ANALISIS Y DIAGNOSTICO AL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA RED VOIP EN EL AREA DE SISTEMAS DEL NIVEL CENTRAL DE LA DEFENSORIA DEL PUEBLO

MARTHA CÁRDENAS ROJAS

Ingeniero
MARTIN CAMILO CANCELADO RUIZ
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C
2015

ANALISIS Y DIAGNOSTICO AL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA RED VOIP EN EL AREA DE SISTEMAS DEL NIVEL CENTRAL DE LA DEFENSORIA DEL PUEBLO

MARTHA CÁRDENAS ROJAS

Trabajo de grado como requisito para optar el título de Especialista en Seguridad Informática

Ingeniero
MARTIN CAMILO CANCELADO RUIZ
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C
2015

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

DEDICATORIA

Desde el momento en que inicie este nuevo camino en mi vida puse toda mi confianza en mi Dios quien me hace fuerte, grande y no me dejo desfallecer ante las adversidades que tuve que pasar.

A mis hijos y nietos a quienes siempre he enseñado que somos personas trabajadores y estudiosas, capaces de lograr cualquier meta en nuestras vidas.

A mi familia que con orgullo piensa en mí como una mujer luchadora que da ejemplo de superación a las personas que la rodean.

Al profesor que fue mi guía, mi consejero y sin darnos cuenta mi amigo, quien supo cómo conducirme para aplicar el conocimiento y lograr los objetivos trazados.

AGRADECIMIENTOS

Cuando se inicia un recorrido muchas veces no sabemos si llegaremos o no, hoy agradezco que un día un hombre puso su fe en que yo lo lograría y me impulso para que así fuera, ayudándome a arrancar, ahora puedo dar gracias a Dios y a mi familia por la satisfacción del deber cumplido. Quizá vengan nuevos retos que deberé afrontar pero estoy segura que lograré llegar a la cima una vez más.

A mis profesores gracias por su apoyo, comprensión, amistad, por sus conocimientos y dedicación, desde que iniciamos el camino, que hoy llega a su recta final de la mano de todos ustedes.

A mi Universidad Nacional Abierta y a Distancia “UNAD”, por brindar la oportunidad de ser parte de ustedes y llevar con orgullo el título de egresada del Alma Mater en donde curse estudios de pregrado y obtuve el título de Ingeniera de Sistemas y ahora en el postgrado como Especialista en Seguridad Informática.

TABLA DE CONTENIDO

TITULO DEL PROYECTO 11
INTRODUCCIÓN 11
1. PROBLEMA DE INVESTIGACIÓN 12
1.1 DESCRIPCIÓN 12
1.2 FORMULACION DEL PROBLEMA 12
2. ALCANCES Y LIMITACIONES 14
2.1 ALCANCES 14
2.2 LIMITACIONES 14
3. OBJETIVOS 15
3.1 OBJETIVO GENERAL 15
3.2 OBJETIVOS ESPECÍFICOS DEL PROYECTO 15
4. JUSTIFICACION 16
5. MARCO REFERENCIAL 17
5.1 ANTECEDENTES TEMÁTICOS DE LA INVESTIGACIÓN 17
5.2 MARCO TEÓRICO 19
5.3 MARCO LEGAL 20
5.3.1 NORMATIVIDAD INTERNACIONAL 20
5.3.2 LEY NACIONAL 23
5.4 MARCO HISTÓRICO 25
5.5 MARCO CONTEXTUAL INSTITUCIONAL 25
6. HERRAMIENTAS DE ANALISIS Y DE VULNERABILIDAD. 27
7. ANÁLISIS DE LA INFORMACIÓN 31
7.1 RECOLECCION DE LA INFORMACIÓN 31
7.1.1 Estructura Física: 31
7.1.2 Diseño de la Solución de Telefonía VOIP 31
7.1.3 Especificaciones Técnicas 32
7.1.3.1 Sistema de Comunicaciones 32
7.1.3.2 Gateway y Troncales Análogas y Digitales 33
7.1.3.3 Terminales IP Tipo Ejecutivo/Gerencial 33
7.1.3.4 Servidor Avaya S8300 35
7.1.3.5 Configuración Swich AVAYA 5530 36

7.1.3.6 Configuración Gateway 38
8. DIAGRAMA DE RED VOIP AREA DE SISTEMAS DEL NIVEL CENTRAL DEFENSORIA DEL PUEBLO 39
9. ACERCA DE LA SEGURIDAD 40
9.1 Analizador de vulnerabilidades 42
9.2 Configuración CISCO ASDM para ASA 46
10. ATAQUES A LA RED VOIP 50
11. Aplicación NTC – ISO- IEC- 27001 53
12. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA ANEXO A ISO 27001 55
DOMINIO: A.5 Políticas de la Seguridad de la Información 55
DOMINIO: A.6 Organización de la Seguridad de la Información 56
DOMINIO: A.7 Seguridad de los Recursos Humanos 57
DOMINIO: A.8 Gestión de Activos 59
DOMINIO: A.9 Control de Acceso 60
DOMINIO: A. 10 Criptografía 62
DOMINIO: A. 11 Seguridad Física y del Ambiente 63
DOMINIO: A. 12 Seguridad de las Operaciones 65
DOMINIO: A. 13 Seguridad de las comunicaciones 68
DOMINIO: A. 14 Adquisición, desarrollo y mantenimiento de sistemas 69
DOMINIO: A. 15 Relaciones con los proveedores 70
DOMINIO: A. 16 Gestión de incidentes de seguridad de la información 71
DOMINIO: A. 17 Aspectos de seguridad de la información de la gestión de continuidad del negocio 73
DOMINIO: A. 18 Cumplimiento 74
13. ANALISIS GAP PARA ISO - 27001 75
14. PORCENTAJE DE IMPLEMENTACION DE DOMINIOS 77
15. PROPORCION DE CONTROLES POR ESTADO DE IMPLEMENTACION 78
16. RESULTADOS SEGÚN NIVEL DE RIESGO 79
17. PROPUESTA DE SEGURIDAD (HALLAZGOS Y RECOMENDACIONES) 80
17.1 PLAN DE CONTINUIDAD DEL NEGOCIO 81
17.2 POLITICAS DE SEGURIDAD PARA LA RED VOIP 82
17.3 PLAN DE CAPACITACION 83
18. PRESUPUESTO 84

19. CRONOGRAMA DE ACTIVIDADES. 85
20. CONCLUSIONES 87
21. REFERENCIAS 88

TABLA DE ILUSTRACIONES

Ilustración 1 Organigrama Estructura Defensoría del Pueblo 26
Ilustración 2 Servidor AVAYA 35
Ilustración 3 Configuración Switch 36
Ilustración 4 Comando Interfase 36
Ilustración 5 Manejador Dispositivo 37
Ilustración 6 Configuración Vlan 37
Ilustración 7 Seleccionador de puertos 37
Ilustración 8 Creando Vlans 38
Ilustración 9 Configuración dirección IP Vlan 38
Ilustración 10 Gateway G430 38
Ilustración 11. Red VOIP área de sistemas de la Defensoría del Pueblo 39
Ilustración 12 Diagrama de seguridad red VOIP 41
Ilustración 13 Red CISCO ASDM para ASA 42
Ilustración 14 Configuración de Captura 42
Ilustración 15 Asistente de la captura. 43
Ilustración 16 Parámetros de captura 43
Ilustración 17 Direccionamiento 44
Ilustración 18 Definición de tamaño de Buffer 45
Ilustración 19 Listas de acceso 45
Ilustración 20 inicio de captura 46
Ilustración 21 CISCO para ASA 46
Ilustración 22 Control de tráfico de Red 47
Ilustración 23Gestion del Riesgo 53
Ilustración 24 Análisis Gap 77
Ilustración 25 Proporción de Controles 78

LISTA DE TABLAS

Tabla 11.1. Nivel del Riesgo 54
Tabla 12.1. Dominio A5 55
Tabla 12.2. Dominio A6 56
Tabla 12.3. Dominio A7 57
Tabla 12.4. Dominio A8 59
Tabla 12.5. Dominio A9 60
Tabla 12.6. Dominio A10 62
Tabla 12.7. Dominio A11 63
Tabla 12.8. Dominio A12 65
Tabla 12.9. Dominio A13 68
Tabla 12.10. Dominio A14 69
Tabla 12.11. Dominio A15 70
Tabla 12.12. Dominio A16 71
Tabla 12.13. Dominio A17 73
Tabla 12.14. Dominio A18 74
Tabla 13.1. Porcentaje de implementación dominios de control.....75
Tabla 16.1. Resultados según nivel del riesgo 79
Tabla 16.2. Dominios de control a implementar.....79
Tabla 18.1. Presupuesto.....84
Tabla 19.1. Cronograma.....85

TITULO DEL PROYECTO

Análisis y diagnóstico al sistema de gestión de seguridad de la información de la red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo.

INTRODUCCIÓN

Actualmente el entorno laboral exige la aplicabilidad del conocimiento de los Ingenieros Especializados en Seguridad Informática, para que la prestación del servicio se realice bajo estándares de calidad; garantizando la seguridad, confiabilidad, confidencialidad, integridad y disponibilidad en el manejo de la información.

La entidad en su Plan Estratégico Institucional contempla el mejoramiento de los sistemas de información y las comunicaciones para facilitar la toma de decisiones lo que deberá contemplar entre otros la Seguridad de la Información en la red VOIP, verificando que se dé cumplimiento a lo establecido en la normatividad vigente y la aplicación de herramientas establecidas para tal fin.

El estudio y aplicación de la guía de mejores prácticas se debe dirigir al control y supervisión de tecnología de la información en la entidad, y tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI.

1. PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN

Teniendo en cuenta que hoy en día, en la Defensoría del Pueblo, todas las personas usan un computador conectado a Internet; para comunicarse, intercambiando datos, correos electrónicos, o a través de mensajería instantánea, y que el concepto de Internet va de la mano con las telecomunicaciones y la utilización de las redes IP para la transmisión de voz, se hace necesaria la implementación a tiempo de mecanismos de defensa, para controlar los ataques y los diferentes tipos de vulnerabilidades que afectan las redes de datos y la telefonía VoIP.

El contenido de las comunicaciones VoIP es vulnerable a los ataques, al hackeo, a las modificaciones, a las intercepciones y a los re enrutamientos. Peor aún, como las comunicaciones de voz y de datos se ejecutan en la misma infraestructura, un ataque al sistema VoIP podría hacer peligrar toda la disponibilidad de la red IP.

Adicionalmente no se cuenta con documentación que permita identificar las diferentes vulnerabilidades tanto administrativas como técnicas a las cuales está expuesta la operatividad.

1.2 FORMULACION DEL PROBLEMA

Las amenazas, los riesgos y vulnerabilidades inherentes a los servicios informáticos a los que están expuestas las organizaciones, incentivan a pensar cómo el nivel directivo de la Defensoría del Pueblo puede tomar decisiones y acciones que le permitan mitigar, transferir o aceptar éstos y los futuros.

Por lo anterior se plantea la aplicación de los conocimientos adquiridos para realizar un análisis y diagnóstico al sistema de gestión de seguridad de la información de la red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo, esto teniendo en cuenta que hoy en día, todos los funcionarios a nivel nacional usan un computador conectado a Internet; para comunicarse, intercambiando datos, correos electrónicos, o a través de mensajería instantánea, siendo claro que el concepto de Internet va de la mano con las telecomunicaciones y la utilización de las redes IP para la transmisión de voz, lo que hace que los contenidos de las comunicaciones VoIP sean vulnerables a ataques, como hackeo, las intercepciones, o redireccionamientos, entre otros, es por esto que es necesaria la implementación a tiempo, de mecanismos de defensa, para controlar los ataques que puedan afectar la red VOIP.

Se considera que el nivel directivo de la Defensoría del Pueblo, a través del documento de análisis y diagnóstico a los componentes del SGSI de la Red VOIP podrá conocer a qué tipo de amenazas están expuestos y tomar decisiones con el fin de salvaguardar la información como principal activo de la entidad.

¿Es necesario que el nivel directivo cuente con un documento de análisis y diagnóstico a los componentes del SGSI de la red VOIP del nivel central, para garantizar tanto al cliente interno como externo, la seguridad de la información transmitida?.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

El Proyecto consiste en realizar un análisis y diagnóstico al sistema de gestión de seguridad de la información de la red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo específicamente en lo relacionado con los componentes que aplican a la red VOIP, desde la implementación que tiene en infraestructura tecnológica y aplicativos de uso de la Entidad, demostrando las posibles deficiencias encontradas.

El análisis de resultados permitirá tomar decisiones desde el punto de vista tecnológico y administrativo aplicando la ISO 27001, en procura de garantizar un servicio con seguridad.

2.2 LIMITACIONES

El Análisis y diagnóstico al sistema de gestión de seguridad de la información de la red VOIP, se realizará a los componentes que apliquen a la red VOIP, las conclusiones, observaciones y recomendaciones se realizaran al grupo directivo quien tomará la decisión de implementarlas o no.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un documento de análisis y diagnóstico al sistema de gestión de seguridad de la información de la Red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo.

3.2 OBJETIVOS ESPECÍFICOS DEL PROYECTO

- Evaluar sistemas de información existentes. (Características de equipos, conexiones)
- Realizar un análisis de recursos de red voz y datos (equipamiento, flujo de datos, topología)
- Realizar análisis de seguridad a los componentes al SGSI que apliquen a la red VOIP.
- Realizar observaciones y recomendaciones de acuerdo con los hallazgos

4. JUSTIFICACION

Este proyecto se realiza con el fin de aplicar el conocimiento y las capacidades para enfrentar un problema y sus posibles soluciones y lograr la satisfacción de las necesidades y requerimientos, cumpliendo con calidad; ofreciendo un documento de análisis y diagnóstico a los componentes del SGSI que apliquen a la red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo, que garantice la confidencialidad, integridad y disponibilidad en el manejo de la información, según la normatividad vigente.

Se plantea realizar el documento de análisis y diagnóstico en el área de sistemas del nivel central de la Defensoría del Pueblo puesto que es allí en donde se realiza la implementación de medidas de seguridad dirigidas a gestión en la red, observando que es en este punto donde se presenta el mayor impacto en los riesgos identificados, y la mayor vulnerabilidad respecto de la información que allí se almacena, y sus posibles pérdidas económicas si le ocurre algo a la misma.

Se hace necesario concientizar a los directivos de la organización sobre los riesgos inherentes a la utilización del Internet y como viajan a través de la red ataques a la información de la empresa, además de saber cómo se pueden tomar decisiones y acciones de tipo administrativo que les permitan mitigar, transferir o aceptar los riesgos actuales y los futuros.

5. MARCO REFERENCIAL

Teniendo en cuenta el conocimiento adquirido, el cual debe ser aplicado para la realización del documento de análisis y diagnóstico a los componentes del SGSI que apliquen a la Red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo, se plantea subdividir el marco referencial en antecedentes, teórico, legal, e histórico.

5.1 ANTECEDENTES TEMÁTICOS DE LA INVESTIGACIÓN

Hacer un recorrido histórico de frente a los diversos avances tecnológicos que se han implementado para mejorar la calidad de vida y cuáles han sido las formas utilizadas por el ser humano para evitar inconvenientes relacionados con la seguridad de la información y protección de datos.

