voz, movilidad y presencia. Estas soluciones utilizan tanto dispositivos físicos como teléfonos IP así como *softtphones* y soporte para ambientes tipo Microsoft o Macintosh.

Las soluciones de telefonía de Cisco permiten aplicar una serie de funciones basadas en SIP, entre las cuales se puede describir:

- Compatibilidad con aplicaciones basadas en presencia.
- Compatibilidad con teléfonos de otros fabricantes que soporten SIP.
- Enlaces con troncales SIP.
- Control de límite de sesiones.
- Administración y mantenimiento de fácil gestión.
- Integración con listas de directorios activos empresariales.

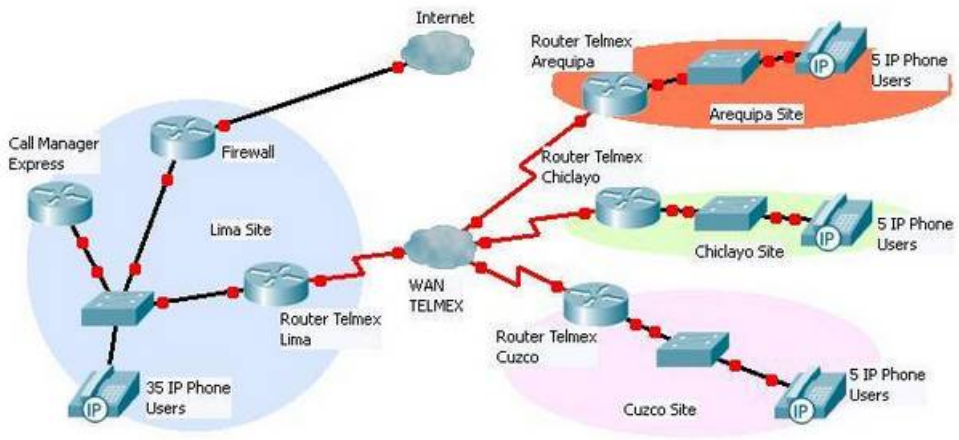


*Figura 13:* **Esquema de servicio de telefonía IP CISCO. (Cisco 2013).**

El diseño de red para la solución de telefonía IP de Cisco, establece tanto el uso de encaminadores a través de una red WAN para la oficina Matriz como las oficinas sucursales, así como el uso del servicio de Internet para la comunicación con otras organizaciones. El ejemplo tomado pertenece a una organización Peruana que utiliza este servicio, para lo cual utiliza solamente equipos terminales telefónicos físicos.

Visión de Seguridad: En cuanto a seguridad, Cisco propone la aplicación de un equipo de control de límites de sesiones SBC (*Cisco Unified Border Element*) escalable, el cual permite interconectividad entre las redes de VoIP independientes y los gateways de teléfonos analógicos. Así también se deben asegurar las siguientes configuraciones:

- Configuración del acceso local y remoto.
- Habilitación de contraseñas cifradas y secretas.
- Restricción del acceso tty y configuración del SSH

- Uso de ACL para acceso SNMP.
- Deshabilitar el protocolo CDP (*Cisco Discovery Protocol*).
- Configuración del core para llamadas entrantes y salientes.
- Restricción de patrones para llamadas salientes.
- Configuración de contabilidad y auditoría para el sistema.

### 2.7.3. Solución de telefonía Microsoft Lync 2013.

Microsoft propone como aplicación para el servicio de telefonía de VoIP dentro de su plataforma de comunicaciones unificadas la aplicación ***Enterprise Voice,*** el cual es un protocolo de voz que permite la comunicación e interacción con los sistemas de telefonía PBX IP. Permite el uso y aplicación de funciones como:

- Presencia.
- Mensajería Instantánea, colaboración y reuniones.
- Respuestas automáticas de llamadas y llamadas en espera.
- Integración con listas de directorios activos empresariales.
- Integración de correo de voz con la mensajería unificada de Microsoft Exchange.
- Compatibilidad con teléfonos de otros fabricantes que soporten SIP.

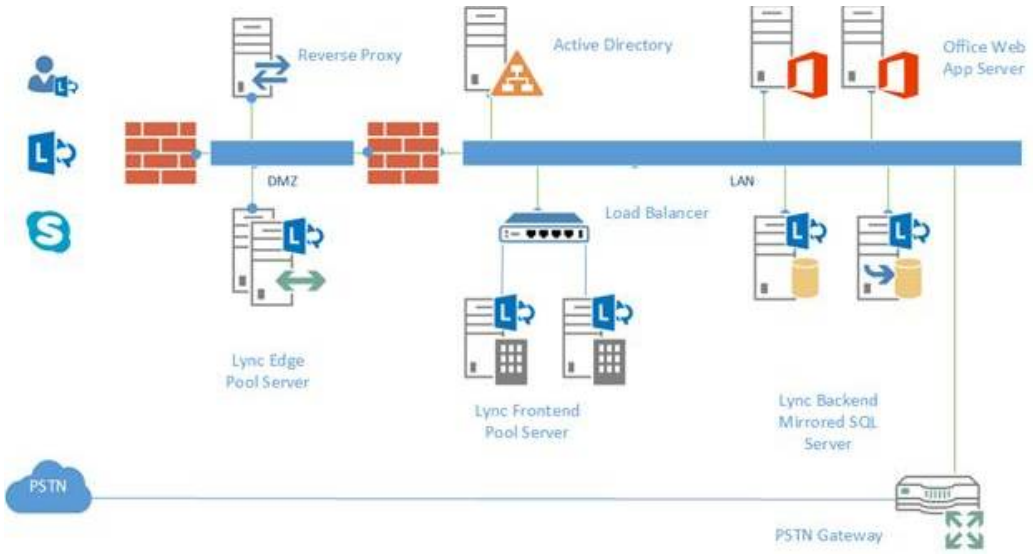


*Figura 14:* **Esquema de servicio de telefonía LYNC 2013. (Microsoft 2013).**

Dentro del diseño de red y uso de la aplicación Lync 2013, se contempla la sincronización y validación de usuarios a través de los servidores de Directorio Activo, Office Web App, Proxy Reverso, los cuales prestan características integrales para el uso de comunicaciones unificadas y con varias opciones de uso en aplicaciones ofimáticas además de las comunicaciones de voz. Lync Server Utiliza el protocolo SIP para el servicio de telefonía IP y es compatible con los codecs de Audio G.711, G722, G.723.1, utiliza también CAC (control de admisión de llamadas) para establecer límites a las conexiones de voz y video de los enlaces establecidos

Visión de seguridad: Para determinar los parámetros de configuración necesarios para la seguridad de la aplicación Microsoft Lync 2013, además de las bases de datos y el hardware, es necesario contemplar los siguientes puntos:

- Definir la autenticación de servidor a servidor.
- Control de acceso basado en roles.
- Certificados para servidores perimetrales.
- Traducción de direcciones de red.
- Configuración y perfiles de la administración tanto por consola de PowerShell como de la interfaz web.

### 2.7.4. Solución de telefonía Avaya IP Office.

La aplicación para brindar el servicio de telefonía de VoIP de Avaya IP Office está orientada a pequeñas empresas. Para grandes corporaciones se determina la solución (*Avaya Aura Application Server* 5300), la cual integra todos los servicios de comunicaciones unificadas.

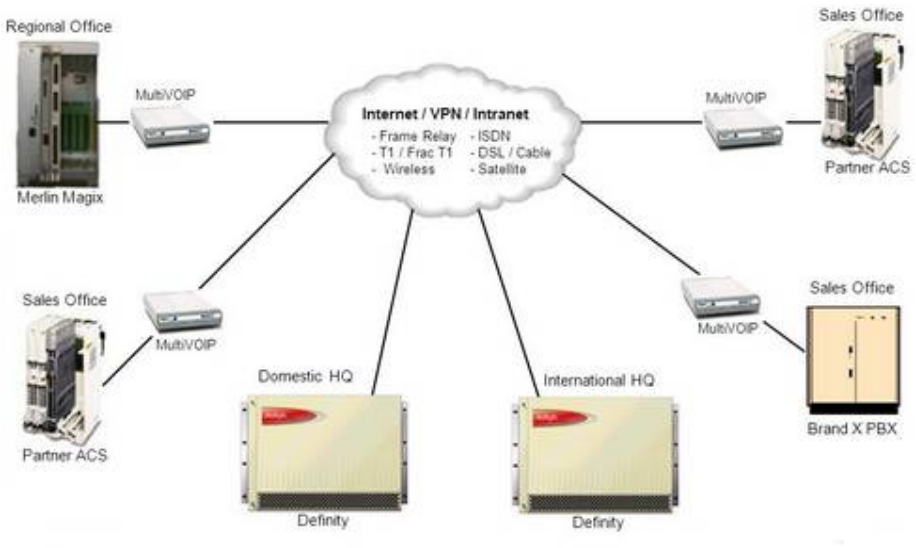


*Figura 15:* **Esquema de servicio de telefonía Avaya IP Office. (Avaya 2013).**

El esquema de red que utiliza el servicio de telefonía IP de Avaya, utiliza sistemas de red tipo Internet, intranet y redes privadas virtuales (VPN) para la conexión de sus usuarios ya sea entre sus diferentes sucursales dependiendo del tipo de servicio y de tecnología utilizada. Determina conexiones de red tipo estrella.

Establece el servicio de comunicación telefónico integrando el servicio de correo de voz, correo electrónico y mensajería instantánea a través de dispositivos físicos como teléfonos IP, *Softphones* y dispositivos móviles inteligentes. Avaya IP Office presenta las siguientes características que diferencia su producto de las otras marcas:

- Colaboración en tiempo real y multi-presencia.
- Solución escalable y adaptable a las necesidades y servicios.
- Integración de correo de voz con la mensajería unificada de Microsoft Exchange.
- Compatibilidad con teléfonos de otros fabricantes que soporten SIP.
- Soporte de tecnología Digital y analógica.
- Enlaces con troncales SIP.
- Fácil administración y mantenimiento de la solución.

Visión de seguridad: Para el manejo y escalabilidad del sistema de gestión de seguridad, Avaya determina el uso de un equipo de control de límites de sesiones SBC (*Session Border Controller*). Así también los siguientes parámetros de configuración sobre la plataforma:

- Configuración de las características TLS, desactivando los cifrados inseguros.
- Configuración de acceso basado en roles (RBAC).

- Activación de dominios de confianza (PKI).
- Desactivación de todos los puertos que no se requieran.
- Habilitar el sistema de auditoría y registro de eventos.
- Filtrado ICMP.
- Bloqueo de llamadas no permitidas.

### 2.7.5. Solución de telefonía Asterisk.

Asterisk es una central telefónica para la provisión del servicio telefónico VoIP en una organización, al igual que las aplicaciones propietarias trabaja con el protocolo SIP y proporciona todas las funcionalidades y características necesarias para la operación del servicio, actualmente Asterisk es el líder mundial de plataformas de telefonía de código abierto, y su aplicación puede ser instalada sobre cualquier tipo de computador que tenga sistema operativo GNU-Linux y con las interfaces apropiadas para telefonía.

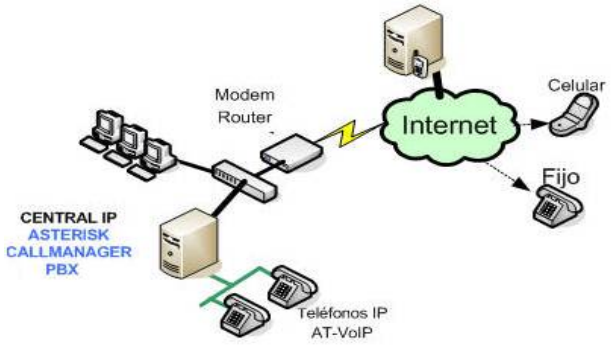


*Figura 16:* **Esquema de servicio de telefonía Asterisk. (Aprenderedes 2013).**

Además de todas las funcionalidades que ofrecen las aplicaciones de telefonía propietaria como Cisco, Microsoft, Avaya. Las principales características de Asterisk se describen a continuación:

- Escalabilidad en sus funcionalidades y capacidad de usuarios.
- Integración de protocolos de comunicación SIP y H.323 e interoperabilidad con todo tipo de centrales.
- Funcionalidad con equipos de control de límites de sesiones SBC (Session Border Controller).
- Compatibilidad con teléfonos de otros fabricantes que soporten SIP.

Visión de seguridad: Para el manejo de seguridad durante la implementación, configuración y mantenimiento preventivo de la herramienta, es necesario considerar las siguientes recomendaciones:

- Configurar la aplicación para rechazar solicitudes de llamadas de direcciones IP no seguras.
- Utilizar contraseñas complejas para todas las entidades SIP.
- Bloquear puertos de interfaz AMI (propias de Asterisk)
- Permitir un máximo de llamadas por entidad SIP.
- Desactivación de todos los puertos que no se requieran.
- Certificados para servidores perimetrales.

## 2.8. Ataques y vulnerabilidades en la tecnología de VoIP.

Como se ha mencionado en el desarrollo del presente trabajo de investigación, la seguridad de los entornos organizacionales que funcionan con la tecnología de voz sobre protocolos de Internet, específicamente el servicio de telefonía IP se ve amenazada constantemente por diferentes tipos y estrategias de ataques efectuados por delincuentes, que van desde el simple vandalismo hasta la apropiación ilegal de recursos para ocasionar fraudes a gran escala y serios daños al funcionamiento de la infraestructura del servicio de VoIP.

A través de la práctica continua de la supervisión de seguridad sobre la infraestructura de voz sobre IP, se han llegado a clasificar las amenazas por tipos de categoría de afectación, las cuales se dividen en los siguientes ítems:

### 2.8.1. Acceso desautorizado y fraudes.

El acceso no autorizado es una de las amenazas actuales de mayor importancia en cuanto a los ataques de seguridad que puede sufrir el servicio de telefonía de VoIP en entornos organizacionales, ya que pueden realizar a través de este, llamadas no autorizadas con perjuicios económicos considerables y fraudes con el robo de información de la facturación, los registros, datos de cuentas bancarias, entre otros, detalles extraídos de diferentes métodos a través de la consola de administración del servicio.

Un método de protección frente a este tipo de ataques se determina a través del control y registro estricto de llamadas o la implementación de un "cortafuegos", así como la aplicación de políticas de seguridad normalizadas por estándares como el ISO 27001.

### 2.8.2. Ataques a los dispositivos.

Los ataques de seguridad en los sistemas de voz sobre el protocolo IP actualmente se enfocan tanto a las aplicaciones así como también a la infraestructura que soporta el funcionamiento del servicio; terminales IP, *gateways,* concentradores, entre otros. Siendo cada uno de ellos potenciales puntos de afectación e infiltración para causar daño. Existen varias técnicas de ataque para tomar el control de estos dispositivos y serán analizadas posteriormente, ataques como por ejemplo; el "*fuzzing"*, *"flooding"*, *"hijacking*", entre otros.

### 2.8.3. Vulnerabilidades de la red sub-adyacente.

Uno de las principales falencias del servicio de telefonía de VoIP, es depender de la infraestructura de la red IP, la cual tiene varios puntos de vulnerabilidad que son aprovechados por diferentes métodos de ataques como; ataques de denegación de servicio, inundación de paquetes, secuestro e interceptación de sesiones, fragmentación IP o cualquier otro tipo de ataque que atente con la disponibilidad de la red en general. Así también el incremento de uso de la red inalámbrica he

permitido incrementar las brechas de seguridad por la mala configuración o aplicación de políticas de seguridad inadecuadas.

El caso particular que con mayor recurrencia se da en este tipo de vulnerabilidades del servicio de telefonía de VoIP, es el denominado “ataque del hombre del medio”, un tipo de ataque que lee todo tipo de información y paquetes entre el emisor o emisores y receptor o receptores de una comunicación, generalmente determinados por herramientas de uso libre de análisis de paquetes.

### 2.8.4. Vulnerabilidad de protocolos.

La mayoría de protocolos utilizados en las tecnologías de comunicaciones unificadas sobre IP son estándares, lo cual determina la interoperabilidad entre equipos de diferentes marcas y fabricantes a nivel mundial. La apertura de información y conocimiento del funcionamiento de estos protocolos han permitido que sean más vulnerables en ataques, entre los tipos de ataques más frecuentes son:

- **Rescritura de cabezales:** Protocolos como SIP (paquetes textuales) o H.323 (paquetes binarios) permiten la modificación de los paquetes en los cabezales de mensajes y sean reemplazados por códigos maliciosos, permitiendo redirigir una llamada o flujo de información de audio o video.
- **Denegación de servicio**: Cambio de contenido o errores en los mensajes de señalización de inicio o finalización de los protocolos, provocan la interpretación incorrecta del mensaje lo cual causa el desbordamiento de la memoria de los equipos y hasta el colapso de toda la red de comunicación.

- **Degradación de calidad:** A través de la captura de los paquetes de control de tiempo real RTCP, se puede enviar información falsa del estado de la conexión, causando consumo innecesario del ancho de banda para el servicio, llegando a causar una baja completa del servicio.

## 2.9. Tipos de ataques al servicio de telefonía IP.

Hoy en día existen diversos tipos de ataques de información al servicio de telefonía IP, cuyos objetivos van desde el robo de información, suplantación de identidad, denegación parcial o total del servicio, llamadas gratuitas, entre otros. De esta manera se han llegado a clasificar las categorías de ataques y vulnerabilidades por el nivel de impacto que conllevan según el tipo de perjuicio que causan a una organización, a continuación se describen los métodos y procedimientos de diferentes tipos de ataques:

### 2.9.1. Denegación de servicios (dos)

El ataque de denegación de servicios pretende de manera mal intencionada degradar el servicio de comunicación hasta el punto de volverlo inaccesible para los usuarios, se basa en la inundación de paquetes que saturan los flujos de datos de la red aprovechando vulnerabilidades en la infraestructura de hardware o en las aplicaciones del servicio, causando que los paquetes de comunicación de VoIP se pierdan o sufran tiempos de retardo excesivos

Es así como los diferentes tipos de herramientas y aplicaciones utilizadas para el servicio de VoIP, antes mencionadas, deben estar bajo constantes aplicaciones de parches y actualizaciones para contra-restar problemas de seguridad y ataques, entre los más comunes se encuentran:

- **UDPFlood**: Envía una tormenta de paquetes UDP al destino, su punto de quiebre es la capacidad de hardware del equipo a atacar.
- **RTPFlood**: Envía una tormenta de paquetes RTP, ataca directamente a los puertos de los equipos de comunicación por encima del puerto 8000, utilizado por defecto para cada conexión RTP.
- **INVITEFlood**: Realiza un requerimiento masivo de conexiones hacia un servidor, provocando el colapso del equipo por la saturación de recursos.
- **TEARDOWN**: Realiza envío de peticiones tipo "BYE" (para finalizar llamadas en curso), previamente el atacante necesita acceder al ID de las llamadas, lo cual se puede hacer a través de un sniffer.
- **SIP-Kill**: Script en lenguaje PERL que captura tráfico en busca de mensajes tipo "INVITE" del protocolo SIP, cortando las nuevas llamadas que detecta.

