AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO

JAVIER ORLANDO MESIAS NARVAEZ
DIEGO FERNANDO ROSERO ALMEIDA

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2016

AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO

JAVIER ORLANDO MESIAS NARVAEZ
DIEGO FERNANDO ROSERO ALMEIDA

Proyecto de Grado para optar al título de: Especialista en Seguridad Informática

Asesor
ING. FRANCISCO SOLARTE

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA “UNAD”
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO, COLOMBIA
2016

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

San Juan de Pasto, Marzo de 2016

Dedico este trabajo a mis padres Francisco y Clemencia, a Paola Andrea Mora, a mi hija María Alejandra y a mi compañero Diego, porque gracias a sus consejos, colaboración y paciencia, hoy consigo un escalón más en mi vida profesional.

Javier

Dedico este trabajo principalmente a Dios mi señor, *a mis padres Magdalena Almeida y Luis Antonio Rosero, a mi esposa Marcela Zamora Bravo Narváez, a mi hija Sara Sofía y a mi compañero Javier.*

Diego

AGRADECIMIENTOS

Los autores de este trabajo de grado, expresan sus más profundos agradecimientos, en primer lugar al ingeniero Francisco Nicolás Solarte, docente de la UNAD y Tutor del CIPAS Auditores, al Ingeniero Gustavo Cuellar, coordinador de la oficina de Sistemas del Instituto Departamental de Salud (IDSN), a nuestros compañeros de la especialización Jesús Cortes y Daniel Álvarez y a todas aquellas personas que, de diversas maneras, han contribuido de forma desinteresada y con profesionalismo en la culminación de este trabajo.

Por todos los conocimientos y la experiencia brindada durante el trascurso de la especialización, nuestros más sinceros agradecimientos a todos los docentes de la Especialización en Seguridad Informática. Y a todos los compañeros y amigos que contribuyeron de alguna forma en la elaboración del presente trabajo de grado, gracias a todos por su apoyo.

CONTENIDO **Pág.**

LISTA DE TABLAS **Pág.**

GLOSARIO

ACCIÓN CORRECTORA: acción adoptada para eliminar las causas de una condición existente indeseable con objeto de minimizar o evitar su reaparición.

ACTIVO: con respecto a la informática, hace referencia a toda información o sistema que la contenga y que sea de importancia para la continuidad del negocio. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

ALERTA: con respecto a la seguridad informática, hace referencia a una aviso de manera formal con el cual se indica que se ha producido un evento adverso relacionado con la seguridad informática, el cual puede desarrollarse hasta que se convierta en un desastre.

AMENAZA: de acuerdo [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ANÁLISIS DE RIESGOS: de acuerdo [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

ANALIZADOR DE REDES: es **un** aparato electrónico que ofrece la posibilidad de medir, graficar y analizar de las variaciones de voltaje en cada una de las fases, el amperaje y el nivel de armónicos de un sistema eléctrico, además permite bajar la información a un computador a través de un puerto, para su posterior estudio.

ARMÓNICOS: distorsiones de las ondas de tensión y/o corriente de los sistemas eléctricos, debido al uso de cargas con impedancia no lineal, a materiales ferromagnéticos, y en general al uso de equipos que necesiten realizar conmutaciones o *switcheo* en su operación normal. La aparición de corrientes y/o tensiones armónicas en el sistema eléctrico crea problemas tales como, el aumento de pérdidas de potencia activa, sobretensiones en los condensadores, errores de medición, mal funcionamiento de protecciones, daño en los aislamientos, deterioro de dieléctricos, disminución de la vida útil de los equipos, entre otros.

AISLANTE: material que impide la propagación de algún fenómeno o agente físico. Material de tan baja conductividad eléctrica, que puede ser utilizado como no conductor.

ATAQUE DE DEFACE, DEFACEMENT O DEFACING: son ataques de modifican parcial o totalmente el contenido de un sitio web.

AUDITADO: persona u organización que se audita.

AUDITOR: persona cualificada para realizar auditorías de la calidad; para llevar cabo una auditoría de la calidad el auditor debe estar autorizado para esta auditoría en particular.

AVISO DE SEGURIDAD: advertencia de prevención o actuación, fácilmente visible, utilizada con el propósito de informar, exigir, restringir o prohibir una actuación.

***BACKUP*:** véase Copia de respaldo.

CARACTERÍSTICA: cualquier propiedad distintiva de un elemento o actividad que se puede describir y medir.

CERTIFICACIÓN DE AUDITORES: acto de determinar, verificar y atestiguar las cualificaciones de una persona para realizar auditorías de acuerdo con los requisitos aplicables; la certificación puede ser interna (por la propia organización a la que pertenece el auditor) o externa (por una sociedad autorizada).

CERTIFICACIÓN: procedimiento mediante el cual un organismo expide por escrito o por un sello de conformidad, que un producto, un proceso o servicio cumple un reglamento técnico o una(s) norma(s) de fabricación.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) creado en 1992 por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y por el Instituto de Administración de las Tecnologías de la Información (ITGI). Su objetivo promover el desarrollo de políticas y optimas prácticas de la Tecnología de Información.

COPIA DE RESPALDO: copia de los datos de un archivo electrónico en un soporte que posibilite su recuperación. El procedimiento de copia de respaldo tiene como propósito garantizar la reconstrucción en el estado en que se encontraban los datos al tiempo de producirse la pérdida o destrucción a fin de mantener la disponibilidad de la información.

COPIA DE SEGURIDAD: véase Copia de respaldo.

DIRECCIÓN IP: Dirección numérica obligatoria de un dominio 'Internet', que identifica de manera organizada la interfaz de red de un dispositivo que utilice el protocolo IP. Está conformada por una serie cuatro cifras (de 0 a 255) decimales separadas por puntos.

EQUIPO AUDITOR: grupo de personas que realizan una auditoría bajo la dirección de un auditor jefe.

ESPECIFICACIÓN: conjunto de requisitos que tiene que satisfacer un producto o servicio.

ESPECIFICACIÓN TÉCNICA: documentó que establece características técnicas mínimas de un producto o servicio.

ESTIMACIÓN: una forma de auditoría del sistema de calidad, realizada normalmente para examinar la eficacia del programa de calidad total y su puesta en práctica; la evaluación la realiza normalmente una tercera parte e informa de ella a la alta dirección de la organización.

EVALUACIÓN: acto de examinar un proceso o grupo con respecto a alguna norma y obtener, en consecuencia, ciertas conclusiones.

EVIDENCIA: soporte de una información. La evidencia surge cuando un acontecimiento empírico o los vestigios del mismo la respalden.

EVIDENCIA OBJETIVA: datos que respaldan la existencia o veracidad de algo y que pueden obtenerse por medio de la medición, observación, ensayo/prueba u otros medios.

INDEPENDIENTE: no responsable directamente de la calidad, del coste y/o de la fabricación de los bienes y servicios que se examinan.

INFORME DE AUDITORÍA: es esencialmente un instrumento de comunicación. A través del informe de auditoría el auditor expresa, en forma resumida, su dictamen profesional y las recomendaciones acerca del área auditada.

INSPECCIÓN: conjunto de actividades tales como medir, examinar, ensayar o comparar con requisitos establecidos, una o varias características de un producto o instalación eléctrica, para determinar su conformidad.

***LOG*:** es un registro oficial de eventos durante un periodo de tiempo en particular, es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.

MANTENIMIENTO: conjunto de acciones o procedimientos tendientes a preservar o restablecer un bien, a un estado tal que le permita garantizar la máxima confiabilidad

MÉTODO: modo de hacer con orden una actividad.

NIVEL DE RIESGO: valoración conjunta de la probabilidad de ocurrencia de los accidentes, de la gravedad de sus efectos y de la vulnerabilidad del medio.

NO CONFORMIDAD: falta de cumplimiento de los requisitos especificados; esta definición comprende el término «desviaciones» o la ausencia de una o varias de las características de la calidad o de elementos del sistema de la calidad respecto a los requisitos especificados.

NORMA: documento aprobado por una institución reconocida, que prevé, para un uso común y repetido, reglas, directrices o características para los productos o los procesos y métodos de producción conexos, servicios o procesos, cuya observancia no es obligatoria.

NORMA DE SEGURIDAD: toda acción encaminada a evitar un accidente.

NORMA TÉCNICA COLOMBIANA (NTC): norma técnica aprobada o adoptada como tal por el organismo nacional de normalización.

OBSERVACIÓN: constatación de hechos, realizada en el marco del proceso de auditoría y justificada por evidencias objetivas. Es una conclusión de una auditoría que identifica un punto débil de un sistema de calidad, bien en la definición o en la

puesta en práctica; una observación de una auditoría identifica una condición que todavía no está causando una degradación grave de la calidad.

PAPELES DE TRABAJO: son los registros que el auditor mantiene de las técnicas y de los procedimientos seguidos, las pruebas efectuadas, la información obtenida y las conclusiones alcanzadas durante la ejecución de la labor de auditoría.

PROGRAMA DE AUDITORÍA: conjunto de instructivos o procedimientos, lógicamente encadenados que aplicados al examen de un hecho sirve para obtener una conclusión demostrable.

PROCEDIMIENTO DE AUDITORÍA: concepto elemental técnico que, en auditoría, orienta una acción encaminada a determinar una evidencia.

REGLAMENTO TÉCNICO: documentó en el que se establecen las características de un producto, servicio o los procesos y métodos de producción, con inclusión de las disposiciones administrativas aplicables y cuya observancia es obligatoria.

REQUISITO: precepto, condición o prescripción que debe ser cumplida, es decir que su cumplimiento es obligatorio.

RESGUARDO: medio de protección que impide o dificulta el acceso de las personas o sus extremidades, a una zona de peligro.

RETIE O Retie: acrónimo del Reglamento Técnico de Instalaciones Eléctricas adoptado por Colombia. Es un el Reglamento Técnico de Instalaciones Eléctricas - RETIE, que fija las condiciones técnicas que garantizan la seguridad en los procesos de Generación Transmisión, trasformación, Distribución y Utilización de la energía eléctrica. Además, este Reglamento tiene el propósito de prevenir riegos para la vida, la salud, eliminar prácticas que puedan inducir a errores a los consumidores y facilitar la adaptación de las normas técnicas, en referencia, al futuro progreso tecnológico.

RIESGO: condición ambiental o humana cuya presencia o modificación puede producir un accidente o una enfermedad ocupacional. Posibilidad de consecuencias nocivas o perjudiciales vinculadas a exposiciones reales o potenciales.

SEÑALIZACIÓN: conjunto de actuaciones y medios dispuestos *para reflejar las advertencias* de seguridad en una *instalación.*

SISTEMA ININTERRUMPIDO DE POTENCIA (UPS): sistema que provee energía a cargas críticas unos milisegundos después del corte de la alimentación normal. Durante ese tiempo, normalmente no debe salir de servicio ninguno de los equipos que alimenta.

***STORAGE*:** es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

TECNOLOGÍA: conjunto de elementos técnicos, herramientas y procedimientos específicos mediante los cuales se puede realizar con eficiencia y eficacia una especialidad o una actividad productiva.

TEST DE PENETRACIÓN o **PENETRATION TESTING:** es un procedimiento de tipo metódico y sistemático con el cual se pretende un ataque real a una red o sistema informático, con el fin de descubrir vulnerabilidades, amenazas y riesgos, con el fin de mitigar los problemas de seguridad existentes.

VERIFICACIÓN: acto de revisar, inspeccionar, ensayar, comprobar, auditar o establecer y documentar de cualquier otro modo si los artículos, procesos, servicios o documentos son conformes con los requisitos especificados.

RESUMEN

En este proyecto de investigación, se realizó una auditoría a la seguridad de la red del Instituto Departamental de Salud de Nariño (IDSN) y tuvo como objetivo general formular unas políticas y procedimientos con el fin de establecer un sistema de control adecuado, para evitar posibles ataques y reducir los niveles de vulnerabilidad en el Instituto Departamental de Salud de Nariño, para este objetivo el proyecto abordo el tema de auditoría aplicada a la seguridad en redes, donde se aplicó la norma ISO 27001. La metodología que se aplicó en la auditoría consistió en cuatro fases.

En la primera fase, la cual es de conocimiento, se identifico el estado y los componentes de la red de datos del instituto departamental de salud de Nariño, con el fin de verificar las vulnerabilidades, riesgos y amenazas existentes y entre las actividades que se desarrollaron están: las visitas de campo, también se solicitó la documentación concerniente a la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos, entrevistas con el administrador de la red y algunos de los usuarios .

La fase dos, la cual es la etapa de planeación, entre las actividades realizadas están las siguientes, se Identifico y selecciono los métodos, pruebas y procedimientos necesarios para la realización de la auditoria.

La fase tres, consistió en la ejecución de la auditoría, para lo cual se realizaron las siguientes actividades: se aplicó las pruebas de intrusión y testeo y se ejecutaron los instrumentos de recolección de la información, después se realizó el Análisis y evaluación de riesgos y por último se organizó los papeles de trabajo de la auditoría

Como fase final presentaron los resultados de la auditoría para lo cual se realizaron la lista de hallazgos y como resultado final se presentó el informe de auditoría con políticas y procedimientos de seguridad para la red.

INTRODUCCIÓN

En un mundo donde la información se ha convertido en un activo de gran valor para las organizaciones, es primordial garantizar que este activo este siempre bien custodiado, garantizando su integridad, confidencialidad y disponibilidad en todo momento y lo más resguardado posible de todas las amenazas que hay alrededor, por lo anterior es importante la seguridad informática y los sistemas de control que sirven para garantizar que los servicios informáticos ofrecidos por las empresas e instituciones sean seguros y confiables.

La auditoría de la seguridad informática a las redes, es un examen crítico que permite evaluar la seguridad en lo referente a políticas, manejo de internet, la red interna LAN y sobre los componentes de la red, realizando las respectivas pruebas sobres la red, lo cual permite dictaminar el estado real de la seguridad informática dentro de una empresa, en la auditoría se van a implementar diferentes pruebas, el resultado de ellas, permitirá evaluar el tipo y extensión de las vulnerabilidades del sistema y de la red,

El objetivo principal al implementar este proyecto es comprobar si la red del instituto departamental de salud es segura frente a posibles ataques y cuál es su nivel de seguridad, además mediante una auditoría de seguridad informática se podrá formular unas recomendaciones que servirán como una guía dentro de la institución.

Este proyecto consta de 11 capítulos que están distribuidos de la siguiente manera: En los capítulos del 1 al 4 se encuentran los aspectos metodológicos del proyecto, en el capítulo 5 están contenidos los marcos del estado del arte, en el capítulo 6 se tiene el marco metodológico, en el capítulo 7 está contenido el desarrollo del proyecto los archivos corriente y permanente, el plan de auditoria, los instrumentos, la pruebas y el informe de auditoría, en el capítulo 10 se encuentran los resultados del proyecto.

1. PLANTEAMIENTO DEL PROBLEMA

De acuerdo a la información inicial recogida en el Instituto Departamental de Salud de Nariño (IDSN) y como uno de los usuarios de los sistemas de información del mismo, se ha detectado que se presentan situaciones de infiltración de usuarios no autorizados a la red del IDSN, estas vulneraciones han tenido como resultado cambios de índex de los sistemas de información y negación de servicios del servidor del IDSN, lo cual ocasiona retrasos en el ingreso de la información, no solamente a los clientes internos de los sistemas de información sino que también afecta a los clientes externos del mismo.

Lo anterior se debe a que no existe un sistema de control en la red del IDSN, lo cual ocasiona que se presenten este tipo de intromisiones.