Cuando hablamos de seguridad de la información nos referimos a cómo proteger y salvaguardar la misma de todos los posibles riesgos o vulnerabilidades que están al asecho es por esto que debemos cumplir con los principios básicos de seguridad: confidencialidad, disponibilidad e integridad, fundamentos que desde el comienzo de la historia han enmarcado lo esencial de la protección de la información.

En la Antigua Grecia la creación de los primeros intentos criptográficos utilizaron el cifrado de transposición llamado escítala; después los romanos, con el emperador Julio Cesar utilizaron un lenguaje de cifrado para referirse a sus guerreros más importantes.

James Anderson militar de las fuerzas armadas norteamericanas a finales de los años 80, publica los primeros libros sobre la seguridad en los computadores, acerca de la detección de intrusos

El primer modelo denominado IDES (Intrusion Detection Expert System) se desarrolló diseñando reglas, los ingenieros Dening y Neumann en 1984 crearon sistemas de detección de intrusos separando claramente los sistemas que efectúan la detección dentro de los computadores y los que la efectúan la detección en el tráfico que circula por la red.

A través de la historia s se han detectado ataques informáticos:[1]

[1] RIES, Brian;. (2012). Hackers' Most Destructive Attacks, págs. http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html.

En junio de 1990: Kevin Poulsen Vs. KISS-FM: Poulsen era un adolescente hacker telefónico -un phreak- quien atacó las redes telefónicas para ganar un Porsche en un concurso de radio de Los Ángeles. Como si eso fuera poco, también intervino la línea telefónica de una famosa actriz de Hollywood y atacó los computadores de la Armada y el FBI.

En noviembre de 1998: Robert Tappan Morris contra el mundo: Tappan mientras estudiante de posgrado en la Universidad de Cornell, creó un gusano capaz de autoreplicarse para determinar el tamaño de Internet. Pero éste experimento escapó de su control, infectando computadores por mucho tiempo, con un costo en daños de millones de dólares. Tappan fue condenado a pagar con US$10.000 y 400 horas de trabajo comunitario.

En marzo de 1999: David L. Smith vs. Microsoft Word y Outlook: Smith le regaló a una stripper en La Florida un virus informático bautizado con su nombre. Para lo que usó una cuenta robada del servicio AOL, publicando un documento de Word infectado con el virus "Melissa" en uno de los grupos de discusión más concurridos de la red. El virus se generalizó muy rápido a través del correo electrónico infectando millones de computadores que utilizaban Outlook, ocasionando más de US$80 millones de dólares en daños.

En agosto de 1999: Jonathan James vs. Departamento de Defensa de Estados Unidos. James se convirtió en uno de los hackers más famosos de la historia al ingresar en los computadores de la Agencia de reducción de Amenazas interceptando mensajes confidenciales, contraseñas y el software principal que controlaba la agencia espacial internacional.

En febrero de 2002: Adrian Lamo Vs. The New York Times: Lamo fue el hacker responsable de la filtración de más de 400 mil cables diplomáticos de WikiLeaks. Y también se hizo famoso por la intrusión en los servidores de compañías como The New York Times, la cadena de tiendas Kinko's, Starbucks y Lexis-Nexis, provocando daños por aproximadamente 300 mil dólares.

En noviembre de 2008: Atacante desconocido vs. Microsoft (y el mundo): el gusano comenzó a utilizar y a atacar vulnerabilidades de los sistemas operativos de Microsoft. Cuando los computadores son controlados pueden ser usados para atacar como red masiva. Conficker puede servir como amenaza de nivel militar.

En enero de 2008: Los anónimos contra la cienciología: pareciera que los ataques anónimos no son siempre malintencionados, el grupo de Anonymous, efectuaron ataques de denegación de servicio a los servidores de Scientology.org, según ellos esta noble causa era salvar al mundo de la cienciología impidiendo que la secta religiosa por medio de amenazas y extorsiones lavara cerebros en el mundo.

En julio de 2009: Atacante desconocido vs. Estados Unidos y Corea del Sur: Durante tres días, los sitios web de un periódico de Corea del Sur, una cadena de subastas, un banco, la Casa Blanca, el Pentágono y las ejército de Corea; fueron víctimas de un ataque masivo de denegación de servicio (DDoS), realizada a través de la red de bots de más de 166 mil computadores controlados desde Corea del Norte por medio del gusano Mydoom.

En agosto de 2009: Rusia vs. El bloguero georgiano "Cyxymu": Debido a que millones los usuarios se dedican día a día a visitar los sitios de redes sociales. El gobierno Ruso inicio una denegación de servicio para intentar silenciar al bloguero Cyxymu quien informaba acerca de la difícil situación que se vivía en la república de Georgia.

Teniendo en cuenta estos antecedentes, se hace necesario conservar bajo cualquier circunstancia un sistema seguro que cumpla con los requisitos básicos de confiabilidad, integridad y disponibilidad, con el fin de que la información sea accedida única y exclusivamente por usuarios que tienen autorización.

En la actualidad existen miles de estadísticas, por ejemplo, la publicada en el año 2000 por el Instituto de Seguridad computacional y el FBI, donde se muestra que el 70% de los ataques informáticos ocurren dentro de la misma empresa ya que no se cuenta con políticas de seguridad interna.

Además se debe garantizar que la información será utilizada para uso exclusivo del cumplimiento de la misión de la Entidad, razón por la cual este estudio se enmarca dentro de la seguridad de la Red VOIP de la Defensoría del Pueblo ya que si su información en alguno de los procesos es alterada perdería validez y confianza ante los usuarios.

5.2 MARCO TEÓRICO

La normatividad vigente plantea la aplicación de la ISO- 27001[2] como base fundamental para la construcción del SGSI (Sistema de Gestión de Seguridad de la Información), se debe desarrollar un proceso documentado, sistemático y socializado en toda la entidad, enfocado al diagnóstico y análisis del sistema de gestión de seguridad de la información de los componentes que apliquen a la Red VOIP en el área de sistemas del nivel central de la Defensoría del Pueblo.

[2] KOSUTIC, Dejan. (2015). ISO 27001 & ISO 22301 Blog. Obtenido de ISO 27001 & ISO 22301 Blog: http://www.iso27001standard.com/es/blog/

Se debe tener en cuenta que garantizar un nivel de protección total es imposible, así se cuente con el recurso económico necesario, por lo cual se debe garantizar que los riesgos de la seguridad de la información en la Red VOIP sean conocidos, asumidos, gestionados y minimizados por los funcionarios de la entidad.

El levantamiento de la información debe ser de manera documentada, sistemática, y adaptada a los cambios que se produzcan en los riesgos.

5.3 MARCO LEGAL

Los conceptos fundamentales, específicamente en lo que tiene que ver con el sistema de gestión de seguridad de la información a los componentes de la Red VOIP, según la norma ISO 27001 y para Colombia la Ley 1273/2009, están basados en la preservación de su confidencialidad, integridad y disponibilidad:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

5.3.1 NORMATIVIDAD INTERNACIONAL

Estándar ISO 27001[3]

Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013, su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005

Estándar oficial. Título completo es BS 7799-2:2005 (ISO/IEC 27001:2005)[4]. El conjunto de estándares que aportan información de la familia ISO-2700x son:

[3] KOSUTIC, Dejan. (2015). ISO 27001 & ISO 22301 Blog. Obtenido de ISO 27001 & ISO 22301 Blog: http://www.iso27001standard.com/es/blog/

[4] ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

ISO/IEC 27002[5] - Mejores prácticas en la gestión de seguridad de la información.

Brinda recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define como:

a. Confidencialidad: asegurando que sólo quienes estén autorizados pueden acceder a la información.
b. Integridad: asegurando que la información y sus métodos de proceso son exactos y completos.
c. Disponibilidad: asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

- **ISO/IEC 27003**[6] ISMS Guía para la Implementación

- **ISO/IEC 27004**[7]: Medición de la Seguridad de la Información

- **ISO/IEC 27005**[8]**:** Gestión de riesgos de la Seguridad la Información

Estándar ISO/IEC 27032[9] :(nuevo estándar de ciberseguridad)

Garantiza directrices de seguridad proporcionando colaboración general entre las partes interesadas para reducir riesgos en Internet; provee un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos.

La norma facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo, ayudando a prepararse, detectar, monitorizar y responder a los ataques, permitiendo identificar, hackers, malware, spyware y otros tipos de software no deseado.

[5] ISO / IEC 27002 (2013) Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información

[6] ISO/ IEC 27003 (2010) ISO / IEC 27003 Obtenido de http://www.iso27001security.com/html/27003.html

7 ISO / IEC 2700 (2009) Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información – Medición. Obtenido de http://www.iso27001security.com/html/27004.html

8 ISO / IEC 27005 (2011) Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. Obtenido de http://www.iso27001security.com/html/27005.html

[9] ISO / IEC 27032 (2012) Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad. Obtenido de http://www.iso27001security.com/html/27032.html

Estándar ISO/IEC 18028-2:2006[10]

ISO/IEC 18028-2:2006 define una arquitectura de seguridad para red, ofreciendo seguridad a redes de extremo a extremo. La arquitectura es aplicada a varias clases de redes. El objetivo es servir como base para el desarrollo de recomendaciones detalladas para la seguridad en redes extremo a extremo.

COMMON CRITERIA: El Criterio Común para la Evaluación de la Seguridad en Tecnologías de la Información (abreviado como Criterio Común o CC), es un estándar internacional (ISO/IEC 5408), para la certificación de la seguridad en computadores. Actualmente en versión 3.1.

Estándar ISO/IEC 21827:2008: [11]

Es un estándar internacional basado en el Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas, desarrollado por la Asociación Internacional de Ingeniería de Seguridad de la Información (ISSEA).

ISO/IEC 21827 especifica el SSE-CMM que describe las características esenciales para el éxito del proceso de ingeniería de la seguridad de una organización, y es aplicable a todas las organizaciones de ingeniería de la seguridad, incluyendo gubernamentales, comerciales y académicas. ISO/IEC 21827 no prescribe una secuencia o proceso particular, pero si captura las prácticas que se observan en la industria. El modelo es una métrica estándar para las prácticas de la ingeniería de seguridad, que cubre lo siguiente:

- Ciclos de vida del proyecto, incluyendo actividades de desarrollo, operación, mantenimiento y desmantelamiento.

- Cubre todos los ámbitos de la organización, incluyendo actividades de gestión, organizacionales y de ingeniería.

- Interacciones concurrentes con otras disciplinas, como software y hardware de sistemas, recurso humano, pruebas de ingeniería, gestión de sistemas, operación y mantenimiento.

[10] ISO/IEC 18028 (2006) Norma de seguridad de redes. Obtenido de http://comunidad.dragonjar.org/f164/iso-iec-18028-norma-de-seguridad-de-redes-12231/

[11] RODRIGUEZ, Ana Maria. (2014). ANALISIS Y DIAGNOSTICO DE LA SEGURIDAD INFORMATICA DE. Obtenido de http://repository.unad.edu.co/bitstream/10596/2692/5/53070244.pdf

5.3.2 LEY NACIONAL

LEY 1273 DEL 2009[12]

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Dicha ley decreta:

CAPITULO I:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

-Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.

- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

- Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes

[12] MINTIC. (2009). LEY 1273. Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.
Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

Por servidor público en ejercicio de sus funciones

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro. Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional. Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II:

De los atentados informáticos y otras infracciones

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un terceros.

5.4 MARCO HISTÓRICO

En el pasado toda la información era almacenada en papel, por lo que la seguridad era puramente física, hoy en día existen variados dispositivos, así como mecanismos abusivos de acceder a la misma. Actualmente la forma de los ataques cambio; anteriormente los hackers buscaban solo producir daños en los sistemas por el simple hecho de darse un poco de fama, actualmente buscan obtener información y dinero aprovechando los recursos disponibles

5.5 MARCO CONTEXTUAL INSTITUCIONAL

La Defensoría del Pueblo de Colombia es un órgano constitucional y autónomo creado por la Constitución de Colombia de 1991 en su Capítulo II: Del ministerio público, con el propósito de "velar por la promoción, el ejercicio y la divulgación de los derechos humanos" dentro del Estado social de derecho, "democrático, participativo y pluralista", así como la divulgación y promoción del Derecho Internacional Humanitario.[13] (DEFENSORIA, 2013)

La Defensoría del Pueblo es uno de los órganos de control del Estado colombiano y está vinculada al Ministerio público; por lo tanto el Defensor del Pueblo ejerce sus funciones bajo la dirección del Procurador General de la Nación.

La organización y funcionamiento de la Defensoría del Pueblo en Colombia está regulada por la Ley 24 de 1992 y demás normas que la adicionan o modifican.

Misión

La Defensoría del Pueblo es la institución del Estado Colombiano responsable de impulsar la efectividad de los derechos humanos de los habitantes del territorio nacional y de los colombianos en el exterior, en el marco del Estado Social de Derecho democrático, participativo y pluralista, mediante las siguientes acciones integradas:

- Promover, ejercer y divulgar los derechos humanos.
- Proteger y defender los derechos humanos y prevenir sus violaciones.
- Fomentar la observancia del derecho internacional humanitario.
- Atender, orientar y asesorar en el ejercicio de sus derechos.
- Proveer el acceso a la administración de justicia, en los casos señalados en la Ley.

[13] DEFENSORIA. (2013). RESOLUCION 1014. Obtenido de http://www.defensoria.gov.co/

Visión

En el 2016, la Defensoría del Pueblo es identificada tanto a nivel nacional como internacional, por su incidencia en la garantía y protección de los derechos humanos y el fomento de la observancia del derecho internacional humanitario, atendiendo de manera prioritaria y reforzada a los sujetos de especial protección, y manteniendo la comunicación directa y transparente con la comunidad, para aumentar su confianza y credibilidad.

Ilustración 1 Organigrama Estructura Defensoría del Pueblo

Fuente: Oficina de Planeación – Defensoría del Pueblo

6. HERRAMIENTAS DE ANALISIS Y DE VULNERABILIDAD.

Hoy en día existen herramientas que han ayudado a identificar vulnerabilidades de seguridad informática:

Nessus: [14] Es la herramienta de evaluación de seguridad "Open Source" que más se utiliza. Es un escáner de seguridad remoto para Linux, BSD, Solaris y Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Se generan reportes en HTML, XML, LaTeX, y texto ASCII.

Ethereal: [15] Sniffer analizador de protocolos de red para Unix y Windows, es un software libre, que permite examinar datos en una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluye un completo lenguaje para filtrar y tiene la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

TCPDump / WinDump: [16] El sniffer clásico para monitoreo de redes y adquisición de información. Analizador de paquetes de red basado en texto. Es utilizado para mostrar los encabezados de los paquetes en una interfaz de red que concuerden con alguna expresión de búsqueda. Se puede utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma.

Snort: [17] Un sistema de detección de intrusiones (IDS) libre, capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Realiza análisis de protocolos, búsqueda e identificación de contenido, es utilizado para detectar una gran variedad de ataques y pruebas, utiliza lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular.