### 2.9.2. Spit (spam)

El SPAM sobre el servicio de telefonía IP, constituye en el envío de mensajes masivos no solicitados hacia otras centrales o dispositivos telefónicos conectados a Internet, lo cual implica buzones de correo de voz saturados con publicidad no

requerida, que al igual que el spam de correo electrónico son emitidos de manera simultánea a miles de usuarios.

Hasta el mes de octubre del 2014 el portal Web de www.baquia.com [8], menciona que no existen casos concretos de amenazas tipo SPIT, según lo investigado por Marketing Box, sin embargo la creciente tendencia de uso hacia aplicaciones de VoIP implica un mayor y creciente riesgo para el uso de este servicio, por lo cual ya se van determinando aplicaciones para la identificación de llamadas no solicitadas en dispositivos móviles a partir de su frecuencia y duración para enfrentar este tipo de amenazas a corto y mediano plazo.

### 2.9.3. Vishing (pishing)

El *vishing* o *pishing* telefónico, es la técnica de suplantación o robo de identidad de una organización o usuario específico en la red telefónica sobre Internet. El objetivo principal de esta práctica criminal penada por las leyes a nivel mundial, es conseguir toda la información posible de la víctima a través de sistemas telefónicos automatizados para establecer fraudes bancarios especialmente con tarjetas de crédito y códigos de acceso para transacciones en línea.

Al acceder a cualquier tipo de servicio telefónico o de comunicaciones sobre Internet, los usuarios deben tener las siguientes consideraciones para salvaguardar su información confidencial:

[8] Tecnología y Negocios. Baquia.com (Octubre, 2014). SPIT. La amenaza del spam en el móvil. Recuperado de: http://www.baquia.com/tecnologia-y-negocios/entry/emprendedores/spit-la-amenaza-del-spam-en-el-movil

- No proporcionar información personal a terceras personas de menara telefónica.
- Solicitar información sobre la persona o entidad que inicia una llamada para pedir información.
- No dar información telefónica de números de tarjeta, cuentas bancarias, cédula de identidad, número de seguro social.
- No anotar información confidencial en lugares de fácil acceso.
- Cambiar frecuentemente las contraseñas de acceso a los servicios digitales.

### 2.9.4. Fuzzing

El método de fuzzing se basa en realizar pruebas de funcionalidad de protocolos, generalmente es utilizando para encontrar errores y brechas de seguridad sobre los protocolos SIP, H.323 o RTP, creando paquetes de datos mal formados que pueden llegar a causar errores de funcionamiento, denegación de servicio y hasta vulnerabilidades más graves. Este tipo de técnicas así como son utilizadas para el desarrollo de seguridades sobre aplicaciones de telefonía IP, también son utilizadas para causar daños e intrusiones, es por lo cual deben ser consideradas en el diseño de seguridad de una organización

Existen varios tipos de herramientas que permiten realizar este tipo de pruebas, entre los más destacados se pueden mencionar:

- **PROTOS**: permite automatizar diferentes tipos de ataques contra protocolos como; SIP, HTTP, SNMP.

- **OHRWURM**: herramienta para ataques bajo protocolo RTP.
- **ASTEROID**: herramienta que permite generar paquetes mal formados para ser probados bajo protocolo SIP.

### 2.9.5. Secuestro de sesiones (hijacking).

El *Hijacking* es el secuestro de sesiones de red, servicios, terminales y todos los servicios y dispositivos tecnológicos informáticos. Existen varios tipos de secuestros de sesión entre ellos se mencionan los más mencionados:

- Secuestro de dirección IP: suplantación de identidad IP a través de terminales telnet o aplicaciones específicas.
- Secuestro de páginas web: a través de un bug de seguridad detectado por atacantes pueden realizar modificaciones y obteniendo el control de la administración de manera definitiva.
- Secuestro de dominio: se lo realiza a través de las direcciones reversas de dominio, donde el atacante puede acceder al control total del mismo.
- Secuestro de DNS: este tipo de ataque se produce cuando se modifican los DNS originales de acceso por parte de un cliente para redirigirlos a unos DNS falsos o maliciosos.

Secuestro de registro SIP: este ataque se produce cuando se desactiva el registro del protocolo SIP válido y se sustituye por una dirección IP falsa, interceptando, reproduciendo o finalizando llamadas inesperadamente.

### 2.9.6. Interceptación (eavesdroping).

Uno de los casos que con más frecuencia se presentan en las empresas con respecto a novedades en la seguridad de los sistemas de telefonía IP, es la interceptación de llamadas, a través de diferentes técnicas se establece este tipo de espionaje que muchas veces es mal intencionado. Una de las técnicas más utilizadas para este propósito es el denominado "hombre en el medio"[9], según la definición que da la revista tecnológica Web Hipertextual: "es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso, tiene la habilidad de desviar o controlar las comunicaciones entre dos partes".

La característica principal de esta amenaza es que el atacante es capaz de enrutar los paquetes de comunicación en la red para analizar el flujo de tramas y paquetes RTP y SIP para capturarlos a través de herramientas sniffer. Una de las más potentes en el mercado es *Wireshark*, la cual incorpora una utilidad que decodifica los paquetes RTP y los transforma en audio reproducible, tal como se determina en la guía de ataque de hombre en el medio tomado como referencia del portal Web Pentestlab[10].

[9] Hipertextual, Revista de contenidos Digitales. (Junio, 2014). Qué es un ataque "Man in The Middle". Recuperado de: http://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/
[10] Penetration testing Lab. (Julio, 2014). Eavesdropping VoIP Calls with Wireshark. Recuperado de: https://pentestlab.wordpress.com/2014/07/22/eavesdropping-voip-calls-with-wireshark/

### 2.9.7. Redirección de llamadas (call redirection).

Los ataques de redirección de llamadas emplean diferentes técnicas y métodos que van desde atacar los servicios de los servidores de administración o suplantación de identidad como se ha mencionado anteriormente. Una de las herramientas más utilizadas para este tipo de ataques es el ataque (*Redirect Poison*), que intercepta las peticiones INVITE del protocolo SIP, y desvía el origen de la llamada hacia donde el intruso desee.

Este tipo de técnica provoca grandes pérdidas económicas año a año para las organizaciones a través de los denominados sistemas de "Bypass" o desvíos de llamadas a servicios de llamadas local, celular o internacional.

Uno de los métodos de protección determinados para enfrentar este tipo de amenazas se realiza cerrando los puertos que no se utilicen y utilizar la autenticación de protocolos.

## 2.10. Seguridad en la Tecnología de VoIP.

Frente a las amenazas y vulnerabilidades a las cuales está expuesta la información dentro de toda organización, es necesario considerar además los aspectos necesarios para brindar las garantías de funcionamiento de los componentes tecnológicos como tal, tomando en cuenta que las tecnologías de las comunicaciones de voz y video transmitidos a través del protocolo IP presentan continuamente nuevas amenazas y ataques, en este aspecto de la seguridad es necesario determinar las mejoras en los

aspectos de confidencialidad aplicadas en varios protocolos de comunicación como SIP y H.323.

### 2.10.1. Seguridad en los protocolos.

El envío de información entre dos o varios dispositivos de comunicación electrónica es susceptible de ser interceptado y modificado, con el incremento de uso de aplicaciones de comunicación sobre diferentes protocolos de comunicación e Internet el aspecto de la seguridad en las comunicaciones dentro de las organizaciones a nivel mundial ha pasado a ser prioridad principal dentro de las políticas de los sistemas de gestión de la seguridad de la información.

Un protocolo es un estándar utilizado para la comunicación entre dispositivos, al cual se deben aplicar reglas y procedimientos para el envío y recepción de información en una red de datos con el fin de garantizar su óptimo funcionamiento y evitar riesgos o intrusiones de seguridad que puedan exponer la información transmitida y causar perjuicios legales y económicos a sus usuarios. De esta manera se establece el uso y aplicación de los protocolos de seguridad que son el conjunto de actividades programadas que emplean esquemas de seguridad criptográfica como; manejo de claves, integridad, autenticación, autorización, entre otros, para que los sistemas de comunicación puedan soportar ataques de carácter malicioso.

Existen diferentes tipos de aseguramiento para los protocolos de acuerdo a su nivel de red, transporte o aplicación.

- **Seguridad a nivel de red**: El ataque a nivel de capa de red es bastante frecuente a pesar de que las pilas de paquetes TCP/IP de los diferentes sistemas operativos son más robustas. La seguridad en este nivel busca garantizar el tráfico de los protocolos a nivel superior, es necesario adaptar la infraestructura de red para gestionar la información. A este nivel es necesario realizar las configuraciones necesarias para evitar un ataque desde el exterior a nivel de red, tomando en cuenta la seguridad sobre todo de puertos de acceso a diferentes tipos de servicio (TCP o UDP). Entre los principales protocolos a configurar en un equipo cortafuegos se encuentran:

| **Nombre** | **Puerto** | **Conexión** | **Servicio** |
|---|---|---|---|
| echo | 7 | tcp/udp | Eco: Devuelve los datos que se reciben |
| systat | 11 | tcp | Información del sistema |
| netstat | 15 | tcp | Información sobre la red |
| chargen | 19 | tcp/udp | Generador de caracteres continuo |
| SMTP | 25 | tcp | Puerto de correo |
| domain | 53 | tcp/udp | Servidor de Nombres (DNS) |
| bootp | 67 | udp | Arranque de estaciones remotas sin disco |
| tftp | 69 | udp | Arranque de equipos remotos, carga de configuraciones |
| link | 87 | udp | |
| supdup | 95 | udp | |
| sunrpc | 111 | tcp/udp | Servicio de RPC (portmapper) |
| news | 119 | tcp | Servidores de News (deberán estar ya filtrados en todos los routers de las organizaciones afiliadas a RedIRIS) |
| NetBios | 137-139 | udp/tcp | Servicios NetBios sobre TCP/IP (Windows) |
| snmp | 161 | udp | Gestión remota de equipos mediante |

| | | | |
|---|---|---|---|
| | | | SNMP |
| xdmpc | 177 | udp | Llegada de correo |
| exec | 512 | tcp | Ejecución remota de comandos (rexec) |
| login | 513 | tcp | Acceso remoto a un sistema (rlogin) |
| shell | 514 | tcp | Shell remoto |
| biff | 512 | udp | |
| who | 513 | udp | Información sobre los usuarios que hay conectados en un equipo remoto |
| syslog | 514 | udp | Almacenamiento de los logs de los sistemas en remoto |
| uucp | 540 | tcp | Envío de ficheros y mensajes mediante uucp, actualmente en desuso |
| route | 520 | udp | Información sobre enrutamientos |
| openwin | 2000 | tcp | |
| NFS | 2049 | tcp/udp | Sistema de ficheros remotos de Sun y Unix en general |

- **Seguridad a nivel de transporte**: Actualiza las implementaciones TCP/UDP en los extremos de la comunicación, para esto es necesario cambiar los enrutadores IP por infraestructura de comunicaciones que entienda IPsec, o a su vez determinar el uso de protocolos de seguridad (SSL, TLS). Los servicios de seguridad que proporcionan estos protocolos son:
    - **Confidencialidad**: intercambio de paquetes con cifrados de datos mediante claves simétricas determinando eficiencia y rapidez, utilizando dos tipos de claves para el envío y recepción de datos entre el servidor y el cliente, evitando que interfieran la comunicación de las claves a través de una clave pública encriptada.

- **Autenticación de entidad**: a través de un protocolo de autenticación de firmas digitales, el cliente puede validar la identidad del servidor.
- **Autenticación de mensaje**: cada paquete de datos además de ir cifrado incorpora un código MAC único del equipo, estas claves en cada sentido (origen y destino) son establecidas en el dialogo inicial de la comunicación.
- **Eficiencia**: La definición de sesiones y la compresión de datos permiten mejorar la eficiencia de la comunicación, identificando y re utilizando los parámetros e identificadores de sesión para optimizar el tiempo de validación de sesión en la conexión.

- **Seguridad a nivel de aplicación:** En este nivel se contemplan y se engloban las capas del modelos OSI: sesión, presentación y aplicación. Debido al gran número de protocolos presenta varias deficiencias de seguridad, por lo cual es necesario contemplar los siguientes puntos de seguridad:
  - Limitar el acceso a la ubicación de los equipos servidores.
  - Especificar las listas o grupos de usuarios con sus permisos correspondientes. Desactivar la cuenta “Anónimos” y a toda aquella que presente nombres de fácil aprovechamiento “Administrador”.
  - Requerir contraseñas seguras.
  - Controlar de manera continua los archivos de eventos tipo “log”
  - Deshabilitar índices de directorios.

- Deshabilitar todos los servicios de red que no sean empleados por el servidor.
- Auditorías permanentes de acceso remoto, de eventos del equipo cortafuegos, servidores de aplicaciones como correo, dns, ftp.

En la actualidad varios tipos de protocolos aceptan la encripción o cifrado en su contenido, para el caso de los protocolos utilizados en las aplicaciones de comunicaciones unificadas se determinan los sistemas de encriptación a nivel de transporte; *"SSL"* (*Secure Socet Layer*) o *"TLS"* (*Transport Layer Security*) tanto para el protocolo *"SIP"* como para el protocolo *"RTP"*. Estos protocolos son criptográficos y proporcionan comunicaciones seguras sobre la red de Internet. SSL proporciona autenticación y privacidad entre los extremos de una comunicación mediante el uso de criptografía, garantizando la autenticidad de los servidores a través de métodos de negociación, intercambio y cifrado.

- **SIPS:** Utiliza SSL, su norma de estandarización es la RFC4346, es un método robusto de protección contra ataques la cual valida y protege la conexión entre cada par de saltos proporcionando seguridad entre los puntos de comunicación con métodos de encriptación.
- **SRTP:** Al utilizar el protocolo RTP mediante un sistema de encriptación TLS, los paquetes son cifrados en la fuente origen de las comunicaciones y descifrado en el destino, utilizando técnicas de cifrado AES o "clave maestra" emitida por una entidad certificadora como por ejemplo: ZRTP o KEYMGT.

## 2.10. Sistemas de Gestión de la Información.

La gestión de la información en síntesis, es un proceso de acción que proporciona los recursos necesarios para la correcta toma de decisiones para la calidad y eficiencia de los servicios y productos de las organizaciones. El objetivo de la gestión de la información, según "La Gestión de Información de las Organizaciones"[11] se basa en 4 pilares fundamentales que son:

- **Maximizar** el valor y los beneficios derivados del uso de la información.
- **Minimizar** el costo de adquisición, procesamiento y uso de la información.
- **Determinar** responsabilidades para el uso efectivo, eficiente y económico de información.
- **Asegurar** un suministro continuo de la información.

La finalidad de un sistema de gestión de la información es generar servicios que respondan y sobrepasen las necesidades y expectativas de los usuarios, manteniendo un balance equilibrado entre la eficiencia y la economía de la organización, para lo cual aprovecha al máximo los recursos y realiza una mejora continua en las decisiones organizacionales a todo nivel.

Entre las principales funciones de la gestión de la información se determinan:

- Desarrollar la base informacional de la organización y garantizar su accesibilidad.

[11] Ponjúan Dante Gloria. (2004). Gestión de Información en las Organizaciones: principios, conceptos y aplicaciones. Recuperado de: file:///C:/Users/valenzuelag/Downloads/3867-3816-0-PB.pdf

- Desarrollar la estructura informacional de la organización y garantizar su operatividad.
- Garantizar la integridad y accesibilidad a la memoria corporativa.
- Establecer, aplicar y supervisar los procedimientos relativos a la seguridad de la información organizacional.
- Garantizar la calidad de los productos informacionales de la organización, y asegurar su dimensión efectiva.
- Entrenar a los miembros de la organización en el manejo o la utilización, de los Recursos informacionales de la organización.

Con respecto a la aplicación vertiginosa de la informática en las actividades comerciales y organizacionales que se han venido desarrollando en los últimos años a nivel mundial, es necesario que estas cuenten con procesos y procedimientos implantados para asegurar el manejo y seguridad en el bien más preciado de hoy en día, la información. De esta manera los *"SGSI"* proporcionan información a los directivos mediante informes o acceso directo a consultas informáticas, los cuales aportan visión de conjunto para el seguimiento y control de un aspecto especifico y la toma de decisiones a tiempo. De esta manera se han llegado a establecer estándares de manejo e implementación de sistemas de gestión de la información, los cuales pueden ser susceptibles o no de certificación o simplemente tomados como guías referenciales para un adecuado manejo de la información dentro de una empresa.

## 2.11. Entidades de regulación para las seguridades de información.

A nivel mundial existen diversas entidades que se encargan de la regularización y normalización de los procedimientos y lineamientos necesarios para la aplicación de las diferentes políticas de seguridades de la información en las entidades públicas o privadas de un país. Estas normas establecen estándares técnicos, industriales y comerciales que aplican, tanto para sus miembros simples, así como para sus miembros suscritos.

### 2.11.1. Organismos de regulación internacional.

La ISO es la Organización Internacional de Normalización, provee de herramientas prácticas, soluciones y beneficios a las empresas, los gobiernos y la sociedad, para el desarrollo sostenible de los entornos, tecnológicos, económicos, ambientales y sociales. Para el caso de las normas y lineamientos en el campo de la Seguridad de la Información, la ISO define los procedimientos a seguirse a través de otras entidades de control como; la Comisión Internacional Electrotécnica IEC, que es la organización dedicada a la elaboración y publicación de las Normas Internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas. Y la Unión Internacional de Telecomunicaciones ITU, que es la organización encargada de regular las telecomunicaciones a través de “recomendaciones” que a nivel mundial muchas veces son establecidas como políticas de uso obligatorio para las administraciones y empresas operadoras de comunicaciones.

La colaboración de estas entidades internacionales: ISO, IEC, ITU definen; reglas oficiales, documentos complementarios y guías de uso que son aplicados por los Organismos Nacionales de Normalización[12] "ONN" propios de cada país.

### 2.11.2. Organismos de regulación nacional en el Ecuador.

Tal como se ha menciona en el ítem anterior, cada uno de los países que se acogen a las normas y recomendaciones establecidas por organismos de estandarización Internacional, deben aplicar de manera interna sus políticas y lineamientos a través de entidades de control como Ministerios, Súper Intendencias o Decretos Presidenciales. Para el caso de Ecuador, las normas y políticas que se utilizan para el manejo de la seguridad de la información en el sector Gubernamental, se determinan a través del Acuerdo Ministerial vigente 166, publicado en el Registro Oficial Suplemento 88 de 25 de septiembre de 2013[13], en el cual señala: "las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.", manteniendo un Esquema Gubernamental de Seguridad de la Información EGSI.