Entre los principales problemas que se pueden evidenciar en el Instituto Departamental de Salud de Nariño (IDSN), están los ataques de defacement, ataques DoS e inyección de código maliciosos, mediante estos ataques por parte de hackers, se ha presentado en varias oportunidades, el cambio del índex de la página principal, también se presenta como un problema alterno que las claves de la red WIFI son públicas y están a la vista de todas de las personas que ingresan a las instalaciones ya que se encuentran publicadas en las carteleras y en cada uno de los cuatro pisos del edificio donde funciona el IDSN, lo cual ha originado que la red se colapse en determinados momentos

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo la auditoría a la seguridad de la red de datos permitirá establecer un sistema de control adecuado que evite los posibles ataques y reduzca los niveles de vulnerabilidad en la red en el Instituto Departamental de Salud de Nariño?

2. JUSTIFICACIÓN

El Departamento de Nariño se compone de 64 municipios, ocupa el quinto puesto en número de municipios en Colombia, en todos los municipios del departamento existen Empresas Sociales del Estado (ESEs), Direcciones Locales de Salud (DLS), Secretarias Municipales de Salud, Empresas Promotoras de Salud (EPS), e Instituciones Prestadoras de Salud (IPS), las cuales ingresan a los aplicativos en línea del Instituto Departamental de salud de Nariño (IDSN), ya sea para ingresar, descargar o consultar información, aparte de los clientes externos, existen aproximadamente 200 usuarios internos conectados a la red interna del IDSN, por lo tanto es primordial para el Instituto Departamental de salud de Nariño IDSN, garantizar la prestación de sus servicios en línea de manera segura, continua y con calidad.

Teniendo en cuenta lo anterior, es importante realizar este proyecto, ya que beneficiara los clientes externos del IDSN, entre los cuales están las Empresas Sociales del Estado (ESEs), Direcciones Locales de Salud (DLS), Secretarias Municipales de Salud e Instituciones Prestadoras de Salud (IPS), del departamento, quienes contaran con una información integra, disponible y confidencial, también se beneficiaran los clientes internos del IDSN, quienes no tendrán problemas al acceder a los sistemas de información del IDSN, de igual manera se beneficia el administrador de la red porque tendrá el informe con los controles y los mecanismos de protección para que pueda implementarlos sobre la red de datos, también se beneficiara a la administración del IDSN, ya que siempre contara con un sistema de información confiable que será su imagen ante el Departamento de Nariño y ante el país.

De acuerdo a lo anterior, se puede mencionar que la realización de una auditoría a la seguridad informática a la red del IDSN, permitirá corregir los problemas que se presentan en la actualidad, como son intromisiones no deseadas y negaciones de servicios, además de permitir conocer las vulnerabilidades, amenazas y riesgos que se presentan en la red.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer un sistema de control adecuado que evite los posibles ataques y reduzca los niveles de vulnerabilidad mediante la aplicación de una auditoría a la seguridad de la red de datos en la red en el Instituto Departamental de Salud de Nariño.

3.2 OBJETIVOS ESPECÍFICOS

- Conocer la red de datos del instituto departamental de salud de Nariño para verificar las vulnerabilidades, riesgos y amenazas existentes, lo que servirá como soporte para determinar el estado actual de la seguridad tanto física como lógica de la red, dentro de la institución.

- Elaborar el plan de auditoría donde se incluya el objetivo y alcances, la metodología, los recursos necesarios para llevarla a cabo, diseñar los instrumentos y el plan de pruebas que se ejecutará sobre la red de datos para determinar las causas de los problemas.

- Ejecutar las pruebas y aplicar los instrumentos que permitan evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes, los recursos afectados y las causas que los originan para proponer los controles adecuados para mitigarlos.

- Mostrar los resultados en el informe final para identificar los niveles de madurez en cada dominio evaluado, los hallazgos confirmados, los controles adecuados para establecer las políticas y procedimientos que permitan mitigarlos.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Los alcances del proceso de auditoría a la seguridad informática están enfocados hacia los aspectos relacionados con la red de datos del Instituto Departamental de Salud de Nariño (IDSN) localizado en la sede Bomboná.

Para el proceso de auditoría se ha elegido las normas ISO/IEC 27001 e ISO/IEC 27002 como estándares de mejores prácticas para evaluar la seguridad informática, y la metodología MAGERIT para realizar el proceso de análisis y evaluación de los riesgos de seguridad informática. También se hará uso de software especializado para ejecutar pruebas que permitan evidenciar las vulnerabilidades y posibles amenazas sobre la red de datos del Instituto Departamental de Salud de Nariño.

Los aspectos que serán evaluados en la red están relacionados con el control de accesos y los servicios que se brindan a través de la red, entre ellos:

- Firewall.
- IPS (sistemas de prevención de intrusos).
- Antivirus – Antimalware – Antispyware AntiSpam.
- Filtros de Contenido Web.
- Servidores de red y puntos de control.

5. MARCO DE REFERENCIA

5.1 ANTECEDENTES

La informática está inmersa en la gestión integral de la organización. A finales del siglo XX, los sistemas de TI (tecnologías de la información) se constituyeron como las herramientas más poderosas para cualquier organización, puesto que apoyan la toma de decisiones, generando un alto grado de dependencia, así como una elevada inversión en ellas. Debido a la importancia que tienen en el funcionamiento de una organización, existe la auditoría informática. Es por ello que las tecnologías de información, necesitan ser evaluadas, controladas y administradas, en su funcionamiento, y esto se logra mediante una auditora informática.

Existen diferentes modelos de auditoría, actualmente un modelo nuevo es el modelo Cobit, (Objetivos de Control para la Información y la Tecnología relacionada). El modelo Cobit brinda un conjunto de buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización. El modelo COBIT es un modelo muy completo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Auditoría Informática en el Área de Sistemas e Indicadores de Funcionamiento del Hardware en el instituto departamental de Salud de Nariño. Desarrollado por CARLOS DANIEL ROMO, la UNIVERSIDAD DE NARIÑO. Este trabajo de grado se desarrolló en las instalaciones de el en el instituto departamental de Salud de Nariño y utilizaron la metodología COBIT para este trabajo.

Auditoría de Sistemas Aplicada al Sistema Integral de Información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto, realizada por OSCAR JULIÁN ESTRADA OBANDO de la UNIVERSIDAD DE NARIÑO. Este trabajo de grado consistió en realizar la evaluación de los controles relacionados con la seguridad de la información, Identificar las fallas en cuestión de seguridad, plantear posibles soluciones para mejorarlas condiciones de seguridad físicas y lógicas del Sistema Integral de Información, además también se utilizó para esto la metodología COBIT.

Auditoría de Sistemas Aplicada a Redes de Datos desarrollado por KAROL JANETH JURADO GARCÍA y BYRON ALEXANDER MUÑOZ de la UNIVERSIDAD CESMAG. Este trabajo de grado que consistió en aplicar la metodología COBIT a la red de datos de la Cámara de comercio de Pasto.

Auditoría de Sistemas al Aula de Informática de la Universidad De Nariño, desarrollado por EDGAR OSWALDO BENAVIDES Y JAVIER ORLANDO MESÍAS NARVÁEZ de la UNIVERSIDAD DE NARIÑO, este trabajo examinó la gestión informática, la seguridad del personal, de las instalaciones físicas, la red de datos, las bases de datos, la red eléctrica, el hardware y el software.

Los proyectos arriba mencionados sirvieron de antecedentes para el desarrollo del proyecto, teniendo en cuenta que aportaron las diferentes técnicas y herramientas para la auditoría.

5.2 MARCO CONTEXTUAL

Para el año de 1995 se reestructura el Instituto Departamental de Salud de Nariño, por medio del Decreto No. 1158 de diciembre 6 de la Gobernación de Nariño, el cual modifica la estructura interna del Instituto Departamental de Salud de Nariño, establecida en el artículo 4° del Decreto 401 de julio 15 de 1993.

Figura 1. Instituto Departamental de Salud de Nariño IDSN

Fuente: www.idsn.gov.co

En el año 2001, mediante el Acuerdo No. 022 del 8 de Agosto de la Junta Directiva del IDSN, se modifica la organización interna del IDSN teniendo en cuenta el artículo 11 del decreto ordenanza No. 401 del 15 de Julio de 1993 de la Gobernación de Nariño y la Ley 617 de 2000. En este año, dando cumplimiento a las nuevas normas de modernización de la Administración Pública, se elaboró el "PROYECTO DE MEJORAMIENTO, FORTALECIMIENTO Y AJUSTE DE GESTIÓN ADMINISTRATIVA", que contempla la supresión de los cargos que por necesidades del servicio y nuevos procesos de reorganización administrativa ya no corresponden a la Visión y Misión del IDSN, ni se consideran necesarios para el cumplimiento de las actividades de la Institución.

En el año 2004 la institución es administrada bajo los principios de la gerencia moderna, retoma el proceso de implementación del Sistema de Gestión de la Calidad y se consolida como una institución líder en el departamento. En esta época la institución inicia un agresivo proceso de cambio que exige de un gran compromiso por parte de todos sus colaboradores, con lo cual busca fortalecer su liderazgo y el cumplimiento del Sistema General de Seguridad Social en Salud en el departamento.

Figura 2. Organigrama IDSN

Fuente: www.idsn.gov.co

Oficina asesora de Planeación tiene a su cargo la oficina de sistemas, la oficina de sistema tiene la siguiente estructura organizacional: un profesional especializado, quien es coordinador de la oficina de sistemas , dos profesionales universitarios uno de ellos tiene a su cargo la administración Web de internet e intranet y el manejo de SYSMAN, y el otro profesional se encarga del desarrollo de aplicaciones, en el siguiente nivel hay dos tecnólogos de sistemas, quienes se encargan del manejo de la Base única de afiliados BDUA y soporte y mantenimiento, esto en cuanto se refiere al personal de planta, en cuanto a contratación existen 8 ingenieros externos que soportan el proceso de cargue de información, evaluación y valoración de sistemas de información en cada una de las líneas de salud.

El IDSN tiene un sistema de gestión de calidad, el cual exige que toda la información debe estar organizada, por lo anterior se llevan los siguientes procesos: la consolidación de base de datos, el análisis de información, desarrollo y soporte a sistemas de información, y como procesos asociados tiene los siguientes: procedimiento de copias de seguridad, publicación y mecanismos de divulgación de información.

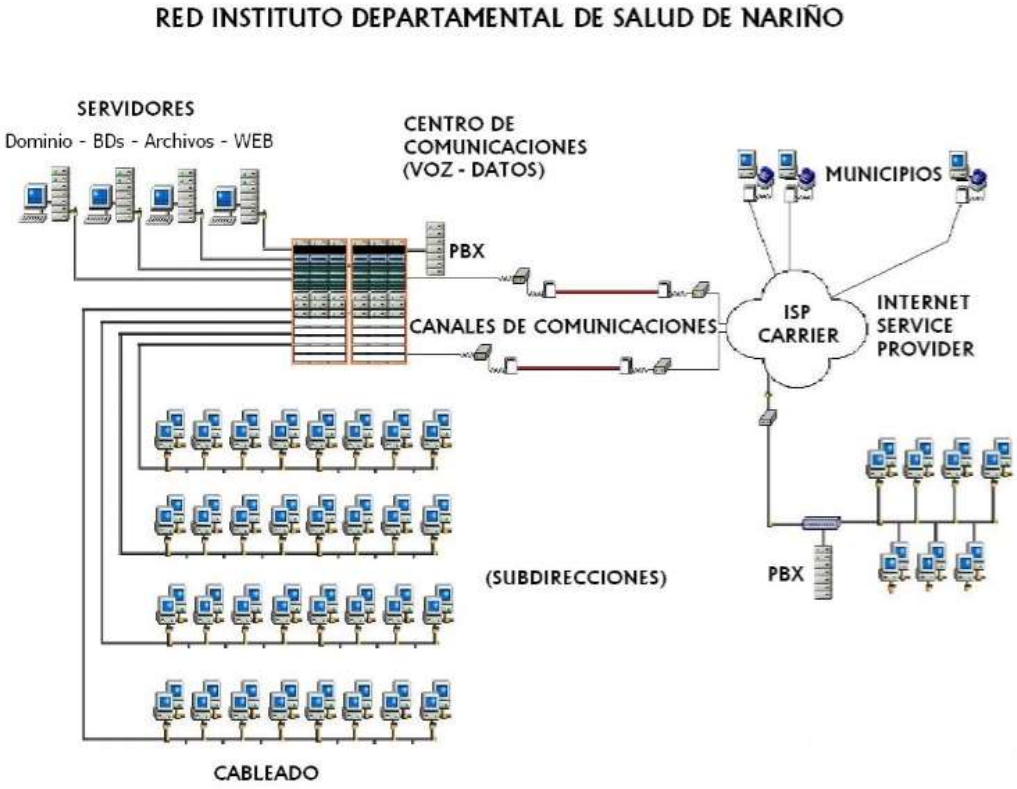
Los sistemas que tiene soportados en la red son administración de sistemas operativos Microsoft y Linux, los sistemas corporativos como son: El Sistema contable SYSMAN maneja un sistema integrado de Contabilidad, Presupuesto y

Tesorería, Nómina, Contratación e Inventarios, también cuenta con desarrollos propios entre los que están:

- SIVEFRONTERA
- Reportes - SIIS
- Resolución 4505
- IAMI - AIEPI
- AIEPI Comunitario
- Salud Sexual y Reproductiva
- Salud Ambiental
- CRUE
- Riesgos y Accidentes de Trabajo
- Salud Oral
- RIPS
- Crónicas - ECNT
- Salud Mental
- Licencias Salud Ocupacional
- Registro de Profesionales de la Salud
- Quejas y Reclamos

Además, también tiene sistemas de información adoptados de proveedores externos como son: FOSYGA y MINSALUD.

Figura 3. Instituto Departamental de Salud de Nariño IDSN



Fuente: Instituto Departamental de Salud de Nariño IDSN

La red de instituto tiene una topología hibrida que esta soportado en 10 servidores, y la cual se conectan internamente 200 terminales, distribuidos así: 180 equipos de escritorio y 20 portátiles.

5.3 MARCO TEÓRICO

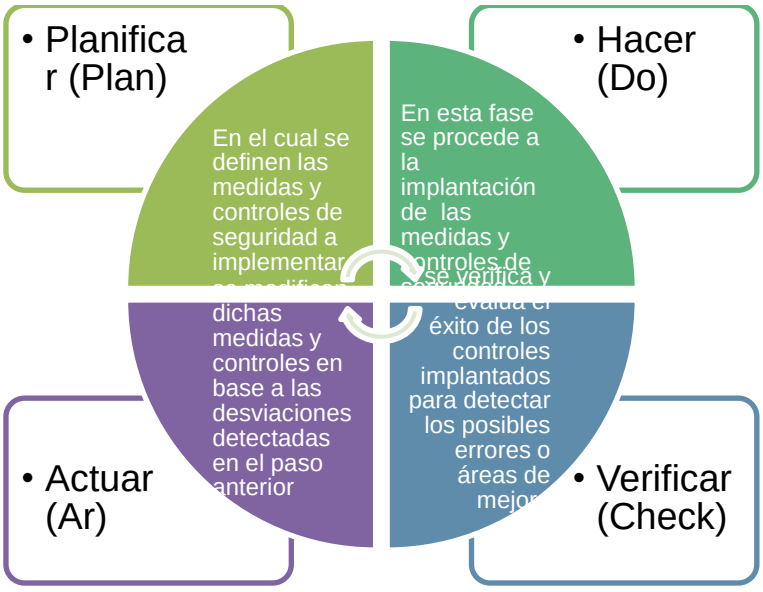
En el desarrollo de este proyecto se hacen necesarios tener en claro ciertos conceptos tales como redes, auditoría de redes, análisis de riesgos, y la ISO 27001 y 27002, normas internacionales emitidas por la Organización Internacional de Normalización (ISO).