Hping2: [18] Ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho

[14] PULGARIN, Diego. (2012). Manual Basico de Nessus en Windows. Bogota. Obtenido de http://diegopulgarinsena.blogspot.com/2012/04/instalacion-de-nessus-en-windows.html

[15] Gerald, C. (2006). Ethereal. Obtenido de http://ethereal.uptodown.com/

[16] ALFON. (2008). Obtenido de https://seguridadyredes.wordpress.com/2008/01/11/analizando-la-red-con-windump-tcpdump-i-parte/

[17] ALFON. (2008). Obtenido de https://seguridadyredes.wordpress.com/2008/01/22/sistemas-de-deteccion-de-intrusos-y-snort-ii-creacion-de-reglas-i/

[18] GATES, Chris. (2006). Tutorial: Hping2 Basics. Obtenido de https://www.ethicalhacker.net/columns/gates/tutorial-hping2-basics

más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP. Es una herramienta útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

DSniff::[19] Herramienta de auditoría y pruebas de penetración de redes. Este popular y bien diseñado set hecho por Dug Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante.

Ettercap: [20] Es un interceptor sniffer registrador para LANs con ethernet basado en terminales. Soporta disecciones activas y pasivas de varios protocolos cifrados, como SSH y HTTPS. También soporta plugins. Tiene la habilidad para comprobar si es una red LAN con switches o no, y de identificar huellas de sistemas operativos (OS fingerprints) para conocer la geometría de la LAN.

NBTscan[21] es un programa que escanea redes IP en busca de información de nombres de NetBIOS. Envía pedidos de "status" de NetBIOS a cada dirección en un rango provisto por el usuario y lista la información recibida de manera legible. Por cada host que responde, se lista su dirección, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina ("logged in"), y dirección de MAC.

Firewalk: [22] traceroute avanzado. Firewalk emplea técnicas similares a las de traceroute para analizar las respuestas a paquetes de IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways.

NTop:[23] Monitor de uso de tráfico de red. Ntop muestra el uso de la red en una manera similar a lo que hace top por los procesos. Muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una

[19] SONG, Dug. (2001). dsniff Frequently Asked Questions. Obtenido de http://www.monkey.org/~dugsong/dsniff/faq.html#What is dsniff

[20] ORNAGHI, Alberto. (2009). ettercap(8) - Linux man page. Obtenido de http://linux.die.net/man/8/ettercap

[21] CHIRILA, Alexandru. (2014). nbtscan. Obtenido de http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/nbtscan.shtml

[22] IRBY, David. (2005). Firewalk : Can Attackers See Through. Obtenido de http://www.giac.org/paper/gsec/312/firewalk-attackers-firewall/100588

[23] NTOP. (2015). Obtenido de http://www.ntop.org/

interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

Hunt: [24] Un "packet sniffer" y un intruso en conexiones ("connection intrusion") avanzado para Linux. Hunt puede observar varias conexiones de TCP, entrometerse en ellas, o resetearlas, fue hecho para ser usado sobre ethernet, y tiene mecanismos activos para olfatear (sniff) conexiones en redes con switches. Sus características avanzadas incluyen "ARP relaying" selectivo y sincronización de conexión luego de ataques.

SPIKE Proxy: [25] Cracking de HTTP. Spike Proxy es un proxy de HTTP "open source", sirve para encontrar fallas de seguridad en sitios web. Es parte del Spike Application Testing Suite, soporta detección de inyección de SQL automatizada, crawling de sitios web, uso de fuerza bruta en formularios de entrada, detección de overflow, y detección de acceso a directorios que debieran estar fuera de los límites del sitio de web ("directory traversal").

THC-Hydra: [26] Cracker de autenticación de red paralelizado. Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada (login) por red, incluyendo FTP, POP3, IMAP, Netbios, Telnet, HTTP Auth, LDAP, NNTP, VNC, ICQ, Socks5, PCNFS, y más. Incluye soporte para SSL y aparentemente es ahora parte de Nessus.

Bactrack: [27] Herramienta diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Wireskark: [28] Analizador de protocolos TCP/IP por medio del cual es posible escuchar conversaciones que se den lugar en la red local, usando el protocolo SIP(Session Initiation Protocol), protocolo de señalización, similar a HTML y SMTP, encargado de la localización usuarios, parámetros, modificaciones e iniciar o finalizar una sesión. Los datos de audio serán transportados mediante el protocolo de transporte RTP (Real Time Transport Protocol) usando UDP**.**

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y

[24] KRAUZ, Pavel. (2000). PACKET STORM. Obtenido de http://packetstormsecurity.com/sniffers/hunt/

[25] AITEL, Dave. (2012). SPIKE Proxy 1.0 Released. Obtenido de http://seclists.org/pen-test/2002/Jul/60

[26] HAUSER, Van. (2015). Obtenido de http://tools.kali.org/password-attacks/hydra

[27] LINUX. (2013). BackTrack Linux – Penetration Testing Distribution. Obtenido de http://www.backtrack-linux.org/

[28] COMBS, Gerald. (2008). Obtenido de https://www.wireshark.org/about.html

sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que se quiera ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Aspectos importantes de Wireshark

- Mantenido bajo la licencia GPL.
- Robusto, tanto en modo promiscuo como en modo no promiscuo.
- Capturar datos de la red o leer datos almacenados en un archivo previo.
- Basado en la librería pcap.
- Capacidad de filtrado.
- Reconstrucción de sesiones TCP
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.
- Puede traducir protocolos TCP IP
- Genera TSM y SUX momentáneamente

Kali Linux - Backtrack 6[29] Es la renovación de la famosa distribución de seguridad Backtrack, características:

- Más de 300 herramientas de pruebas de penetración
- Gratis
- Git – árbol de código abierto:
- Obediente a FHS: Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros.
- Paquetes firmados con PGP y repos: Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos.

[29] LINUX. (2014). Kali Linux NetHunter. Obtenido de https://www.kali.org/kali-linux-nethunter/

7. ANÁLISIS DE LA INFORMACIÓN

7.1 RECOLECCION DE LA INFORMACIÓN

El área de sistemas del nivel central de la Defensoría del Pueblo, cuenta con una infraestructura modular de un solo nivel, donde se ubican todas y cada de las dependencias intervinientes en el cumplimiento de la misión. En lo referente a la Red VOIP se recolectó información del contrato realizado con la Unión Europea en donde las especificaciones técnicas hacen parte de una de las cláusulas de cumplimiento.

7.1.1 Estructura Física:

HARDWARE

- Un Servidor AVAYA S8300D
- Dos GATEWAY G430
- Tres tarjetas MM710B para enlaces
- Una tarjeta MM714
- Trece Switches AVAYA
- 25 Teléfonos 1603 y 962

7.1.2 Diseño de la Solución de Telefonía VOIP

- **CORE**
  - 24 puertos 1 Gbps en fibra
  - Stckable
  - 1 rack

- **ACCESO**
  - 6 Switches de 48 puertos 10/100/1000 base –t con 2 combos SFP multimodo
  - POE (Power On Energy) 8 hilos (2 energía y 6 datos) en cada puerto
  - Por stack 4 puertos
  - 1 rack unit
  - Realiza interconexión con el ISPBX DEFINITY 4 GUEST WORK en la sede central de la Defensoría del Pueblo (en razón a que la placa Lucent vieja no se puede expandir, debido al incremento de personal).

7.1.3 Especificaciones Técnicas

7.1.3.1 Sistema de Comunicaciones

- El sistema propuesto soporta el manejo de telefonía IP y es utilizado a través de la Red y forma parte de una arquitectura de voz y datos
- El sistema es capaz de escalar a 1000 usuarios cada uno por medio de una licencia
- Se cuenta con un servidor en el cual reside el software de comunicaciones, está conformado por:
    - Un disco duro de 80 GB
    - 4 GB de DRAM con un DIMM de 1 GB
    - Un puerto de administración de consola
    - Sistema Operativo Linux
    - Interfaz vía web
    - Realiza Backups
    - Configuración de alarmas
    - Permite extender servicios complementarios y mejorados como retención, transferencia reenvío, conferencia, selección automática de ruta, marcación rápida, llamada al último numero
    - Distribuye todos los teléfonos , Gateways y aplicaciones por una red IP
    - Selección automática de ruta ante la ocupación de los enlaces de la red WAN
    - Control, administración y registro de llamadas
    - Tratamiento y análisis de la llamada (inserción, borrado y extracción de cadena de dígitos y códigos de acceso de llamada)
    - Sistema centralizado y/o distribuido de llamadas
    - FAX a través de IP G.711 PASS – THROUGH
    - Envío de faxes a través del protocolo T.38
    - Interfaz H.323 a dispositivos seleccionados
    - Bloqueo de llamadas salientes.
    - Enrutamiento de backups en caso de fallas de la PSTN
    - Manejo de conferencias de tres hasta seis participantes
    - Seguridad: El servidor de comunicaciones permite usar la característica denominada AVAYA Media Encryption para encriptar los paquetes que conforman la llamada de VOIP antes de atravesar la RED IP.
    - Captura de llamadas desde otros teléfonos
    - Códigos de autorización de llamadas a larga distancia y celulares.
    - Operadora automática

7.1.3.2 Gateway y Troncales Análogas y Digitales

- El Gateway recibe la conexión a la PSTN del bloque A troncal E1.
- Manejo simultaneo de interfaces de voz digital E1
- Manejo de calidad de servicio QoS y codecs de compresión.
- Soporte de interfaces físicas como módulos seriales síncronos, asíncronos, de alta velocidad, Ethernet, FastEthernet y E1, PRI, BRI.
- Tecnología LAN/WAN (Ethernet, Fast Ethernet, Telefonía sobre IP)
- Puerto de consola.
- Protocolo de administración SNMP.

7.1.3.3 Terminales IP Tipo Ejecutivo/Gerencial

- Visualizador: Pantalla de 5 pulgadas (12,5 cm), pantalla gráfica a color TFT de 16-bit profundidad de color, 320 x 240 píxeles de resolución efectiva, con luz de fondo.
- Audio de banda ancha: Apoyo a la banda ancha (códec G.722, la adhesión a la TIA 920).
- Soporte de códec: G.711a, G.711µ, G.729a, G.729ab, G.722, e iLBC códecs de compresión de audio son compatibles.
- Altavoz: Altavoz full-duplex con cancelación de eco acústico.
- Mensajes clave: Proporciona acceso directo al buzón de voz.
- Directorios número: Acceso fácil a las llamadas perdidas, recibidas o llamadas realizadas (además de la historia de intercomunicación y directorios).
- La clave de opciones: Permite al usuario ajustar el brillo de la pantalla, imágenes de fondo, seleccione (si está disponible), y el timbre de seleccionar los sonidos a través del menú de la preferencia del usuario.
- Entre los servicios clave permite a los usuarios acceder rápidamente a información diversa, como la meteorología, las existencias, la cita del día, o cualquier información basada en la Web con XML.
- Botón de Ayuda: Ayuda en línea ofrece a los usuarios información sobre las teclas del teléfono, los botones y funciones.
- Altavoz, Mute, y botones de auriculares: Altavoz incluye Speaker On / Off, de silencio del micrófono, auriculares y los botones que se encienden cuando se activa. Para mayor seguridad, lo audible multifrecuencia de tono dual (DTMF) son enmascarados cuando se utiliza el modo de altavoz.
- De navegación Cluster con Botón de selección: Clúster de cuatro de navegación permite a los usuarios a desplazarse vertical y horizontalmente. En el centro de la agrupación es un «botón de selección que puede ser utilizado

para la selección de un enfoque en el tema (por ejemplo, para abrir un menú subyacente).

- Botón de visualización: Indica que cuando el teléfono está en el ahorro de energía de sueño / modo de inactividad (el botón está iluminado), y puede ser utilizado para despertar a la pantalla. Periodo de inactividad es configurado por el administrador del sistema.
- Ethernet Switch Interior 2-puertos switch Ethernet Cisco permite una conexión directa a una base de red Ethernet 10/100/1000-T a través de una interfaz RJ-45 con conexión inalámbrica a internet solo por teléfono y un PC. Administrador del sistema puede designar VLAN separada (802.1Q) para el PC y el teléfono, proporcionando una mayor seguridad y fiabilidad de tráfico de voz y datos.
- Puerto de auriculares: Puerto de auriculares dedicado elimina la necesidad de un amplificador de auriculares independiente y permite que el teléfono para permanecer en su cuna, haciendo uso de auriculares simples. Tanto de banda ancha (G.722) y auriculares de banda estrecha son compatibles.
- Control de volumen: Proporciona fácil de decibelios los ajustes de nivel para el altavoz, auricular, auricular y del timbre. El auricular es compatible con audífonos. Adicional hacerse con el control de volumen se puede conseguir con un amplificador de teléfono en línea.
- Ajustable pie-soporte: El soporte es ajustable de plano a 60 grados para proporcionar visión de la pantalla óptima y un uso cómodo de todos los botones y teclas. El pie-pie es clave para igualar la pared-jack estándar de configuraciones de montaje en pared. En pared opcional de montaje en soportes también se ofrecen.
- Múltiples tonos de timbre: Más de 24 definidas por el usuario, tonos de llamada seleccionables están disponibles. Los tonos de timbre también puede ser personaliza mediante el uso del Teléfono Unificado de Cisco Application Suite.
- Calidad de Servicio (QoS): Apoya el punto de código de servicios diferenciados (DSCP) y 802.1Q / p normas.
- Seguridad: De identidad dispositivo positivos a través de certificados X.509v3, firmado digitalmente las imágenes, criptográficamente segura de aprovisionamiento, y seguro de señalización y los medios de comunicación segura con AES-128.
- Soporte de idiomas: Soporte integrado por más de 30 idiomas
- Opciones de configuración: Asignación de dirección IP puede ser configurada de forma estática o configurada a través del cliente DHCP.

7.1.3.4 Servidor Avaya S8300

Ilustración 2 Servidor AVAYA

Fuente: Sistemas .Defensoría del Pueblo

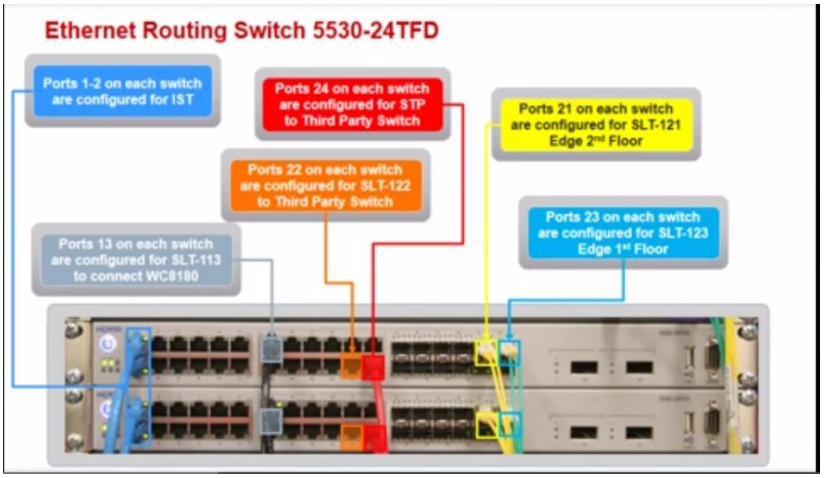
Avaya S8300 Server El S8300 Server es un procesador basado en Intel Celeron que ejecuta el sistema operativo Linux. Es residente en uno de los siguientes gateways de medios: G250, G350, G430, G450 ó G700.