Para el caso de las empresas privadas, depende de cada administración o gerencia el uso y aplicación de las normas técnicas ecuatorianas NTE-INEN y de los

[12] Organización Internacional de Normalización. (2010). Organismos Nacionales de Normalización en vías de desarrollo, Actividades y estructura de un Organismo Nacional de Normalización (ONN). Recuperado de: http://www.iso.org/iso/fast_forward-es.pdf

[13] Suplemento del Registro Oficial No.88, Revista Judicial electrónica, Derecho Ecuador (2013), Recuperado de: http://www.derechoecuador.com/productos/producto/catalogo/registros-oficiales/2013/septiembre/code/RegistroOficialNo88-Miercoles25deSeptiembrede2013P/registro-oficial-no-88---miercoles-25-de-septiembre-de--2013-primer-suplemento

estándares internacionales para la normalización de sus procesos internos de seguridad y manejo de la información ISO / IEC / ITU.

## 2.12. Estándares para aplicación de la seguridad de la información.

La aplicación de políticas y estándares para la seguridad de la información demanda la normalización y definición de requisitos y recomendaciones para establecer, implementar, operar y mejorar todo Sistema de Gestión de Seguridad de la Información. Es así como a nivel internacional se determinan parámetros específicos para la iniciación, implementación y mantenimiento de la seguridad de una organización, tomando en cuenta que no todos los controles son aplicables para todas las situaciones pero si conllevan obligaciones legales para su cumplimiento, de esta manera, para el presente caso de investigación se determinan 2 estándares principales para la seguridad de la información; los estándares ISO/IEC 27002 e ISO/IEC 27001 los cuales están enfocados a todo tipo de organización, pequeña, mediana o grande: empresas comerciales, agencias de gobierno, entidades bancarias, organizaciones sin ánimo de lucro.

### 2.12.1. Estándar ISO/IEC 27002.

La norma ISO/IEC 27002 ex ISO 17799, determina un código de buenas prácticas no obligatorias y sin prioridad entre controles para implementar dominios de control

y mecanismos de control en la gestión de la seguridad de la información, la cual es considerada como la base para la implementación de medidas de seguridad tras un breve y primer análisis de riesgos dentro de una organización. La versión actual de esta norma o estándar es la 27002: 2013, la cual contiene 114 controles frente a su antecesora versión 27002: 2005 que contiene 133 controles. Según el Directorio de la Norma ISO[14], el estándar ISO 27002 fue originalmente escrito por el gobierno del Reino Unido en 1995 y convertido en el estándar BS7799, posteriormente en el año 2000 fue re-publicado por la ISO como el estándar 17799 y re-editado en el año 2005. Actualmente se encuentra sometido a varias revisiones y ampliaciones a sectores como salud, manufactura, entre otros.

El uso y aplicación de las versiones que tiene este estándar para cada país, depende de cada Instituto Nacional de Normalización y la definición que este determine como política de Estado, como ejemplo tenemos: Perú ISO/IEC 27002:2000, Chile ISO/IEC 27002:2005, en el caso de Ecuador se aplica la ISO/IEC 27002:2005

Para la gestión de la seguridad en redes, el Portal de ISO 27002 en Español[15], señala que el objetivo de control del estándar ISO27002 es: “evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.”.

[14] ISO 27000 Directory (2013). The Information Portal for ISO27002, Recuperado de: http://www.27000.org/iso-27002.htm
[15] El Portal de ISO 27002en Español (2005), Términos de uso información iso27000, Recuperado de: http://iso27000.es/iso27002_13.html#seccion2

Es importante señalar que este estándar más que un requerimiento es una serie de recomendaciones que pueden ser o no aplicadas, por lo cual no es susceptible de certificación a diferencia del estándar ISO/IEC 27001.

A esta norma se anexa una serie de controles que permiten establecer los lineamientos base para determinar un SGSI dentro de una organización como política de seguridad, en su lisado se determina:

- Organización de la información de seguridad.
- Administración de recursos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Administración de las comunicaciones y operaciones.
- Control de accesos.
- Adquisición de sistemas de información, desarrollo y mantenimiento.
- Administración de los incidentes de seguridad.
- Administración de la continuidad de negocio.
- Cumplimiento (legales, de estándares, técnicas y auditorías).

### 2.12.2. Estándar ISO/IEC 27001.

El estándar ISO/IEC 27001 determina los requisitos necesarios y obligatorios para establecer, implementar, mantener, mejorar y cumplir a detalle un Sistema de Gestión de Seguridad de la Información. La adopción de este estándar dentro de una organización es el pilar estratégico para la gestión de seguridad del recurso más

valioso de toda Organización pública o privada, la información, para lo cual es necesario tomar en cuenta el análisis y gestión de los riesgos basados en los procesos de negocio y servicios de TI.

La versión actual de este estándar es la ISO/IEC 27001:2013 que cuenta con 133 requisitos a diferencia de los 104 de su predecesora versión ISO/IEC27001:2005, originalmente desarrollada en el año 2005 y que resume una evolución incorporando prácticas o controles establecidos en el estándar ISO/IEC 27002:2005, información referenciada por el Blog SGSI[16]

La implementación y certificación de este estándar dentro de una organización depende del grado de seguridad de la información que esta posee y del SGSI que haya decidido adoptar e implementar, para lo cual tomaría aproximadamente un año el cumplimiento de los requisitos que se necesitan para su estricto cumplimiento. El equipo de proyecto de ejecución de certificación deberá estar integrado necesariamente por cada integrante de las diferentes áreas de la organización involucradas con el SGSI. Para el caso del Ecuador la aplicación y certificación del estándar ISO/IEC 27001 en cualquiera de sus versiones es de carácter VOLUNTARIO según la resolución establecida en el artículo No.01 del Registro Oficial No.699 del 09 de mayo del 2012[17].

[16] Blog SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información (2013), Recuperado de: http://www.pmg-ssi.com/2013/12/iso27001-origen/

[17] Suplemento del Registro Oficial No.699, Revista Judicial electrónica, Derecho Ecuador (2012), Recuperado de: http://www.derechoecuador.com/productos/producto/catalogo/registros-oficiales/2012/mayo/code/20263/registro-oficial-no-699--miercoles,-09-de-mayo-de-2012-suplemento

### 2.12.3. Diferencias y Similitudes entre ISO/IEC 27001y 27002.

ISO 27002 no es susceptible de certificación ISO, porque no es una norma de gestión, a diferencia de la ISO 27001.

Los elementos de planificación, implementación, supervisión, revisión y mejoras son implementados en la ISO 27001 al ser un sistema de gestión de seguridad de la información, a diferencia de la ISO 27002.

Los controles de la norma ISO 27002 tienen la misma denominación que los controles del anexo A de la norma ISO 27001, pero su detalle y explicación es mínima a diferencia de lo detallado en la ISO 27002.

La ISO 27002 no distingue entre los controles que son aplicables o no a una organización, a diferencia de la ISO 27001 que realiza una evaluación a detalle de los riesgos de cada control y hasta qué punto pueden aplicarse.

Para la creación de una estructura de seguridad de información dentro de una organización es necesario establecer la norma ISO 27001, para establecer controles, evaluaciones y tratamiento de riesgos se debe establecer la norma ISO 27002.

Para el caso de ambos estándares ISO/IEC 27002 y 27001 en sus últimas versiones se denota la integración de controles en los campos relacionados con los dispositivos móviles, el teletrabajo asociado con el control de acceso y la criptografía como un nuevo dominio de control, entendiendo que estos estándares manejan: dominios, objetivos de control y controles, los mismos que serán examinados, valorados y analizados en las Matrices de Riesgos del presente trabajo investigativo.

### 2.12.4. Estándar ISO/IEC 21827:2002

Dentro del proceso de desarrollo de un Sistema de Gestión de Seguridad de la Información para una organización bajo el estándar ISO/IEC 27001, la primera dificultad a la que se enfrentan los líderes de este proyecto es la identificación de una estrategia para definir las fases de análisis, diseño e implementación del proceso global de seguridad, tomando en cuenta que el estándar para la determinación de los procesos de seguridad son tratados a través del estándar internacional ISO/IEC 21827:2002 (*Information Technology - Systems Security Engineering – Capability Maturity Model* "SSE-CMM"). Esto debido a que el éxito para todo tipo de implementación SGSI siempre está determinado por el éxito de la implementación del proceso global de seguridad, encargado de alcanzar niveles concretos de capacidad, cumplimiento de leyes y normas de seguridad, así como la certificación conjunta con otros estándares internacionales.

La ingeniería de la seguridad viene dado por las siguientes características:

- **Seguridad**: Establecer y mantener todo tipo de medidas de protección ante actos de ataques de seguridad.
- **Supervivencia**: Determinar la continuidad de funcionamiento mínimo del servicio durante y después de un evento de intrusión que afecte la seguridad y el tiempo mínimo que le tome sobreponerse ante un nuevo evento.
- **Sistema**: Organizar los recursos por personas, equipos y métodos organizados para cumplir un conjunto específico de funciones.

La utilidad del modelo SSE-CMM viene determinado en base a dos dimensiones; su dominio y capacidad. La dimensión del dominio define la ingeniería de la seguridad, a través de 60 prácticas divididas en 11 áreas de proceso. En cuanto a la dimensión de la capacidad o denominada también, prácticas genéricas, comprende las prácticas que indican la capacidad de gestión y la institucionalización del proceso.

El modelo de referencia para la seguridad en proyectos SGSI viene determinado por seis disciplinas fundamentales[18]: seguridad fundamental; seguridad ambiental y en infraestructuras; seguridad en los sistemas; seguridad en comunicaciones y redes; seguridad física y la seguridad de las personas.

Las ventajas de utilizar procesos de seguridad dentro de un proyecto SGSI, integrando los estándares SSE-CMM (ISO/IEC 21827) y 27001, viene dado por tres ejes fundamentales que son: seguridad fundamental (asegurar la continuidad del negocio), proyectos en ámbitos sectoriales nivel de capacidad 3 (objetivos y ámbitos bien definidos), leyes y reglamentos para definir políticas de manejo, uso y aplicación.

## 2.13. Sistemas de gestión de la seguridad de la información - SGSI.

En la actualidad las organizaciones y sus sistemas informáticos enfrentan nuevos y variados tipos de ataques a sus sistemas de información, desde fraudes, sabotaje o

[18] José Antonio Calvo-Manzano / Ana de las Heras Artículo No.75 Revistasic.com. (Junio 2007). La Ingeniería de Seguridad como ayuda al desarrollo de los SGSI. Recuperado de: http://revistasic.com/revista75/pdf_75/sic75_articulo.fpd

vandalismo, es por esta razón que se determina la aplicación y uso de los Sistemas de Seguridad para la Información *"SGSI"*, que en resumidas palabras es el conjunto de políticas de administración de la información aplicadas a través del estándar ISO/IEC 27001.

Según el Código de buenas práctica para la gestión de la seguridad de la información[19]: "las amenazas no solamente pueden estar dirigidas a la información que está en medio magnético, sino también a la información que está impresa o escrita en papel, la que es transmitida por correo normal, la que mostrada en video o la que se transmite a través de las conversaciones."

La gestión de la Seguridad de la Información garantiza la confidencialidad, integridad y disponibilidad de la información en cuanto acceso, protección, exactitud y métodos de procesamiento. Esta debe realizarse a través de un proceso documental sistemático y debe ser de conocimiento de toda la organización. Proceso que está ligado con el cumplimiento del estándar ISO 9001 y es adoptado al estándar ISO tal como se muestra en la **Figura 17** y detallado por niveles según lo establecido en la **Figura 18**:


*Figura 17:* **Modelo de SGSI ISO/ 27001 (ISO 2012)**

[19] Instituto colombiano de Normas Técnicas y Certificación. Normas Técnicas sobre sistema de gestión de la seguridad de la información (SGSI). Bogotá: ICONTEC, 2005, 157p. (NTC.BS-7799-2)

<table>
<tr><td>Nivel 1</td><td colspan="2">Nivel 2</td><td colspan="3">Nivel 3</td></tr>
<tr><td>Manual de seguridad</td><td colspan="2">Procedimientos</td><td colspan="3">Instrucciones, checklist y formularios</td></tr>
<tr><td colspan="6">Nivel 4</td></tr>
<tr><td colspan="6">Registros, evidencia objetiva del cumplimiento del SGSI</td></tr>
<tr><td colspan="6">Documentos</td></tr>
<tr><td>Alcance</td><td>Políticas y objetivos de seguridad</td><td>Procedimientos y mecanismos de control</td><td>Enfoque de evaluación de riesgos</td><td>Informe de evaluación de riesgos</td><td>Plan de tratamiento de riesgos</td></tr>
<tr><td colspan="2">Procedimientos documentados</td><td colspan="2">Registros</td><td colspan="2">Declaraciones de aplicabilidad</td></tr>
</table>

*Figura 18:* **Modelo detallado de niveles de SGSI (ISO 2012)**

Para la aplicación de un SGSI, basado en el estándar ISO 27001, se determina el uso del ciclo *"PDCA"*[20] (*Plan, Do, Check, Act*), Planificar, Hacer, Verificar, Actuar; determinado en los sistemas de gestión de calidad.

- **Planificar**: Definir el alcance del objeto del negocio de la organización, así como sus tipos tecnologías, debe contemplar una política de seguridad clara y consistente; que permita establecer los objetivos de un sistema de seguridad de la información, así como sus requerimientos legales y criterios de evaluación de riesgo. Definir metodología de evaluación del riesgo,

[20] ISO 27000.ES (2013). Sistema de Gestión de la Seguridad de la Información (SGSI). Recuperado de: http://www.iso27000.es/download/doc_sgsi_all.pdf

identificar los riesgos, analizar y evaluar los riesgos, identificación de y evaluación de opciones de tratamiento de riesgos, establecer riesgos residuales y los objetivos de control.

- **Hacer**: Determinar un plan de manejo de riesgos que contemple recursos, actividades, dueños del servicio y prioridades de implementación para implementar el plan de tratamiento de riesgos con el fin de alcanzar los objetivos de control identificados a través de controles, con la finalidad deestablecer una rápida detección y respuesta a incidentes de seguridad.
- **Verificar**: Estructurar métodos de monitoreo y validación para detectar errores originados durante el proceso de comunicación, analizar posibles brechas de seguridad a través de resultados de indicadores de monitoreo de uso y gestión de la información. Revisar de manera periódica la efectividad del SGSI, revisando constantemente los riesgos por categorías, efectuar auditorías internas y llevar la vitácora de acciones y eventos que impacten la efectividad del rendimiento del SGSI.
- **Actuar**: Implementar en el SGSI las mejoras identificadas, además de determinar las acciones preventivas y correctivas, poner en conocimiento las acciones y mejoras dentro de la organización, asegurarse de alcanzar los objetivos determinados.

# CAPÍTULO 3: TRATAMIENTO DE LA SEGURIDAD EN LA ARQUITECTURA DE VOIP.

En cuestión de estrategias y manejos de temas de aseguramiento de información para los aplicaciones y servicios de voz sobre IP existen varias organizaciones a nivel nacional e internacional que se dedican a emitir y aplicar lineamentos de buenas prácticas para el tratamiento de la seguridad en el área de las comunicaciones de VoIP, hoy en día denominada; "Voip Security". La empresa Techtarget, especialista en soluciones de seguridad para sistemas informáticos y de comunicaciones establece la siguiente definición acerca de la seguridad de sistemas de VoIP: "no es más que una serie de recursos enfocados en las prácticas de seguridad necesarias para protocolos y normas de VoIP y proporciona información sobre los riesgos de seguridad de VoIP".

En base a esta definición, se determinan los diversos mecanismos usados para el tratamiento normalizado de la seguridad determinado en; prevención, detección y respuesta en los sistemas de voz sobre IP del presente trabajo investigativo en particular.

## 3.1 Metodologías para la prevención de amenazas a la seguridad.

La aplicación de una metodología de seguridad informática en la infraestructura de red de datos y los sistemas de comunicaciones de voz sobre IP que funcionan dentro de una organización requieren de un proceso continuo de: análisis, detección, protección y acción continua, de tal forma se establecen mecanismos de prevención que identifican y eliminan las amenazas de seguridad para garantizar el normal funcionamiento de los procesos y aplicaciones de comunicación. De esta manera se mencionan cuatro mecanismos de prevención general que deben ser aplicados para el correcto funcionamiento de un sistema de comunicación de voz sobre IP.

- **Autenticación**: Identifica y autentica a los usuarios del sistema de voz sobre el protocolo IP, comprobando su identidad, permisos y accesos respectivos.
- **Control de acceso:** Controla todos los tipos de acceso que tienen los objetos con el sistema de comunicación de voz sobre IP.
- **Separación:** Maneja diferentes niveles entre objetos y entidades de seguridad, aplicando modelos físicos, temporales, lógicos dentro de los sistemas de voz sobre IP.
- **Seguridad en las comunicaciones:** Garantiza la seguridad en los sistemas de comunicación de voz sobre IP a través de la red de datos, utiliza métodos de criptografía, cifrados públicos y privados, firmas digitales y hasta protocolos de seguridad.

De manera global se enmarcan dos metodologías o mecanismos de aplicación para las seguridades, por software y por hardware, los cuales integran métodos y procedimientos para asegurar la operación del servicio de telefonía de VoIP.

Existen diferentes métodos para la identificación, protección y eliminación de riesgos de seguridad que se determinen para el servicio de voz sobre IP. Utilizar software de monitoreo y equipos especializados en el análisis y administración para evitar inconvenientes en los servicios de infraestructura y comunicaciones es una necesidad vital para el correcto desempeño de la organización. Entre los mecanismos más utilizados a nivel empresarial y personal para la aplicación de la seguridad se establecen los siguientes lineamientos:

### 3.1.1 Certificados digitales.

Con el uso de los certificados digitales se asocia una organización civil o jurídica a una clave pública de identificación única, el certificado debe ser otorgado por una entidad certificadora (CA) especializada en este ámbito. Tanto la clave pública como el certificado digital, deben ser socializados y aprobados por organismos de control y regulación mundial para garantizar su correcta operación. Este tipo de mecanismo de seguridad hoy en día también es aplicado al servicio de telefonía de voz sobre IP, estableciendo mecanismos seguros y confiables de protección en la seguridad de las comunicaciones. En base a esta definición se mencionan algunos tipos de certificados aplicados para este servicio.

- **Firmas Digitales RSA.**

  Para la gestión de claves compartidas y automáticas se utiliza el protocolo **IKE,** este el mismo emplea un intercambio secreto de claves entre los emisores y receptores para el establecimiento de sesiones, permite también establecer el tiempo de vida de la sesión IPSEC, actualmente se encuentra en aplicación su versión 2 (IKEv2) a través de sus respectivas especificaciones RFC 4309, RFC 4301, RFC 4309. Este tipo de seguridad está compuesta por dos fases, la primera; utilizando un algoritmo de intercambio de claves denominado "*Diffie-Hellman*" para establecer el canal de comunicación, y la segunda; negociar la asociación de seguridad a través de IPSEC entre los dispositivos o terminales de comunicación.