5.3.1 ISO/IEC 27001:2013

Su nombre completo es ISO/IEC 27001:2013, es una norma internacional emitida por la ISO (Organización Internacional de Normalización) y su contenido sirve como base para implantar los sistemas de gestión de la seguridad de la información (SGSI) dentro de las organizaciones, su versión más reciente fue publicada en el año 2013 y la primera versión se publicó en el año 2005, su desarrollo se basó en el estándar británico BS 7799-2, el cual era tomado como base para la implementación de los SGSI, antes de antes de la publicación del ISO/IEC 27001:2005.

Un aspecto básico de la ISO 27001 es la gestión de la Seguridad de la Información mediante procesos basados en el método de mejora continua, el ciclo PDCA: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act), también conocido como Círculo de Deming, este método se basa en un procedimiento cíclico mediante el cual se determinan las medidas y controles de seguridad que se planean implementar (Plan); luego se procede a su implantación (Do); se realiza la verificación y la evaluación del éxito de los controles implementados con el fin de detectar errores o posibles áreas de mejora (Check); y, como paso final, se realizan las modificaciones de las medidas y controles basándose en las desviaciones encontradas en el anterior paso (Act).

Figura 4. Ciclo PDCA



Fuente: Autor

5.3.2 ISO/IEC 27002:2013

Su nombre completo es ISO/IEC 27002:2013, es una norma internacional emitida por la ISO (Organización Internacional de Normalización) en conjunto con IEC (Comisión Electrotécnica Internacional), su contenido sirve para proporcionar recomendaciones de las buenas prácticas en la gestión de la seguridad de la información, para todos los encargados de iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Su versión más reciente fue publicada en el año 2013 y la primera versión se publicó en el año 2007, antiguamente era conocida como la norma ISO/IEC 17799, pero desde julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002. Contiene 14 dominios, 35 objetivos de control y 114 controles

La versión de 2013 del estándar describe los siguientes catorce dominios[1] principales:

A5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

A6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguridad de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

A7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en seguridad de la información.
7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

A8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.

8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

A9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

A10. CIFRADO.

10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

A11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

A12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

A13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

A15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

A16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

A18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento

Cada sección determinada los objetivos dé cada uno de los controles para la seguridad de la información. Cada uno de los controles posee su propia guía para su implantación. La ISO 27002 tiene en total 114 controles, resultado de la suma de todas sus secciones: Es importante que toda organización considere que controles se va a implementar de acuerdo a sus requerimientos[1].

5.3.3 Auditoría

La palabra auditoría proviene del vocablo auditorius, y de esta proviene la palabra auditor, la cual significa oír, la auditoría es un examen crítico y sistemático que se realiza a una empresa, con el fin de evaluar el cumplimiento de normas, proyectos, la parte financiera, el cumplimiento de objetivos, en general evalúa la eficiencia y eficacia de todos los procesos que tienen que ver con el mejoramiento y desarrollo empresarial, estableciendo diferentes alternativas de soluciones para garantizar organización y logro de objetivos.

La eficiencia, definida como lograr el objetivo en menor tiempo posible y la eficacia definida como lograr el objetivo sin importar el tiempo, se convierte en la clave para obtener una auditoría de calidad.

Un auditor debe ser una persona capaz de observar cada movimiento y comportamiento de los procesos, encaminado siempre al objetivo específico, que es el de evaluar la eficacia y eficiencia de cada proceso tomado como caso de estudio, para que por medio del señalamiento de alternativas de acción, la empresa como tal tome decisiones que permita corregir hallazgos en caso de que sean

[1] Dominios tomados de la norma ISO/IEC 27002:2013

encontrados, mejorando las funciones de cada proceso permitiendo así el cumplimiento de los objetivos propuestos por la empresa.

Clasificación de la Auditoría

De acuerdo al modo de cómo se ejecuta la auditoría, se puede clasificar de dos maneras, auditoría externa y auditoría interna.

Auditoría Externa

La auditoría externa se caracteriza porque la realiza un profesional totalmente independiente de la empresa, el cual después de examinar y evaluar el área de los sistemas de información genera una opinión veraz y creíble de los casos de estudio tomados, para luego presentarlos como resultados o hallazgos a la empresa u organización.

Auditoría Interna

La auditoría interna es la evaluación exhaustiva y detallada de cada uno de los procesos llevados dentro de una empresa, se evalúan sistemas de información como también operaciones contables y financieras, evaluando siempre la eficiencia y eficacia de todos los procesos. Generalmente la empresa es quien asigna a un profesional calificado perteneciente a la misma con el objeto de utilizar diferentes técnicas que permitan realizar un examen, dando como resultado la detección de fallas a tiempo, para corregirlas y mejorar algunos procesos que así el informe de la auditoría final lo sugiera.

Auditoría Informática.

Es una evaluación integral, que no solo abarca los equipos de cómputo y los sistemas de información sino también que comprende la evaluación y comprobación de las políticas, controles, procedimientos y la seguridad en general, con el fin de garantizar que todo el sistema en general, garantice que la información cuente con sus características de confiabilidad, disponibilidad e integridad, lo cual permitirá que la información sirva para una adecuada toma de decisiones

Según José A. Echenique, la auditoría en informática “es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el

procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización especifica que hará posible el uso de los equipos de cómputo"[2].

Según Mario Piattini Velthuis, la auditoría informática es "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos"[3].

Auditoría de sistemas.

Es el examen que se aplica a los sistemas de información, o a una parte o sección de ellos, con el fin de evaluar su eficiencia y eficacia con el fin de emitir unas recomendaciones que permitan mejorar su rendimiento.

Auditoría a los sistemas de redes.

Es el examen que se realiza a los sistemas de redes de una organización o institución, con el fin de revisar los tipos de redes, arquitectura, topología, protocolos de comunicación, las conexiones, accesos, privilegios, administración y todos los factores que tengan injerencia como pueden ser: la administración, el funcionamiento y el aprovechamiento. También se considera la revisión de las instalaciones, el software y hardware de la red, los recursos informáticos las bases de datos y el software que sirva para la continuidad del negocio.

---

[2] Echenique, José Antonio. Auditoría en informática. Pág. 16
[3] Piattini, Mario. Auditoría de tecnologías y sistemas de información. Pág. 7

5.3.4 Papeles de Trabajo en la Auditoría.

Son todos los formatos que han sido diseñados para recolección de la información y para mostrar los resultados de la auditoría, y servirán como soporte al informe generado por parte del equipo auditor. Estos se preparan de acuerdo al objetivo de la auditoría y los criterios del equipo auditor y se organizan teniendo en cuenta su uso y contenido. Según José Dagoberto Pinilla Define los papeles de trabajo así: "comprende el conjunto de cédulas preparadas por el auditor y/o personal colaborador, con motivo del desarrollo del programa de auditoría para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado".

Objetivos de los papeles de trabajo

- Proporcionar la información necesaria y básica para el desarrollo de las fases etapas de la auditoría.
- Respaldar el resultado de la auditoría.
- Permiten realizar una adecuada planeación para el proceso de la auditoría.
- Permiten establecer un registro cronológico permanentemente para sustentar cualquier tipo de requerimiento
- Sirven como referencia para futuras auditorías.

Tipos de papeles de trabajo

Archivo permanente: La información que aquí se almacena es toda la documentación de la empresa como son: inventarios, organigramas, planos de red, programas, menús, diagramas del sistema.

Archivo corriente: Se almacena toda la documentación correspondiente al trabajo de auditoría realizado.
En una auditoría los papeles de trabajo se organizan en dos tipos de archivos, Archivo permanente y Archivo Corriente

Archivo permanente: contiene todos los papeles propios del instituto, como son documentación como políticas, organigramas, planos de la red, inventarios, contratos, inventarios facturas procedimientos y manuales de funciones

Archivo Corriente: contiene todos los papeles e instrumentos propios de la auditoría como fuentes de recolección de información como son cuestionarios, listas de chequeo, entrevistas, pruebas, formatos de hallazgos y los informes.

5.3.5 Metodologías de gestión de riesgos

5.3.5.1 ISO/IEC 27005:2011

Su nombre completo es ISO/IEC 27002:2013, es una norma internacional emitida por la ISO (Organización Internacional de Normalización) en conjunto con IEC (Comisión Electrotécnica Internacional), esta norma posee recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la Información. Es compatible con la norma ISO/IEC 27001 y fue diseñada para servir de soporte para la implementación de un SGSI con perfil de gestión de riesgos.

Su versión más reciente fue publicada en el año 2011 y la primera versión se publicó en el año 2008, antiguamente era conocida como la norma ISO13335-2 Gestión de seguridad de la información y la tecnología de las comunicaciones.

5.3.5.2 Metodología NIST SP 800-30

El NIST (National Institute of Standards and Technology) ha creado una serie de publicaciones, entre las cuales está la metodología SP 800, dedicada a la seguridad de la información. Dentro de la cual se incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, la cual se complementa con toda la serie de documentos.

La Metodología NIST SP 800-30, se basa en 9 pasos básicos, los cuales son básicos para realizar el análisis de riesgo:

- Caracterización del sistema.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación del riesgo.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control.

- Resultado de la implementación o documentación

5.3.5.3 Metodología OCTAVE

El método OCTAVE es un método de que se encuentra en la evaluación y la gestión de riesgos garantizando la seguridad del sistema informativo desarrollado por ISO270001, además OCTAVE es un conjunto de principios, atributos y resultados de los cuales se puede desarrollar varias metodologías Octave

- Respecto a lo mencionado anteriormente Octave se divide en dos tipos
- Sistemas, (Hardware. Software y Datos)
- Personas

Respecto a la metodología OCTAVE está formada en tres fases:

- Visión de organización: En esta fase se detecta las exigencias de seguridad y normas existentes como son los activos, vulnerabilidades de organización,
- Visión tecnológica: Son componentes claves y vulnerabilidades técnicas.

5.3.5.4 Metodología MAGERIT

En esta metodología se tiene en cuenta, los riesgos que se derivan del uso de las tecnologías de la información, todas las tecnologías buscan el análisis de riesgos para saber qué tan seguros son o el grado de inseguridad que presentan, por eso es necesario una aproximación metódica fiable que no dependa solamente del analista.

Se puede encontrar los siguientes objetivos en esta fase

- Tomar conciencia de los riesgos a los que se está expuesto y a las necesidades de aportar una solución confiable.

- Verificar el mejor método analizando los riesgos que nos ofrece el uso de las TICS.

- Desarrollar un control para mantener los riesgos bajo nuestro control sin la necesidad de depender de la persona encargada del análisis.
- Siempre se tiene que tener presente los procesos que se hagan y deben conllevar a un proceso de evaluación, auditoria, certificación dependiendo de le caso que se esté manejando, brindando buenos informes dependiendo de los hallazgos y conclusiones de las actividades todos esto representa de un gran valor para los activos de la empresa para lo que se debe tener en cuenta las salvaguardas existentes en relación al riesgo que se pueda afrontar todo esto para proteger al sistema de posibles amenazas.

En la actualidad, todas las empresas se han venido incluyendo en el mundo de la tecnología , todo esto para no quedarse atrás en el ámbito competitivo laboral para esto se hace necesario que todas las empresas tengan una buena organización y que utilice la tecnología para tener comunicación en un sistema en red de datos obteniéndola mejor administración de los recursos de la empresa, para todo este proceso de manejo de la red la empresa necesita ser auditada y obtener una evaluación eficiente y eficaz tanto en la parte física como lógica en todo el diseño de la red , instalaciones, cableado estructurado, ups, cuartos de comunicaciones, centros y equipos de cómputo , teniendo en cuenta lo mencionado anteriormente se hace necesario tener un plan estratégico y corporativo que genere a la empresa seguridad y confiablidad en todo el entorno que se maneja

5.3.6 Análisis De Vulnerabilidades

5.3.6.1 herramientas para la evaluación de vulnerabilidades

En todas las organizaciones se utiliza varias herramientas para la evaluación de vulnerabilidades en los cuales se verifican los mecanismos de seguridad que funcionen de la mejor manera además es posible verificar nuevas medidas que se pueda aplicar seleccionando las más adecuadas para la empresa.

Para todo lo mencionado anteriormente se analizan los siguientes aspectos

- Parches del sistema operativo.
- Servicios y aplicaciones instaladas.
- Protocolos y servicios de red.
- Seguridad del sistema de ficheros.
- Control de accesos a los recursos.

- Registro y auditoria de eventos.
- Cuentas de usuarios.
- Configuración de las herramientas de seguridad: antivirus, cortafuegos personales, gestores de coplas de seguridad.

Cuando se utiliza estas herramientas para el análisis y evaluación de vulnerabilidades de un sistema informático, se tiene en cuenta lo siguiente

- Alcance y objetivos de las pruebas a realizar.
- Pruebas de intrusión.
- Herramientas y metodologías adecuadas.
- Actualización periódica de la base de datos para detectar vulnerabilidades.
- Registrar los mejores resultados de todas las pruebas obtenidas.

Uno de los objetivos principales son las conclusiones y Recomendaciones

Finalmente se procede con el Informe técnico detallado, que describe el sistema objeto de estudio y los recursos analizados, las pruebas realizadas, las vulnerabilidades que han sido detectadas y las recomendaciones para mejorar la seguridad del sistema.

Por otra parte, en estos últimos años se han propuesto distintos estándares para asegurar la calidad de los trabajos realizados y su evaluación por parte de terceros:

Existen distintos estándares para asegurar la calidad de los trabajos realizados y la evaluación de terceros.

ejemplo, OSSTMM (Open Source Security Testing Methodology Manual) del ISECOM (Institute for Security and Open Methodologies) manual con una serie de secciones compuestas por nódulos que incluyen las distintas pruebas que se podrían realizar en una auditoría técnica de seguridad: seguridad física, seguridad de la información, seguridad de los procesos, seguridad de las tecnologías de Internet seguridad en comunicaciones inalámbricas.

Se podría recomendar OWASP (Open Web Application Security Project) evalúa la seguridad de las aplicaciones Web.

Se Podría utilizar para identificar las vulnerabilidades la herramienta estándar llamada CVE (Common Vulnerabilities and Exposures, Vulnerabilidades y Exposiciones Comunes), se encarga de asignar un identificador único a cada vulnerabilidad publicada, facilitando de este modo su seguimiento y Control.

También se ha propuesto llevar a cabo una categorización de vulnerabilidades según el formato Common Advisory Format Description del EISPP (European Information Security Promotion Programme), publicado en mayo de 2004.

5.3.7 Ejecución de Test de penetración en el Sistema

Se puede evaluar en un sistema informático mediante los Test de Penetración que representan una valiosa herramienta metodológica.

- Reconocimiento del sistema para averiguar qué tipo de información podría obtener un atacante o usuario malicioso.

- Escaneo detectando y verificando las vulnerabilidades.
- Penetración: intento de explotación de las vulnerabilidades detectadas.
- Generación de informes, con el análisis de los resultados que conllevan a unas conclusiones.