El S8300 Server (versión B) es un procesador basado en Intel Celeron que ejecuta el sistema operativo Linux. Reside en la ranura V1 del G700 Media Gateway e incluye:

- Un disco duro de 30 GB
- 512 MB de RAM
- Dos puertos USB y un puerto 10/100 Base-T - Un puerto USB soporta un CD-ROM de lectura, que se usa para actualizaciones del sistema
- Un puerto de servicios Ethernet S8300 versión C El S8300C Server es compatible con Avaya Communication Manager versión 4.0 y posteriores.

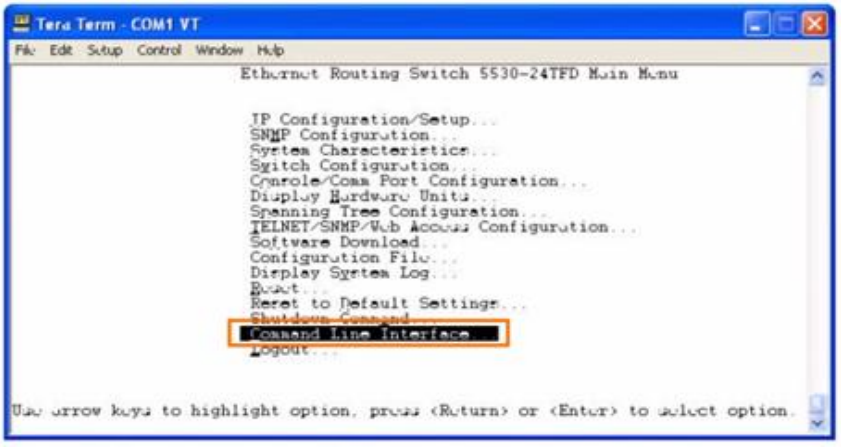
7.1.3.5 Configuración Swich AVAYA 5530[30]

Ilustración 3 Configuración Switch



Fuente: AVAYA

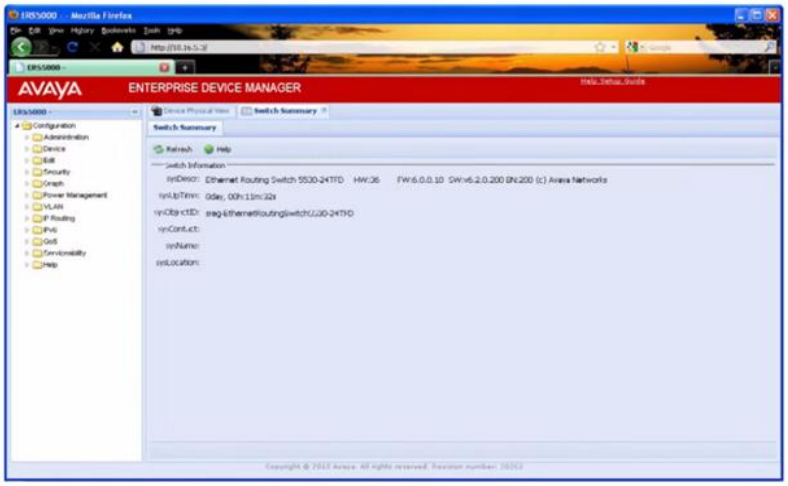
Ilustración 4 Comando Interfase



Fuente: AVAYA

[30] AVAYA. (2013). ERS Switch Complete Training Guide. Obtenido de https://www.youtube.com/watch?v=s3ww6jGXV04

Ilustración 5 Manejador Dispositivo



Fuente: AVAYA

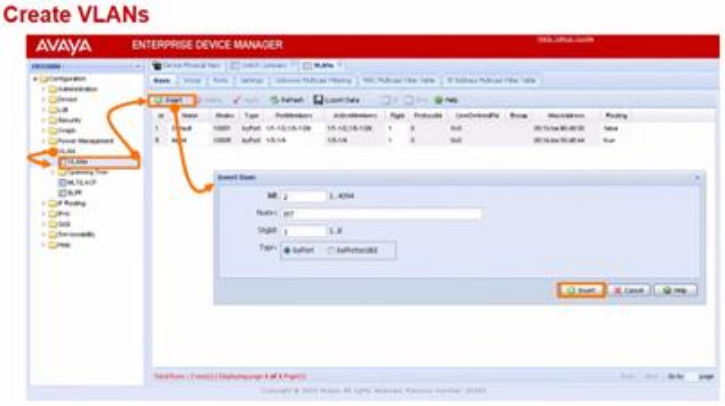
Ilustración 6 Configuración Vlan

Fuente: AVAYA

Ilustración 7 Seleccionador de puertos

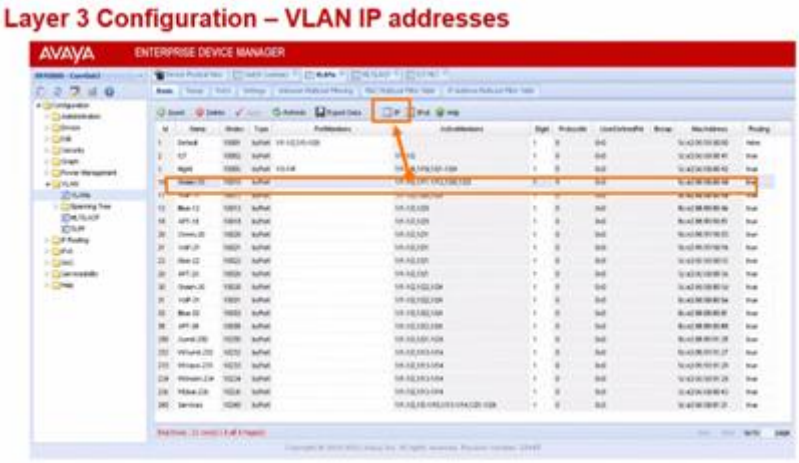
Fuente: AVAYA

Ilustración 8 Creando Vlans



Fuente: AVAYA

Ilustración 9 Configuración dirección IP Vlan



Fuente: AVAYA

7.1.3.6 Configuración Gateway[31]

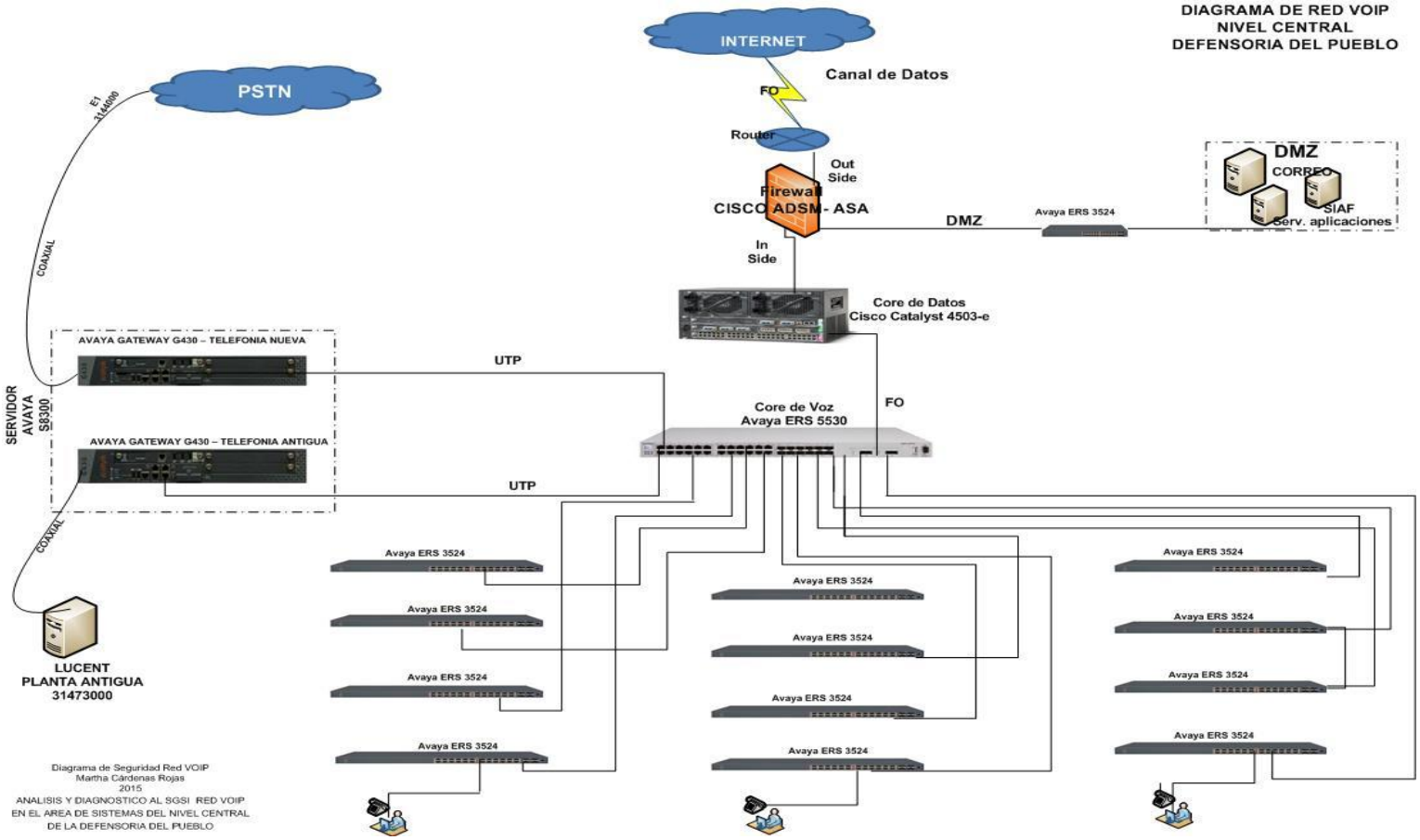
Ilustración 10 Gateway G430

Fuente: Sistemas

[31] AVAYA. (2011). Obtenido de Avaya Aura Communication Manager: https://downloads.avaya.com/css/P8/documents/100066807

8. DIAGRAMA DE RED VOIP AREA DE SISTEMAS DEL NIVEL CENTRAL DEFENSORIA DEL PUEBLO

Ilustración 11. Red VOIP área de sistemas de la Defensoría del Pueblo



Fuente: Autoría propia

9. ACERCA DE LA SEGURIDAD

Avaya trata el tema de seguridad a través del servidor de comunicaciones que permite usar la característica denominada Media Encryption para encriptar los paquetes que conforman la llamada de VOIP antes de atravesar la RED IP[32].

La mayoría de los proveedores de telefonía IP y VoIP utilizan protocolo de tiempo real de la IETF en combinación con codecs conocidos como G.711 y G.729 para la transmisión de la voz, como un canal portador sobre una red IP.

Avaya desarrolló una solución de privacidad basada en la UIT H.235 (Seguridad y cifrado para H.323 de la serie H y otras terminales multimedia basados en H.245) estándar.

De igual forma Avaya investigó y desarrolló el algoritmo de cifrado conocido como el algoritmo de cifrado de Avaya (AEA), adoptando lo establecido por el Instituto Nacional de Estándares y Tecnología (NIST).

El FIPS 197 algoritmo de cifrado AES, Advanced Encryption Standard, utiliza criptografía simétrica, ha pasado por un intensivo proceso de revisión pública antes de ser seleccionado como el reemplazo para el cifrado de datos Standard (DES).

La selección de un algoritmo de cifrado subyacente tiene que enfrentarse a los muy exigentes requerimientos de flujos de medios en tiempo real, que incluyen la escalabilidad, la capacidad de procesamiento de punto final y la alta tolerancia a la pérdida de paquetes y de reordenamiento.

La sobrecarga de procesamiento de cifrado debe minimizar los ciclos de la CPU y el resultado en una latencia mínima. En términos no técnicos, esto significa que las diferencias en la calidad de voz resultante del proceso de cifrado / descifrado debe ser imperceptible para el usuario final.

Aplicación pionera de Avaya de cifrado Media ofrece los siguientes beneficios:

1. La capacidad de admitir el cifrado de medios de extremo a extremo en toda la telefonía IP de Avaya.

2. La flexibilidad para determinar cuándo utilizar AEA vs. AES. Avaya desarrolló AEA algoritmo de cifrado de 104 bits ofrece el algoritmo de encriptación RC-4 basada en la secuencia de los medios de comunicación.

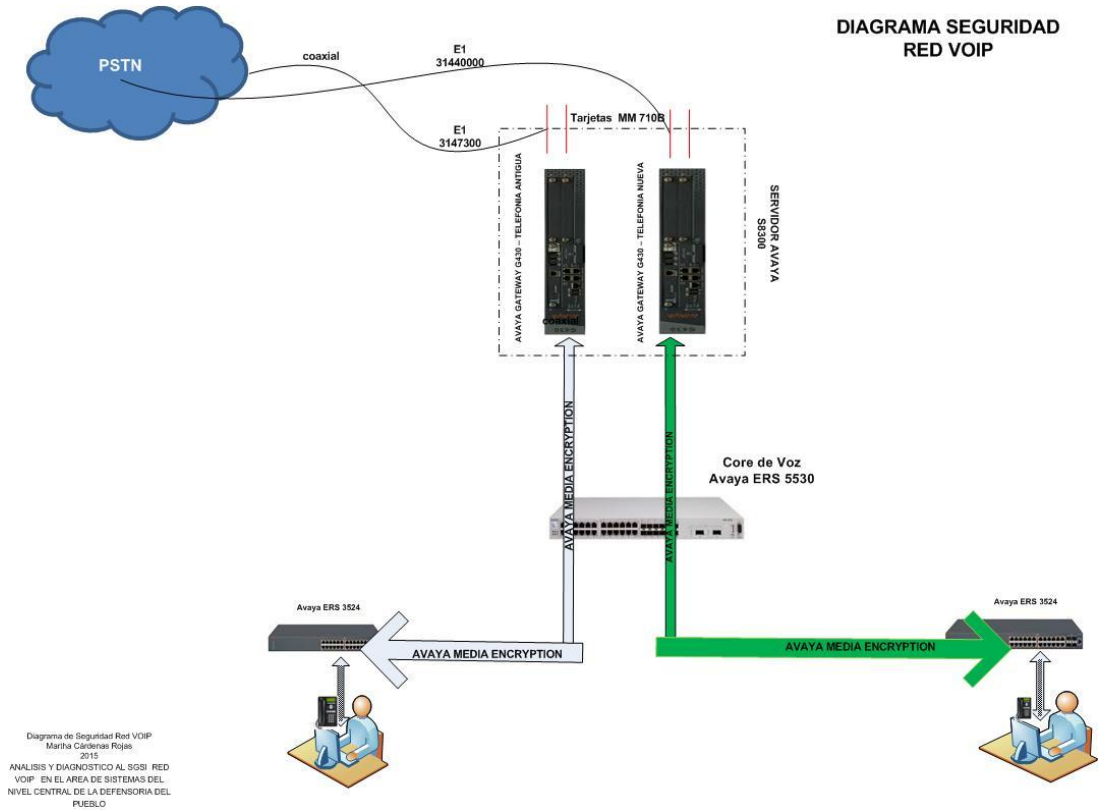
[32] AVAYA. (2004). Configuring Avaya Communication Manager for Media. En JRR, Solution & Interoperability Test Lab Application Notes

Avaya implementó el NIST FIPS 197 Advanced Encryption Algoritmo (AES) que utiliza 128 bit clave de cifrado. La implementación de arquitectura de cifrado de medios Avaya permite la adición de algoritmos de cifrado y modos de cifrado (suites).