- **Certificados digitales (X.509).**

  Este tipo de certificados contienen las llaves públicas del propietario de la comunicación así como su respectiva identificación, a través de una Autoridad Certificadora se generan los llaves públicas y privadas, para la validación o revocación de los certificados en los integrantes de la comunicación telefónica , este tipo de certificados utilizan IPSEC y el protocolo SCEP, que es un estándar para solicitar y obtener certificados digitales de forma automática, originalmente desarrollado por CISCO y VERISIGN.

- **Autenticación de usuarios XAuth.**

  Este tipo de autenticación utiliza además de los certificados X.509 métodos de autenticación mediante usuarios y contraseñas de directorios activos o servidores de Radius implementados para la organización.

- **Clave compartida.**

  Este tipo de clave está formada por una cadena de caracteres que solo identifican y saben los dos extremos de la comunicación, estableciendo así la conexión IPSEC. A través de la comprobación mediante algoritmos tipo HASH se valida la autenticación de la clave, la cual es única para cada pareja de participantes del servicio de telefonía, este tipo de metodología es útil en redes pequeñas pero inviable para grandes corporaciones.

### 3.1.2 Infraestructura de clave pública PKI.

La infraestructura de clave pública es necesaria para la interpretación y autenticación de las entidades certificadoras y los certificados digitales emitidos para una organización. Esta infraestructura de clave pública (PKI), permite a los usuarios autenticarse entre ellos y usar de manera conjunta los certificados de identidad, el cifrado de mensajes, y la firma digital de información. Actualmente es determinado como una solución técnica robusta y segura para los sistemas de comunicación de voz sobre IP, utilizando sistemas de reglas y modelos matemáticos para la identificación de posibles amenazas en tiempo real.

A continuación se detallan los métodos de aplicación de seguridad criptográfica para brindar seguridad a las comunicaciones de VoIP:

- **Enterprise Java Bean Certificate Authority (EJBCA)**

  EJBCA es un framework de software libre basado en tecnología Java J2EE, que permite determinar entidades de autoridad de certificación funcionales, para la emisión de certificados digitales tanto a usuarios o servidores del servicio de telefonía IP. Incorpora servicio de tiempo NTP (*Network Time Protocol*) y SSL como protocolo de seguridad para las comunicaciones.

  Soporta autenticación y publicación de certificados validados con credenciales de seguridad de directorios activos organizacionales.

- **OpenCA.**

  Es un proyecto de tipo solución criptográfica libre, permite implementar toda la jerarquía de servicios PKI deseables como: entidades certificadoras raíz y subordinadas en plataformas Linux, Solaris y Mac OS X, actualmente sus proyectos más importantes de aplicación de entidades de certificación son: LibPKI, OpenCA PKI, OpenCA OCSPD, Open CAPRQPD, cada uno de ellos aplicaciones o servicios enfocados en el marco del sistema para llevar a cabo verificaciones de certificado de seguridad en línea.

- **Aplicación de Certificados sobre una arquitectura de VoIP**

  Para cifrar los datos de comunicación mediante certificados PKI en el servicio de telefonía IP, es necesario determinar el siguiente procedimiento:

- Estructuración de una entidad certificadora PKI para las puertas de enlace de voz sobre IP, Centrales PBX para IP y Controladores de sesión de borde SBC.
- Importación de certificados a ser utilizados por todos los servidores de telefonía de la organización.
- Habilitación de los certificados que serán utilizados por el servicio de telefonía IP.
- Importación del certificado para las puertas de enlace de voz sobre IP, Centrales PBX para IP y Controladores de sesión de borde SBC.
- Configuración del modo de inicio de sesión en los servidores de telefonía.
- Creación de puertas de enlace IP con el dominio respectivo de la organización.
- Creación de puertos para enlace TLS.
- Reinicio de equipos servidores para aplicación de configuración.

### 3.1.3 Firewalls y Proxys.

Los *firewalls*, *proxys* y *gateways* son aplicaciones integrales o equipos de aplicación que se utilizan para el control de acceso de una red interna empresarial LAN, protegiendo su entorno y funcionalidad de las redes externas; WAN e Internet, este método filtra todo el tráfico desde y hacia la red de datos, direcciones IP y puertos para permitir o denegar su procesamiento. En la actualidad este tipo de equipos se han determinado como dispositivos de seguridad indispensable en toda

organización; y sobre todo para el uso de los sistemas de comunicación de voz sobre IP.

En el mercado tecnológico de las comunicaciones existen varios modelos y especificaciones de equipos que presentan las características requeridas para la protección media y avanzada de las redes de datos y el servicio de telefonía IP, destacan entre sus características principales las siguientes funciones:

- **Nivel de Red:** La seguridad a nivel de red inspecciona los encabezados de los paquetes SIP o H.323, protocolos de transporte RTP y RTCP, filtra el tráfico a nivel de origen y destino por dirección IP, analiza los puertos utilizados en el proceso de comunicación telefónica: puerto 1720 para la configuración de llamadas, y los puertos aleatorios 1024 - 65535 para servicios implicados en la telefonía IP.

- **Entrada a nivel de circuito:** La seguridad a nivel de circuito funciona en la capa de sesión, conjuntamente con el protocolo de control de transmisión TCP/IP. Determinando la legitimidad de una sesión requerida y el monitoreo la comunicación entre los paquetes de comunicación telefónica. La característica a nivel de circuito de los equipos cortafuegos permite ocultar la red del mundo exterior y restringir normas de sesión de equipos de telefonía IP conocidos.

- **Entradas a nivel de aplicación:** La seguridad por aplicación determina el uso y acceso por tipo de aplicación específica; incluyendo los diferentes sub

servicios de telefonía IP; como directorio compartido, telepresencia, entre otras. Controla y previene ataques intrusivos como virus, spyware y spam, durante el procesos de llamada telefónica. Esta característica en los equipos cortafuegos permite bloquear tipos de ataques basados en el contenido y no por dirección IP, este tipo de configuración a este nivel requiere de un nivel de programación donde el administrador del equipo configure los tipos y contenidos de acceso para el equipo, usuarios, listas de control de acceso, sitios de confianza.

- **Protección Multicapa:** Esta es la característica de mayor seguridad en los equipos cortafuegos para el servicio de telefonía IP, filtran paquetes en la capa de red, evalúan la legitimidad del paquete como tal y evalúan los contenidos del paquete en la capa de aplicación. Ofrecen un nivel más profundo de inspección a nivel medular de paquetes que por aplicación, determinan y evitan ataques tipo día cero, spyware, virus, troyanos, amenazas de spam, y amenazas combinadas antes, durante y después de una llamada telefónica IP.

- **Priorización de tráfico:** La priorización de paquetes de datos dentro de la red organizacional permiten aprovechar y optimizar el uso del recurso de ancho de banda y el desempeño de la red, aquí se determina una mayor ponderación de servicio a la telefónia IP, a diferencia de los paquetes de datos, asegurando calidad y menor tiempo de retardo en la trasnferencia y recepción de paquetes..

- **Detección y prevención de intrusiones:** A través de tres elementos fundamentales se determina la detección y prevención de intrusiones en los equipos de seguridad en relación al servicio de telefonía IP; con ellos se asegura y determina la corercta operación del servicio, estos son: motores de aprendizaje, análisis dinámico del control de tráfico en tiempo real, configuración de políticas de seguridad propias de administración de red.

### 3.1.4 Encriptación.

Los mecanismos de encriptación permiten codificar y decodificar los mensajes que contengan información confidencial entre un emisor y un receptor de un tipo de comunicación. Esta metodología de protección integral brinda seguridad y protección contra las sofisticadas técnicas de ataque, ya que utiliza complejos algoritmos matemáticos y criptográficos para la seguridad en el cifrado de la información.

Dentro de un sistema de voz sobre IP y de comunicaciones en general, es imperativo el uso de este tipo de metodología de seguridad, ya que a través de él se determina que la información viaje de manera segura, manteniendo las características de autenticidad, integridad y confidencialidad de la información, existen varios métodos de encriptación, entre ellos los más utilizados son las redes virtuales y el cifrado de software a través de los diferentes protocolos de seguridad:

- **Redes Privadas Virtuales (VPN)**: Una VPN es una tecnología de red que determina una extensión de la red LAN para conectar una o más computadoras

o clientes de VoIP a una red privada a través de una red pública o Internet, con el fin de acceder a recursos y servicios tecnológicos corporativos de manera segura, puede utilizar los siguientes protocolos:

- **IPsec (*Internet Protocol Security*):** Protocolo de seguridad que trabaja en la capa de red y transporte tanto para TCP como UDP, es utilizado tanto en redes tipo home como en entornos corporativos, este protocolo proporciona tres tipos de servicio: confidencialidad, integridad y autenticación para los paquetes IP en flujos de datos
- **PPTP *(Point to Point Tunnel Protocol)*:** Desarrollado originalmente por Microsoft este protocolo ha sido estándar para la estructuración de conexiones VPN (cliente – servidor), actualmente es vulnerable de romper su seguridad por la longitud de clave.
- **L2TP y L2TP / IPsec *(Layer 2 Tunnel Protocol)***: Este tipo de protocolo de encriptación viene integrado en todos los sistemas operativos que soportan VPN, requiere el tipo de cifrado IPsec, este protocolo utiliza el puerto UDP 500 por lo que puede ser bloqueado por los cortafuegos en políticas NAT, el tipo de encapsulación de paquetes que utiliza hace que sea más lento que otros protocolos como PPTP y OpenVPN.
- **OpenVPN *(Virtual Private Network)***: Este tipo de protocolo utilizado en tecnología de código abierto utiliza protocolos de seguridad *OpenSSL, SSLv3, TLSv1* entre otros, puede ser ejecutado en cualquier puerto, por defecto utiliza el puerto 443, utiliza a demás algoritmos

criptográficos de 28 bits como: AES de 128 bits, Blowfish, 3DES, CAST entre otros.

- **Software de cifrado para VoIP:** A través de diferentes modelos de cifrados de paquetes se determina la seguridad en las aplicaciones y servicios de VoIP y telefonía IP, los paquetes de cifrados más utilizados son:
    - **VoVPN *(Voice over Virtual Private Network)*:** este tipo de cifrado combina el servicio de voz sobre IP y las redes privadas virtuales para proteger la información y proveer un servicio de voz seguro, utiliza el proceso de encapsulación y cifrado de paquetes utilizado en las redes virtuales como; IPSec, OpenVPN, L2TP, etc. Una de las desventajas de este tipo de cifrado es la demanda de consumo de ancho de banda, debido a la encapsulación de paquetes.
    - **SIPS *(SIP Secure)***: Es el protocolo utilizado para el control de llamadas sobre el protocolo SIP a través de la capa de transporte de seguridad TLS, este tipo de encriptación es mucho más efectiva y de fácil procesamiento que la utilizada a través de MD5 utilizada también para comunicaciones de VoIP. SIPS mantiene la seguridad de la comunicación en cada salto del proceso de comunicación evitando el tipo de ataque “hombre en el medio”.
    - **SRTP *(Secure Real Time Transport Protocol)***: Este tipo de cifrado contempla todas las características del protocolo RTP para comunicaciones de VoIP, ofrece alto rendimiento y bajo consumo de

ancho de banda, incorpora el uso de una llave maestra para la seguridad y confidencialidad en el flujo de las comunicaciones.

Así como se determinan los mecanismos de seguridad mediante software, se determina la implementación de mecanismos de prevención de seguridad física en las con lo cual se garantiza el acceso a los recursos y servicio de VoIP. En razón al incremento de riesgos y tipos de ataques de infiltración física con el fin de causar daño o espionaje de información, se debe abarcar una serie de elementos o mecanismos de prevención y detección que incluyan:

- Control de acceso físico al sistema de comunicación a través de códigos de acceso a los diferentes servicios que se puedan determinar, llamadas, locales, a teléfonos móviles o internacionales.
- Uso de cableado estructurado certificado, normalizado y con protección de acceso, categoría 6 o posterior.
- Contratación de seguros para los equipos de comunicación de red y de VoIP, en caso de desastres, daños o robo de equipos, se debe contar con seguros que restituyan en un 100% los mismos y así brindar la garantía de continuidad del negocio.

### 3.1.5 Mecanismos de detección y respuesta ante amenazas.

Son todos los procedimientos que se determinan para detectar y localizar intrusiones o accesos no autorizados a los sistemas de voz sobre IP, estos mecanismos deben ser continuos y de manera aleatoria a través de los cuales se

garantiza la mínima incidencia de ataques posibles, existen varios tipos de procesos de detección de riesgos como:

- Procedimientos de auditoría interna y externa estructurados mediante la Norma ISO/IEC 27001 y las recomendaciones técnicas establecidas en los Sistemas de Gestión de Seguridad de la Información SGSI. Para el caso de Ecuador se determina el uso de la norma NTE INEN-IDO/IEC 27001:2011 bajo el modelo PDCA, La aplicación de estas auditorías se las puede realizar a través de procesos de control interno o mediante la ayuda de empresas externas a la organización.
- Programas de monitoreo en tiempo real que evalúen las métricas de comportamiento y eventos de sucesos en las aplicaciones de comunicación y de VoIP, supervisadas por un centro de control pre establecido para esta actividad. Una de las herramientas con mayor uso para esta actividad son las PRTG Network Monitor, las cuales monitorean en tiempo real los dispositivos de red y utilización del ancho de banda, y el tráfico de VoIP. Además se determinan dos sistemas importantes de detección de intrusiones; IDS e IPS.
    - **IDS** ***(Intrusion Detection System)***: Es un mecanismo que escucha el tráfico de red para determinar actividades anormales o sospechosas para reducir los riesgos por intrusión, maneja dos tipos de análisis; por intrusiones de red N-IDS y por intrusiones de host H-IDS, ambos sistemas identifican y analizan de manera interna o externa los paquetes de datos que viajan por la red a través de equipos o

interfaces configuradas para este efecto, una vez analizados los paquetes de datos se establecen técnicas de detección de amenazas como son:

- **Verificación de la lista de protocolos:** identificación de puertos TCP, UDP e ICMP por los cuales se puede efectuar los ataques.
- **Verificación de los protocolos de la capa de aplicación**: valida el comportamiento de protocolos no válidos, por lo cual es necesario que las interfaces o equipos de análisis identifiquen el origen y objeto de cada protocolo.
- **Reconocimiento de ataques de "comparación de patrones"**: esta técnica analiza patrones de ataques efectuados a través de diccionarios o filtros pre-establecidos.

o **IPS *(Intrusion Prevention System)*:** Es un sistema de prevención y protección para proteger sistemas de comunicación de intrusiones diferenciando de los IDS en base a las siguientes características:

- El IPS se coloca en línea directamente en la red de datos para enfrentar los problemas de intrusiones de manera preventiva y reactiva.
- Bloquea todo tipo de intrusión en tiempo real sin importar el tipo de protocolo y de manera nativa, tomando decisiones de control de acceso basado en el contenido de tráfico en lugar de direcciones IP o puertos.

Los IPS se clasifican además por el tipo de análisis y bloqueo por entorno de red; basados en redes LAN, Wireless, Análisis por comportamiento de LAN y basados en Hosts y la categorización en la forma de detección de ataques maliciosos se determina por: firmas (similar a los sistemas de antivirus), políticas (declaraciones de políticas de seguridad), anomalías (en base al patrón de comportamiento del tráfico).

## 3.2 Mecanismos de respuesta ante amenazas.

Son los procedimientos de respuestas que se determinan en el caso de que se haya detectado una intrusión o falla de seguridad en los sistemas de voz sobre IP, reduciendo el impacto de riesgo de operación y regresando el sistema a un estado óptimo y funcional. Uno de los procedimientos con mayor resultado se determina a través del análisis forense, el cual se encarga de seguir los pasos y procedimientos que se determinaron antes, durante y después del ataque perpetrado a una red de comunicaciones enfocado en el servicio de comunicaciones de VoIP a fin de tomar los correctivos necesarios para evitar la ocurrencia de un nuevo incidente, y encontrar al o los culpables de este incidente para los fines legales correspondientes.

Ante un ataque y posterior daño en los sistemas de voz sobre IP, uno de los procedimientos efectivos para restaurar la operación y funcionamiento de toda la operación es a través de la restauración de respaldos y configuraciones propias de los equipos de comunicación de VoIP de manera inmediata, luego de identificar y corregir plenamente el origen del problema.

### 3.2.1 Técnicas de auditoria en una arquitectura de VoIP.

Las técnicas de auditoría en una arquitectura de VoIP, proporcionan los métodos de evaluación y reportes de todos los componentes de la infraestructura, aplicaciones y sistemas de comunicación de VoIP; clasificando y categorizando la información por grupos de acceso para la toma de decisiones por parte del área gerencial en coordinación con la supervisión de las áreas técnicas y de seguridad. Al día de hoy existen diferentes tipos de técnicas o metodologías que permitan ejecutar esta actividad, entre las principales se establecen:

- **Test de Penetración:** Las pruebas de penetración son la manera de medir la seguridad de los sistemas de información, utilizando herramientas y técnicas que utilizan delincuentes informáticos dentro de ambientes controlados. El objetivo de estas pruebas es identificar todo tipo de falla de seguridad interna o externa que pueda tener una organización en la red de datos.

  Se recomienda establecer este tipo de pruebas a las infraestructuras de red que se encuentren conectadas hacia el Internet, existen tres tipos de pruebas generales de penetración:

  - **De Caja Negra:** Los analistas de seguridad no conocen el funcionamiento del sistema y trabajan con la información obtenida mediante todo tipo de ataques.
  - **De Caja Blanca:** Los analistas de seguridad tienen total conocimiento del funcionamiento interno del sistema, trabajan con información proporcionada por funcionarios de la organización.

- **De Caja Gris:** Los analistas de seguridad pueden o no tener información del funcionamiento de la organización.

- **Análisis Forense:** Es el proceso de investigación de incidentes informáticos dentro de una organización, con lo cual permite tomar medidas necesarias para que los eventos de seguridad ocurridos no vuelvan a ocurrir, a través del análisis forense se determina:
  - Descubrir las vulnerabilidades por las que se originó el ataque.
  - Determinar el origen y autor del ataque.
  - Identificar y determinar las acciones realizadas, herramientas y métodos utilizados para el ataque.
  - Establecer medidas adecuadas para que el evento de riesgos de seguridad no se repita.
  - Descubrir las vulnerabilidades que han originado el evento de seguridad dentro de la organización.

  A través del análisis forense se identifica además si se han determinado la filtración de documentos oficiales, accesos no autorizados, problemas derivados con funcionarios de la organización, uso no autorizado del material informático.

- **Programas de monitoreo en tiempo real (PRTG):** A través del uso de estas herramientas se puede determinar el monitoreo proactivo tanto de la

infraestructura de equipos servidores así como de la red de datos en tiempo real, entre sus principales funciones se establecen:

- Monitoreo de disponibilidad y rendimiento.
- Monitoreo de ancho de banda y consumo de canal de comunicaciones.
- Monitoreo de calidad de servicio y tipo de conexión.
- Sistema de alertas y gestión de errores.
- Monitoreo de tráfico basado en Packet Sniffer y NetFlow.
- Monitoreo de latencia de paquetes.