Los Test de Penetración Externos se realizan desde el exterior de la red aplicando protocolos estandarizados mediante pruebas de escaneo pruebas de usuarios y políticas de contraseña por otra parte se debe evaluar los intentos de ataque, intentos de conexión vía Internet, líneas telefónicas, centrales telefónicas o redes inalámbricas.

Se puede Mencionar algunas aplicaciones comerciales y freeware que permiten llevar a cabo la evaluación de vulnerabilidades y los tests de penetración.

Una de las más importantes es Nessus esta es una herramienta construida en un código abierto para los sistemas Unisx y Windows permitiendo definir pruebas de vulnerabilidad (www.nessus.org), Whisker (reemplazada-por Nikto en 2003), SATAN (Security Analysis Tool for Auditing Networks), [55 (Internet SecurIty Scanner), Retina (www.eEye.com) FoundStone (www.foundstone.com) 0 SPIKE (www.immunitysec.com).

5.3.8 ANÁLISIS DE CAJA NEGRA Y DE CAJA BLANCA

Los tests de penetración pueden ser realizados de dos maneras distintas:

5.3.8.1 Análisis de "caja negra"

En los test de caja negra el equipo de auditoria trata de replicar los métodos de explotación de vulnerabilidades que podría utilizar un atacante externo, y por este motivo solo dispone de información pública sobre el sistema informático que se va a analizar.

El equipo de auditoría, no debe descuidar la existencia de algunas vulnerabilidades parciales del sistema.

5.3.8.2 Análisis de "caja blanca"

En los test de caja blanca el equipo de auditoría tiene toda la información previa necesaria para evaluar la seguridad del sistema.

Como principales objetivos se obtienen los siguientes.

- La configuración de los elementos de red.
- Documentación técnica sobre las medidas de seguridad implantadas.
- manuales de uso.
- Archivos de configuración de los servidores y aplicaciones.
- Búsqueda de fallos de diseño y programación.
- Revisión de las configuraciones potencialmente peligrosas.

Como conclusión principal se puede decir que el test de caja blanca requiere de un buen análisis, colocando un mayor esfuerzo por parte del equipo de Auditoria dando recomendaciones precisas para corregir las vulnerabilidades encontradas.

5.3.9 Contraste de vulnerabilidades e informe de auditoría

Tras realizar el análisis de vulnerabilidades con los diferentes test de penetración seleccionado previamente, el equipo de auditoria procede a realizar la verificación de las distintas vulnerabilidades y errores de diseño o configuración detectados en el sistema.

Para lo cual se elabora un informe, donde se presenta de manera detallada cada uno de los test de penetración realizados.

- Listado de vulnerabilidades y tipos de ataque que han sido probados.
- Listado de vulnerabilidades detectadas en el sistema informático.
- Listado de los dispositivos (servidores, elementos de red, equipos informáticos), servicios y aplicaciones que son vulnerables.
- Valoración del nivel de riesgo que representa cada una de las vulnerabilidades detectadas para la organización.
- Listado de las herramientas y técnicas utilizadas en el análisis de las distintas vulnerabilidades.

5.4 Marco Conceptual

Dentro de las variables que se va a medir con el desarrollo del proyecto se encuentran las características de la información que se contemplan en la ISO 27001, entre ellas están las siguientes:

5.4.1 Confidencialidad

Es la propiedad de la información que dice que los datos deben estar disponible y no ser divulgada a personal no autorizado. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

5.4.2 Disponibilidad

Es la propiedad de la información la cual dice que siempre debe estar disponible y utilizable cuando sea requerido. Según [ISO/IEC13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

5.4.1 Integridad

Es la propiedad de la información que consiste en la salvaguardia, exactitud e integridad de los datos contenidos en cualquier medio de almacenamiento Integridad. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

5.5 MARCO LEGAL

5.5.1 Ley 1273 del 5 de enero de 2009

Colombia ha sido uno de los pioneros en Latinoamérica en cuanto a la legislación de seguridad informática se refiere con la puesta en marcha de la ley 1273 del 5 de enero de 2009.

“Por medio de la 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". 4.

Con la ley 1273 del 5 de enero del 2009, se crea una norma encaminada a proteger uno de los activos más importantes de las empresas como son los datos informáticos y sistemas de información, entre los delitos que tipifica se encuentra los siguientes:

Artículo 269A: Acceso abusivo a un sistema informático toda persona que acceda a un sistema informático y permanezca en el sin autorización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación incurrir en este delito toda persona que sin estar autorizado no permita el acceso a una red, sistema informático o los datos informáticos.

Artículo 269C: Interceptación de datos informáticos incurrirá en este delito toda persona que sin tener orden judicial intercepte ya sea en su origen, trasmisión, destino o al interior de un sistema informático los datos informáticos.

Artículo 269D: Daño Informático este delito contempla que toda persona quien no tenga la debida autorización que borre, altere, suprima o modifique datos informáticos o dentro de un sistema sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso aquí se contempla como delito la producción, tráfico, venta, distribución importación o exportación de software considerado como dañino o malicioso

---

[4] Ley 1273 de 5 de enero de 2009 tomado de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

Artículo 269F: Violación de datos personales, incurrirá en este delito toda persona que obtenga beneficio para sí mismo o para terceros de información personal contenida en bases de datos, ficheros.

Artículo 269G: Suplantación de sitios web para capturar datos personales, este delito contempla el diseño, creación distribución o venta de sitios web, enlaces o ventanas emergentes diseñados para capturar ilegalmente datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes, incurrirá en este delito toda persona que a través de un sistema informático, red de un sistema electrónico o telemático cometa hurto.

Artículo 269J: Transferencia no consentida de activos. Este delito contempla la trasferencia no autorizada de activos en perjuicio de otra persona, mediante manipulaciones de tipo informático.

Entre los delitos más comunes en Colombia se encuentran: Hurto por medios informáticos y semejantes, Uso de software malicioso, Violación de datos personales, Acceso abusivo a un sistema informático

5.5.2 Ley 1150 de 2007

Medios y Sistemas Electrónicos. Introduce modificaciones a la Ley 80 de 1993, y dicta disposiciones generales aplicables a toda contratación con recursos públicos. Establece que las actuaciones, la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual, podrán tener lugar por medios electrónicos.

5.5.3 Ley 1341 de 2009

Establece que la Comisión de Regulación de Telecomunicaciones -CRT, de que trata la Ley 142 de 1994, se denominará Comisión de Regulación de Comunicaciones (CRC), Unidad Administrativa Especial, con independencia administrativa, técnica y patrimonial, sin personería jurídica adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

5.5.4 Ley 527 de 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones5.

Comercio Electrónico

Reglamentación. Aplicación jurídica de los mensajes de datos, art. 6 a 14. Comunicación de mensajes de datos, art. 14 a 25.

Firmas Digitales

Concepto, Características y Uso. Ámbito de aplicación, art. 1. Definiciones, art. 2. Firmas digitales, certificados y entidades de certificación, art. 28 a 42.

Mensajes De Datos

Reglamentación. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación. Dicta disposiciones sobre la aplicación de los requisitos jurídicos de los mensajes de datos y comunicación de los mensajes de datos.

Telecomunicaciones

Mensajes de Datos y Documentos Electrónicos. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación. Dicta disposiciones sobre la aplicación de los requisitos jurídicos de los mensajes de datos y comunicación de los mensajes de datos.

5.5.5 Ley 37 De 1993

ARTÍCULO 5. INVERSIÓN EXTRANJERA EN TELECOMUNICACIONES.
La inversión extranjera, en las materias reguladas por la presente ley, valor agregado, servicio e infraestructura satelital, se regirá por la Ley 9a de 1991 (Por la cual se dictan normas generales a las que deberá sujetarse el Gobierno Nacional

[5] Ley 527 de 1999 http://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

para regular los cambios internacionales y se adoptan medidas complementarias) y las normas que la modifiquen o complementen y no tendrán más limitaciones que las señaladas en esas disposiciones.

5.5.6 LEY 72 DE 1989

Por la cual se definen nuevos conceptos y principios sobre la organización de las telecomunicaciones en Colombia y sobre el régimen de concesión

6. MARCO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

El proyecto que se va a desarrollar es de enfoque cuantitativo, teniendo en cuenta que se pretende medir las variables de seguridad de la información en la red.

El proyecto tendrá los siguientes tipos de investigación:

- **Exploratoria,** el objetivo Principal de este tipo de investigación es permitir una mejor compenetración y comprensión del problema, el proyecto se ajusta a este tipo de investigación por cuanto se pretende descubrir las vulnerabilidades amenazas y riesgos en la red del IDSN.

- **Descriptiva,** su objetivo es describir situaciones y eventos, buscando especificar las propiedades importantes o cualquier otro fenómeno que sea sometido a análisis, el proyecto se ajusta a este tipo de investigación porque presenta medir confiabilidad, disponibilidad y confidencialidad de la red en cuanto a la seguridad.

6.2 UNIVERSO Y MUESTRA

El universo lo conforman los 200 usuarios internos que integran la planta de trabajo y que se conectan a la red del instituto departamental de salud de Nariño, distribuido entre personal de plata y contratistas, para la muestra se seleccionarán cinco usuarios, los cuales se escogieron porque tienen mayor experiencia en el manejo y el estado de seguridad de la red del IDSN, los cuales fueron:

- Gustavo Cuellar, coordinador de la oficina de sistemas.
- Horacio Guerra, administrador web.
- Marcial Muñoz, ingeniero desarrollador
- Jorge Paz, tecnólogo de BDUA
- Jesús Rosero, tecnólogo soporte y mantenimiento.

6.2.1 Fuentes de Recolección de la Información

Para el desarrollo se utilizará de fuentes primarias y secundarias, como se describe a continuación:

- **Primarias:** La primera fuente de información será a través de las visitas a las instalaciones de la red del IDSN y mediante el contacto con el personal que maneja la red de datos, la recolección de la información será mediante entrevistas, cuestionarios y listas de chequeo, las cuales permitirán conocer el estado de la red del IDSN.

- **Secundarias:** Como fuentes de información secundaria se utilizarán manuales técnicos, normas ISO, metodologías y documentos como libros de auditoría y seguridad informática, revistas, artículos, archivos multimedia consultados a través de Internet, ensayos, blogs y páginas web que hagan relación a la auditoría a la seguridad informática de las redes y pruebas de pentesting.

6.2.2 Técnicas e instrumentos

- Entrevistas para conocer y profundizar en temas relacionados con la red de datos en cuanto a la documentación, manejo y administración, las entrevistas se aplicarán al coordinador de la oficina de sistemas y algunos usuarios como los ingenieros que manejan los aplicativos de las líneas de salud.
- Listas de chequeo para determinar que controles existen dentro de la seguridad en la red.
- Pruebas de Pentesting para evidenciar las vulnerabilidades y amenazas existentes en la red.
- Cuestionarios para confirmar la existencia de riesgos en la red.

6.3 METODOLOGÍA DE DESARROLLO

- Objetivo 1: Conocer la red de datos para verificar las vulnerabilidades, riesgos y amenazas existentes.

Actividades:

- Realizar una visita de campo para conocer la infraestructura de la red de datos y el hardware que la soporta.
- Solicitar la documentación de la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos, entre la información que se solicitara están los siguientes documentos:

    - Planos de la red de datos
    - Inventario de la red.
    - Manual de funciones del administrador de la red
    - Manual interno de funciones
    - Organigrama de la dependencia
    - Descripción los puestos de trabajo relacionados con el manejo de la red.
    - Reporte de fallas e incidentes
    - Manual de procedimientos para configurar un servicio en la red
    - Copia del contrato de servicios de internet
    - Plan de mantenimiento de la red.
    - Planes de contingencia relacionados con la red

- Realizar unas entrevistas con el administrador de la red y algunos de los usuarios que permita identificar algunos de los problemas de seguridad en la red de datos.

- Objetivo 2: Elaborar el plan de auditoría, diseñar los instrumentos y el plan de pruebas que se ejecutará sobre la red de datos.

  Actividades:

- Determinar los puntos que serán evaluados.
- Identificar y seleccionar los métodos, pruebas y procedimientos necesarios.

- Objetivo 3: Ejecutar las pruebas y aplicar los instrumentos que permitan evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes.

Actividades

- Ejecutar las acciones programadas.
- Aplicar las pruebas e instrumentos seleccionados.
- Elaborar el dictamen preliminar.
- Organizar los papeles de trabajo de la auditoría

- Objetivo 4: Mostrar los resultados en el informe final.

Actividades

- Examinar la información y los resultados obtenidos en las pruebas.
- Preparar el dictamen final
- Presentar el informe de auditoría a la dirección del IDSN.

6.4 PRODUCTO A ENTREGAR

En la etapa final de la auditoría se realizará el informe final, el cual es un documento técnico que contendrá todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa con los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo.

Este informe se presentará y se entregará al coordinador del área de sistemas, la cual hace parte de la oficina de planeación, del Instituto Departamental de Salud de Nariño para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

7. DESARROLLO DEL PROYECTO

7.1 ETAPA DE PLANEACIÓN

7.1.1 ARCHIVO PERMANENTE

Contiene aquella información de naturaleza histórica o continua y que conserva su importancia a través de los años. Este legajo incluye: la descripción del entorno organizacional, los servicios que soporta la red, organigrama de la Oficina de sistemas y el manual de funciones.

7.1.1.1 Entorno organizacional:

Oficina asesora de Planeación tiene a su cargo la oficina de sistemas, la oficina de sistema tiene la siguiente estructura organizacional: un profesional especializado quien es coordinador de la oficina de sistemas , dos profesionales universitarios uno de ellos tiene a su cargo la administración Web de internet e intranet y el manejo de SYSMAN, y el otro profesional se encarga del desarrollo de aplicaciones, en el siguiente nivel hay dos tecnólogos de sistemas, quienes se encargan del manejo de la Base única de afiliados BDUA y soporte y mantenimiento, esto en cuanto se refiere al personal de planta, en cuanto a contratación existen 8 ingenieros externos que soportan el proceso de cargue de información, evaluación y valoración de sistemas de información en cada una de las líneas de salud.

El IDSN tiene un sistema de gestión de calidad, el cual exige que toda la información debe estar organizada, por lo anterior se llevan los siguientes procesos: la consolidación de base de datos, el análisis de información, desarrollo y soporte a sistemas de información, y como procesos asociados tiene los siguientes: procedimiento de copias de seguridad, publicación y mecanismos de divulgación de información.

La red de instituto tiene una topología hibrida que esta soportado en 10 servidores, y la cual se conectan internamente 200 terminales, distribuidos así: 180 equipos de escritorio y 20 portátiles.

Figura 5. Organigrama Oficina de Sistemas IDSN

Fuente: Autor

La Oficina de sistemas funcionalmente está tiene a los siguientes profesionales:

Tabla 1. Funciones del coordinador de la oficina de Sistemas.

COORDINADOR
PROFESIONAL ESPECIALIZADO
Coordinar los componentes de TICs: Sistemas de Información, RIPS, redes, comunicaciones, seguridad de la información, soporte y desarrollo tecnológico del IDSN.
Administrar el Sistema Integral de Información en Salud garantizando oportunidad y veracidad en el mismo.
Administrar los Servidores que soportan las Bases de Datos y Sistemas de Información del IDSN.
Asesorar los niveles superiores en la proyección de las políticas y normas relacionadas con el Tecnologías de la Información y las Comunicaciones - TICs.
Coordinar el mantenimiento, actualización, capacitación y asesoría en el manejo de los Sistemas de Información en Salud de la institución.
Apoyar y asesorar a las dependencias del Instituto Departamental de Salud de Nariño y a los municipios e instituciones del sector salud en la formulación de proyectos relacionados con el desarrollo de sistema de información en salud.