AES implementa el RFC 3711, Secure Real-Time, protocolo mediante la adición de una cabecera de autenticación.

Para mantener la interoperabilidad de los sistemas con productos de terceros, cifrado de medios Avaya tiene algoritmos de opciones y cifrado configurables que se pueden pedir por preferencia de uso.

Ilustración 12 Diagrama de seguridad red VOIP



Fuente: Autoría propia

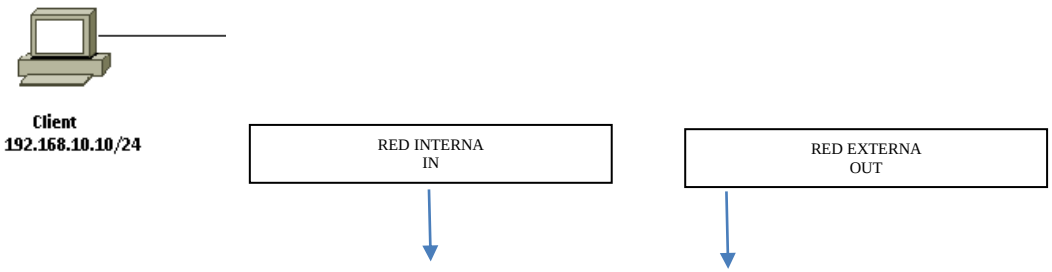
AVAYA garantiza proteger la operatividad y los datos de la red contra ataques y detener la suplantación, intercepción de llamadas, fraudes telefónicos, espionaje telefónico, robo de información y demás.

Con respecto a la RED VOIP del área de sistemas de la Defensoría del Pueblo, se realizó la integración entre AVAYA y Cisco.

A través de CISCO ASDM- ASA se mejora la protección de protocolos de aplicaciones como web, correo electrónico, voz sobre Protocolo Internet (VoIP), mensajería instantánea, transferencia de archivos y protocolos de red Microsoft.

El analizador de vulnerabilidades de CISCO ASDM para ASA, permite el proceso de la captura de paquetes de datos y se usa para resolver problemas de conectividad, además monitoriza cualquier actividad sospechosa; creando capturas múltiples para analizar diversos tipos de tráfico en las interfaces múltiples[33].

Ilustración 13 Red CISCO ASDM para ASA



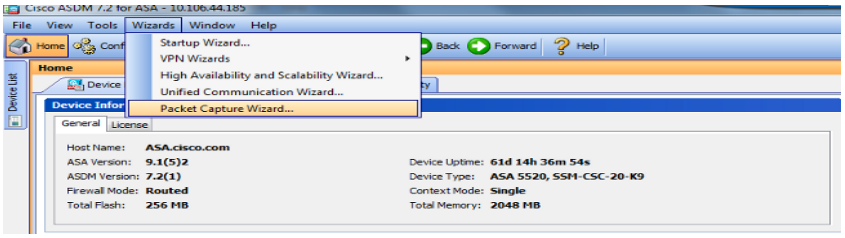
Fuente: CISCO- complemento autoría- propia

9.1 Analizador de vulnerabilidades

A través del analizador de vulnerabilidades se logran identificar ataques tanto a datos, como a VOIP, es por esta razón que se revisa la configuración del CISCO ASA para la captura de paquetes.

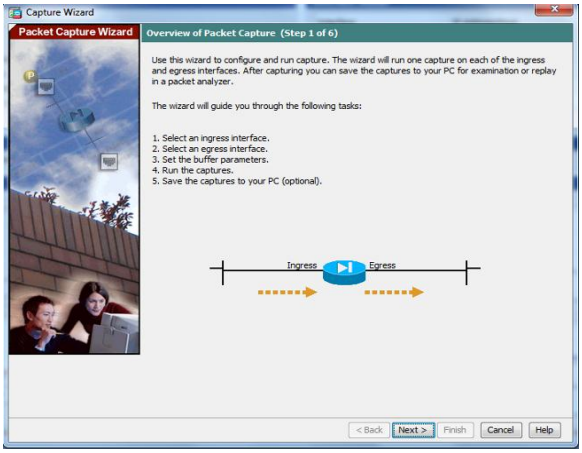
Ilustración 14 Configuración de Captura

[33] CISCO. (2014). PIX/ASA: Actualice una imagen del software usando el ASDM o el ejemplo de la configuración CLI. Obtenido de http://www.cisco.com/cisco/web/support/LA/103/1030/1030085_upgrade-pix-asa7x-asdm.html



Fuente: CISCO

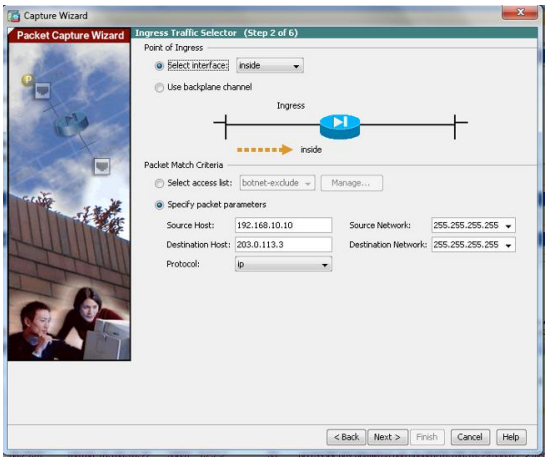
Ilustración 15 Asistente de la captura.



Fuente: CISCO

Se proporcionan los parámetros que se utilizan para capturar el tráfico de ingreso. Selecciona el interior para la interfaz de ingreso, la fuente y los IP Address de destino de los paquetes que se capturarán, junto con su máscara de subred.

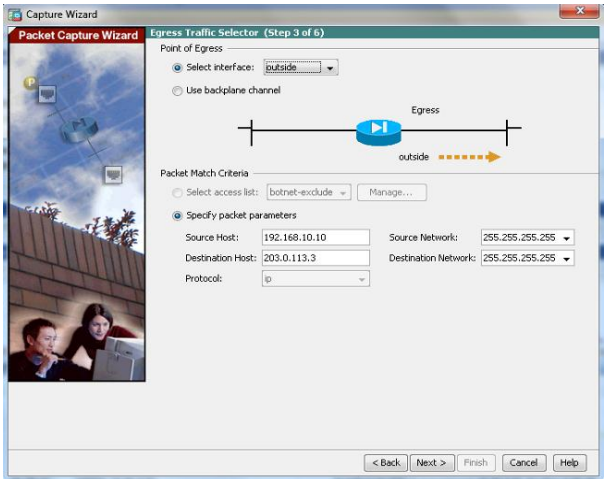
Ilustración 16 Parámetros de captura



Fuente: CISCO

Selecciona el exterior para la interfaz de egreso y proporciona la fuente y los IP Address de destino, junto con su máscara de subred, en los espacios.

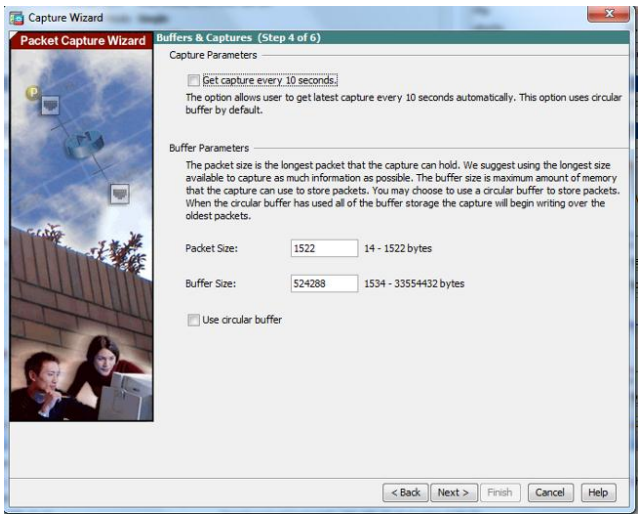
Ilustración 17 Direccionamiento



Fuente: CISCO

En este pantallazo se observa cómo se ingresan los tamaños de paquetes apropiados y los tamaños de Buffer en el espacio respectivo proporcionado.

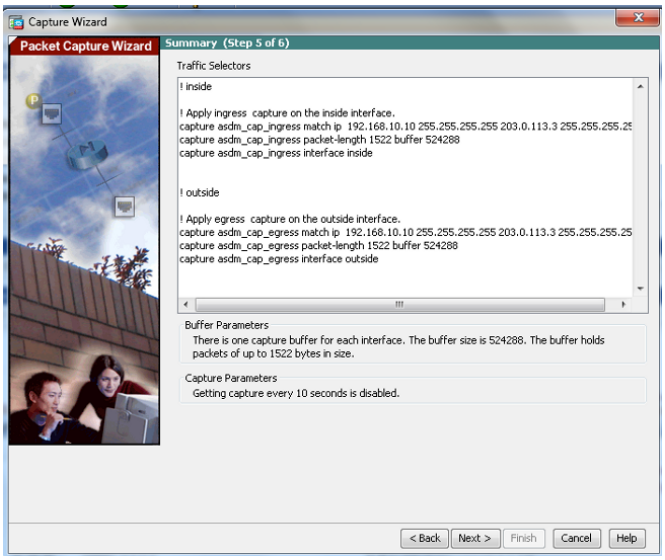
Ilustración 18 Definición de tamaño de Buffer



Fuente: CISCO

Listas de acceso que se deben configurar en el ASA para capturar los paquetes deseados, y muestra el tipo de paquetes que se capturarán (los paquetes IP se capturan en este ejemplo).

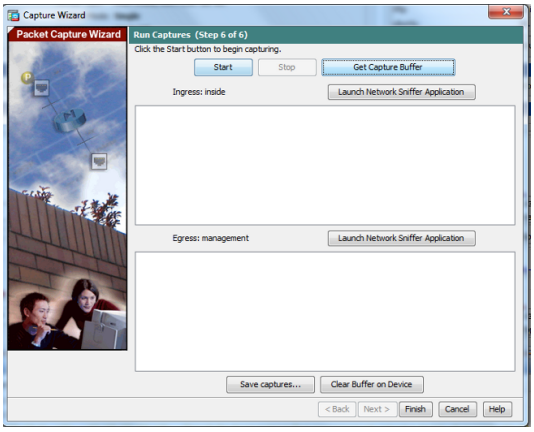
Ilustración 19 Listas de acceso



Fuente: CISCO

Comienzo del tecleo para comenzar a la captura de paquetes:

Ilustración 20 inicio de captura



Fuente: CISCO

Al comenzar la captura de paquetes, hacer ping de la red externa a la red interna de modo que los paquetes que fluyen entre la fuente y los IP Address de destino sean capturados por el buffer de la captura ASA.

9.2 Configuración CISCO ASDM para ASA

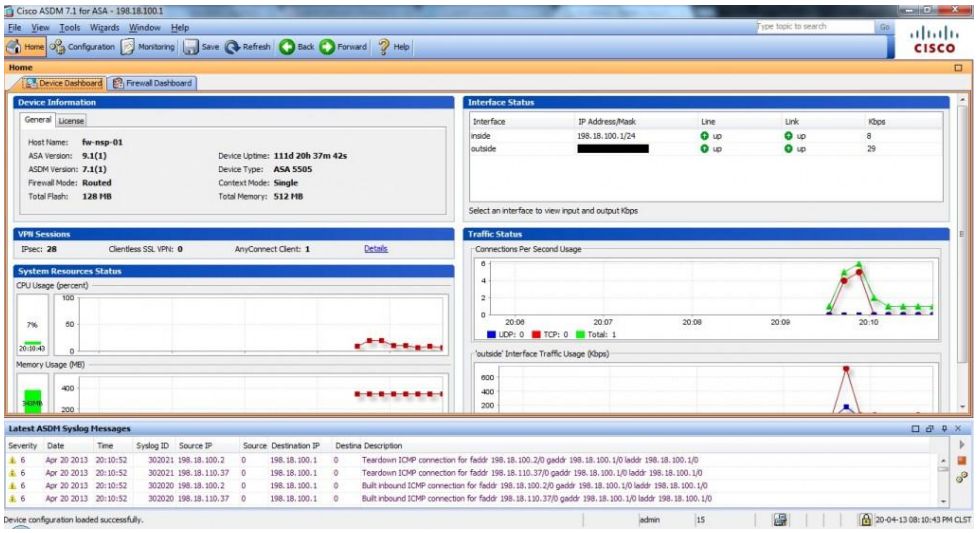
El Cisco ASA 5550 incluye el firewall de Cisco y los servicios IPsec/SSL VPN dirigidos al entorno de red. Proporciona más de 1,2 gigabits por segundo (Gbps) de rendimiento de firewall y da soporte a 200 redes de área local virtuales (VLAN).

Es importante para la Entidad la protección de protocolos de aplicaciones como web, correo electrónico, voz sobre Protocolo Internet (VoIP), mensajería instantánea, transferencia de archivos y protocolos de red Microsoft.

Ilustración 21 CISCO para ASA

Fuente: Cisco

Ilustración 22 Control de tráfico de Red



Fuente: Sistemas – Defensoría del Pueblo

9.3 ACTIVACION DETECCION DE AMENAZAS

El ASA muestra un ejemplo de cómo se inicia la detección de amenazas a través de la siguiente configuración:

Configuración inicial del ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
```

```
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host 172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0 255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0
static (inside,outside) 192.168.1.100 172.22.1.254 netmask 255.255.255.255
access-group outside_acl in interface outside
access-group inside_acl in interface inside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
```

```
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Cuando ocurre una amenaza, la solución por parte del administrador del ASA/PIX es recopilar toda la información posible del usuario.

- Dirección IP de origen: suele ser la estación de trabajo o el equipo del usuario.
- Dirección IP de destino: dirección IP del servidor a la que se intenta conectar el usuario o la aplicación.
- Puertos y protocolos que utiliza la aplicación.

10. ATAQUES A LA RED VOIP

Es necesario estudiar en este apartado la gran cantidad de ataques a los cuales está expuesta la Red de Telefonía VOIP.

VoIPhreaking[34]**:** nueva amenaza a la seguridad en VoIP

Mientras que para ahorrar costos el mundo de los negocios abraza rápidamente la tecnología VoIP (Voice-over-Internet Protocol), poca atención están dando a los nuevos peligros que se introducen en las redes telefónicas. Los despliegues de VoIP están ocurriendo sin la debida atención al tema de la seguridad, lo que podría afectar seriamente a las empresas y a los consumidores.

VoIPhreaking es en Internet el hermano moderno, más joven, del tradicional "phreaking", que es el término usado para las acciones de hackear, explorar y explotar la infraestructura telefónica convencional (PSTN), a los efectos de realizar llamadas telefónicas gratuitas, robándole dinero a las compañías.