### 3.2.2 Identificación y clasificación de riesgos.

Los riesgos se determinan como un factor latente dentro del campo de la seguridad en cualquier tipo de sistema, especialmente en los sistemas de comunicación de voz sobre IP, ya que siempre están presentes bajo una u otra circunstancia de riesgo, con esta premisa es necesario tomar en cuenta que todo riesgo puede ser minimizado pero nunca eliminado. EL objetivo de determinar y clasificar un riesgo es determinar la factibilidad de minimizar el impacto del mismo, por esta razón es necesario identificar a tiempo los riesgos que enfrenta una organización para desarrollar las políticas y procedimientos necesarios para recuperar la información con el mínimo impacto de afectación. Aun así los riesgos que no se pueden combatir a pesar de todas las políticas implementadas se denominan riesgos restantes y son factores que se encuentran fuera del alcance del poder humano, como por ejemplo las catástrofes naturales.

Los riesgos para un sistema de voz sobre IP se clasifican según su impacto, determinados en: mediano y alto, los cuales deben ser tratados y corregidos en el menor tiempo posible utilizando todos los procedimientos y recursos necesarios para asegurar la continuidad del negocio de una organización. La identificación y valoración de los riesgos se determina mediante las preguntas: ¿Qué?, ¿Por Qué? y ¿De quién? se necesita proteger la información, para lo cual se necesita identificar los siguientes factores:

- Recursos y vulnerabilidades.
- Amenazas y probabilidades de incidencia.
- Contramedidas de ataques.
- Análisis costo-beneficio.
- Desarrollo de políticas de seguridad.

Una vez determinado el análisis de potenciales riesgos y tipos de vulnerabilidades en el **Capítulo 2.8** del presente trabajo investigativo, se plantea el siguiente listado de riesgos para la seguridad dentro de los sistemas de comunicación de VoIP, los cuales serán posteriormente estructurados, analizados, evaluados y tratados a través de las matrices de riesgos correspondientes.

## 3.3 Políticas de seguridad para sistemas de VoIP.

Las políticas de seguridad, son el conjunto de reglas y procedimientos que regulan como una organización; procesa, administra, protege y distribuye la información de manera interna y externa. La aplicación de las políticas de seguridad garantiza la

continuidad del servicio de comunicación. Para determinar el cumplimiento de los objetivos en la seguridad de los sistemas de comunicación de voz sobre IP, es necesario considerar el desarrollo y aplicación de las políticas y procedimientos de seguridad necesarios a través de los mecanismos de prevención antes establecidos. De esta manera se puede considerar los siguientes elementos determinantes para la ejecución e identificación de la seguridad en todos sus ámbitos:

- Identificar todos los recursos de la organización; físicos, lógicos, técnicos, internos y externos que utilizan los servicios de comunicación de VoIP.
- Definir los riesgos; bajos, medios y altos que se determinan en los servicios de comunicación de VoIP, como la telefonía.
- Definir la administración de los recursos informáticos, por áreas técnicas y funcionales que intervienen en los sistemas de comunicación de VoIP.
- Definir los procesos de autenticación para las aplicaciones y servicios organizacionales que acceden al servicio de comunicaciones de VoIP.
- Definir el uso apropiado de los recursos de comunicación de VoIP para la aplicación de los servicios de una organización.
- Definir el acceso y distribución de la información por los diferentes tipos de medios de comunicación.
- Definir los controles de acceso a la información mediante el servicio de telefonía de voz sobre el protocolo IP.
- Notificar a los usuarios, los procedimientos de monitoreo, auditoria y divulgación de información y las consecuencias de incumplimiento de normas sobre los sistemas de comunicación de VoIP.

- Definir responsables de la ejecución de los procedimientos y políticas de seguridad en los sistemas de VoIP a ser cumplidos.
- Determinar la secuencia de pasos a seguir antes, durante y después de un evento de seguridad en los servicios de comunicación de VoIP dentro de la organización.

### 3.3.1 Implementación de políticas de seguridad para sistemas de VoIP.

Para implementar las políticas de seguridad para un sistema de comunicaciones de voz bajo el protocolo IP dentro de una organización, es necesario establecer los siguientes procedimientos:

- Desarrollar el manual de políticas y procedimientos de seguridad para un sistema de comunicaciones de VoIP.
- Desarrollar un programa educacional para el conocimiento y aplicación de las políticas de seguridad en el sistema de comunicaciones de VoIP.
- Desarrollar el proceso para la ejecución, implementación y seguimiento de las políticas y procedimientos de seguridad para un sistema de comunicaciones de VOIP.
- Desarrollar el proceso para evaluar y actualizar permanentemente las políticas y procedimientos de seguridad para un sistema de comunicaciones de VoIP.

### 3.3.2 Ejecución de políticas de seguridad.

El proceso de monitoreo y auditorias continuas, aseguran el cumplimiento de las políticas de seguridad establecidas para los sistemas de comunicación de voz sobre protocolo IP, de manera obligatoria por la gerencia de la organización para todas las áreas funcionales de la misma. Estas políticas deben ser establecidas dentro del contrato de los funcionarios y deben constar dentro del manual organizacional, recordando el uso y aplicación de manera continua mediante campañas de información y retro alimentación.

### 3.3.3 Políticas de Seguridad para el servicio de telefonía IP.

La tecnología de VoIP permite implementar actualmente una serie de servicios y aplicaciones para las organizaciones, dentro de ellas se puede determinar el uso del servicio de telefonía IP, para lo cual se requiere aplicar las políticas de seguridad necesarias que permitan evitar problemas de intrusiones de seguridad, para lo cual es necesario considerar los siguientes ítems:

- El sistema de telefonía debe ser de uso exclusivo para funciones de trabajo de la organización y salvo temas emergentes para el uso personal.
- El uso de perfiles para llamadas telefónicas deberá ser requeridos y avalados por la Gestión de Control y Seguridad de la Información con la supervisión del jefe de la gestión respectiva.

- La asignación de una terminal física o virtual a un usuario, es de responsabilidad única del funcionario y no puede ser transferida, alterada o modificada.
- La alteración de la configuración del sistema de telefonía sin autorización, será considerada una contravención grave alineamiento de las políticas de aplicación Institucional.
- El centro de cómputo en donde se encuentren los servidores y equipos de comunicación y telefonía deben ser áreas de acceso restringido para el personal no autorizado.
- El uso del sistema de telefonía por parte de los funcionarios será continuamente monitoreado para evitar incumplimiento de las políticas establecidas.
- El registro de llamadas es un factor importante para el sistema de monitoreo y análisis, su divulgación parcial o total sin previa autorización será considerada una contravención grave a estas políticas de seguridad.
- La habilitación de puntos y sesiones de conferencias para llamadas entrantes se determinará bajo la autorización de las gestiones de seguridad de la información en coordinación con la gestión de tecnología de la información.

### 3.3.4 Políticas de seguridad para el diseño e infraestructura de red

Dentro del esquema de implementación de una red de comunicaciones de telefonía de VoIP es importante determinar el diseño de red e infraestructura para la

arquitectura de seguridad perimetral, para lo cual es necesario considerar los siguientes puntos:

- Diseñar la red de comunicaciones independiente tanto para el servicio de voz como para el servicio de datos a través de redes diferentes lógicas VLANS.
- Implementar equipos físicos de cortafuegos (*firewalls*) y controladores de frontera para sesiones (*sesion border controllers*), así como la configuración de reglas de ingreso y salida de paquetes de voz sobre estos equipos.
- Incorporar al sistema organizacional de administración y actualización de parches de seguridad y manejo centralizado de antivirus todos los equipos servidores utilizados para la implementación de estas soluciones.
- Considerar el diseño del sistema eléctrico para sistemas de contingencia, a fin de garantizar la operación de los dispositivos de telefonía y de red en caso de una falla de energía eléctrica.
- Implementar equipos de monitoreo COS (*class of restriction*) para prevenir fraudes económicos y alertas de seguridad sobre el servicio de voz.
- Habilitar equipos para el servicios de monitoreo de registros de eventos de llamadas en la red.

## 3.4 Modelo de implementación de políticas de seguridad.

Los sistemas de gestión de seguridad de la información determinados por la aplicación del estándar ISO/IEC 27001 dentro de los sistemas de comunicación de VoIP, permiten reducir los riesgos de seguridad mediante la implementación de

políticas y controles que siguen una secuencia metódica desde la elaboración de políticas de seguridad hasta la auditoria y certificación del cumplimiento de las mismas. En la **Figura 19** se determina la secuencia de implementación de políticas de seguridad en un sistema de comunicaciones de VoIP.

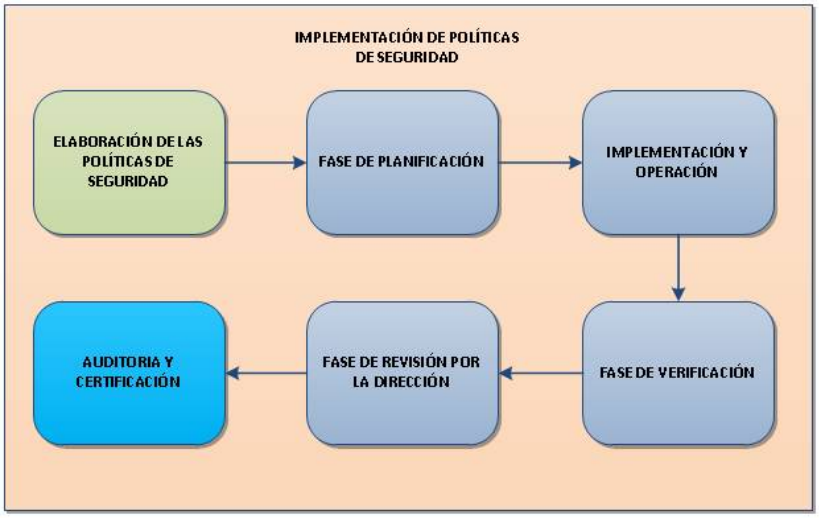


*Figura 19:* **Modelo de implementación de políticas de seguridad. Elaborado por el Autor.**

Se detalla a continuación cada uno de los componentes de la secuencia de implementación de las políticas de seguridad dentro de una organización:

- **Elaboración de las políticas de seguridad:** En esta fase se establecen los principios asumidos por la alta dirección y el área de tecnología para mejorar las seguridades en los servicios de comunicación de VoIP dentro de la organización y garantizar el uso y continuidad del servicio de telefonía. Esta fase debe contar con las siguientes características:
    - Mejora continua de las políticas de seguridad en los sistemas de comunicación de VoIP.

- Debe contemplar todo tipo de riesgos de seguridad para los sistemas de comunicación de VoIP internos y externos de la organización.
- Definición de los requisitos necesarios para la aplicación y cumplimiento de las políticas de seguridad.
- Establecer el marco de referencia para la aplicación de los objetivos de las políticas; normas nacionales internacionales, reglamentos internos y demás referencias técnicas y legales.
- Comunicar la definición y aplicación de las políticas de seguridad para los riesgos en los sistemas de comunicación de VoIP, a todos los miembros de la organización de manera continua.
- Revisión y seguimiento permanente del cumplimiento de las políticas de seguridad para sistemas de comunicación de VoIP dentro de la organización.

- **Planificación:** En esta fase se deben establecer tanto los procedimientos para la identificación y evaluación de amenazas y riesgos para los sistemas de comunicación de VoIP, así como la aplicación de controles para el cumplimiento de las políticas determinadas a través de un plan de acción para el cumplimiento de las mismas. Como procedimientos establecidos para una planificación ordenada se determina el cumplimiento de los siguientes puntos:
  - Identificación de riesgos de seguridad.
  - Evaluación de riesgos de seguridad.

- Control de las políticas de seguridad para controlar los riesgos de seguridad.

- **Implementación y Operación:** Una vez definida la política e identificación de riesgos de seguridad y planteado el plan de seguridad a implementar, se determina la fase de implementación, la cual se encarga de aplicar las políticas de seguridad para los sistemas de comunicación de VoIP a través de los siguientes puntos:
  - Definir y concretar funciones y responsabilidades.
  - Informar a los miembros de la organización los riesgos de seguridad internos, y externos para los sistemas de comunicación de VoIP.
  - Determinar los documentos necesarios para el control y seguimiento de las políticas y las seguridades de la organización.

- **Verificación:** Una vez determinado la ejecución de los pasos anteriores; elaboración de políticas, planificación, implementación y operación, es necesario establecer el cumplimiento y verificación los resultados de las evaluaciones de riesgo de seguridad de las comunicaciones de VoIP, para lo cual se determinan procesos de control como auditorías internas y externas y la aplicación de los siguientes puntos:
  - Establecer procesos de seguimiento para determinar el nivel de cumplimiento de objetivos de seguridad en los sistemas de comunicación de VoIP.
  - Identificar, detectar y analizar los incidentes de seguridad.

- Tomar acciones preventivas y correctivas de los riesgos de seguridad detectados e identificados.
- Realizar procesos de auditoria interna para evaluar el desempeño de la aplicación de las políticas de seguridad y el nivel de acción preventiva o correctiva aplicada.

- **Revisión por la dirección:** Dentro del modelo de implementación de políticas de seguridad para los sistemas de comunicación e VoIP, la alta dirección en coordinación con el área de tecnología deben revisar la documentación y casos prácticos de las políticas de seguridad aplicadas frente a los riesgos determinados para los sistemas de comunicación de VoIP para establecer la validez y funcionamiento del sistema.

- **Auditoría y Certificación:** Tras el proceso de revisión por la alta dirección, se puede gestionar la certificación el sistema de seguridad para los sistemas de comunicación de VoIP, a través de una entidad certificadora nacional o internacional para los Sistemas de Gestión de la Seguridad de la Información SGSI y los procesos de seguridad de la información que son determinados en la norma ISO/IEC 27001. Una vez determinado y avalado el sistema de seguridad de la información a través de la metodología de implementación de políticas de seguridad, es necesario establecer procesos continuos de auditoría interna y externa para renovar anualmente la certificación bajo los estándares antes mencionados.

## 3.5 Modelo de esquema SGSI para comunicaciones de VoIP.

Se determina el modelo de esquema del Sistema de Gestión de Seguridad de la Información para el tratamiento de riesgos que enfrenta de manera continua el proceso de comunicación de VoIP. Al ser la metodología SGSI un esquema de aplicación cíclica se aplica a toda la estructura organizacional de manera continua.

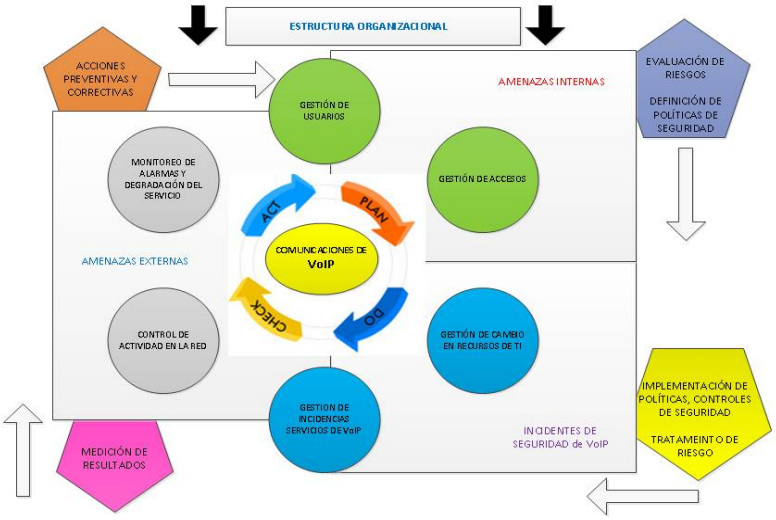


*Figura 20: 1***Esquema SGSI para sistemas de comunicaciones de VoIP. Elaborado por el Autor.**

En la **Figura 20**, se determina mediante el presente trabajo de investigación los componentes que integran el modelo de esquema de los sistemas de gestión de seguridad de la información SGSI para los sistemas de comunicación de VoIP dentro de una organización. Se detalla a continuación cada uno de sus componentes y la manera que integran la sinergia y funcionalidad dentro del esquema.

- El servicio de comunicaciones de VoIP es el eje central para la ejecución del sistema de gestión de seguridad de la información, al mismo se aplica la

metodología (*Plan-Do-Check-Act*) "Planificar-hacer-verificar-actuar", que integra y se adapta a la gestión de los sientes sub procesos:

- **Gestión de usuarios:** Se encarga de la organización, información y supervisión de los usuarios de los sistemas de comunicaciones de VoIP.
- **Gestión de accesos:** Administra los permisos y niveles de accesos para el uso del servicio de comunicación de VoIP y otras aplicaciones de comunicaciones unificadas.
- **Gestión en cambio de recursos de TI**: Se refiere a la actualización de equipos y servicios para el funcionamiento óptimo de los servicios de comunicación de VoIP.
- **Gestión de incidencias servicios de VoIP**: Se realiza una clasificación de los diferentes tipos de incidentes, su análisis, evaluación y tratamiento de cada uno de los riesgos de seguridad a los que están expuestos los servicios de comunicación de VoIP.
- **Control de actividad en la Red:** Analiza el comportamiento de la red de datos de comunicaciones a nivel local (*Red Lan)*, red extendida *(Red Wan)* y red de datos a nivel mundial *(Internet)*, necesarias para la ejecución del servicio de VoIP.
- **Monitoreo de alarmas y degradación del servicio:** Se determina el monitoreo y seguimiento de eventos y alertas en las aplicaciones e infraestructura que utiliza el servicio de comunicaciones de VoIP, a fin de identificar la ocurrencia o reiteración de un riesgo de seguridad de manera inmediata.

- La organización de cada uno de los componentes mencionados y su interacción dentro de la organización, está sujeta a riesgos de seguridad, los cuales se definen en tres grandes grupos:
    - **Riesgos Internos:** Se refiere a todos los tipos de riesgos de seguridad que se determinan dentro de la organización y afectan al servicio de comunicaciones de VoIP,
    - **Riesgos Externos:** Se refiere a todos los tipos de riesgos de seguridad que se determinan fuera de la organización y afectan al servicio de comunicaciones de VoIP.
    - **Incidentes de Seguridad de VoIP**: Se refiere a todos los eventos que afectan el funcionamiento del servicio de comunicación de VoIP y deben ser solucionados mediantes las acciones de tratamiento correspondientes y la implementación de políticas de seguridad.

- Tanto los componentes del proceso de comunicaciones de VoIP, como los tipos de riesgos se encuentran dentro del procesos de gestión de seguridad de la información, demarcado por los siguientes esquemas para su análisis, definición, implementación y seguimiento:

    - **Evaluación de Riesgos:** Evalúa los diferentes tipos de riesgos de seguridad que se establecen para un sistema de comunicaciones de VoIP, identifica los procesos, procedimientos y actores que tienen

algún tipo de impacto en el funcionamiento de las aplicaciones y procesos de la organización.