Fuente: Autor

Tabla 2. Funciones del Administración de la red de datos.

Administración de la red de datos e Internet
PROFESIONAL UNIVERSITARIO 1
Formular, presentar, ejecutar y asesorar proyectos relacionados con el desarrollo de los Sistemas de Información.
Monitorear y controlar los proyectos relacionados con el Sistema de Información de todas las áreas del IDSN.
Prestar soporte, actualización y mantenimiento de los sistemas de información desarrollados en el IDSN.
Asesorar los niveles superiores en la proyección de las políticas y normas relacionadas con el Sistema de Información.

Fuente: Autor

Tabla 3. Funciones del Desarrollador.

Desarrollador
PROFESIONAL UNIVERSITARIO 2
Funciones
Formular, presentar, ejecutar y asesorar proyectos relacionados con el desarrollo de los Sistemas de Información.
Monitorear y controlar los proyectos relacionados con el Sistema de Información de todas las áreas del IDSN.
Prestar soporte, actualización y mantenimiento de los sistemas de información desarrollados en el IDSN.
Asesorar los niveles superiores en la proyección de las políticas y normas relacionadas con el Sistema de Información.

Fuente: Autor

Tabla 4. Funciones del Administrador de la Base Única de Afiliados (BDUA).

Administrador de la Base Única de Afiliados (BDUA).
TÉCNICO OPERATIVO 1
Funciones

Realizar la validación de la Bases de Datos Única de Afiliados - BDUA y generar reportes de inconsistencias y múltiples afiliaciones para EPS y DLS.
Prestar asistencia técnica y mantener actualizados a los actores en salud en las normas y procedimientos que se expidan para el manejo de las bases de datos del régimen subsidiado.
Prestar apoyo trasversal al cruce de base de datos institucionales
Generar informes del estado de aseguramiento del departamento de Nariño.
Apoyar a los entes municipales en el envío oportuno de reporte de novedades ante el consorcio SAYP.
Apoyo a los entes territoriales en la generación de la Base de Datos de Población Pobre No Asegurada. - PPNA

Fuente: Autor

Tabla 5. Funciones del Encargado de Soporte y mantenimiento

Encargado de Soporte y mantenimiento
TÉCNICO OPERATIVO 2
Funciones
Brindar soporte técnico informático (hardware, software u otros bienes electrónicos o mecánicos) a los funcionarios públicos de la sede principal del IDSN y sus sedes alternas.
Ejecutar el plan de mantenimiento preventivo y correctivo de los equipos de cómputo del IDSN.
Llevar el inventario de Hardware y Software (licenciamiento) de Software asociado a los computadores tales como sistemas operativos y herramientas de ofimática.
Brindar capacitación a los funcionarios públicos del IDSN en el manejo de herramientas de Ofimática, antivirus, acceso a páginas web y comunicación a través de dispositivos móviles.

Fuente: Autor

7.1.1.2 Procesos

En la gráfica 1 se indican los diferentes procesos que se maneja en la oficina de sistemas del Instituto Departamental de Salud de Nariño IDSN.

Figura. 4 Grafica de Procesos IDSN

Fuente: intranet IDSN

Descripción de los Procesos que maneja la oficina de sistemas del IDSN y que son soportados en la sobre la red, los cuales son los siguientes:

Tabla 6. Procesos Oficina de Sistemas IDSN

Procesos Oficina de Sistemas IDSN
1. Proceso Desarrollo y actualización de software
El procedimiento de Desarrollo de Software se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas), está orientado a fortalecer el uso y aplicación de las Tecnologías de la Información

y las Comunicaciones TICs del Departamento a través de los sistemas de información, están dirigido a todos los usuarios del Sistema de Salud.

Para el desarrollo de este procedimiento se requiere contar con:

- Infraestructura Tecnológica Actualizada
- Normatividad en salud.
- Solicitudes de información por parte de los actores del SGSSS y de los procesos internos del IDSN
- Bodega de datos IDSN

En este proceso se encuentra contemplado el desarrollo de software y actualización de los desarrollos propios del IDSN, entre los que están:

- SIVEFRONTERA
- Reportes - SIIS
- Resolución 4505
- IAMI - AIEPI
- AIEPI Comunitario
- Salud Sexual y Reproductiva
- Salud Ambiental
- CRUE
- Riesgos y Accidentes de Trabajo
- Salud Oral
- RIPS
- Crónicas - ECNT
- Salud Mental
- Licencias Salud Ocupacional
- Registro de Profesionales de la Salud
- Quejas y Reclamos

2. Proceso Administración de respaldos y recuperación

El procedimiento de administración de respaldos y recuperación se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas), está orientado a fortalecer el uso y aplicación de las Tecnologías de la Información y las Comunicaciones TICs del Departamento a través del uso de los sistemas de información, salvaguardando la integridad de la información.

Condiciones Generales

- Acceso a servidores de aplicativos, bases de datos, pagina web y correo electrónico.
- El servidor debe estar configurado para aceptar accesos bajo el protocolo SSH y/o escritorio remoto.

3. Proceso Soporte de Software

El procedimiento de Soporte de Software se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas), está orientado a brindar apoyo y soluciones a los diferentes tipos de software administrados en el Instituto Departamental de Salud de Nariño.

Condiciones Generales

- Adopción de Tecnologías de la Información y la Comunicación TIC´s. Mejoramiento basado en las nuevas tecnologías.
- Fortalecimiento de las comunicaciones internas del IDSN.
- Fortalecimiento de las comunicaciones entre el IDSN y los actores del Sistema General de Seguridad Social en Salud.
- Implementar mecanismos que faciliten la comunicación de las acciones del IDSN.

4. Proceso Análisis de indicadores

Este procedimiento se aplica en el proceso Administración del Sistema Integral de Información en Salud para el análisis de la información producida en el IDSN

Condiciones Generales

- Coordinación con los actores de los sistemas de información para el fortalecimiento de los procedimientos de validación de la información
- Diseñar metodologías técnicas que permitan hacer una evaluación de la calidad de los datos contenida en las bases de datos de los sistemas de información del IDSN
- Identificar las Unidades Primarias Generadoras de Datos (UPGD) de cada uno de los sistemas de información
- Evaluar la cobertura en el reporte de datos para cada uno de los sistemas de información

5. Proceso Administración del sitio web

Este documento se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas) y está orientado a fortalecer la imagen corporativa del Instituto Departamental de Salud de Nariño haciendo uso y aplicación de las Tecnologías de la Información y las Comunicaciones TICs del Departamento

Condiciones Generales

- Adopción de nuevas tecnologías informáticas. Mejoramiento basado en las nuevas tecnologías. Fortalecimiento de las comunicaciones internas del IDSN.
- Fortalecimiento de las comunicaciones entre el IDSN y los actores del Sistema General de Seguridad Social en Salud.
- Implementar mecanismos que faciliten la comunicación de las acciones del IDSN.

6. Proceso Administración de redes

Este documento se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas) y está orientado a fortalecer el uso y aplicación de las Tecnologías de la Información y las Comunicaciones TICs del Departamento

Condiciones Generales

- Adopción de Tecnologías de la Información y la Comunicación TICs. Mejoramiento basado en las nuevas tecnologías.
- Fortalecimiento de las comunicaciones internas del IDSN.
- Fortalecimiento de las comunicaciones entre el IDSN y los actores del Sistema General de Seguridad Social en Salud.
- Implementar mecanismos que faciliten la comunicación de las acciones del IDSN.

7. Proceso Administración de BDUA

Este procedimiento se aplica a Direcciones Locales de Salud, quienes presenten inconvenientes en el reporte de novedades de acuerdo a la Resolución 1344 de 2012 a través de la plataforma WEB de FOSYGA, descargar archivos FTP, actualización de la Base de Datos del Software “BuscaAfiWeb” y generación de informes con la BDUA, este proceso es aplicable por la oficina de Planeación –

Sistemas, del Instituto Departamental de Salud de Nariño como parte del proceso de Planificación y desarrollo del sistema territorial de salud.

Condiciones Generales

- Suministro de Archivos de Novedades de acuerdo a la Resolución 1344 de 2013 por parte de aquellos municipios que tienen dificultad con la plataforma WEB de FOSYGA, Suministro de archivos por parte del Consorcio SAYP a través del FTP asignado para el Departamento de Nariño.

- Herramientas tecnológicas para almacenamiento, validación, cargue, análisis de información y generación de informes estadísticos.

8. Administración de RIPS

El procedimiento de Administración de RIPS se aplica en el proceso de Planificación y Desarrollo del Sistema Territorial en Salud (Área de Sistemas), está orientado a consolidar la base de datos de prestación de servicios de salud contratado y autorizado por el Instituto Departamental de Salud de Nariño.

CONDICIONES GENERALES

- Adopción de Tecnologías de la Información y la Comunicación TICs. Software validador y manejador de bases de datos

- Fortalecimiento de las comunicaciones entre el IDSN y los actores del Sistema General de Seguridad Social en Salud.

- Implementar mecanismos que faciliten la comunicación de las acciones del IDSN.

Fuente: Autor

7.1.2 ARCHIVO CORRIENTE

Para realizar la auditoría a la seguridad de la red del IDSN, se hizo una recopilación de documentos que sirvieron para su desarrollo.

7.1.2.1 PLAN DE AUDITORÍA

Objetivo General

Evaluar la seguridad y revisar el tráfico en la red para determinar que vulnerabilidades, amenazas y riesgos existen en la prestación de los servicios que están soportados en la red.

Objetivos Específicos

- Conocer la red de datos del instituto departamental de salud de Nariño para verificar las vulnerabilidades, riesgos y amenazas existentes, lo que servirá como soporte para determinar el estado actual de la seguridad tanto física como lógica dentro de la institución.

- Elaborar el plan de auditoría donde se incluya el objetivo y alcances, la metodología, los recursos necesarios para llevarla a cabo, diseñar los instrumentos y el plan de pruebas que se ejecutará sobre la red de datos para determinar las causas de los problemas.

- Ejecutar las pruebas y aplicar los instrumentos que permitan evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes, los recursos afectados y las causas que los originan para proponer los controles adecuados para mitigarlos.

- Mostrar los resultados en el informe final para identificar los niveles de madurez en cada dominio evaluado, los hallazgos confirmados, los controles adecuados para establecer las políticas y procedimientos que permitan mitigarlos.

Alcance

Este trabajo de auditoría de sistemas se dividirá en dos partes las cuales son:

- El análisis del tráfico de la red.

- La evaluación de la seguridad de la red.

En el análisis del tráfico de la red, se revisará lo siguiente:

- Las restricciones
- Pruebas en el día para analizar las horas pico
- Restricciones de acceso a páginas de uso no institucional
- Controles en cuanto al tráfico.
- Dispositivos móviles dentro de la red
- Controles de usuarios

En la evaluación de la Seguridad de la red se revisa lo siguiente:

- Niveles de acceso de cada usuario
- La administración de la red
- Realización de pruebas entre las que se encuentran
    - Pruebas de intrusión
    - Pruebas de testeo

Metodología

Para conocer la red de datos se realizar las siguientes actividades:

- Realizar una visita de campo para conocer la infraestructura de la red de datos y el hardware que la soporta.
- Solicitar la documentación de la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos.
- Realizar una entrevistas con el administrador de la red y algunos de los usuarios que permita identificar algunos de los problemas de seguridad en la red de datos.

Para realizar la planeación de la auditoría se realizaran las siguientes actividades:

- Determinar los puntos que serán evaluados.
- Identificar y seleccionar los métodos, pruebas y procedimientos necesarios.

Para realizar la ejecución de la auditoría se realizaran las siguientes actividades:

- Aplicar las pruebas e instrumentos de recolección de la información seleccionados.
    - Pruebas de intrusión
    - Pruebas de testeo

- Análisis y evaluación de riesgos.
- Organizar los papeles de trabajo de la auditoría

Para presentar los resultados de la auditoría se realizaran las siguientes actividades:

- Realizar la lista de hallazgos y con las causas que los originan.
- Realizar el informe final de auditoría con políticas y procedimientos de seguridad para la red.

Recursos

Talento Humano

La auditoría se llevará a cabo por los estudiantes de la especialización en seguridad Informática:

- Javier Orlando Mesías Narváez
- Diego Fernando Rosero Almeida.

También se contara con la colaboración de los ingenieros Gustavo Cuellar, coordinador de la oficina de sistemas del IDSN y del ingeniero Francisco Nicolás Solarte, tutor y asesor académico del grupo de Estudio CIPAS Auditores.

Físicos

En el área de la oficina de sistemas donde se encuentra el área de redes y comunicaciones

Recursos Tecnológicos

Hardware

- 2 Computadores portátiles.
- Impresora multifuncional
- Dispositivos de almacenamiento USB
- Grabadora de voz audio.
- Cámara de video.

- Cámara fotográfica.

Software

- Procesadores de texto.
- Herramienta para escanear puertos
    - Superscan versión 3.0 herramienta de uso libre de McAfee
    - Advanced IP Scanner Versión 2.4.2601 herramienta de uso libre
    - https://incloak.es/ports/ herramienta online
    - www.cmyip.com herramienta online
    - http://www.t1shopper.com/tools/port-scan/ herramienta online
- Suite Kali Linux, versión 2016 1, herramienta de software libre con más de 300 aplicaciones para pruebas de penetración, entré las herramientas que se aplicara están:
    - Nmap
    - Metasploit
    - Wireshark

Documentos y Manuales Técnicos.

- Magerit Metodología de análisis y gestión de riesgos.
- Norma ISO/IEC 27001, Norma ISO/IEC 27002, Norma ISO/IEC 27005
- Reglamento Técnico de Instalaciones Eléctricas – RETIE.

- Tabla 7. Presupuesto de auditoria

Presupuesto			
Cant.	Descripción	Precio Unitario	Precio Total
2	Computadores.	2000000	$4,000,000
2	Impresora multifuncional.	400000	$800,000
2	USB	20000	$40,000
1	Resma de papel carta	8000	$8,000
100	DVDs. Torre	20000	$20,000
1	ISO/IEC 27001, ISO/IEC 27002	145000	$145,000
1	Grabadora de audio.	250000	$250,000
1	Cámara de video.	500000	$500,000
1	Cámara fotográfica.	1000000	$1, 000,000
2	Auditor 1 (valor Mensual)	2000000	$16, 000,000
Presupuesto Total			$23.363.000

Fuente: Autor

Nota aclaratoria: Los costos de la auditoría serán asumidos en su totalidad por los ingenieros Javier Orlando Mesías Narváez y Diego Fernando Rosero Almeida.

Tabla 8. Cronograma de actividades

ACTIVIDAD	MES 1				MES 2				MES 3				MES 4				MES 5				MES 6			
	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4
Vista preliminar al área que será evaluada.																								
Solicitar la documentación de la red																								
Realizar entrevistas																								
Determinar los puntos que serán evaluados.																								
Identificar y seleccionar los métodos, pruebas y procedimientos necesarios																								
Aplicar las pruebas e instrumentos seleccionados.																								
Organizar los papeles de trabajo de la auditoría																								
Examinar la información y los resultados obtenidos en las pruebas.																								
Preparar el Informe final																								
Presentar el informe de auditoría a la dirección del IDSN.																								
Documentación																								

Fuente: Autor

7.1.2.2 PROGRAMA DE AUDITORÍA:

En el programa se define el estándar que se va aplicar, que para este caso es la ISO 27001, se seleccionan los dominios dentro del estándar y se asignan al grupo auditor para ser evaluados a continuación se muestra la selección de los dominios que serán aplicados a la auditoría a la seguridad de la red

Dominios de la ISO 27001

La versión 2013 del estándar describe catorce dominios principales, de los cuales se seleccionaron para el desarrollo de la auditoría los siguientes:

A5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

A6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguridad de la información.
6.1.2 Segregación de tareas.