Explotar la telefonía convencional vía VoIPhreaking, proporciona una abundancia de vectores potenciales de ataques, permitiendo múltiples y diferentes resultados que evitan o derriban las características confiables del sistema telefónico.

Ataques más avanzados permiten que los piratas informáticos controlen totalmente las conexiones telefónicas, incluyendo por ejemplo los datos usados por los identificadores de llamadas (Caller-ID). Esta información se utiliza con frecuencia para la autentificación de las casillas de mensajes de voz, tarjetas de crédito, y en algunos países, incluso para pagar facturas de servicio público.

La empresa WatchGuard Technologies, proveedor global de soluciones de seguridad de red, escribió un artículo de prensa con una lista de las principales amenazas para la seguridad de la Voz sobre IP (VoIP):[35]

Denegación de Servicio (DoS): Al igual que sucede en las redes de datos, existen ataques de denegación de servicio en las redes VoIP. Esto ocurre cuando un atacante envía múltiples paquetes, tales como solicitudes y registros, al punto donde los servicios VoIP fallan. Estos tipos de ataque a menudo tienen como objetivo el protocolo SIP (Protocolo de Inicio de Sesiones), provocando un gran consumo de recursos en el servidor de VoIP, derivando en la señal de ocupado o desconectado.

---

[34] ADAMS Nela . (2006). VoIPhreaking, nueva amenaza a la seguridad en VoIP. Obtenido de http://www.vsantivirus.com/na-voiphreaking.htm

[35] VIEIRA Carlos . (2009). WatchGuard anuncia las principales amenazas para la. pág. https://www.watchguard.com/international/es/press/wg04142009.pdf

Spam sobre Telefonía en Internet (SPIT): El spam ha dejado de ser exclusivo de los buzones de correo electrónico y comienza a propagarse de forma similar hacia los usuarios de VoIP mediante botnets. Al igual que el correo basura, los mensajes SPIT pueden ralentizar el rendimiento del sistema, obstruir los buzones de voz e inhibir la productividad del usuario.

Robo del Servicio de Voz: Puede ocurrir cuando un usuario no autorizado accede a una red de VoIP, por lo general, mediante un nombre de usuario y contraseña válidas, o bien obteniendo un acceso físico a un dispositivo VoIP y realizando llamadas salientes. A menudo, se trata de llamadas internacionales para aprovecharse de los beneficios que aporta la VoIP.

Secuestro de Registro: Un secuestro de registro SIP sucede cuando un hacker desactiva un registro SIP válido de un usuario y lo sustituye por una dirección IP pirata. Esto permite al hacker interceptar y redirigir las llamadas entrantes, reproducirlas o finalizarlas en función de sus intereses.

Escuchas no autorizadas: Al igual que los paquetes de datos, los paquetes de voz son objeto de ataques a través de un intermediario cuando un hacker falsifica la dirección MAC de dos partes, obligando a los paquetes de VoIP a circular a través del sistema del hacker. Al hacerlo, el atacante puede regresar a los paquetes de voz y escuchar las conversaciones en tiempo real. Con este ataque, los hackers también pueden robar todo tipo de datos sensibles y de información, tales como nombres de usuario, contraseñas e información del sistema de VoIP.

Directory Harvesting o Recogida de Direcciones (DHA): Esta amenaza se produce cuando los atacantes tratan de encontrar direcciones válidas de VoIP mediante el uso de la fuerza en una red. Cuando un hacker envía miles de direcciones VoIP a un dominio VoIP particular, la mayoría de éstas "rebotan" como si fueran no válidas, si bien hay algunas que no se devuelven y el pirata informático puede identificar las direcciones válidas de VoIP.

Mediante esta “recogida de direcciones” de usuarios de VoIP, el hacker puede obtener una nueva lista de suscriptores de VoIP que en un futuro pueden ser objetivo de amenazas, tales como ataques Vishing o SPIT.

Vishing (Phishing sobre VoIP): El Vishing imita las formas tradicionales de phishing (modalidad de estafa cuyo objetivo es intentar obtener de un usuario información personal y sensible como nombres de usuario, cuentas bancarias o números de tarjeta de crédito, entre otros). Esta táctica se realiza a través de correo basura o suplantando la imagen de una empresa o entidad pública con el objetivo de que el usuario verifique alguna información confidencial. Cuando el usuario cae en la trampa y aporta los datos correctos que le piden, los

delincuentes tienen libertad para vender esta información a otras personas o, en muchos casos, utilizan directamente las tarjetas de crédito o cuentas bancarias.

Eavesdropping (escucha no autorizada): La escucha en la VoIP no es el tradicional eavesdropping que se realiza en las redes de datos, aunque el concepto general continúa siendo el mismo. Las escuchas en VoIP requieren interceptar la señalización y los flujos de medios de una conversación. Hay que tener en cuenta que los mensajes de señalización y la media usan diferentes protocolos y puertos (UDP, TCP, RTP). Los flujos de media son transportados sobre UDP utilizando el protocolo RTP (Real Time Protocol).

Norton presenta más información acerca de los riesgos y las formas de mantener segura la Red VoIP[36]:

Pérdida de privacidad. La mayor parte del tráfico de VoIP no está cifrado, lo que facilita a que intrusos escuchen sus conversaciones de VoIP.

Hacking. Los hackers pueden obtener acceso a su conexión de VoIP y utilizar su línea para hacer llamadas. En algunos casos, también venden sus datos de conexión en el mercado negro. Una vez que ingresa en la red de su hogar, los hackers pueden atacar para descubrir información confidencial que puede tener guardada en la PC.

Necesita red y energía. Cada vez que su servicio de Internet o el suministro de energía se interrumpen, también se interrumpirá el servicio de VoIP.

[36] NORTON. (2015). Las vulnerabilidades de VoIP. Obtenido de http://co.norton.com/voip-security-a-primer/article

11. Aplicación NTC – ISO- IEC- 27001

La norma ISO 27001 permite la aplicación de requisitos para la implantación de un sistema de gestión de seguridad de la información y define la forma de gestionar la misma para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 y contiene una guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información, los cuales se aplicaran a los componentes del SGSI de la Red VOIP.[37]

Se debe tener en cuenta que la gestión de la seguridad de la información no se limita solamente a la seguridad de TI (cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de recursos humanos, con la protección jurídica, la protección física, entre otros, es por esto que se aplicó el anexo A herramienta a los componentes del SGSI de la Red VOIP.

Ilustración 23Gestion del Riesgo

NIVEL DE RIESGO

El nivel de riesgo permite valorar las amenazas y las vulnerabilidades que afectan y la probabilidad de ocurrencia, es decir, la facilidad de las amenazas para causar daños.

[37] ICONTEC. (2013). NORMA TECNICA COLOMBIANA NTC - ISO -IEC 27001. 12: 20.

Es por esto que se diseñó la siguiente tabla de riesgo, para que de manera porcentual permita identificar según el resultado del análisis del Anexo A, cuales son los dominios más vulnerables a los que se deberá aplicar o desarrollar una estrategia para contrarrestar posibles daños.[38]

Tabla 11.1. Nivel del Riesgo

%	RIESGO
0 - 20	MUY ALTO
21- 40	ALTO
41 - 60	MEDIO
61- 80	BAJO
81 - 100	MUY BAJO

[38] SUAREZ SIERRA, L. (2013). SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

12. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA ANEXO A ISO 27001

DOMINIO: A.5 Políticas de la Seguridad de la Información

Tabla 12.1. Dominio A5

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.5. Políticas de la Seguridad de la Información			2	1	1	1	1	50%	50%	100%	
A.5.1. Orientación de la dirección para la Gestión de Seguridad de la Información.			2	1	1	1	1	50%	50%		
Objetivo: Brindar orientación y soporte, por parte de la Dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes											
A.5.1.1.	Políticas para la Seguridad de la Información	Se evidencian políticas de seguridad.	1	0	0	0	1	0%	0%		Actualizar: no se encuentra ninguna enfocada a la seguridad de la Red VOIP
A.5.1.2.	Revisión de las Políticas para seguridad de la información	Se evidencian revisiones por parte de Control Interno	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A.6 Organización de la Seguridad de la Información

Tabla 12.2. Dominio A6

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.6. Organización de la Seguridad de la Información			5	4	4	4	1	80%	80%	100%	
A.6.1. Organización Interna			5	4	4	4	1	80%	80%		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización											
A.6.1.1.	Roles y Responsabilidades para la Seguridad de la información	El nivel directivo asegura la asignación y comunicación de las responsabilidades para los roles del SGSI	1	1	1	1	0	100%	100%		
A.6.1.2.	Separación de deberes	se evidencia	1	1	1	1	0	100%	100%		
A.6.1.3.	Contacto con las autoridades	Se evidencian políticas de seguridad.	1	0	0	0	1	0%	0%		Ajustar
A.6.1.4.	Contacto con grupos de interés Especial	Contrato	1	1	1	1	0	100%	100%		
A.6.1.5.	Seguridad de la información en gestión de Proyectos	La entidad maneja la seguridad de proyectos a través de la plataforma SUIFP	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A.7 Seguridad de los Recursos Humanos

Tabla 12.3. Dominio A7

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.7. Seguridad de los Recursos Humanos			6	2	2	3	3	33%	50%	100%	
A.7.1. Antes de Asumir el empleo			2	0	0	0	2	0%	0%		
A.7.1.1.	Selección	Personal de planta	1	0	0	0	1	0%	0%		Contratar más personal de acuerdo con procesos de selección que cumplan con la ley y reglamentaciones vigentes y conocimiento específico del tema de seguridad de la información de Red VOIP
A.7.1.2.	Términos y condiciones del empleo	Manual de Funciones	1	0	0	0	1	0%	0%		Actualizar manual de funciones
A.7.2. Durante la ejecución del Empleo			3	2	2	3	0	67%	100%		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan											
A.7.2.1.	Responsabilidades de la Dirección	El nivel directivo asegura la asignación, y comunicación de las responsabilidades a sus empleados	1	1	1	1	0	100%	100%		

A.7.2.2.	Toma de Conciencia, educación y formación en la Seguridad de la información	Desde la Oficina de Control Interno se establecen mecanismos de concientización y autocontrol dirigidas al personal	1	0	0	1	0	0%	100%		
A.7.2.3.	Proceso Disciplinario	La entidad tiene una oficina de control disciplinario denominada Veeduría que es la encargada de investigar a los funcionarios que incurran en presuntas fallas	1	1	1	1	0	100%	100%		
A.7.3. Terminación y Cambio de Empleo			1	0	0	0	1	0%	0%		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio y/o terminación del empleo											
A.7.3.1	Terminación o Cambio de responsabilidades de empleo	No se tiene ninguna contingencia	1	0	0	0	1	0%	0%		Elaborar plan de inducción, capacitación y acompañamiento de acuerdo al Régimen Laboral dirigido a los funcionarios del área de sistemas

Fuente: Autoría propia

DOMINIO: A.8 Gestión de Activos

Tabla 12.4. Dominio A8

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.8. Gestión de Activos			8	5	5	8	0	63%	100%	80%	
A.8.1. Responsabilidad por los activos			4	4	4	4	0	100%	100%		
Objetivo: Identificar los activos organizaciones y definir las responsabilidades de protección apropiadas											
A.8.1.1	Inventario de activos	Se tiene plenamente identificado el inventario de activos	1	1	1	1	0	100%	100%		
A.8.1.2.	Propiedad de los Activos	Defensoría del Pueblo	1	1	1	1	0	100%	100%		
A.8.1.3.	Uso aceptable de los Activos	Existen reglas de uso y manejo de los activos del área de sistemas	1	1	1	1	0	100%	100%		
A.8.1.4.	Devolución de los Activos	A través de Paz y salvos expedidos por la oficina de Inventarios	1	1	1	1	0	100%	100%		
A.8.2. Clasificación de la información			3	0	0	3	0	0%	100%		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección de acuerdo con la importancia:											
A.8.2.1	Clasificación de la información	Plan de manejo de riesgos	1	0	0	1	0	0%	100%		
A.8.2.2.	Etiquetado de la información	Plan de manejo de riesgos	1	0	0	1	0	0%	100%		
A.8.2.3.	Manejo de Activos	Plan de manejo de riesgos	1	0	0	1	0	0%	100%		
A.8.3. Manejo de medios de soporte			1	1	1	1	0	100%	100%		
Objetivo: Evitar la divulgación , la modificación el retiro o la destrucción no autorizada de información almacenada en los medios											
A.8.3.1.	Gestión de medios removibles	se establece en el Plan de riesgos	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!		
A.8.3.2.	Disposición de los medios	se establece en el Plan de riesgos	1	1	1	1	0	100%	100%		
A.8.3.3.	Transferencia de medios físicos	se establece en el Plan de riesgos	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!		

DOMINIO: A.9 Control de Acceso

Tabla 12.5. Dominio A9

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.9. Control de Acceso			14	12	12	13	1	86%	93%		
A.9.1. Requisitos del negocio para control de acceso			2	1	1	2	0	50%	100%	100%	
Objetivo: Limitar el acceso a la Información y a instalaciones de procesamiento de información											
A.9.1.1.	Política de control de acceso	Se establece en las Políticas de seguridad de la Información	1	0	0	1	0	0%	100%		
A.9.1.2	Acceso a redes y a servicios en red	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.2. Gestión de acceso de usuarios.			6	5	5	5	1	83%	83%	100%	
Objetivo: asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistema y servicios											
A.9.2.1.	Registro y cancelación de registro de usuarios	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.2.2.	Suministro de acceso de usuarios	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.2.3	Gestión de derechos de acceso privilegiado	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

A.9.2.4.	Gestión de Información de Autenticación secreta de usuarios	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.2.5.	Revisión de los derechos de acceso de usuarios	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.2.6.	Retiro o ajuste de los derechos de acceso	Se establece en las Políticas de seguridad de la Información	1	0	0	0	1	0%	0%		se debe implement ar
A.9.3. Responsabilidades de los usuarios			1	1	1	1	0	100%	100%	100%	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación											
A.9.3.1.	Uso de información de autenticación secreta	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.9.4. Control de Acceso a Sistemas y Aplicaciones			5	5	5	5	0	100%	100%	100%	
Objetivo: Evitar el acceso no autorizado											
A.9.4.1	Restricción de acceso a información	Existen políticas de control de acceso	1	1	1	1	0	100%	100%		
A.9.4.2.	Procedimiento de ingreso seguro	Existen políticas de control de acceso	1	1	1	1	0	100%	100%		
A.9.4.3.	Sistema de gestión de contraseñas	Existen políticas de control de acceso	1	1	1	1	0	100%	100%		
A.9.4.4.	Uso de Programas utilitarios privilegiados	Existen políticas de control de acceso	1	1	1	1	0	100%	100%		
A.9.4.5.	Control de Acceso a Códigos fuente de programas	Existen políticas de control de acceso	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A. 10 Criptografía

Tabla 12.6. Dominio A10

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.10. Criptografía			2	1	1	2	0	50%	100%	100%	
A.10.1. Controles Criptográficos			2	1	1	2	0	50%	100%		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad , la autenticidad y/o la integridad de la información											
A.10.1.1.	Política sobre el uso de controles criptográficos	no se tiene establecido en las políticas de seguridad	1	0		1	0	0%	100%		
A.10.1.2.	Gestión de Claves	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A. 11 Seguridad Física y del Ambiente