- **Definición de Políticas de Seguridad:** Define las políticas de seguridad para enfrentar y contrarrestar los riesgos de seguridad en un sistema de comunicaciones de VoIP.
- **Implementación de políticas y controles de seguridad**: Implementa las políticas de control de seguridad necesarias y previamente definidas para el uso y correcto desempeño de las aplicaciones e infraestructura de los sistemas de comunicación de VoIP.
- **Medición de resultados**: Evalúa los parámetros para la medición de resultados obtenidos de la aplicación de las políticas frente a los riesgos identificados en los sistemas de comunicación de VoIP.
- **Acciones preventivas y correctivas:** Determina las acciones necesarias para prevenir y corregir riesgos de seguridad en las aplicaciones de comunicaciones de VoIP de manera periódica.

# CAPÍTULO 4: APLICACIÓN DE LA METODOLOGÍA SGSI PARA LA IDENTIFICACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD SOBRE SISTEMAS DE VOIP Y EL SERVICIO DE TELEFONIA IP

## 4.1 Norma Técnica SGSI aplicada.

A nivel mundial el uso, adopción y aplicación de la norma internacional ISO/IEC 27001 se encuentra abierta para cada país que desee adoptarla según sus necesidades, es así como se puede mencionar a nivel de Latinoamérica como ejemplo el uso e implementación de varias normas, entre ellas: la norma colombiana (NTC-BS-7799-2), la norma ecuatoriana (NTE INEN-IDO/IEC 27001:2011 o 27001:2013), la norma peruana (NTP-ISO/IEC 27001:2014), entre otras.

Para determinar la metodología de aplicación del Sistema de Gestión de Seguridad de la Información, mediante la identificación y aplicación de políticas de seguridad sobre arquitecturas de VoIP y sobre el servicio de telefonía IP dentro de una organización, se determina el uso de las normas técnicas; ecuatoriana *NTE INEN-IDO/IEC 27001:2011*, que establece las técnicas de seguridad para los Sistemas de Gestión de Seguridad de la Información. Y la norma internacional *ISO 17799:2005* que se refiere a los códigos de buenas prácticas para la gestión de la seguridad de la información. A través del uso de estas normas se logra determinar un análisis y procedimientos secuenciales de todos los puntos que involucran el tratamiento de los riesgos de seguridades que permiten ejecutar fraudes en el servicio

telefónico IP, objeto de esta investigación. A través de la metodología PDCA (*Plan-Do-Check-Act*). Es necesario considerar además dentro de este análisis; los tipos de riesgos de seguridad que mayor afectación tienen al servicio de telefonía IP, las políticas de tratamiento para minimizar la incidencia de eventos de seguridad e indisponibilidad de servicio y el esquema de tratamiento global para determinar de manera objetiva el Sistema de Gestión de Seguridad de la Información mediante la determinación de matrices de análisis, evaluación y manejo de riesgos.

Como premisa para la aplicación de la norma SGSI por aplicar a este trabajo de investigación, se menciona que la norma ecuatoriana NTE INEN-IDO/IEC 27001:2011 sigue el modelo PDCA que se aplica para estructurar todos los procesos del SGSI y ha sido determinada por el Servicio Ecuatoriano de Normalización INEN, competente de la normalización, reglamentación, técnica y metrología, relacionados con la seguridad, la protección y preservación de la vida y el medio ambiente, la promoción y mejoramiento de la productividad y competitividad en la sociedad ecuatoriana.

## 4.2 Consideraciones de seguridades en el servicio de telefonía IP.

En base al tratamiento de riesgos de seguridades para el servicio de telefonía IP y las diferentes características y aplicaciones técnicas expuestas anteriormente para evitar fraudes en este servicio, se enmarcan tres consideraciones de seguridad técnica que abarcan de manera global los aspectos necesarios para contemplar al momento

de determinar un sistema de prevención de riesgos y asegurar de manera segura la operación del servicio de telefonía dentro de una organización:

- **Infraestructura de red:** contempla la protección a nivel físico (cortafuegos y puertas de enlaces) y lógico (certificados digitales, claves públicas PKI), los tipos de redes en el que se implementa la infraestructura del servicio de VoIP; a través de controles de acceso y cifrado. Así también es necesario determinar el control de tráfico entre las diferentes zonas de seguridad a través de protocolos y políticas de códigos de seguridad perimetral (encriptación). Se debe considerar todo el equipamiento que integrará el servicio de telefonía IP (terminales, *gateways*, centrales IP) a fin de evaluar todos los parches y actualizaciones de seguridad necesarios para no comprometer la seguridad del servicio como tal.

- **Metodología de seguridad:** La seguridad del servicio de telefonía IP dentro de una organización está determinada en primera instancia por el nivel de seguridad que se determine en la red IP, luego de esto, es necesario establecer el nivel de seguridad tanto para el servicio de telefonía como para la organización como tal. Se establecen cuatro parámetros fundamentales para determinar la seguridad del servicio de telefonía IP;

    - **Evaluación de riesgos:** evaluación de impacto en el negocio de amenazas y vulnerabilidades.

- **Arquitectura de diseño de seguridad:** Sistemas de gestión de riesgos y seguridades, normas y políticas de control para el servicio de telefonía.
- **Implementación, operación y mantenimiento del servicio de telefonía IP:** Implementación de procesos de seguridad durante todo el proceso de implementación del servicio y monitoreo de la operación del servicio, determinando un proceso de mejora continua.

## 4.3 Contextualización de la matriz de riesgos.

Como parte fundamental para la aplicación de un sistema de gestión de seguridad SGSI para la identificación y aplicación de políticas de seguridad, es necesario establecer un esquema de análisis de riesgos de seguridad, mediante la elaboración de la matriz de riesgos en la cual se establecen: el análisis, la evaluación y el tratamiento de riesgos para el servicio de telefonía IP. Así también se requiere identificar la estructura organizacional y los procesos funcionales de una organización, relacionados y enfocados en los tipos de amenazas de seguridad que se presentan en estos sistemas de comunicación.

Debido a que los sistemas de comunicación y especialmente a que el servicio de telefonía IP dentro de una organización son de vital importancia para el funcionamiento de la estructura del Core de negocio se determina 3 tipos de ponderación para las amenazas y magnitud de daños obteniendo los siguientes valores: (2-Bajo, 3-Medio, 4-Alto), se desestima el valor 1 identificado como tipo de

amenaza o riesgo (insignificante o nula) ya que en todo momento va a existir algún tipo de afectación al servicio de comunicación y su influencia en el proceso del negocio.

Una matriz de riesgos constituye una herramienta de control y gestión utilizada para identificar los procesos o productos de una organización y los tipos de riesgos implícitos a esta actividad. Así también permite evaluar la efectividad de la gestión y administración de los riesgos que pudieran afectar los resultados y objetivos de la organización. El factor riesgo; se determina en base a la multiplicación de la amenaza por la magnitud de daño y de lo cual se agrupan en tres rangos que serán identificados por colores para su fácil identificación:

- Bajo Riesgo: (1 a 6 puntos), color **verde**.
- Medio Riesgo: (8 a 9 puntos), color **naranja**.
- Alto Riesgo: (12 a 16 puntos), color **rojo**.

Dentro del modelo PDCA para la estructuración de un sistema de gestión de seguridad de la información SGSI, es necesario identificar y determinar los riesgos que se aplican, en este estudio específicamente al servicio de telefonía IP dentro de una organización. Para lo cual se determina la formulación de 3 matrices en las cuales se pueda realizar el análisis, evaluación y tratamiento de riesgos. Así también resulta indispensable plantear una matriz de riesgos en la cual se identifiquen los procesos de una organización que se vean afectados por los diferentes tipos de riesgos identificados en el servicio de telefonía IP.

### 4.3.1 Valoración de Riesgos en los servicios de comunicaciones IP.

Cada uno de los servicios de comunicación que se utilizan dentro de una organización y se mencionan a continuación son valorados de acuerdo al impacto que sufrirán de acuerdo al funcionamiento en las operaciones en el caso de que llegaran a sufrir algún tipo de fallo.

**Tabla 1. Valoración de riesgos en los servicios de comunicaciones IP**

| Activo | Definición | Valoración | Descripción |
|---|---|---|---|
| Servicio de Navegación Web | Confidencialidad | 4 | Proteger los accesos de internet para que permanentemente se encuentren disponibles |
| | Integridad | 4 | Comprobar que la información transmitida o recibida no sea alterada |
| | Disponibilidad | 4 | Garantizar que el servicio se encuentre disponible en todo momento |
| Servicio de Correo Electrónico | Confidencialidad | 4 | Proteger el servicio de correo electrónico de accesos no autorizados |
| | Integridad | 4 | Comprobar que la información transmitida o recibida no sea alterada |
| | Disponibilidad | 4 | Asegurar que el servicio de correo electrónico esté disponible en todo momento |
| Servicio de Mensajería Unificada | Confidencialidad | 4 | Proteger el servicio de mensajería unificada de accesos no autorizados |
| | Integridad | 4 | Comprobar que la información transmitida o recibida no sea alterada |
| | Disponibilidad | 3 | Asegurar que el servicio de mensajería unificada esté disponible en todo momento |
| Servicio de Telefonía IP | Confidencialidad | 4 | Proteger el servicio telefónico para que no sea intervenido |
| | Integridad | 3 | Mantener un estándar de uso del servicio para minimizar fallos |
| | Disponibilidad | 3 | Asegurar que el servicio telefónico esté disponible en todo momento |

### 4.3.2 Identificación de Riesgos en función de los activos.

Los activos que son utilizados para brindar y mantener el servicio de telefonía IP son susceptibles de sufrir daños por causas naturales, fallos técnicos intervención humana no intencionada y ataques premeditados, de lo cual se pude resumir a través de la siguiente información.

**Tabla 2. Identificación de riesgos en función de activos.**

| Riesgo | Amenaza | Afectación | Activo |
|---|---|---|---|
| Desastres Naturales | Terremotos<br>Incendios<br>Inundaciones | Funcionamiento de Infraestructura de comunicaciones y servicio de telefonía | Equipos de Comunicación, Routers, Gateways, Proxys, servidor de comunicaciones, servidor de telefonía |
| Fallos Técnicos | Fallo en el sistema eléctrico, y proveedor de servicio de Internet | Funcionamiento de Infraestructura de comunicaciones y servicio de telefonía | Equipos de Comunicación, Routers, Gateways, Proxys, servidor de comunicaciones, servidor de telefonía |
| Intervención humana no intencionada | Robo, daño de los equipos por golpes o caídas | Acceso al servicio de infraestructura de comunicaciones y telefonía | Equipos de Comunicación, Routers, Gateways, Proxys, servidor de comunicaciones, servidor de telefonía, dispositivos de telefonía |
| Ataques Premeditados | DoS, Spit, Vishing, Fuzzing, Flooding, Hijacking | Acceso al servicio de infraestructura de comunicaciones y telefonía | Equipos de Comunicación, Routers, Gateways, Proxys, servidor de comunicaciones, servidor de telefonía, dispositivos de telefonía |

## 4.4 Análisis de las Matrices de Riesgos para el servicio de telefonía IP.

La estructuración de las matrices de análisis, evaluación y tratamiento de riesgos para el servicio de telefonía, ha permitido identificar, analizar y determinar los diferentes tipos de riesgos que las organizaciones enfrentan día a día, así también la descripción de los problemas generados, sus consecuencias, la probabilidad de suceso y el impacto que tiene la organización en su conjunto. Frente a ello se determinan y describen además los tipos de control, su eficacia y frecuencia de aplicación, y las acciones de tratamiento con su tiempo de implementación integrando costos y responsables de ejecución.

### 4.4.1 Matriz de análisis de riesgos.

**Tabla 3. Matriz de análisis de riesgos.**

| DESCRIBCIÓN DE RIESGOS | | | | ANÁLISIS DE RIESGOS | | | | |
|---|---|---|---|---|---|---|---|---|
| **CODIGO** | **RIESGO** | **DESCRIPCIÓN** | **CONSECUENCIAS** | **VALOR** | **PROBABILIDAD** | **VALOR** | **IMPACTO** | **SEVERIDAD** |
| R001 | Denegación de Servicios (DoS) | Degradación del servicio de voz hasta volverlo inaccesible para los usuarios del servicio. | 1. Indisponibilidad del servicio de telefonía. | 3 | ALTA | 4 | ALTO | 12 |
| R002 | SPIT (Spam) | Envío o recepción de mensajes masivos telefónicos no solicitados. | 1. Sobrecarga de operación en las centrales de telefonía.<br>2. Aumento considerable de estadísticas de uso del servicio | 2 | BAJA | 4 | MEDIO | 8 |
| R003 | Vishing (Pishing) | Suplantación o robo de identidad de usuarios | 1. Acceso y robo de información confidencial. | 4 | ALTA | 4 | ALTO | 16 |
| R004 | Fuzzing | Examina errores y brechas de seguridad sobre protocolos de comunicación de VoIP (SIP, H.323, RTP) | 1. Acceso no autorizado al servicio de telefonía.<br>2. Indisponibilidad de servicio. | 3 | MEDIA | 4 | ALTO | 12 |
| R005 | Flooding | Inundación de paquetes sobre la red de datos para colapsar las servicios de comunicación | 1. Indisponibilidad de servicio. | 3 | MEDIA | 4 | ALTO | 12 |
| R006 | Secuestro de sesiones (Hijacking) | Secuestro de sesiones, terminales y dispositivos de comunicación | 1. Acceso y robo de información confidencial. | 4 | ALTA | 4 | ALTO | 16 |
| R007 | Interceptación (Eavervesdroping) | Interceptación de llamadas telefónicas para obtener información confidencial | 1. Acceso y robo de información confidencial. | 4 | ALTA | 4 | ALTO | 16 |
| R008 | Redirección de llamadas (Call Redirections) | Redirecciona llamadas de entrada o salida a través de sistemas de telefonía agenos | 1. Sobre valoración de planillas de consumo de servicio | 3 | MEDIA | 4 | ALTO | 12 |

- **Detalle de la Matriz de análisis de riesgos.**

La matriz de análisis de riesgos permite identificar las principales consecuencias que se determinan por las vulnerabilidades de ataques al servicio de Telefonía IP. La probabilidad de ocurrencia de estos eventos y el impacto en el funcionamiento del servicio se catalogan como Medios y Altos, ya que cada uno produce una afectación severa al giro del negocio en el servicio telefónico de la organización.

- Indisponibilidad del servicio de telefonía. (***DoS, Flooidng, Fuzzing***)
- Acceso y robo de información confidencial. (***Vishing***)
- Sobre valoración de planillas de consumo de servicio. (***Call Redirection)***
- Sobrecarga de operación en las centrales de telefonía. (***SPIT***)
- Acceso no autorizado al servicio de telefonía. (**Hijacking, Eaveresdroping**)

### 4.4.2 Matriz de evaluación de riesgos.

**Tabla 4. Matriz de evaluación de riesgos.**

| EVALUACIÓN DE RIESGOS | | | | | | |
|---|---|---|---|---|---|---|
| **CODIGO** | **RIESGO** | **CONTROL** | **DESCRIPCIÓN DEL CONTROL** | **TIPO DE CONTROL** | **EFICACIA DEL CONTROL** | **FRECUENCIA DEL CONTROL** |
| R001 | Denegación de Servicios (DoS) | Sistema de monitoreo y alertas preventivo | Revisión, análisis y corrección de alertas en el sistema de monitoreo preventivo | PREVENTIVO | ALTA | SEMANAL |
| R002 | SPIT (Spam) | Validación de políticas de configuración | Revisión y depuración de parámetros y scripts de configuraciónes de la central telefónica | PREVENTIVO | MEDIA | SEMANAL |
| R003 | Vishing (Pishing) | Validación del listado de usuarios autenticados | Revisión de logs de acceso de usuarios en el sistema de telefonía y directorio activo | PREVENTIVO | ALTA | DIARIO |
| R004 | Fuzzing | Pruebas de Hackeo ético y ataques de intrusión | Estructuración y ejecución de pruebas de hackeo ético y accesos no autorizados al sistema de comunicaciones y sistema de telefonía. | PREVENTIVO | ALTA | TRIMESTRAL |
| R005 | Flooding | Revisión de tamaño en las tramas de paquetes | Revisión y validación del promedio de paquetes de datos que son recibidos y transmitidos para el servicio de telefonía | PREVENTIVO | ALTA | SEMANAL |
| R006 | Secuestro de sesiones (Hijacking) | Validación del listado de usuarios autenticados | Validación del logs de eventos de usuarios, número, tiempo e intervalo de conexiones | PREVENTIVO | ALTA | DIARIO |
| R007 | Interceptación (Eavervesdroping) | Revisión de puertos de comunicación en el firewall | Revisión de políticas y reglas de acceso y salida de servicios en el equipo cortafuegos de comunicaciones | PREVENTIVO | ALTA | SEMANAL |
| R008 | Redirección de llamadas (Call Redirections) | Sistema de monitoreo y alertas preventivo | Revisión, análisis y corrección de alertas en el sistema de monitoreo preventivo | PREVENTIVO | ALTA | DIARIO |

- **Detalle de la Matriz de evaluación de riesgos.**

La matriz de evaluación de riesgos establece tanto los tipos de control que se deben determinar para evitar la ocurrencia de las amenazas de seguridad tanto en el servicio de telefonía IP, así como la frecuencia de su aplicación. La eficacia de la aplicación en los eventos de control preventivo, determinará un ahorro en los costos de operación en caso de que los eventos de ataque sean mayores y se tenga que recurrir a métodos de control correctivos.

- Sistema de monitoreo y alertas preventivo. (**Semanal**).
- Validación de políticas de configuración. (**Semanal**).
- Validación del listado de usuarios autenticados. (**Diario**).
- Pruebas de hackeo ético y ataques de intrusión. (**Trimestral**).
- Revisión de tamaño en las tramas de paquetes. (**Semanal**).