A9. Control de Accesos.

A9.1 Requisitos de negocio para el control de accesos.
A9.1.2 Control de acceso a las redes y servicios asociados.

A9.4 Control de acceso a sistemas y aplicaciones.
A9.4.1 Restricción del acceso a la información.

A13. Seguridad en las Telecomunicaciones.

A13.1 Gestión de la seguridad en las redes.
A13.1.1 Controles de red.
A13.1.2 Mecanismos de seguridad asociados a servicios en red.

7.1.2.3 PLAN DE PRUEBAS

En este documento se hace una descripción de las herramientas que se utilizaran para realizar las diferentes pruebas sobre la red.

Tabla 9. Plan de pruebas

Herramienta	Descripción de la prueba	Quien Ejecutó la Prueba	Prueba Propuesta
Nmap	Sirve para detectar puertos abiertos y servicios activos	Ing. Javier Mesías N.	
Zenmap	Sirve para detectar puertos abiertos y servicios activos	Ing. Diego Rosero A.	
Wireshark	Es un analizador de paquetes		X
OWASP Zed Attack	Permite realizar un testeo de vulnerabilidades	Ing. Diego Rosero A.	
Superscan versión 3.0 herramienta de uso libre de McAfee	Herramienta para escanear rangos IP y puertos	Ing. Javier Mesías N	
Advanced IP Scanner Versión 2.4.2601 herramienta de uso libre	Herramienta que permite realizar un Escaneo de la red	Ing. Diego Rosero A.	
https://incloak.es/ports/ herramienta online	Herramienta online para escanear puertos	Ing. Diego Rosero A.	
www.cmyip.com herramienta online	Herramienta online para conocer las IPs	Ing. Javier Mesías N	
http://www.t1shopper.com/tools/port-scan/ herramienta online	Herramienta online para escanear puertos	Ing. Diego Rosero A.	

Fuente: Autor

7.1.2.4 DISEÑO DE INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para realizar el proceso de auditoría al IDSN, se utilizaron diferentes instrumentos de recolección de información, a continuación, se describe cada uno de ellos:

Formato fuentes de conocimiento

Este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios de la norma ISO 27002, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios la norma ISO 27002 que se está revisando.

MATERIAL DE SOPORTE: En este espacio se indicará el nombre del material que soporta el proceso, para el caso será la norma ISO 27002.

DOMINIO: Espacio reservado para colocar el nombre del dominio de norma ISO 27002 que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios de la norma ISO 27002.

FUENTES DE CONOCIMIENTO: En este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoría lo que servirá como respaldo del proceso.

REPOSITORIO DE PRUEBAS: Se divide en dos tipos de pruebas:

DE ANÁLISIS: Este espacio está destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Este espacio está destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Tabla 10. Formato de Fuentes de conocimiento

CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS DE AUDITORIA	REF.

ENTIDAD AUDITADA		PAGINA		
		1	DE	1
PROCESO AUDITADO	Seguridad de la red de datos			
RESPONSABLE				
MATERIAL DE SOPORTE	ISO 27002			
DOMINIO				
PROCESO				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
Documento, o persona que tiene la información que necesita el auditor	Pruebas que se hacen por análisis de documentos (contratos, manuales) o comparaciones (compara los contenidos de un manual respecto a lo que dice la teoría que debe contener) comparar(la empresa auditada con una empresa certificada)	Pruebas mediante uso de software, pruebas para levantar inventarios, pruebas de seguridad en redes, pruebas de seguridad en bases de datos, pruebas de intrusión, pruebas de testeo.

AUDITOR RESPONSABLE:

Fuente: Autor

Formato de lista de chequeo

Las listas de chequeo se utilizan para realizar la verificación de la existencia de controles en el proceso o procesos auditados, en la lista de chequeo se puede aplicar diferentes escalas por ejemplo respuestas cerradas de SI/NO, o respuestas de cumplimiento por ejemplo Cumple Totalmente (CT)/Cumple Parcialmente (CP)/No Cumple (NC).

Las preguntas de las listas de chequeo se deben hacer teniendo en cuenta los objetivos de control, que serán los controles que deben existir en el proceso y se elabora preguntas sobre la existencia de dicho control, el auditor encargado de evaluar el proceso será quien aplique la lista de verificación de controles o lista de chequeo y de acuerdo a la respuesta se determina los hallazgos sobre la no existencia de controles en el proceso.

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**

Lista de chequeo Dominio **Subdominio**

OBJETIVO:

NOMBRE	**CARGO**
	Administrador Red de Datos

Ítem	**Si**	**No**
¿Pregunta 1?		
¿Pregunta 2?		
¿Pregunta 3?		
¿Pregunta 4?		

Elaboro por:		Reviso por	
Entrevistado		Firma del entrevistado	

Formato de entrevista

Las entrevistas pueden ser aplicadas al inicio, en la fase de conocimiento para o también durante fase de ejecución de la auditoria, sirven para identificar los aspectos generales de los procesos que se van a evaluar, usualmente, las entrevistas sirven para recoger la opinión de algunos de los encargados que conozcan el proceso y que puedan responder con claridad las preguntas que se hayan preparado para la entrevista. Es importante determinar a quienes se aplicará la entrevista y los cuestionarios, ya que no se pueden aplicar a todos los auditados únicamente al personal que conozca los aspectos que se vayan a auditar.

Para la entrevista se debe determinar primero los temas sobre los cuales se va a centrar la entrevista y en cada uno de los temas se debe elaborar preguntas puntuales con la intención de descubrir otros riesgos, que ya se hayan detectado en las visitas realizadas a la empresa auditada.

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**
Red de Datos			

ENTREVISTA EVALUACIÓN DE LA RED DE DATOS

OBJETIVO:

NOMBRE	**CARGO**

Cuestionario
1. ¿Pregunta 1?
2. ¿Pregunta 2?
3. ¿Pregunta 3?

Formato de cuestionario cuantitativo

El cuestionario cuantitativo es un instrumento que proporcionar una calificación numérica a un requerimiento, de acuerdo a los procesos, que se realiza la auditoria con el fin de determinar su vulnerabilidad.

El cuestionario cuantitativo contiene los siguientes ítems:

REF: Se refiere al ID del elemento.

FECHA: En este espacio se indicará la fecha de diligenciamiento del instrumento.

ENTIDAD AUDITADA – NOMBRE DE LA AUDITORÍA: En este espacio se indicará el nombre de la entidad y el tipo de auditoría que se está realizando.

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

ELABORO POR: REVISO POR: En este espacio se indicarán los nombres de los miembros del equipo auditor que está llevando a cabo el proceso de auditoría.

DOMINIO: Espacio reservado para colocar el nombre del dominio de la norma ISO 27002, que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios de la norma ISO 27002.

PREGUNTA: Espacio donde se indicara la descripción de la consulta de la cual se indagara.

SI – NO: Posibilidades de respuesta, cumple, no cumple, o no aplica para la entidad.

OBSERVACIÓN: Aclaraciones sobre cada una de las preguntas

PORCENTAJE DE RIESGO: Hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

El cálculo de este porcentaje se hace de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Las equivalencias utilizadas para la puntuación serán de uno a cinco, siendo uno el valor mínimo considerado de poca importancia y cinco el máximo considerado de mucha importancia.

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

Universidad Nacional Abierta y a Distancia	**ENTIDAD AUDITADA**	**REF.**

ÁREA	**D**	**M**	**A**

Cuestionario de control

Dominio	
Proceso	

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Pregunta 1?	3		
¿Pregunta 2?		4	
¿ Pregunta 3?	4		
¿ Pregunta 4?		4	
¿ Pregunta 5?	3		
¿ Pregunta 6?		4	
TOTALES	10	12	

Puntaje Total		22	
Elaboro por:		Reviso por	

Formato de hallazgos

En este formato se describe las inconsistencias o no conformidades encontradas. Esta información será desglosada de la siguiente manera:

REF: Se refiere al ID del elemento.

FECHA: En este espacio se indicará la fecha de diligenciamiento del instrumento.

ENTIDAD AUDITADA – NOMBRE DE LA AUDITORÍA: En este espacio se indicará el nombre de la entidad y el tipo de auditoría que se está realizando.

ÁREA: En este espacio se indicará el área a evaluar

EVALUACIÓN: Se encuentra el tipo de evaluación que se va a realizar.

REFERENCIA DOCUMENTOS: En este ítem se registra el documento que sirve de soporte para el hallazgo o la no conformidad.

PREGUNTA: En este ítem se registra la pregunta que sirve de soporte para el hallazgo o la no conformidad.

DESCRIPCIÓN DE HALLAZGO – NO CONFORMIDAD: Se encuentra la descripción de cada hallazgo.

RIESGO – EVALUACIÓN CAUSA / EFECTO: En este apartado se encuentra la descripción de las consecuencias del hallazgo, así como la su causa y efecto.

RECOMENDACIONES - ACCIÓN CORRECTIVA: En este apartado se hace una descripción de las recomendaciones u acciones correctivas que el equipo auditor presenta a la institución auditada.

EVIDENCIAS: En este último ítem se encuentra el nombre de la evidencia y el número del anexo donde ésta se encuentra.

	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO	**REF.** **R0016**

ÁREA	EVALUACIÓN	D	M	A

FORMATO DE HALLAZGOS

REFERENCIA DOCUMENTOS	PREGUNTA

Descripción de Hallazgo – No Conformidad :

Riesgo – Evaluación Causa / Efecto :

Recomendaciones, Acción Correctiva :

Evidencias :

7.2 ETAPA DE EJECUCIÓN

En esta etapa se aplican los instrumentos de recolección de información que han sido diseñados anteriormente por los auditores y que permiten evaluar cada uno de los dominios con respecto a las vulnerabilidades, amenazas y riesgos existentes, así como para determinar el cumplimiento de los controles de acuerdo a la norma ISO/IEC 27002.

A continuación se muestra cada uno de los instrumentos aplicados en la auditoría y los resultados encontrados:

7.2.1 Entrevistas aplicadas al administrador de la red de datos

Para indagar sobre los temas de las funciones, tareas y actividades relacionadas con la administración de la red de datos de la Institución

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

ENTREVISTA EVALUACIÓN DE LA RED DE DATOS

OBJETIVO:
Indagar al funcionario acerca de las funciones, tareas y actividades relacionadas con la administración de la red de datos de la Institución.

NOMBRE	CARGO
	Administrador Red de Datos

Cuestionario
4. Descripción de la red de datos:

5. ¿Existe el diseño actualizado de la red de datos?

6. ¿Existe un inventario actualizado de todos los dispositivos de la red de datos en el cual se registre la numeración y ubicación geográfica?

7. ¿Se realiza mantenimiento preventivo a los dispositivos de conexión de la red (cajas*, racks, patchs coros, etc.*)?

8. ¿Se lleva un registro del mantenimiento preventivo realizado a los dispositivos y cableado de red. El cual incluya fecha y hora, identificación del equipo, actividades realizadas, novedades, responsable?

9. ¿Se lleva un registro del mantenimiento correctivo de los dispositivos y cableado?

10. ¿Los dispositivos de red están identificados mediante etiquetas externas?

11. El local asignado a los servidores de datos tiene:

a) ¿Aire acondicionado?

b) ¿Cerradura especial?

c) ¿Protección contra el fuego?

d) ¿Se cuenta con detectores de humedad?

e) ¿Detector de intrusos?

12. ¿Se realiza aseo a los *racks*?

13. ¿El cableado de datos va en un canal aparte del cableado eléctrico?

14. ¿Se cuenta con UPS de protección para los equipos servidores?

15. ¿Existen mecanismos que permitan monitorear el tráfico de la red?

16. ¿Existen mecanismos que permitan la detección de intrusos?

17. ¿Existe un mecanismo de encriptación de la información que viaja por la red?

18. ¿Existen mecanismos para controlar el acceso a la red?

19. ¿Herramientas de seguridad implantadas en la red?

20. ¿Se restringe el acceso a sitios de Internet que no tengan relación con las actividades laborales?

21. ¿Se controla el acceso a la sala de equipos?

22. ¿Se permite la conexión de computadores portátiles a la red?

23. ¿la responsabilidad operativa por las redes está separada de las operaciones de computador, según sea apropiado?

24. ¿Existen las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios?

25. ¿Existen controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas?

26. ¿Existen controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados?

27. ¿Se aplican registros y el monitoreo adecuado para permitir el registro de acciones de seguridad pertinentes?

28. ¿Se coordina las actividades de gestión tanto para?

- Optimizar el servicio para la organización.
- garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

Características de los servicios de red:

1. ¿Existe tecnología aplicada para la seguridad de los servicios de red?

- Autenticación.
- Encriptación.
- Controles de conexión de red.

2. ¿Existen parámetros técnicos requeridos para la conexión segura a los servicios de red según las reglas de seguridad y conexión de red?

3. ¿Existen los respectivos procedimientos para la utilización de los servicios de red?

4. ¿Existen los procedimientos necesarios para restringir cuando sea necesario la utilización de:

- El acceso a los servicios de red.
- Las aplicaciones.

Entre los resultados de la entrevista, en los que están los siguientes:

La oficina de sistemas del IDSN no cuenta con el diseño actualizado de la red de datos.

La oficina de sistemas del IDSN no existe un inventario actualizado de todos los dispositivos de la red de datos en el cual se registre la numeración y ubicación geográfica.

No se realiza mantenimiento preventivo a los dispositivos de conexión de la red (cajas, racks, patchs coros, etc.).

No se lleva una bitacora con el registro del mantenimiento preventivo y correctivo realizado a los dispositivos y cableado de red.

Los dispositivos de red no se encuentran debidamente identificados mediante etiquetas externas.

El centro de computo donde se encuentran los servidores de datos no tiene:

- Aire acondicionado.
- Cerradura especial contra intrusos.

- Protección contra el fuego.

- Detectores de humedad.
- Detector de intrusos.

No se realiza aseo periodico a los racks.

El IDSN no cuenta con mecanismos que permitan monitorear el tráfico de la red.

El IDSN no cuenta mecanismos que permitan la detección de intrusos.

El IDSN no cuenta con mecanismos que permitan encriptar la información que viaja por la red.

El IDSN no cuenta con mecanismos para controlar el acceso a la red.

El IDSN no cuenta con herramientas de seguridad implantadas en la red.

El IDSN no restringe el acceso a sitios de Internet que no tengan relación con las actividades laborales.

El IDSN permite la conexión de computadores portátiles a la red.

El IDSN no tiene separada la responsabilidad operativade las redes, de las operaciones de computador.

El IDSN cuenta con las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.

El IDSN no cuenta con controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.

El IDSN no cuenta con tecnología de encriptacion de la informacion aplicada para la seguridad de los servicios de red.