Tabla 12.7. Dominio A11

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.11. Seguridad Física y del Ambiente			12	12	12	12	0	100%	100%	84%	
A.11.1. Áreas Seguras			6	6	6	6	0	100%	100%	100%	
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización											
A.11.1.1	Perímetro de seguridad física	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.1.2.	Controles de acceso físicos	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.1.3.	Seguridad de oficinas, recintos e instalaciones	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.1.4.	Protección contra amenazas externas y ambientales	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.1.5.	Trabajo en áreas seguras	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.1.6.	Áreas de despacho y carga	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.11.2. Equipos			6	6	6	6	0	100%	100%	67%	
Objetivo: Prevenir la perdida, daño, robo o compromisos de activos y la interrupción de las operaciones de la organización.											
A.11.2.1.	Ubicación y protección de los equipos	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.11.2.2.	Servicios de	Plan de manejo de	1	1	1	1	0	100%	100%		

	suministro	riesgos									
A.11.2.3.	Seguridad del cableado	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.11.2.4.	Mantenimiento de equipos	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.11.2.5.	Retiro de activos	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.11.2.6.	Seguridad de equipos y activos fuera de las instalaciones	Plan de manejo de riesgos	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!		
A.11.2.7.	Disposición segura o reutilización de equipos	Plan de manejo de riesgos	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!		
A.11.2.8.	Equipos de usuario desatendido	Plan de manejo de riesgos	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!		
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A. 12 Seguridad de las Operaciones

Tabla 12.8. Dominio A12

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.12. Seguridad de las Operaciones			14	9	9	10	4	64%	71%	100%	
A.12.1. Procedimientos Operacionales y responsabilidades			4	2	2	2	2	50%	50%	100%	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información											
A.12.1.1.	Procedimientos de operación documentados	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.12.1.2	Gestión de Cambios	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.12.1.3.	Gestión de Capacidad	Se establece en las Políticas de seguridad de la Información	1	0	0	0	1	0%	0%		Existen por parte de AVAYA y CISCO, pero se deben adoptar las Políticas de seguridad Institucionales
A.12.1.4.	Separación de los ambientes de desarrollo, ensayo y operación	Plan de manejo de riesgos	1	0	0	0	1	0%	0%		
A.12.2. Protección contra códigos maliciosos			1	1	1	1	0	100%	100%	100%	
Objetivo: asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos											

A.12.2.1	Controles contra códigos maliciosos	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.12.3. Copias de Respaldo.			1	1	1	1	0	100%	100%	100%	
Objetivo: Proteger contra la perdida de datos											
A.12.3.1	Respaldo de la información	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		se realiza a través de copias de seguridad
A.12.4. Registro y seguimiento			4	2	2	3	1	50%	75%	100%	
Objetivo: registrar eventos y generar evidencia											
A.12.4.1.	Registro de eventos	Plan de manejo de riesgos	1	0	0	0	1	0%	0%		Se registran datos sobre fallas y eventos de seguridad a través del analizar de vulnerabilidades de Cisco pero no documentados
A.12.4.2.	Protección de la información de registro	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.12.4.3.	Registros del administrador y del operador	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.12.4.4.	Sincronización de relojes	No se evidencia	1	0	0	1	0	0%	100%		
A.12.5. Control de Software Operacional			1	1	1	1	0	100%	100%	100%	
Objetivo: Asegurarse de la integridad de los SO											
A.12.5.1.	Instalación de software en Sistemas Operativos	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.12.6. Gestión de la vulnerabilidad técnica			2	2	2	2	0	100%	100%	100%	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas											

A.12.6.1.	Gestión de las vulnerabilidades técnicas	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.12.6.2.	Restricciones sobre la instalación de Software	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.12.7. Consideraciones sobre auditorias de sistemas de información			1	0	0	0	1	0%	0%	100%	
Objetivo Minimizar el impacto de las actividades de auditoria sobre los SO											
A.12.7.1.	Controles de auditorías de sistemas de información	Oficina de Control Interno	1	0	0	0	1	0%	0%		interventor del contrato

Fuente: Autoría propia

DOMINIO: A. 13 Seguridad de las comunicaciones

Tabla 12.9. Dominio A13

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.13. Seguridad de las comunicaciones			7	7	7	7	0	100%	100%	100%	
A.13.1. Gestión de la seguridad de redes			3	3	3	3	0	100%	100%	100%	
Objetivo: Asegurar la Protección de la información en las redes y sus instalaciones de procesamiento de información de soporte											
A.13.1.1.	Controles de redes	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.13.1.2.	Seguridad de los servicios de red	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.13.1.3.	Separación en las redes	Están separados	1	1	1	1	0	100%	100%		
A.13.2. Transferencia de información			4	4	4	4	0	100%	100%	100%	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa											
A.13.2.1.	Políticas y procedimientos de transferencia de información	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.13.2.2.	Acuerdos sobre transferencia de información	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.13.2.3.	Mensajería Electrónica	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.13.2.4.	Acuerdos de confidencialidad o de no divulgación	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A. 14 Adquisición, desarrollo y mantenimiento de sistemas

Tabla 12.10. Dominio A14

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.14. Adquisición, desarrollo y mantenimiento de sistemas			12	12	12	12	1	100%	100%	96%	
A.14.1. Requisitos de seguridad de los sistemas de información			3	3	3	3	0	100%	100%	100%	
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida esto incluye redes publicas											
A.14.1.1.	Análisis y especificación de requisitos de seguridad de la información	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.14.1.3.	Protección de transacciones de servicios de aplicaciones	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.14.2. Seguridad en los procesos de desarrollo y de soporte			8	8	8	8	1	100%	100%	89%	
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información											
A.14.2.1.	Política de desarrollo seguro	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.2.2.	Procedimientos de control de cambios en sistemas	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

A.14.2.3.	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		89%
A.14.2.4.	Restricciones sobre cambios en los paquetes de Software	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.2.5.	Principios de construcción de sistemas seguros	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.2.6.	Ambiente de desarrollo seguro	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.2.7.	Desarrollo contratado externamente	Se establece en las Políticas de seguridad de la Información	0	0	0	0	1	#¡DIV/0!	#¡DIV/0!		
A.14.2.8.	Pruebas de seguridad de sistemas	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.2.9.	Pruebas de aceptación de sistemas	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.14.3 Datos de prueba			1	1	1	1	0	100%	100%	100%	
Objetivo: Asegurar la protección delos datos usados para pruebas											
A.14.3.1.	Protección de datos de prueba	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

DOMINIO: A. 15 Relaciones con los proveedores

Tabla 12.11. Dominio A15

SI = 1	NO =0		**ANALISIS DEL CONTROL QUE APLICA A VOIP**

		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.15. Relaciones con los proveedores			5	5	5	5	0	100%	100%	100%	
A.15.1. Seguridad de la información en las relaciones con los proveedores			3	3	3	3	0	100%	100%	100%	
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores											
A.15.1.1.	Política de seguridad de la información para las relaciones con proveedores	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.15.1.2.	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.15.1.3.	Cadena de suministro de tecnología de información y comunicación	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.15.2. Gestión de la prestación de servicios de proveedores			2	2	2	2	0	100%	100%	100%	
Objetivo: Mantener el nivel acordado de seguridad de información y prestación del servicio en línea según acuerdos con proveedores											
A.15.2.1.	Seguimiento y revisión de los servicios de los proveedores	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.15.2.2.	Gestión de cambios en los servicios de los proveedores	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		

DOMINIO: A. 16 Gestión de incidentes de seguridad de la información

Tabla 12.12. Dominio A16

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP

		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.16. Gestión de incidentes de seguridad de la información			7	5	5	5	2	71%	71%	100%	
A.16.1. Gestión de incidentes y mejoras en la seguridad de la información			7	5	5	5	2	71%	71%	100%	
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades											
A.16.1.1	Responsabilidades y procedimientos	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.16.1.2.	Reporte de eventos de seguridad de la información	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.16.1.3	Reporte de debilidades de seguridad de la información	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.16.1.5.	Respuesta a incidentes de seguridad de la información	Plan de manejo de riesgos	1	1	1	1	0	100%	100%		
A.16.1.6.	Aprendizaje obtenido de los incidentes de seguridad de la información	Plan de manejo de riesgos	1	0	0	0	1	0%	0%		Lo aprendido sirve para resolver incidentes de seguridad y reducir la posibilidad de impacto a los futuros incidentes
A.16.1.7.	Recolección de Evidencia	Plan de manejo de riesgos	1	0	0	0	1	0%	0%		Establecer procedimientos para la recolección de evidencia en caso que ocurra un incidente a la Red VOIP

Fuente: Autoría propia

DOMINIO: A. 17 Aspectos de seguridad de la información de la gestión de continuidad del negocio

Tabla 12.13. Dominio A17

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio			4	1	1	1	3	25%	25%	100%	
A.17.1. Continuidad de la seguridad de la información			3	0	0	0	3	0%	0%	100%	
Objetivo: La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización											
A.17.1.1.	Planificación de la continuidad de la seguridad de la información	Documento	1	0	0	0	1	0%	0%		Se debe contar con un Plan de continuidad de negocio que incluya la seguridad de la información en el proceso de gestión, capítulo específico para la Red VOIP
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Documento	1	0	0	0	1	0%	0%		Se debe contar con un Plan de continuidad de negocio que incluya la seguridad de la información en el proceso de gestión, capítulo específico para la Red VOIP
A.17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Documento	1	0	0	0	1	0%	0%		Se debe contar con un Plan de continuidad de negocio que incluya la seguridad de la información en el proceso de gestión, capítulo específico para la Red VOIP
A.17.2. Redundancias			1	1	1	1	0	100%	100%	100%	
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento											
A.17.2.1.	Disponibilidad de instalaciones de procesamiento de información	Centro de computo	1	1	1	1	0	100%	100%		

DOMINIO: A. 18 Cumplimiento

Tabla 12.14. Dominio A18

SI = 1	NO =0		ANALISIS DEL CONTROL QUE APLICA A VOIP								
		HALLAZGOS SGSI	APLICA A VOIP	DEFINIDO	IMPLEMENTADO	CONTEMPLA VOIP?	AJUSTAR PARA VOIP	PORCETAJE DE REQUISITOS DEFINIDOS	PORCENTAJE DE IMPLEMENTACION	PORCENTAJE DE APLICABILIDAD	RECOMENDACIONES PARA VOIP
A.18. Cumplimiento			8	8	8	8	0	100%	100%	100%	
A.18.1. Cumplimiento de requisitos legales y contractuales			5	5	5	5	0	100%	100%	100%	
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con seguridad de la información y cualquier requisito de seguridad											
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	La normatividad está identificada	1	1	1	1	0	100%	100%		
A.18.1.2.	Derechos de propiedad intelectual	Contratación	1	1	1	1	0	100%	100%		
A.18.1.3.	Protección de los registros	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.18.1.4.	Privacidad y protección de información de datos personales	Se establece en las Políticas de seguridad de la Información	1	1	1	1	0	100%	100%		
A.18.1.5	Reglamentación de controles criptográficos	No se evidencia	1	1	1	1	0	100%	100%		
A.18.2. Revisiones de seguridad de la información			3	3	3	3	0	100%	100%	100%	
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales											
A.18.2.1.	Revisión independiente de la seguridad de la información	Auditorías internas	1	1	1	1	0	100%	100%		
A.18.2.2.	Cumplimiento con las políticas y normas de seguridad	Auditorías Internas	1	1	1	1	0	100%	100%		
A.18.2.3.	Revisión del cumplimiento técnico	Auditorías Internas	1	1	1	1	0	100%	100%		

Fuente: Autoría propia

13. ANALISIS GAP PARA ISO - 27001

A través del análisis de diferencias se logra identificar los dominios de control definidos en el Anexo A de ISO 27001 según su porcentaje de implementación para la Red VOIP[39].

Tabla 13.1. Porcentaje de implementación dominios de control

DOMINIOS DE CONTROL	PORCENTAJE DE IMPLEMENTACION
A.5. Políticas de la Seguridad de la Información	50%
A.6. Organización de la Seguridad de la Información	80%
A.7. Seguridad de los Recursos Humanos	50%
A.8. Gestión de Activos	100%
A.9. Control de Acceso	93%
A.10. Criptografía	100%
A.11. Seguridad Física y del Ambiente	100%
A.12. Seguridad de las Operaciones	71%
A.13. Seguridad de las comunicaciones	100%
A.14. Adquisición, desarrollo y mantenimiento de sistemas	100%
A.15. Relaciones con los proveedores	100%
A.16. Gestión de incidentes de seguridad de la información	71%
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	25%
A.18. Cumplimiento	100%

Fuente: Autoría propia

[39] ISO 27001. (2013). Statement of Applicability of ISO/IEC 27001 Annex A controls. Obtenido de www.ISO27001security.com

14. PORCENTAJE DE IMPLEMENTACION DE DOMINIOS

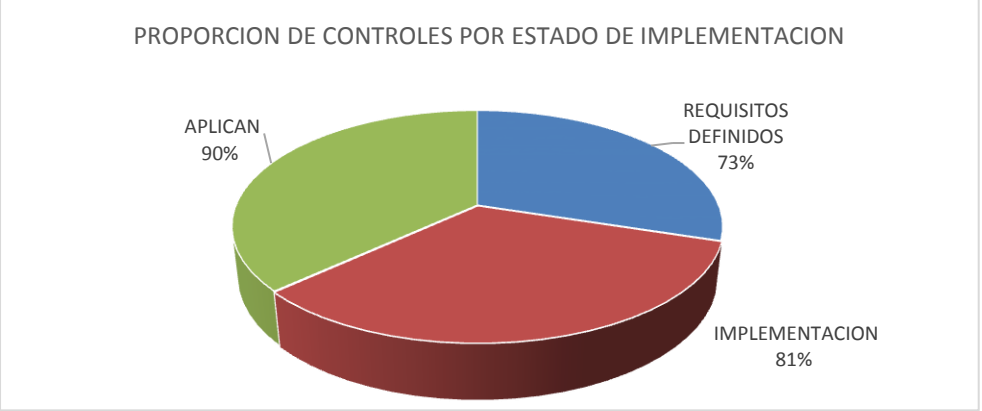
Se presenta de forma más precisa la evaluación de cada dominio

Ilustración 24 Análisis Gap

Fuente: Autoría propia

15. PROPORCION DE CONTROLES POR ESTADO DE IMPLEMENTACION

Ilustración 25 Proporción de Controles



Fuente: Autoría propia

Una vez analizados los resultados de la aplicación del anexo A se demuestra la importancia de implementar en el Sistema de Gestión de Seguridad de la Información que maneja la entidad los dominios identificados que no están implementados, para la Red VOIP.

A través de la identificación de los riesgos que afronta la entidad queda al descubierto las vulnerabilidades y amenazas a las que se está expuesta por lo cual es necesaria la implementación de acciones correctivas.