### 4.4.3 Matriz de tratamiento de riesgos.

**Tabla 5. Matriz de tratamiento de riesgos.**

| TRATAMIENTO DE RIESGOS | | | | | |
|---|---|---|---|---|---|
| **CODIGO** | **RIESGO** | **ACCIÓN DE TRATAMIENTO** | **TIEMPO DE IMPLEMENTACIÓN** | **COSTO** | **RESPONSABLE** |
| R001 | Denegación de Servicios (DoS) | 1. Corregir políticas y scripts de configuración en los equipos de comunicación de datos.<br>2. Restaurar respaldos de archivos de configuración de los equipos de comunicación en caso de un daño mayor.<br>3. Identificar técnicamente el origen del ataque de DoS y tomar las acciones legales pertinentes. | INMEDIATO | BAJO | TECNOLOGÍA<br>DEPARTAMENTO LEGAL |
| R002 | SPIT (Spam) | 1. Depurar parámetros y scripts de configuraciónes de la central telefónica.<br>2. Editar y corregir políticas de accesos y requerimientos en la central telefónica. | SEGÚN LA OCURRENCIA | BAJO | TECNOLOGÍA |
| R003 | Vishing (Pishing) | 1. Implementar seguridades en el equipo cortafuegos.<br>2. Implementar scripts de seguridades y autenticación de usuarios, validación de llaves públicas y privadas.<br>3. Implementar métodos de encriptación robustos. | INMEDIATO | ALTO | ASESORÍA TECNICA EXTERNA |
| R004 | Fuzzing | 1. Implementar sistemas de seguridad por capas y algoritmos de encriptación.<br>2. Implementar seguridades a nivel de puertos de acceso en el equipo cortafuegos y los equipos de la red de comunicaciones. | INMEDIATO | MEDIO | TECNOLOGÍA<br>ASESORIA TÉCNICA EXTERNA |
| R005 | Flooding | 1. Implementar seguridades en el equipo cortafuegos. | SEGÚN LA OCURRENCIA | BAJO | TECNOLOGÍA |
| R006 | Secuestro de sesiones (Hijacking) | 1. Implementar scripts de seguridades y autenticación de usuarios, validación de llaves públicas y privadas.<br>2. Implementar métodos de encriptación robustos.<br>3. Identificar técnicamente el origen del ataque y tomar las acciones legales pertinentes. | INMEDIATO | ALTO | TECNOLOGÍA<br>DEPARTAMENTO LEGAL<br>ASESORÍA TÉCNICA EXTERNA |
| R007 | Interceptación (Eavervesdroping) | 1. Implementar seguridades en el equipo cortafuegos.<br>2. Implementar herramientas de monitoreo y alertas preventivas de tráfico de paquetes In/out, Up/Down | SEGÚN LA OCURRENCIA | MEDIO | TECNOLOGÍA |
| R008 | Redirección de llamadas (Call Redirections) | 1. Implementar seguridades en el equipo cortafuegos.<br>2. Implementar scripts de seguridades y autenticación de usuarios, validación de llaves públicas y privadas.<br>3. Implementar métodos de encriptación robustos.<br>4. Identificar técnicamente el origen del ataque de DoS y tomar las acciones legales pertinentes. | INMEDIATO | ALTO | TECNOLOGÍA<br>DEPARTAMENTO LEGAL<br>ASESORÍA TÉCNICA EXTERNA |

- **Detalle de la Matriz de tratamiento de riesgos.**

La matriz de tratamiento de riesgos determina la acción o procedimiento que se requiera implantar para contrarrestar el riesgo de ataque sufrido en el servicio de telefonía IP, la ocurrencia de estos eventos determina el costo económico que deberá asumir la organización en consecuencia de su afectación de servicio y el impacto causado en el giro de negocio de la misma, de esta manera se contempla los planes de acción.

- **Inmediato, según la ocurrencia de Costo Bajo.**
    - Implementar o Corregir políticas y scripts de configuración en los equipos de comunicación de datos con la finalidad de brindar mayor seguridad al servicio de telefonía IP.
    - Restaurar respaldos de archivos de configuración de los equipos de comunicación en caso de un daño mayor.
    - Identificar técnicamente el origen del ataque y tomar las acciones legales pertinentes con las autoridades correspondientes a nivel nacional como internacional..
    - Depurar parámetros y scripts de configuraciones de la central telefónica con la finalidad de blindar y asegurar el correcto funcionameinto del servicio de telefonía IP.
    - Editar y corregir las políticas de accesos y requerimientos en la central telefónica, listas de control de accesos, tipos de llamadas, tanto para dentro como fuera de la organización.

- **Inmediato, según la ocurrencia de Costo Medio.**
    - Implementar sistemas de seguridad por capas y algoritmos de encriptación para fortalecer todos los componentes del servicio de telefonía IP.
    - Implementar seguridades a nivel de puertos de acceso en el equipo cortafuegos y los equipos de la red de comunicaciones.
    - Implementar mayor número de reglas de seguridades en el equipo cortafuegos.
    - Implementar herramientas de monitoreo y alertas preventivas de tráfico de paquetes In/Out, Up/Down.

- **Inmediato, Costo Alto.**
    - Implementar seguridades en el equipo cortafuegos.
    - Implementar scripts de seguridades y autenticación de usuarios, validación de llaves públicas y privadas.
    - Implementar métodos de encriptación robustos.
    - Identificar técnicamente el origen del ataque y tomar las acciones legales pertinentes.

## 4.5 Aplicación del Modelo de Esquema SGSI sobre sistemas de VoIP y el servicio de telefonía IP.

Para el tratamiento de la seguridad, identificación de riesgos y aplicación de políticas se identifican los siguientes componentes que permiten desarrollar íntegramente el servicio de telefonía IP dentro de una organización:

- **Gestión de usuarios:** Como acción de tratamiento a los riesgos de seguridad, se identifica el usuario y el perfil con el que se produce el ataque de seguridad, también determina la revisión de eventos de acceso de usuarios en el sistema de telefonía y directorio activo.

- **Gestión de accesos:** Como acción de protección frente a los riesgos de seguridad, se determina la revisión y depuración de parámetros y archivos de procesamiento y de configuración tanto de la central telefónica, así como de los equipos de seguridad perimetral; cortafuegos, proxys, controladores de sesión de borde, autorizando y denegando así el acceso a usuarios, aplicaciones y puertos de conexión de todo tipo de aplicaciones que intenten generar algún tipo de amenaza de seguridad.

- **Gestión en cambio de recursos de TI**: Como acción de protección frente a los riesgos de seguridad que se determinen en los recursos de TI en el caso de un daño mayor de causa física o lógica en el servicio de telefonía IP, es necesario considerar la restauración de los respaldos de archivos de

configuración de los equipos de comunicación en los equipos, previamente solucionados los problemas de intrusión, o a su vez en equipos de respaldo de ser el caso de que estos resulten afectados en su funcionamiento de hardware o sistema operativo.

- **Gestión de incidencias servicios de VoIP**: Con esta actividad se lleva una bitácora de eventos de las diferentes acciones de tratamientos de seguridad frente a los riesgos presentados, en base a estas incidencias se pueden: diseñar, implementar y evaluar las diferentes políticas de seguridad para garantizar la continuidad del negocio y la correcta operación del servicio de telefonía IP. Dentro de la **matriz de riesgos por procesos** se identifica para este análisis, que los tipos de amenazas con mayor magnitud de daño e incidencia en los diferentes procesos de la organización con respecto al servicio de telefonía IP son: la suplantación de identidad (*Vishing*), el secuestro de sesiones (*Hijacking*) y la interceptación (*Eaevervesdroping*)

- **Control de actividad en la Red:** Como acción de protección frente a los diferentes riesgos de seguridad, se determina la implementación de herramientas de monitoreo y alertas preventivas de tráfico en tiempo real de paquetes que son enviados y recibidos por los sistemas de VoIP, especialmente en el servicio de telefonía IP. Así también implementa métodos de encriptación de datos robustos e identifica técnicamente el origen del ataque de denegación de servicio *DoS*.

- **Monitoreo de alarmas y degradación del servicio:** Como acción de protección frente a los diferentes riesgos y una vez establecida la línea de control de las diferentes actividades y sucesos en las redes de comunicación, sistemas de VoIP, y en especial en el servicio de telefonía IP se determinan: sistemas de monitoreo y alertas preventivos en tiempo real, con lo cual se establecen políticas de acción para prevenir y corregir presente y futuros incidentes de seguridad en estas aplicaciones de telefonía.

- **Grupos de Riesgos de Seguridad:**
    - **Riesgos Internos:** Incluye factores humanos y técnicos que deben ser solventados a través de la implementación y aplicación de políticas y mecanismos de acción para evitar fraudes telefónicos.

    - **Riesgos Externos: :**Se refiere a los ataques de seguridad determinados y clasificados en: Denegación de Servicios, SPIT, Vishing, Fuzzing, Flooding, Secuestro de sesiones (Hijacking), Interceptación (Eavervesdroping), Redirección de llamadas (Call Redirections), para enfrentar la ocurrencia de estos eventos se determinan políticas de acción, tanto internas y externas y han sido mencionadas y detalladas mediante la **Matriz de acción de tratamiento de riesgos de seguridades**, así como también a través de los componentes del esquema SGSI para el servicio de telefonía IP.

- **Incidentes de Seguridad en el servicio de telefonía IP**: Integra los diferentes tipos de riesgos e incidentes de seguridad identificados mediante las matrices de análisis y evaluación de riesgos determinados en los **Capítulos 4.4.1 y 4.4.2** respectivamente y deben ser solucionados mediantes las acciones de tratamiento correspondientes y la implementación de políticas de seguridad definidas en las políticas de seguridad del **Capítulo 3.3** del presente trabajo.

- Procedimientos de análisis, definición, implementación y seguimiento de riesgos de seguridad dentro de la organización:

  - **Evaluación de Riesgos**: Determinar las consecuencias, probabilidad de impacto y severidad en la afectación del servicio de telefonía IP, determinados en las Matrices de evaluación y tratamiento de riesgos **Capítulos 4.4.2 y 4.4.3** respectivamente.

  - **Definición de Políticas de Seguridad**: Establecer lineamientos técnicos y administrativos para contrarrestar la ejecución de todo tipo de riesgo de seguridad en el servicio de telefonía IP, interno o externo a la organización, determinados en el **Capítulo 3.3** Políticas de Seguridad para sistemas de VoIP

- **Implementación de políticas y controles de seguridad**: Implementar las políticas de seguridad para acceso a la información, políticas de seguridad para el uso de comunicaciones externas e Internet, políticas de seguridad para aplicaciones de voz y el servicio de telefonía IP y políticas de seguridad para el diseño e infraestructura de red.

- **Medición de resultados**: Evaluar los parámetros de los resultados obtenidos mediante métricas de impacto en cada uno de los procesos de la organización a través de la indisponibilidad del servicio de telefonía IP.
- **Acciones preventivas y correctivas:** Prevenir y corregir los riesgos de seguridad en tiempo real y a corto plazo a través de los procesos de auditoría interna y externa.

## 4.6 Tratamiento de Riesgos de Seguridades para evitar fraudes en el servicio de telefonía IP, casos prácticos.

El proceso de evaluación y tratamiento de los riesgos de seguridad para el servicio de telefonía IP dentro de una organización; permite; identificar, cuantificar y priorizar cada una de las amenazas de riesgo de fraudes telefónicos en relación con los objetivos principales de la organización y su giro de negocio. Es así que los resultados establecen una guía de aplicación e implementación de mecanismos de acción para contrarrestar la magnitud de impacto y la ocurrencia de los mismos.

Es necesario denotar que además de contar tanto con un modelo de Sistema de Gestión de Seguridad para la Información (*SGSI*), así como de las políticas de seguridad que puedan ser aplicadas a cualquier herramienta tecnológica que permita gestionar el servicio de telefonía IP privada o de código abierto dentro de una organización, se requiere establecer los métodos y herramientas de configuración tecnológicas necesarios que en la actualidad permiten operar y garantizar de manera segura el servicio de telefonía IP evitando todo tipo de riesgo por fraude. A través de esta premisa se mencionan como ejemplo de caso práctico; tres soluciones de telefonía corporativa que utilizan el protocolo IP con sus respectivas aplicaciones y características de seguridad las cuales permiten garantizar la seguridad de operación del servicio y evitar todo tipo de riesgo de seguridad que cause algún tipo de fraude dentro de la organización.

Estas soluciones pertenecen a marcas reconocidas a nivel mundial; dos de ellas son determinadas como Líderes dentro del cuadrante mágico de Gartner de telefonía corporativa[21]; *CISCO Systems* con su solución empresarial *Cisco Unified CallManager* y Avaya con su solución *IP Office.* Sin embargo, no puede dejarse a un lado las soluciones de código abierto que a pesar de no constar dentro de la clasificación del cuadrante mágico mencionado, por su aplicación y uso a nivel mundial es necesario mencionar a *Digium* con su solución de telefonía *Elastix/ Asteris.*

Dentro de la clasificación de riesgos que se ha mencionado en el presente trabajo de investigación a través de la Matriz de análisis de Riesgos detallada en el

[21] Gartner, Inc. (Octubre 2014). Magic Cuadrant for Corporate Telephony. Recuperado de: http://www.gartner.com/technology/reprints.do?id=1-23HXCI1&ct=141022&st=sb

**Capítulo 4.4.1** Las principales consecuencias determinadas por los riesgos de seguridad son; la indisponibilidad del servicio, el acceso no autorizado al servicio y el robo de la información., frente a lo cual se han establecidos las siguientes características de seguridad por aplicación:

***Cisco Unified Communications Manager***: Realiza el procesamiento de llamadas para centrales y teléfonos IP, integra *gateways* de voz y *ruteadores* de servicios integrados para comunicaciones unificadas, en cuanto a seguridad para evitar posibles ataques de seguridad y fraudes telefónicos establece diversas herramientas de seguridad de control y de función de restricción, las cuales se describen a continuación:

- ***Direct-inward-dial (DID):*** Se utiliza en puertas de enlaces de voz con el fin de bloquear cualquier tipo de discado mientras una llamada se encuentra en ejecución, evitando un marcado secundario en el cual se puedan determinar amenazas de intrusión.
- ***After-hours toll restriction:*** Es una herramienta de seguridad de Cisco que permite configurar las directivas de restricción de acceso y bloqueo del servicio de telefonía determinado por hora y fecha para los usuarios en referencias a comunicaciones internas o externas.
- ***Access-list to restrict H323/SIP trunk Access:*** Debido a la conexión de la central telefónica IP mediante enlaces WAN hacia otros dispositivos de telefonía en diferentes sucursales que utilizan el servicio de Cisco Manager a través de H.323 o SIP, se restringe el acceso a estos protocolos para evitar que puedan transmitir llamadas ilegales a la PSTN.

- ***Secure Cisco Unity Express: AA PSTN Access:*** Permite desactivar la transferencia o reenvío de llamadas externas a la PSTN desde la central telefónica de Cisco.
- ***Cisco Unity Express Restriction Tables***: Las tablas de restricción se utilizan para restringir destinos y evitar fraudes en cuanto a llamadas salientes desde la Central telefónica o reenvío de llamadas.
- ***Call Logging:*** Se configura el sistema para almacenar el registro de llamadas internas y externas y evaluar permanentemente el uso del servicio, a través de la función de contabilidad de archivo permite capturar los registros contables en relación a los tipos de llamadas y evaluar costos de operación.

***Avaya IP Office y Aourora***: Son plataformas de comunicaciones IP para pequeñas, medianas y grandes empresas, que entre sus características se determina el uso de centrales telefónicas a través de características de movilidad, tele presencia, administración centralizada y convergencia. Este tipo de plataforma ofrece características de; soporte y operatividad con multi-marca de equipos telefónicos, servidor de mensajería, conferencia, centro de contacto, entre otras. Como característica de seguridad para evitar fraudes telefónicos, establece la aplicación Session Border Controller:

- ***Avaya Session Border Controller:*** Es la solución de seguridad que provee un corta fuegos de protección basado en el protocolo de comunicaciones SIP, ofrece funciones avanzadas de cifrado para conexiones sin necesidad de uso

de redes virtuales privadas VPN, esta aplicación tiene las siguientes características:

- **Seguridad avanzada para llamadas dentro y fuera de la organización:** Implementación de protocolos y esquemas de seguridad para impedir re-direccionamiento de llamadas o ejecución de llamadas de larga distancia.
- **Inspección profunda de paquetes de señalización:** Inspección y filtrado de paquetes a través de los protocolos de comunicación utilizados SIP/H.323.
- **Lista de control de acceso:** Manejo de listas de usuarios, grupos, códigos regionales o de países para la ejecución o recepción de llamadas.
- **Control de admisión de llamadas:** Categorización de ingreso de llamadas telefónicas, desactiva la transferencia o reenvío de llamadas externas a la PSTN.
- **Encubrimiento de topología:** Enmascara el diagrama de red y de conexión de toda la infraestructura de comunicaciones utilizada para la ejecución del servicio telefónico.
- **Configuración de servicio nocturno:** Permite configurar las directivas de restricción de acceso y bloqueo del servicio de telefonía determinado por horas y usuarios.
- **Administración de grupos:** Maneja y categoriza grupos con privilegios de acceso al servicio, manteniendo los esquemas de seguridad y encriptación propios de la marca.

- **Vectorización de llamadas:** manejo, clasificación y categorización de llamadas para el enrutamiento automático y seguro.
- **Sistema de reportes:** permite visualizar la estadística de uso del servicio y comparar con reportes contables por la facturación del servicio, permite el análisis de costo beneficio del uso del servicio y determina patrones de análisis para fraudes por llamadas telefónicas a la organización.

***Elastix:*** El producto estrella de Digium es una plataforma de código abierto que permite establecer el servicio de comunicaciones unificadas dentro de una organización, uno de sus principales servicios es el de la telefonía IP, que al igual que otras marcas propietarias ofrece gran variedad de características técnicas para el uso dentro de una organización. Para garantizar la seguridad y evitar riesgos de afectación por fraude, determina una serie de aplicaciones denominadas "*Addons*", entre las cuales se mencionan las más importantes:

- ***Anti-Hacker:*** Este módulo protege al servidor de telefonía y evita ataques a sus servicios principales como ASTERISK, INTERFAZ WEB (http/https), SSH, VSFTPD (ftp). Detiene ataques de fuerza bruta por denegación de servicios, determina listas de control de acceso para el uso del servicio de telefonía.
- ***Eagle-Eye:*** es una suite de módulos que permite administrar, bloquear y auditar el sistema de telefonía para evitar el abuso de los recursos telefónicos pro parte de intrusos, establece la primer línea de defensa determinando listas blancas de acceso al sistema por usuarios, ciudades, países.

- ***Humbug Analytics:*** Herramienta para la detección y prevención de fraudes, analiza en tiempo real el tipo de tráfico que es procesado por la central telefónica, analiza el tráfico de red IP y compara con una base de datos central de información fraudulenta, gestiona todo tipo de reportes de eventos de la central para análisis de acciones fraudulentas.
- ***Monitoring Services:*** establece informes periódicos y en tiempo real acerca del rendimiento del equipo servidor de telefonía, manejando valores y rangos de operación que permiten determinar rangos de seguridad de intrusión o afectación del servicio.

Es necesario mencionar además que existen diferentes aplicaciones y líneas de productos que son integrales a soluciones de telefonía IP existentes y permiten determinar los niveles y esquemas de seguridades necesarios para una correcta operación del servicio, enfocándose en la reducción de riesgos de seguridad y fraudes. Entre ellas se puede mencionar dos soluciones corporativas:

- ***RedShift Networks:*** ofrecer soluciones de seguridad integrales para redes, sistemas y aplicaciones de Voz por IP, Video, Comunicaciones Unificadas y Colaboración, en su línea de productos determina:
    - ***Protección:*** a través de la identificación de amenazas estáticas y dinámicas con motores de aprendizaje y monitoreo en tiempo real.
    - ***Visibilidad:*** análisis y reporte de sesiones de tráfico de redes.
    - ***Control:*** aplicación de políticas de control de tráfico para incrementar la operación del servicio.