7.2.2 Listas de chequeo

Aplicadas para cada uno de los Dominios del estándar ISO/IEC 27002 para determinar el cumplimiento de los controles especificados en la norma**.**

7.2.2.1 Lista de chequeo Dominio A5. Políticas de Seguridad de la información

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** CRD-01

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A5 Políticas de Seguridad de la Información Subdominio A 5.1.1 A 5.1.2

OBJETIVO:
Brindar orientación y apoyo 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. **Control** Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

NOMBRE	CARGO

Las políticas de la seguridad de la información, fueron creadas con requisitos propuestos por:		
Ítem	**Si**	**No**
¿El área que maneja la estrategia de negocios?		
¿El área que maneja Reglamentaciones, legislación y contratos?		

¿El entorno actual y proyectado hacia las amenazas de la seguridad de la información?		
La política de la seguridad de la información contiene declaraciones concernientes a:		
¿La definición de la seguridad de la información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información?		
¿La asignación de las responsabilidades, generales y específicas para la gestión de la seguridad de la información, a roles definidos?		
¿Procesos para manejar desviaciones y excepciones?		
¿Copias de respaldo?		
¿Transferencia de información?		
¿Protección contra códigos maliciosos?		
¿Gestión de las vulnerabilidades técnicas?		
¿Controles criptográficos?		
¿Seguridad de las comunicaciones?		
¿Privacidad y protección de información de datos personales?		
¿Relación con los proveedores ?		
Las políticas de seguridad incluyen temas como:		
¿Control de acceso?		
¿Clasificación de la información?		
¿Seguridad física y del entorno?		
Temas orientados a los usuarios finales, tales como.		
¿Uso aceptable de los activos?		
¿Políticas de escritorio y pantalla limpia?		
¿Transferencia de información?		
¿Dispositivos móviles y teletrabajo?		
¿Restricciones sobre instalaciones y uso del software?		
¿Se realiza revisión periódica de las políticas de seguridad?		

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

No se aplico la lista de chequeo pa el dominio A5 relacionado PoliticaS de Seguridad de la Informacion, porque en el IDSN, no se encuentran implementadas las politicas de seguridad de la informacion.

7.2.2.2 Lista de chequeo Dominio A6. Aspectos organizativos de la seguridad de la información

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A6
Subdominio A 6.1.1 A 6.112

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.

Control

Se debería definir y asignar todas las responsabilidades de la seguridad de la información.

NOMBRE	CARGO

Se deben establecer las áreas de las cuales son responsables los encargados de la seguridad informática, en particular se efectúa con los siguientes ítems:

Ítem	Si	No
¿Se identifica y define los activos y los procesos de seguridad de la información?		
¿Se asigna en la entidad responsable de cada activo o procesos de seguridad de la información. Y se documenta los detalles de esta responsabilidad?		
¿Se define y documenta los niveles de autorización?		
Para tener la capacidad de cumplir las responsabilidades en el área de seguridad de la información el personal nombrados para estas funciones son:		
• ¿Son competentes en el área?		

• ¿Se brinda oportunidades de mantenerse actualizados con los avances en este tema?			
¿Se identifica y documenta la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores?			
Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

No se aplico la lista de chequeo para el Dominio A6. Aspectos organizativos de la seguridad de la información, porque en el IDSN, no se encuentran implementado, este aspecto en el IDSN.

7.2.2.3 Lista de chequeo Dominio A 9 Control de Acceso

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 9 Control de Acceso
Subdominio A 9.1.2

OBJETIVO:

Verificar el control A 9.1.2 Acceso a redes y a servicios en red, de acuerdo a la norma ISO 27001:2013

Control

Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

NOMBRE	CARGO
	Administrador Red de Datos

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Ítem	Si	No
¿Qué redes y que servicios de red tiene el acceso el usuario autorizado?	X	
¿Los procedimientos de autorización para determinar a quién se permite acceder a las redes y servicios de red?		X
¿Los controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?	X	
¿Los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		X
¿Los requisitos de autenticación de usuarios para acceder a diversos servicios de red?	X	
¿El monitoreo del uso de servicios de red?		X

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida

Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

Entre los resultados de la lista de chequeo Dominio A 9 Control de Acceso Subdominio A 9.1.2, en los que están los siguientes:

- El IDSN no cuenta con procedimientos de autorización para determinar quién tiene acceso a la red y sus servicios.
- El IDSN con cuenta con VPN para acceder a las redes y servicios de red.
- El IDSN no tiene implementado el monitoreo de la red y los servicios que corren por ella.

7.2.2.4 Lista de chequeo Dominio A 9 Control de Acceso

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	**D**	**M**	**A**
Red de Datos			

Lista de chequeo Dominio A 9 Control de Acceso Subdominio A 9.4.1

OBJETIVO:
Verificar el control A 9.4.1 Restricción de acceso a la información, de acuerdo a la norma ISO 27001:2013 **Control** El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

NOMBRE	**CARGO**
	Administrador Red de Datos

Se cuenta con los siguientes requisitos de restricción de acceso:

Ítem	Si	No
¿Menús para controlar acceso a la funcionalidad de las aplicaciones?	X	
¿Control de los datos a los que puede tener acceso un usuario particular?	X	
¿Control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?	X	
¿Control de los derechos de acceso de otras aplicaciones?	X	
¿Limitación de la información contenida en las salidas?	X	
¿Controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?		X

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

Entre los resultados de la lista de chequeo Lista de chequeo Dominio A 9 Control de Acceso Subdominio A 9.4.1, en los que están los siguientes:

- El IDSN no cuenta con controles de acceso físico o lógico para el aislamiento de aplicaciones, datos o sistemas críticos.

7.2.2.5 Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones Subdominio A 13.1.1

OBJETIVO:

Verificar el control A 13.1.1 Controles de redes, de acuerdo a la norma ISO 27001:2013

Control

Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

NOMBRE	CARGO
	Administrador Red de Datos

Se tiene implementado los siguientes controles en la red con el fin de proteger la información:		
Ítem	**Si**	**No**
Se establecen las responsabilidades y procedimientos para la gestión de equipos de redes?		X
¿Se separa la responsabilidad operacional por las redes, de las operaciones de cómputo?		X
Se tienen establecido controles especiales para : • salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?	X	
• para proteger los sistemas y aplicaciones conectados?		X
• Se cuenta con controles especiales para mantener disponibilidad de los servicios de red y computadores conectados?	X	
¿Se cuenta con registro (Logging) y el seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?	X	
¿Se coordinan las actividades de gestión para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?		X
Los sistemas en la red se autentican?	X	
Se restringe la conexión de los sistemas a la red?	X	

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

Entre los resultados de la Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones, Subdominio A 13.1.1, en los que están los siguientes:

- El IDSN no se establecen las responsabilidades y procedimientos para la gestión de equipos de redes.
- El IDSN no se separa la responsabilidad operacional por las redes, de las operaciones de cómputo.
- El IDSN no se tienen establecido controles especiales para proteger los sistemas y aplicaciones conectados

- En el IDSN no se coordinan las actividades de gestión con el fin de optimizar el servicio de la organización y de asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.

7.2.2.6 Lista de chequeo Dominio A 13 Seguridad de las Comunicación

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	**D**	**M**	**A**
Red de Datos			

Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones Subdominio A 13.1.2

OBJETIVO:

Verificar el control **A 13.1.2 13.1.2 Seguridad de los servicios de red**, de acuerdo a la norma ISO 27001:2013

Control

Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

NOMBRE	**CARGO**
	Administrador Red de Datos

Se cuenta con las siguientes características de seguridad en las redes de servicio:

Ítem	**Si**	**No**
tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red;		X
Los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;		X
Los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario		X

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

Entre los resultados de la Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones, Subdominio A 13.1.1, en los que están los siguientes:

- El IDSN no cuenta con tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red;
- El IDSN no cuenta con los parámetros técnicos requeridos para la conexión segura con los servicios de red, de acuerdo con las reglas de conexión de seguridad y de red;
- El IDSN no cuenta con los procedimientos necesarios para el uso de los servicios de red, los cuales permitan restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

7.2.3 Cuestionarios cuantitativos de control

7.2.3.1 Cuestionario Control de Accesos

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**
Red de Datos			

Cuestionario de control

Dominio	A9. Control de accesos
Proceso	A 9.1.2 acceso a redes y servicios de red

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:			
Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Se determina que redes y que servicios de red tiene el acceso el usuario autorizado?	3		El control existe pero sería óptimo mejorar su implementación.
¿Existen procedimientos de autorización para determinar a quién se permite acceder a las redes y servicios de red?		4	
¿Se determina los controles y procedimientos de gestión con el fin de proteger el acceso a red y a los servicios de red?	4		
¿Existen medios para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		4	No existe uso de VPN entre los nodos de la red del IDSN
¿Se determina los requisitos de autenticación de usuarios para acceder a diversos servicios de red?	3		
¿Existe herramientas para el monitoreo del uso de servicios de red?		4	No existen herramientas para gestionar y controlar el tráfico, la administración del rendimiento y de las posibles fallas presentes en la red.
TOTALES	10	12	
Puntaje Total	22		

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos		Firma del entrevistado

Porcentaje del riesgo = (Puntaje opción SI*100)/ puntaje total

Porcentaje del riesgo = 10*100/22

Porcentaje del riesgo = 45.5

Riesgo Total 100-45.5= 54.5

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

RIESGO:

Porcentaje de riesgo parcial = 45.5%
Porcentaje de riesgo = 54,5
Impacto según relevancia del proceso: Riesgo Medio

7.2.3.2 Cuestionario Control de Accesos

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**
Red de Datos			

Cuestionario de control

Dominio	A9. Control de accesos
Proceso	A 9.4.1 Restricción de acceso a la información.

Se cuenta con los siguientes requisitos de restricción de acceso:

Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Existen menús para controlar acceso a la funcionalidad de las aplicaciones?	4		
¿Existen controles para determinar a qué tipo de datos, puede tener acceso un usuario particular?	3		

¿Existen controles para determinar qué tipo de derechos de acceso, tienen los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?		3		
¿Existen controles para determinar qué tipo de derechos de acceso a otras aplicaciones, tienen los usuarios?		3		
¿Existen Limitaciones de la información contenida en las salidas?		3		
¿Existen de controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?			4	
TOTALES		16	4	
Puntaje Total		20		
Elaboro por:	Javier Mesías Narváez	Revis o por		Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos			Firma del entrevistado

Porcentaje del riesgo = (Puntaje opción NO*100)/ puntaje total

Porcentaje del riesgo = 16*100/20

Porcentaje del riesgo = 80

Riesgo Total 100- 80 = 20

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

RIESGO:

Porcentaje de riesgo parcial: $= 80\ \%$
Porcentaje de riesgo = 20%
Impacto según relevancia del proceso: Riesgo Medio

7.2.3.3 Cuestionario Seguridad en las comunicaciones

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**
Red de Datos			

Cuestionario de control

Dominio	Dominio A 13 Seguridad de las Comunicaciones
Proceso	A 13.1.1 Controles de redes.

Se tiene implementado los siguientes controles en la red con el fin de proteger la información:

Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Se establecen las responsabilidades y procedimientos para la gestión de equipos de redes?		4	
¿Se separa la responsabilidad operacional por las redes, de las operaciones de cómputo?		4	
Se tienen establecido controles especiales para : • ¿salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?	4		
		4	

• para proteger los sistemas y aplicaciones conectados? • Se cuenta con controles especiales para mantener disponibilidad de los servicios de red y computadores conectados?	3		
¿Se cuenta con registro (Logging) y el seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?	4		Si se cuenta con registro de loggs pero no está categorizado a través de un inventario
¿Se coordinan las actividades de gestión para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?		5	El IDSN no cuenta con controles para realizar un seguimiento adecuado.
¿Los sistemas en la red se autentican?	4		
Se restringe la conexión de los sistemas a la red?	3		
TOTALES	18	17	
Puntaje Total	35		

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos		Firma del entrevistado

Porcentaje del riesgo = (Puntaje opción SI*100)/ puntaje total

Porcentaje del riesgo = 18*100/35

Porcentaje del riesgo = 51.4

Riesgo Total 100 = 51.4 %=48.6

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

RIESGO:

Porcentaje de riesgo parcial: $= 51.4\%$
Porcentaje de riesgo = 48.6 %
Impacto según relevancia del proceso: Riesgo Medio

7.2.3.4 Cuestionario Seguridad en las comunicaciones

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.**

ÁREA	**D**	**M**	**A**
Red de Datos			

Cuestionario de control

Dominio	Dominio A 13 Seguridad de las Comunicaciones
Proceso	A 13.1.2 Seguridad de los servicios de red.

Se cuenta con las siguientes características de seguridad en las redes de servicio:

Pregunta	**Si**	**No**	**OBSERVACIONES**
¿Existen tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red?		4	
¿Se definen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red?		4	
¿Existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario?		5	
TOTALES	0	13	
Puntaje Total	13		

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida

Entrevistado	Gustavo Cuellar De los Ríos		Firma del entrevistado

, Porcentaje del riesgo = (Puntaje opción SI*100)/ puntaje total

Porcentaje del riesgo = 0*100/13

Porcentaje del riesgo = 0

Riesgo Total 100 = 0 %= 100

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

RIESGO:

Porcentaje de riesgo parcial: = 0%
Porcentaje de riesgo = 100 %
Impacto según relevancia del proceso: Riesgo Alto

7.3 Ejecución de Pruebas

Las pruebas se realizaron en su mayoría con la suite de Kali Linux, mediante las herramientas que dispone para realizar para pruebas de penetración y auditorías de seguridad, las pruebas que se realizaron para recolectar información igual que las pruebas por medio de herramientas online fueron realizadas con el sistema operativo Windows 10.

Las dos primeras pruebas Recolección de información (Information Gathering) y la Prueba con protocolo Whois, se utilizaron para la recolección de la información, con lo cual se busca recolectar información sensible de la empresa de la misma forma que lo haría un hacker.

7.3.1 Recolección de información (Information Gathering)

Mediante la página http://www.zone-h.org/archive, la cual permite ingresar el campo DOMAIN, el dominio de la página, en donde se procede a ingresar el dominio del IDSN, el cual es: www.idsn.gov.co, como se puede observar que el Instituto Departamental de Salud de Nariño, ha sido víctima de 6 ataques.

Figura 5 Zone - h

Fuente: Autor

Al consulta este sitio web, se puede observar en la figura 5, que el ultimo ataque reportado fue en 16/02/2016 el cual fue perpetrado por el grupo de hackers Alfabeto Virtual, el ataque consistio en una desconfiguracion del sitio web

Figura 6 Zone - h

Fuente: Autor

En las figuras 6 y 7, se muestra como quedo el sitio web después del ataque, donde en índex fue cambiado por el logo del grupo de hackers Alfabeto Virtual.