16. RESULTADOS SEGÚN NIVEL DE RIESGO

Tabla 16.1. Resultados según nivel del riesgo

DOMINIOS DE CONTROL	% DE IMPLEMENTACION	RIESGO
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	25%	ALTO
A.5. Políticas de la Seguridad de la Información	50%	MEDIO
A.7. Seguridad de los Recursos Humanos	50%	MEDIO
A.12. Seguridad de las Operaciones	71%	BAJO
A.16. Gestión de incidentes de seguridad de la información	71%	BAJO
A.6. Organización de la Seguridad de la Información	80%	BAJO
A.9. Control de Acceso	93%	MUY BAJO
A.8. Gestión de Activos	100%	MUY BAJO
A.10. Criptografía	100%	MUY BAJO
A.11. Seguridad Física y del Ambiente	100%	MUY BAJO
A.13. Seguridad de las comunicaciones	100%	MUY BAJO
A.14. Adquisición, desarrollo y mantenimiento de sistemas	100%	MUY BAJO
A.15. Relaciones con los proveedores	100%	MUY BAJO
A.18. Cumplimiento	100%	MUY BAJO

Fuente: Autoría propia

El resultado muestra que los componentes que aplican al SGSI de la Red VOIP que deben ser objeto de implementación son:

Tabla 16.2. Dominios de control a implementar

DOMINIOS DE CONTROL	% DE IMPLEMENTACION	RIESGO
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	25%	ALTO
A.5. Políticas de la Seguridad de la Información	50%	MEDIO
A.7. Seguridad de los Recursos Humanos	50%	MEDIO

Fuente: Autoría propia

De acuerdo al nivel del riesgo se establece que los dominios de control a los cuales se debe diseñar una propuesta de seguridad, que desde el nivel directivo se deberá o no implementar

17. PROPUESTA DE SEGURIDAD (HALLAZGOS Y RECOMENDACIONES)

El análisis del anexo A permitió identificar hallazgos que pueden resultar fatales si no se logran controlar razón por la cual es importante tener en cuenta la definición de criticidad del riesgo con el fin de realizar observaciones y recomendaciones de acuerdo con los hallazgos.

Dentro de la Gestión de la Seguridad de la Información en la Entidad es importante contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.

Una de las principales características que debe poseer la entidad es buscar cómo establecer un SGSI enfocado por procesos, teniendo como marco la norma ISO 27001 que resalta la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas a los componentes que aplican a la Red VOIP, cuyo propósito se encamine a mitigar los riesgos encontrados.

Para lo cual se plantea la necesidad de contar con:

17.1 PLAN DE CONTINUIDAD DEL NEGOCIO

En el análisis y diagnóstico del Sistema de Gestión de Seguridad de la Información de la Entidad en lo relacionado con los componentes de la Red VOIP, se observó que no se cuenta con un Plan de Continuidad de Negocio por lo cual se recomienda diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar la auditorías periódicas al SGSI con la finalidad de verificar que los objetivos de control, procesos y procedimientos cumplan con los requisitos de la norma ISO/IEC 27001.

Se debe dar a conocer la importancia del Plan de Continuidad de Negocio a los funcionarios adscritos al área de sistemas para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.[40]

Se deberán diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

El Plan deberá contemplar que una vez identificados y analizados los riesgos se debe adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la Red VOIP, esto de acuerdo con los siguientes enfoques:

- Aceptar el riesgo
- Definir controles y efectuar las implementaciones respectivas,
- Transferir el riesgo detectado

Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

- Política de copia de seguridad de datos
- Procedimientos de almacenamiento fuera de sitio
- Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones
- Corte por parte del proveedor de Internet.

[40] SUAREZ SIERRA, Lorena. (2013). SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

17.2 POLITICAS DE SEGURIDAD PARA LA RED VOIP

El análisis GAP permitió identificar que en lo relacionado con las políticas de seguridad no se tiene nada específico para la Red VOIP lo cual debilita al SGSI de la entidad; por lo cual debe quedar integrado con el documento actual.[41]

Se recomienda entre otros tener en cuenta:

- Habilitar protocolos de cifrado que brinden protección más adecuada**,** mediante algoritmos matemáticos con operaciones de sustitución, desplazamiento, mezcla de estado, para garantizar un cifrado fuerte.
- Implementación de firewalls y filtros entre los segmentos de voz y datos. Los firewalls proporcionan un solo punto de concentración para la aplicación de políticas de seguridad.
- Definir recursos tienen acceso
- Registro de las actividades realizadas.
- Si se realiza administración remota de los dispositivos de red esta deberá ser realizada sobre conexiones encriptadas.
- Política de claves, que incluya el no utilizar claves por default y tener una rotación de claves cada cierto periodo de tiempo.
- Manejo de antivirus.
- Ambiente con la seguridad física adecuada.
- Energía de respaldo para mantener la operación de los dispositivos de telefonía y de red en caso de una falla de energía eléctrica.
- Definir medidas de control para las amenazas que proceden de la red pública, para prevenir fraudes económicos.
- En los puntos críticos habilitar códigos de cuentas para permitir un mejor rastreo de las llamadas.
- Habilitar los logs de SMDR (Station Message Detail Recording) para monitorear el uso de las llamadas en la red.

[41] SUAREZ SIERRA, Lorena. (2013). SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.

17.3 PLAN DE CAPACITACION

Teniendo en cuenta que una de las principales necesidades detectadas es la falta de personal capacitado para la administración y manejo de la Red VOIP, así como del seguimiento constante al analizador de vulnerabilidades, se requiere de manera urgente contar con un plan de capacitación para los ingenieros adscritos al área de sistemas del nivel central de la Defensoría del Pueblo, para lo cual se sugieren los siguientes pasos:[42]

- Detectar las necesidades
- Clasificar y jerarquizar
- Determinar objetivos de capacitación
- Evaluar los resultados
- Elaborar un programa de capacitación
- Ejecutar el programa
- Evaluar los resultados

[42] SUAREZ SIERRA, Lorena. (2013). SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.

18. PRESUPUESTO

Para el desarrollo de ésta investigación se requiere:

Tabla 18.1. Presupuesto

NOMBRE	CANTIDAD	COSTO
Recurso Humano	Integrantes del Proyecto	$0.
Equipo de Computo	1	$1.800.000
Papelería y Materiales		$70.000
Imprevistos		$100.000
TOTAL		$1.970.000

Fuente: Autoría propia

19. CRONOGRAMA DE ACTIVIDADES.

Se presenta propuesta cronograma el cual está sujeto a cambios.

Tabla 19.1. Cronograma

	2013 (II sem)	2014 (I sem)	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
PROYECTO I								
PROYECTO II								
TRABAJO DE GRADO								
Recolección de información								
Desarrollo del Informe								
Entrega de la Propuesta								

Fuente: Autoría propia

PROYECTO I

La asignatura Proyecto I se desarrolló durante el segundo semestre de 2013, durante este periodo de tiempo se realizaron avances relacionados con el reconocimiento de cómo se iba a plasmar el documento de Proyecto de grado.

PROYECTO II

La asignatura se desarrolló permitió identificar y corregir falencias del documento inicial de esta forma se logró trabajar con el apoyo de los compañeros y del tutor en la mejora continua de un proyecto de grado con calidad en su investigación.

RECOLECCIÓN DE INFORMACIÓN

Desde el momento que nace la idea para trabajar este proyecto, se procedió formular el planteamiento del problema, y a conseguir información necesaria para el desarrollo de la investigación y el logro del objetivo trazado.

DESARROLLO DEL INFORME

Este desarrollo se realizó desde el comienzo de la idea de trabajar sobre el análisis y diagnóstico del sistema de gestión de seguridad de la información de la

Red VOIP del área de sistemas del nivel central de la Defensoría del Pueblo teniendo en cuenta los objetivos específicos que se trazaron.

- Evaluar sistemas de información existentes. (Características de equipos, conexiones)
- Realizar un análisis de recursos de red voz y datos (equipamiento, flujo de datos, topología)
- Realizar análisis de seguridad a los componentes al SGSI que apliquen a la red VOIP.
- Realizar observaciones y recomendaciones de acuerdo con los hallazgos

ENTREGA DE LA PROPUESTA

Teniendo en cuenta los resultados de la aplicación de la ISO 27001 en su anexo A, se establecieron dos meses para demostrar la importancia de implementar en el Sistema de Gestión de Seguridad de la Información que maneja la entidad los dominios identificados que no están implementados, para la Red VOIP.

A través de la identificación de los hallazgos se realizaron observaciones y recomendaciones de acuerdo con los riesgos que afronta la entidad quedando al descubierto las vulnerabilidades y amenazas a las que se está expuesta la Red VOIP y recomendando que es necesaria la implementación de acciones correctivas, como la implementación de un Plan de Continuidad de negocio, establecer Políticas de Seguridad específicas para la Red VOIP y un Plan de capacitación dirigido a los funcionarios del área de sistemas de la entidad.

20. CONCLUSIONES

- La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la entidad. Este proceso es el que constituye un SGSI, que basado en la norma ISO 27001, lo que brinda un sistema de calidad para la seguridad de la información de la red VOIP de la Defensoría del Pueblo.

- La evaluación de los sistemas de información en lo relacionado con la Red VOIP y las características de los equipos, y sus conexiones, mostró que está garantiza la calidad de los mismos, son equipo de marca reconocida y cuyas conexiones están en su mayoría resguardadas bajo estándares de seguridad que brinda el área de sistemas y exigidas a través del contrato de donación con la Unión Europea.

- El análisis de seguridad a los componentes del SGSI que aplican a la Red VOIP, permitió identificar dominios que no están implementados, quedando al descubierto las vulnerabilidades y amenazas a las que se está expuesta la red, por lo cual es necesaria la implementación de acciones correctivas.

- De acuerdo a los hallazgos evidenciados se realizaron recomendaciones enfocadas la implementación de un capítulo específico para la Red VOIP, dentro del SGSI de la entidad.

- Es importante resaltar que el análisis y diagnóstico permite al grupo directivo de la entidad tomar las medidas necesarias para garantizar que el SGSI, aplique las recomendaciones de este documento:

    - Es necesario que la entidad contemple en las políticas de seguridad actuales la inclusión de un capítulo dedicado a la Red VOIP.
    - Se debe contar con un plan de capacitación al personal del área de sistemas; por que la información no se puede concentrar sólo en una persona. De igual forma que el Plan permita mantener actualizado al personal del área, para que la entidad cumpla con lo establecido en la Norma ISO 27001, para lo cual se puede contar con el acompañamiento de la Oficina de Control Interno.

21. REFERENCIAS

ADAMS Nela . (2006). VoIPhreaking, nueva amenaza a la seguridad en VoIP. Obtenido de http://www.vsantivirus.com/na-voiphreaking.htm

AITEL, Dave. (2012). SPIKE Proxy 1.0 Released. Obtenido de http://seclists.org/pen-test/2002/Jul/60

ALFON. (2008). Obtenido de https://seguridadyredes.wordpress.com/2008/01/11/analizando-la-red-con-windump-tcpdump-i-parte/

ALFON. (01 de 2008). Obtenido de https://seguridadyredes.wordpress.com/2008/01/22/sistemas-de-deteccion-de-intrusos-y-snort-ii-creacion-de-reglas-i/

AVAYA. (2004). Configuring Avaya Communication Manager for Media. En JRR, Solution & Interoperability Test Lab Application Notes .

AVAYA. (2011). Obtenido de Avaya Aura Communication Manager: https://downloads.avaya.com/css/P8/documents/100066807

AVAYA. (02 de 04 de 2013). ERS Switch Complete Training Guide. Obtenido de https://www.youtube.com/watch?v=s3ww6jGXV04

CHIRILA, Alexandru. (2014). nbtscan. Obtenido de http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/nbtscan.shtml

CISCO. (2014). PIX/ASA: Actualice una imagen del software usando el ASDM o el ejemplo de la configuración CLI. Obtenido de http://www.cisco.com/cisco/web/support/LA/103/1030/1030085_upgrade-pix-asa7x-asdm.html

COMBS, Gerald. (2008). Obtenido de https://www.wireshark.org/about.html

DEFENSORIA. (2013). RESOLUCION 1014. Obtenido de http://www.defensoria.gov.co/

GATES, Chris. (2006). Tutorial: Hping2 Basics. Obtenido de https://www.ethicalhacker.net/columns/gates/tutorial-hping2-basics

Gerald, C. (2006). Ethereal. Obtenido de http://ethereal.uptodown.com/

HAUSER, Van. (2015). Obtenido de http://tools.kali.org/password-attacks/hydra

ICONTEC. (2013). NORMA TECNICA COLOMBIANA NTC - ISO -IEC 27001. 12: 20.

IRBY, David. (2005). Firewalk : Can Attackers See Through. Obtenido de http://www.giac.org/paper/gsec/312/firewalk-attackers-firewall/100588

ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

ISO 27001. (2013). Statement of Applicability of ISO/IEC 27001 Annex A controls. Obtenido de www.ISO27001security.com

ISO / IEC 27002 (2013) Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información

ISO/ IEC 27003 (2010) ISO / IEC 27003 Obtenido de http://www.iso27001security.com/html/27003.html

ISO / IEC 2700 (2009) Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información – Medición. Obtenido de http://www.iso27001security.com/html/27004.html

ISO / IEC 27005 (2011) Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. Obtenido de http://www.iso27001security.com/html/27005.html

ISO / IEC 27032 (2012) Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad. Obtenido de http://www.iso27001security.com/html/27032.html

ISO/IEC 18028 (2006) Norma de seguridad de redes. Obtenido de http://comunidad.dragonjar.org/f164/iso-iec-18028-norma-de-seguridad-de-redes

KOSUTIC, Dejan. (2015). ISO 27001 & ISO 22301 Blog. Obtenido de ISO 27001 & ISO 22301 Blog: http://www.iso27001standard.com/es/blog/

KRAUZ, Pavel. (2000). PACKET STORM. Obtenido de http://packetstormsecurity.com/sniffers/hunt/

LINUX. (2013). BackTrack Linux – Penetration Testing Distribution. Obtenido de http://www.backtrack-linux.org/

LINUX. (2014). Kali Linux NetHunter. Obtenido de https://www.kali.org/kali-linux-nethunter/

MINTIC. (2009). LEY 1273. Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

NORTON. (2015). Las vulnerabilidades de VoIP. Obtenido de http://co.norton.com/voip-security-a-primer/article

NTOP. (2015). Obtenido de http://www.ntop.org/

ORNAGHI, Alberto. (2009). ettercap(8) - Linux man page. Obtenido de http://linux.die.net/man/8/ettercap

PULGARIN, Diego. (2012). Manual Basico de Nessus en Windows. Bogota. Obtenido de http://diegopulgarinsena.blogspot.com/2012/04/instalacion-de-nessus-en-windows.html

RIES, Brian;. (2012). Hackers' Most Destructive Attacks, págs. http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html.

RODRIGUEZ, Ana Maria. (2014). ANALISIS Y DIAGNOSTICO DE LA SEGURIDAD INFORMATICA. Obtenido de http://repository.unad.edu.co/bitstream/10596/2692/5/53070244.pdf

SONG, Dug. (2001). dsniff Frequently Asked Questions. Obtenido de http://www.monkey.org/~dugsong/dsniff/faq.html#What is dsniff

SUAREZ SIERRA, Lorena. (2013). SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.

VIEIRA Carlos . (2009). WatchGuard anuncia las principales amenazas para la. pág. https://www.watchguard.com/international/es/press/wg04142009.pdf.