- ***Fortivoice de Fortinet***: Es la solución se seguridad para la administración del servicio de telefonía IP, permite establecer todas las bondades de un potente cortafuegos, manejando y administrando todo tipo de paquetes de datos desde y hacia el servicio de telefonía IP de una organización, administración de políticas de listas de control de acceso, administración de redes virtuales privadas y administración centralizada de seguridad para toda la organización.

## 4.7 Consideraciones de Seguridades sobre el servicio de telefonía IP.

En base al tratamiento de riesgos de seguridades para el servicio de telefonía IP y las diferentes características y aplicaciones técnicas expuestas anteriormente para evitar fraudes en este servicio, se enmarcan 3 consideraciones de seguridad técnica que abarcan de manera global los aspectos necesarios para contemplar al momento de determinar un sistema de prevención de riesgos y asegurar de manera segura la operación del servicio de telefonía dentro de una organización:

- **La infraestructura de red:** contempla la protección a nivel físico y lógico las redes Ethernet e inalámbrica a través de controles de acceso y cifrado, así también es necesario determinar el control de tráfico entre las diferentes zonas de seguridad a través de protocolos y políticas de códigos de seguridad perimetral. Es necesario además considerar todo el equipamiento que integrará el servicio de telefonía a fin de evaluar todos los parches y

actualizaciones de seguridad necesarios para no comprometer la seguridad del servicio como tal. A través de procesos de auditoria de redes se evalúa continuamente la infraestructura de comunicaciones en su totalidad.

- **Metodología de seguridad:** La seguridad del servicio de telefonía IP dentro de una organización está determinada en primera instancia por el nivel de seguridad que se determine en la red IP, luego de esto, es necesario establecer el nivel de seguridad tanto para el servicio de telefonía como para la organización en sí. Se establecen cuatro parámetros fundamentales para determinar la seguridad del servicio de telefonía IP;

    - **Evaluación de riesgos:** evaluación de impacto en el negocio de amenazas y vulnerabilidades.
    - **Arquitectura de diseño de seguridad:** Sistemas de gestión de riesgos y seguridades, normas y políticas de control para el servicio de telefonía IP.
    - **Implementación, operación y mantenimiento del servicio de telefonía IP:** Implementación de procesos de seguridad durante todo el proceso de implementación del servicio y monitoreo de la operación del servicio, determinando un proceso de mejora continua.

## 4.8 Mecanismos de acción para evitar fraudes en el servicio de telefonía IP.

A continuación se mencionan las recomendaciones necesarias para evitar la ocurrencia de riesgos por fraudes internos en el servicio de telefonía IP dentro de una organización, la aplicación de las mismas aseguran el correcto funcionamiento y operación de este sistema.

- Desactivar las funciones de la central telefónica que no vayan a ser requeridas, como por ejemplo; buzones de voz, desvió de llamadas, acceso a servicio de operadoras, servicios de acceso directo (*DISA*).
- Evitar el uso de puertos estándar o por defecto para la configuración de centrales y aplicaciones en los servicios de telefonía IP.
- Mantener al día las actualizaciones y parches de seguridad de la infraestructura y aplicaciones funcionales que son utilizadas para el servicio de telefonía IP.
- Implementar herramientas que brinden seguridad al funcionamiento de la red de datos y aplicaciones de comunicación como; firewalls, proxys y controladores de sesión de borde.
- Cambiar los códigos de acceso configurados por defecto para el uso de los servicios de llamadas en la central telefónica.
- Configurar el sistema de telefonía para no acceder a tono de discado, esta característica presenta gran vulnerabilidad en la seguridad de las aplicaciones telefónicas.

- Revisar de manera periódica el estado inactivo de las características y servicios no configurados para el funcionamiento de la central telefónica.
- No mantener contraseñas por defecto para el uso y configuración de los dispositivos y servicios de comunicación, como teléfonos, y buzones de voz respectivamente.
- Cambiar periódicamente las contraseñas de acceso a los servicios de telefonía, buzones de voz y buzones de correo.
- Definir categorías, políticas internas y niveles de acceso para todo tipo de llamadas; nacionales, regionales, internacionales o móviles.
- Configurar la central telefónica en modo nocturno para evitar llamadas entrantes fuera del horario de oficina para evitar intrusiones por códigos de acceso.
- Mantener bajo estrictas normas de seguridad y confidencialidad la documentación y esquemas de configuración de la central telefónica y todo el servicio de telefonía IP.
- Determinar en los informes de instalación, soporte y mantenimiento de la central realizados por personal técnico de la organización, clausulas legales de responsabilidad por cambios no acordados o programados dentro de la aplicación del servicio de telefonía.
- Vigilar y comprobar el trabajo de personal técnico externo a la organización, durante y después de los trabajos de mantenimiento de la central de telefonía.
- Llevar mediante una bitácora, los mantenimientos, reprogramaciones, o cambios al sistema de telefonía, a través de fecha, hora, responsable y detalle de la actividad realizadas.

- Revisar de manera periódica la facturación del consumo de servicio de telefonía, comparando entre los reportes internos del sistema y el valor de facturación de las empresas telefónicas.
- Realizar el monitoreo continuo y en tiempo real de los destinos de llamadas telefónicas entrantes y salientes de la organización con el fin de detectar tráfico irregular y posibles ataques de seguridad.
- Realizar programas periódicos de auditoría a la configuración y funcionamiento de la central telefónica y los procesos que integran el funcionamiento del servicio de telefonía IP, con el fin de comprobar la seguridad, puntos débiles y la estructura de funcionamiento con la organización.
- Establecer y socializar políticas claras del empleo y uso del servicio de telefonía dentro de la organización y realizar el seguimiento continuo de su cumplimiento y aplicación a cada uno de sus funcionarios.

# CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES.

## 5.1 Conclusiones.

- A través de la estructuración de las matrices de análisis, evaluación y tratamiento de riesgos de seguridad sobre el servicio de telefonía IP, que se han determinado en el presente trabajo de investigación se proponen los diferentes mecanismos de acción y políticas de seguridad necesarias para evitar fraudes en el servicio de telefonía IP dentro de una organización.
- Mediante la propuesta del esquema de Sistema de Gestión de Seguridad de la Información SGSI se determina la metodología secuencial para identificar, valorar, estructurar y cuantificar los procedimientos necesarios para el tratamiento de los riesgos de seguridad por tipo de afectación en el servicio de telefonía IP sobre una arquitectura de VoIP.
- El esquema del Sistema d Gestión de Seguridad de la Información - SGSI propuesto para el servicio de telefonía IP se basa en la metodología: Planificar, Hacer, Verificar y Actuar, esta identifica y determina los parámetros necesarios de seguridad tanto de hardware como de software para el funcionamiento del servicio de telefonía IP dentro de una organización, garantizando la continuidad y disponibilidad del giro de negocio de manera ininterrumpida.
- Es importante denotar la diferencia entre la arquitectura de VoIP y el servicio de telefonía IP, la implementación y convergencia de las dos permiten la operación y funcionalidad del servicio de comunicación de voz sobre el protocolo IP como

tal, teniendo en cuenta que el servicio de telefonía depende de la tecnología de VoIP.

- Uno de los principales pilares de la seguridad de la información para la arquitectura de VoIP y el servicio de telefonía IP es mantener constantemente informado a los usuarios de la organización acerca de los potenciales riesgos que se presentan a diario en las tecnologías de la. Así también es necesario controlar continuamente a través de procesos de auditoría, la aplicación y uso de las políticas de seguridad para el uso de estos servicios dentro de la organización.
- La definición y aplicación de las políticas de seguridad determinadas a través de la aplicación de la Norma ISO/IEC 27001 y los Sistemas de Gestión de Seguridad de la Información SGSI para la arquitectura de VoIP requiere de un modelo de implementación secuencial y continuo que integra los componentes de: elaboración, planificación, implementación, verificación, revisión y auditoría para cada uno de los procesos de la organización que utilizan el servicio de telefonía IP.
- El uso del servicio de telefonía IP, sobre protocolos de comunicaciones en tiempo real, demanda de manera obligatoria y eficaz la aplicación de Sistemas de Gestión de Seguridad de la Información a través de la implementación y el uso, tanto de protocolos de seguridad y cifrado, así como mecanismos de prevención, detección y respuestas de amenazas, no obstante es necesario aplicar la normalización de políticas de seguridad bajo estándares nacionales e internacionales como el NTE INEN-IDO/IEC 27001:2011 y el ISO/IEC 27001, respectivamente, los mismos que permiten y evitan la incidencia de riesgos por fraudes, causando grandes perjuicios económicos y legales para la organización

- Una de las tecnologías que mayor demanda tiene hoy por hoy es la comunicación de telefonía mediante el protocolo de Internet IP, soportada por la arquitectura de VoIP, manejando normas y estándares regulados tanto internacionales a través de la ISO / IEC, como nacionales, que para el caso de Ecuador mediante la resolución TEL-069-04-CONATEL-2013 se establecieron las directrices y regulaciones que deberán seguir y cumplir los prestadores de servicios de telecomunicaciones.
- El monitoreo continuo del funcionamiento de la infraestructura y aplicaciones que integran el servicio de telefonía IP sobre una arquitectura de VoIP, son un factor importante para la identificación y valoración temprana de los riesgos de seguridad que se clasifican según el detalle de la Matriz de análisis de riesgos **Capítulo 4.4.1** en: indisponibilidad del servicio de telefonía, acceso y robo de la información confidencial, sobrevaloración de planillas de consumo de servicio, sobrecarga de operación en las centrales de telefonía y acceso no autorizado al servicio de telefonía.
- Tanto los procesos de auditoría interna y externa estructurados mediante la Norma ISO/IEC 27001, así como la ejecución de análisis forense, constituyen mecanismos eficaces de evaluación, reportes y toma de decisiones para la detección, tratamiento y corrección de los diferentes tipos de riesgos de seguridad que se determinan en el servicio de telefonía IP dentro de las organizaciones.

## 5.2 Recomendaciones.

- Una de las recomendaciones principales al momento de evitar riesgos de seguridad en el servicio de telefonía IP es la implementación y uso de redes privadas virtuales VPN para la conexión y acceso a los servicios de telefonía y teleconferencia, con el fin de preservar la seguridad e integridad de la información de la organización.
- Es recomendable el uso de infraestructura de hardware para brindar las seguridades en la arquitectura de VoIP y sobre todo en el servicio de telefonía IP, se determina a través de la implementación de equipos de protección de acceso como: cortafuegos, gateways, proxys y equipos de control de sesión de borde, cuya característica principal es la aplicación de protocolos de seguridad robustos y esquemas de cifrado avanzado.
- Al implementar el uso de la norma ISO/IEC 27001 para el Sistema de Gestión de Seguridad de la Información en los sistemas de comunicación de VoIP, se recomienda adicionalmente determinar la aplicación y uso de las normas: ISO/IEC 27003, ISO/IEC 27004 que se refieren a la guía de implementación y medición respectivamente de los sistemas de gestión de la seguridad de la información dentro de la organización.
- Se recomienda determinar y asignar parte del presupuesto anual de costos de inversión de una organización, en adquirir, mantener y actualizar los sistemas de monitoreo y alertas en tiempo real para el sistema de telefonía IP, a fin de identificar, analizar, evaluar y tratar los posibles fallos y problemas de fraudes de seguridad que puedan afectar el funcionamiento del servicio de telefonía.

- Mediante el desarrollo del presente trabajo de investigación, se recomienda mantener y almacenar de manera segura copias y respaldos de configuración certificados y funcionales, de los equipos y aplicaciones que integran el servicio de telefonía IP, a fin de reducir el impacto y tiempo de recuperación de la aplicación de telefonía en caso de una ocurrencia de falla, o riesgo de seguridad determinado en la organización.
- Para el caso de uso y aplicación de los Sistemas de Gestión de Seguridad de la Información para organizaciones ecuatorianas que utilizan el servicio de telefonía IP, se sugiere la implementación de la norma NTE INEN-IDO/IEC 27001:2011 bajo el modelo PDCA. Norma referenciada en base al estándar internacional ISO/IEC 27001 y adaptada al medio organizacional y políticas de regulación del Ecuador. Siendo además susceptible de certificación nacional e internacional para el beneficio de la organización.

# BIBLIOGRAFÍA


*BORRMART*. (s.f.). Obtenido de http://www.borrmart.es/articulo_redseguridad.php?id=2078

*BURODEANALISIS*. (s.f.). Obtenido de http://www.burodeanalisis.com/2011/08/08/robos-electronicos-alertan-sobre-fragilidad-en-ecuador/

*COSO*. (s.f.). Obtenido de http://www.coso.org

*DLP*. (s.f.). Obtenido de http://m.b5z.net/i/u/6113204/f/Est%20DLP/Presentacion_DLP.pdf

*F5*. (s.f.). Obtenido de http://www.f5networks.es/es/es/news-press-events/press-releases/2013/20130617.html

*GOBERNABILIDAD*. (s.f.). Obtenido de http://www.gobernabilidad.cl/documentos/martinez.pps

*GRUPOBANCOLOMBIA*. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/pdf/informeSistemaControlInterno.pdf

*GRUPOBANCOLOMBIA*. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/buenGobierno/sistemaControlInterno.asp

*IDG*. (s.f.). Obtenido de http://www.idg.es/iworld/articulo.asp?id=152376

*ISACA*. (s.f.). Obtenido de http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

*ISACAMTY*. (s.f.). Obtenido de http://www.isacamty.org.mx/archivo/Evento%20Anual%202010.pdf

*KASPERSKY*. (s.f.). Obtenido de http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/blog-de-kaspersky/troyanos-brasil

Mantilla, S. (2013). [D]. *Auditoría del control interno*. Colombia: ECOE EDICIONES.

*NETWORKWORLD*. (s.f.). Obtenido de http://www.networkworld.es/Prevencion-de-intrusiones_Como-desplegar-sistemas-IPS/seccion-/articulo-190083

*OSIATIS*. (s.f.). Obtenido de http://itil.osiatis.es/

*PCI DSS*. (s.f.). Obtenido de http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/pci_dss_v2-0.pdF

*REPOSITORIO UASB*. (s.f.). Obtenido de http://repositorio.uasb.edu.ec/bitstream/10644/2415/1/T0358-MBA-Silva-An%C3%A1lisis.pdf

*REVISTAVANGUARDIA*. (s.f.). Obtenido de http://www.revistavanguardia.com/index.php?option=com_content&view=article&id=204&Itemid=216

*SBS*. (s.f.). Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=7&vp_tip=2

*SCRIBD*. (s.f.). Obtenido de http://es.scribd.com/doc/39934738/Metodos-y-tecnicas-para-la evaluaciondecontrol-interno

Telefónica. (2010). [B]. *Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. España: AENOR.

Torres, G. (2013). [A]. *Desarrollo de una guía metodológica para la gestión de tecnología que asegure el control interno en empresas del sector financiero*. Ecuador: PUCE.

Torres, G., & Villegas, F. (2008). [C]. *Evaluación y Auditoria del Sistema de Información de la Escuela Politécnica del Ejército: Dominio, Evaluación y Monitoreo*. Ecuador: ESPE.

*UBIOBIO*. (s.f.). Obtenido de http://www.ubiobio.cl/miweb/webfile/media/42/version%206/acuerdo.pdf

*UNAP*. (s.f.). Obtenido de http://www.unap.cl/~setcheve/cobit/CobiT-106_1.gif

*BORRMART*. (s.f.). Obtenido de http://www.borrmart.es/articulo_redseguridad.php?id=2078

*BURODEANALISIS*. (s.f.). Obtenido de http://www.burodeanalisis.com/2011/08/08/robos-electronicos-alertan-sobre-fragilidad-en-ecuador/

*COSO*. (s.f.). Obtenido de http://www.coso.org

*DLP*. (s.f.). Obtenido de http://m.b5z.net/i/u/6113204/f/Est%20DLP/Presentacion_DLP.pdf

*F5*. (s.f.). Obtenido de http://www.f5networks.es/es/es/news-press-events/press-releases/2013/20130617.html

*GOBERNABILIDAD*. (s.f.). Obtenido de http://www.gobernabilidad.cl/documentos/martinez.pps

*GRUPOBANCOLOMBIA*. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/pdf/informeSistemaControlInterno.pdf

*GRUPOBANCOLOMBIA*. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/buenGobierno/sistemaControlInterno.asp

*IDG*. (s.f.). Obtenido de http://www.idg.es/iworld/articulo.asp?id=152376

*ISACA*. (s.f.). Obtenido de http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

*ISACAMTY*. (s.f.). Obtenido de http://www.isacamty.org.mx/archivo/Evento%20Anual%202010.pdf

*KASPERSKY*. (s.f.). Obtenido de http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/blog-de-kaspersky/troyanos-brasil

Mantilla, S. (2013). [D]. *Auditoría del control interno*. Colombia: ECOE EDICIONES.

*NETWORKWORLD*. (s.f.). Obtenido de http://www.networkworld.es/Prevencion-de-intrusiones_Como-desplegar-sistemas-IPS/seccion-/articulo-190083

*OSIATIS*. (s.f.). Obtenido de http://itil.osiatis.es/

*PCI DSS*. (s.f.). Obtenido de http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/pci_dss_v2-0.pdF

*REPOSITORIO UASB*. (s.f.). Obtenido de http://repositorio.uasb.edu.ec/bitstream/10644/2415/1/T0358-MBA-Silva-An%C3%A1lisis.pdf

*REVISTAVANGUARDIA*. (s.f.). Obtenido de http://www.revistavanguardia.com/index.php?option=com_content&view=article&id=204&Itemid=216

*SBS*. (s.f.). Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=7&vp_tip=2

*SCRIBD*. (s.f.). Obtenido de http://es.scribd.com/doc/39934738/Metodos-y-tecnicas-para-la evaluaciondecontrol-interno

Telefónica. (2010). [B]. *Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. España: AENOR.

Torres, G. (2013). [A]. *Desarrollo de una guía metodológica para la gestión de tecnología que asegure el control interno en empresas del sector financiero*. Ecuador: PUCE.

Torres, G., & Villegas, F. (2008). [C]. *Evaluación y Auditoria del Sistema de Información de la Escuela Politécnica del Ejército: Dominio, Evaluación y Monitoreo*. Ecuador: ESPE.

*UBIOBIO*. (s.f.). Obtenido de http://www.ubiobio.cl/miweb/webfile/media/42/version%206/acuerdo.pdf

*UNAP*. (s.f.). Obtenido de http://www.unap.cl/~setcheve/cobit/CobiT-106_1.gif