Figura 7 Zone - h

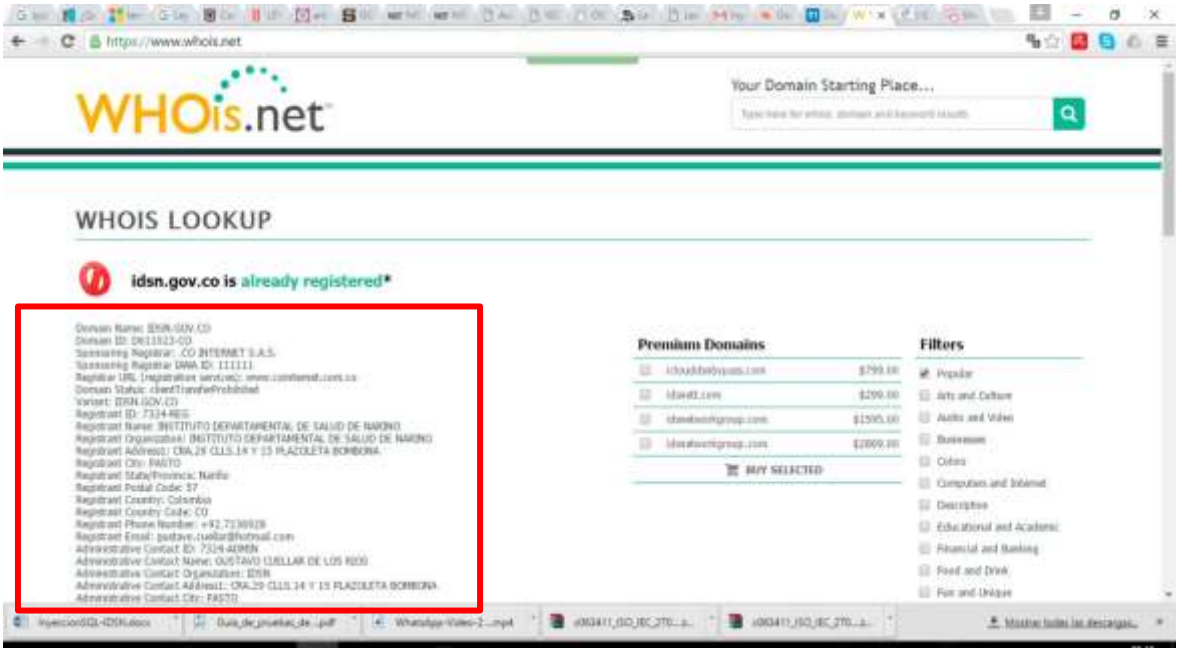
Fuente: Autor

En las figura 7, se muestra como se quedo el sitio web despues del ataque, donde se cambio el index por la figura de un gato, para acceder a esta informacion se ingresa al link mirror a la derecha de la descripcion de cada ataque.

7.3.2 Prueba con protocolo Whois

Mediante la página www.whois.net, la cual permite ingresar el campo DOMAIN, el dominio de la página, en donde se procede a ingresar el dominio del IDSN, el cual es: www.idsn.gov.co,

Figura 7 Prueba protocolo Whois



Fuente: Autor

La prueba con el protocolo Whois, se realiza en línea a ingresando a la página web www.whois.net, al ejecutar esta prueba nos suministra información sensible de la empresa entre la cual se puede observar el nombre de la empresa, su dirección, teléfonos de contacto, nombre del administrador, nombres de los servidores, a continuación se encuentra el informe con toda la información que se puede obtener mediante esta prueba.

Domain Name: IDSN.GOV.CO
Domain ID: D611023-CO
Sponsoring Registrar: .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID: 111111
Registrar URL (registration services): www.cointernet.com.co
Domain Status: clientTransferProhibited
Variant: IDSN.GOV.CO
Registrant ID: 7324-REG
Registrant Name: INSTITUTO DEPARTAMENTAL DE SALUD DE NARINO
Registrant Organization: INSTITUTO DEPARTAMENTAL DE SALUD DE NARINO
Registrant Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Registrant City: PASTO
Registrant State/Province: Nariño
Registrant Postal Code: 57
Registrant Country: Colombia
Registrant Country Code: CO
Registrant Phone Number: +92.7236928
Registrant Email: gustavo.cuellar@hotmail.com
Administrative Contact ID: 7324-ADMIN
Administrative Contact Name: GUSTAVO CUELLAR DE LOS RIOS
Administrative Contact Organization: IDSN
Administrative Contact Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Administrative Contact City: PASTO
Administrative Contact State/Province: Nariño
Administrative Contact Postal Code: 57
Administrative Contact Country: Colombia
Administrative Contact Country Code: CO
Administrative Contact Phone Number: +92.7236928
Administrative Contact Email: gcuellar100@gmail.com
Billing Contact ID: 7324-BILLING
Billing Contact Name: DIRECTOR
Billing Contact Organization: IDSN
Billing Contact Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Billing Contact City: PASTO
Billing Contact State/Province: Nariño
Billing Contact Postal Code: 57
Billing Contact Country: Colombia
Billing Contact Country Code: CO

Billing Contact Phone Number: +92.7236928
Billing Contact Email: gcuellar@idsn.gov.co
Technical Contact ID: 7324-TECH
Technical Contact Name: gustavo cuellar de los rios
Technical Contact Address1: CRA 29 CLLS 14 Y 15 PLAZOLETA BOMBONA
Technical Contact City: pasto
Technical Contact Country: Colombia
Technical Contact Country Code: CO
Technical Contact Phone Number: +571.0000000
Technical Contact Email: gcuellar@idsn.gov.co
Name Server: NS.COMPUTRONIX.COM.CO
Name Server: NS.IDSN.GOV.CO
Created by Registrar: NEULEVELCSR
Last Updated by Registrar: .CO INTERNET S.A.S.
Domain Registration Date: Wed Jun 09 00:00:00 GMT 1999
Domain Expiration Date: Mon Jun 08 23:59:59 GMT 2020
Domain Last Updated Date: Tue Jun 09 10:15:02 GMT 2015
DNSSEC: false

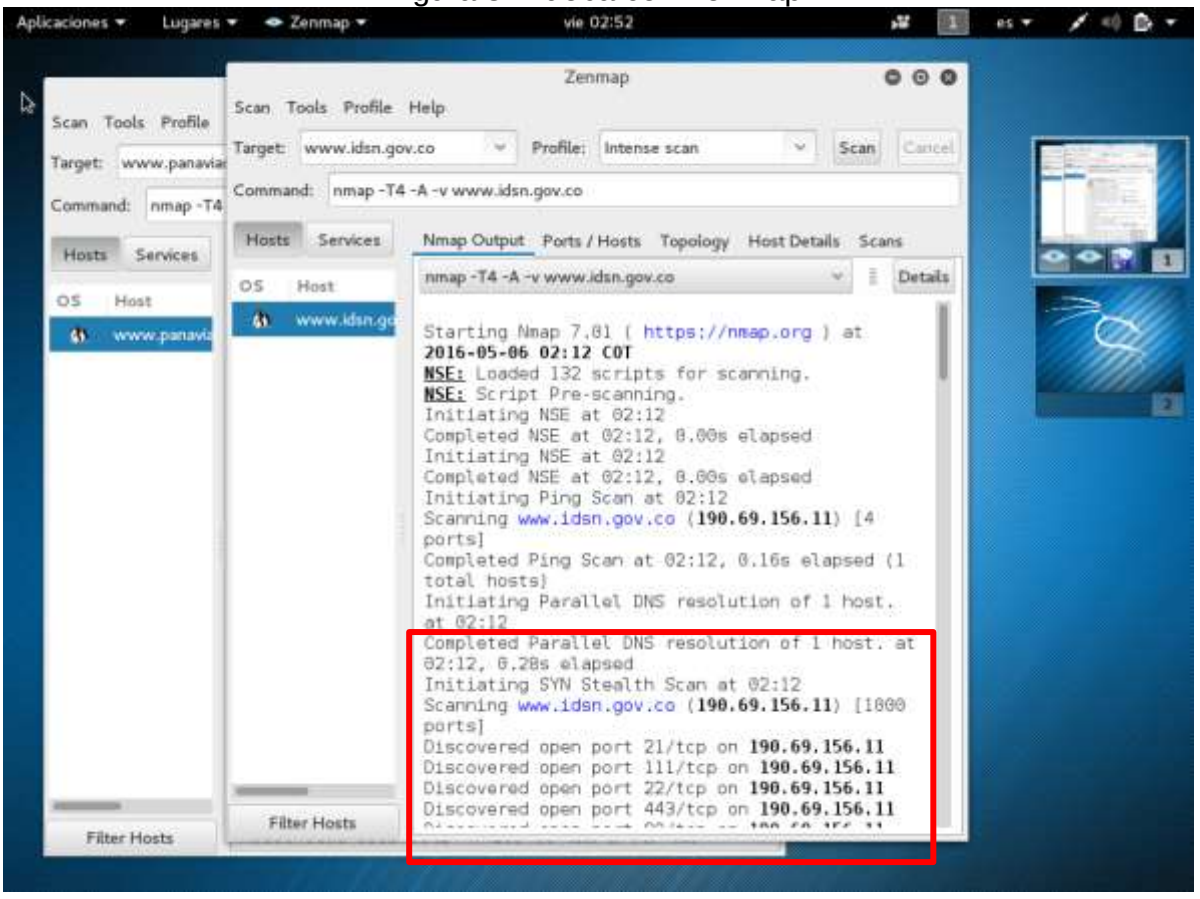
7.3.3 Prueba de escaneo de puerto con la herramienta Zenmap

Escaneo de puertos, se realiza con Zenmap, esta herramienta grafica está disponible en la suite Kali Linux versión 2016.1 ejecutando el siguiente comando en Nmap:

```
nmap –T4 –A –v www.idsn.gov.co
```

En la siguiente figura se aprecia el escaneo realizado a la página del IDSN, mediante la introducción de la dirección URL o también mediante la dirección IP en la ventana **Target**

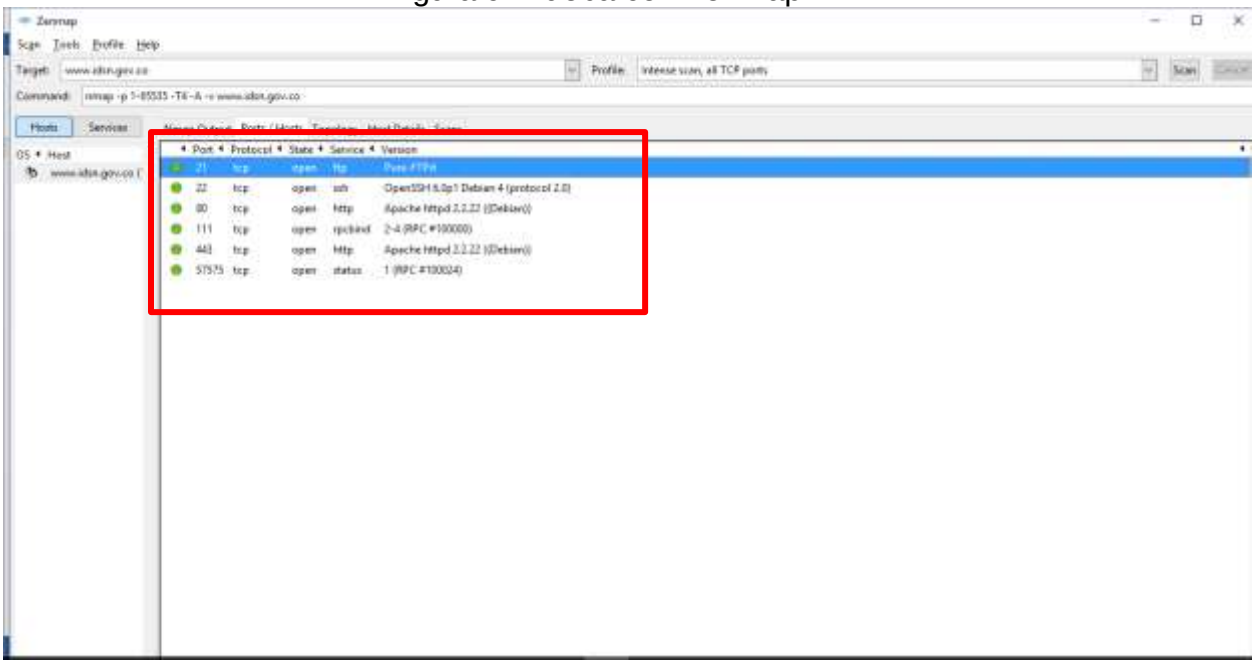
Figura 8 Prueba con Zenmap



Fuente: Autor

En la figura 8, se observa el inicio del escaneo con la herramienta Zenmap, disponible en la suite de Kali Linux, en el recuadro rojo se observa los primeros puertos abiertos que se identifican en el servidor del IDSN.

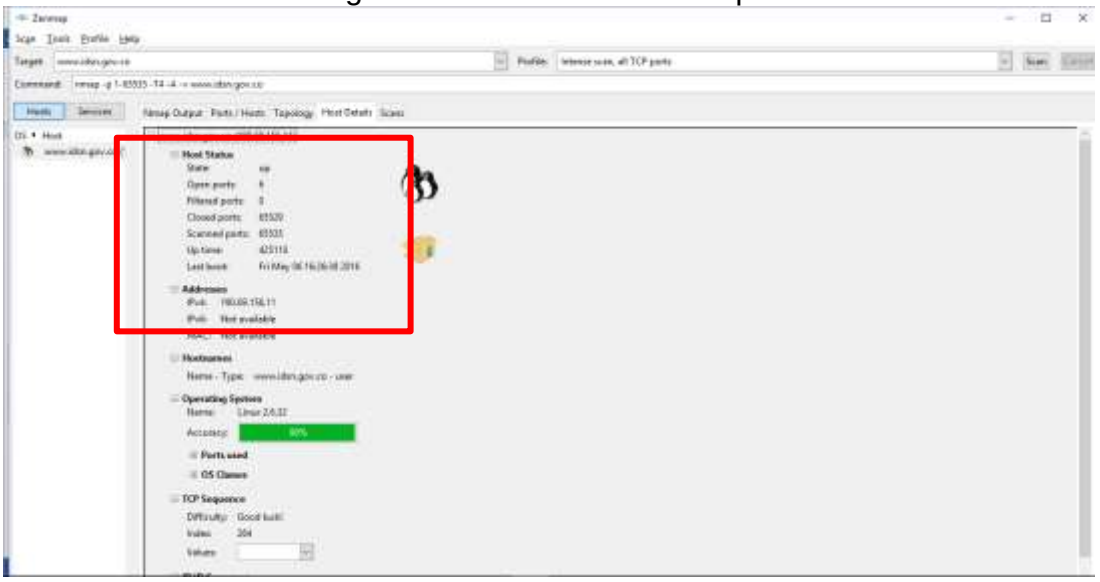
Figura 9 Prueba con Zenmap



Fuente: Autor

En la figura 9, como resultado de la aplicación de la prueba con la herramienta Zenmap de la suite Kali Linux, como resultado del escaneo se puede observar los puertos abiertos y los servicios que corren sobre estos puertos y de acuerdo al servicio que corre por el puerto, con esta información se puede. analizar la importancia que estén cerrados estos puertos.

Figura 10 Prueba con Zenmap 1



Fuente: Autor

En la figura 10, como resultado de la aplicación de la prueba con la aplicación de Kali Linux, Zenmap se puede observar los puertos abiertos y la cantidad de puertos que fueron escaneados durante la realización de la prueba. El informe de Zenmap muestra 5 puertos abiertos, 989 puertos cerrados, servidores Dyamic, Static-IP telecom, a continuación se puede observar, los resultados en forma detallada del procedimiento ejecutado.

Starting Nmap 7.01 (https://nmap.org) at 2016-05-06 02:12 COT
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating Ping Scan at 02:12
Scanning www.idsn.gov.co (**190.69.156.11**) [4 ports]
Completed Ping Scan at 02:12, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:12
Completed Parallel DNS resolution of 1 host. at 02:12, 0.28s elapsed
Initiating SYN Stealth Scan at 02:12
Scanning www.idsn.gov.co (**190.69.156.11**) [1000 ports]
Discovered open port 21/tcp on **190.69.156.11**
Discovered open port 111/tcp on **190.69.156.11**
Discovered open port 22/tcp on **190.69.156.11**
Discovered open port 443/tcp on **190.69.156.11**
Discovered open port 80/tcp on **190.69.156.11**
Increasing send delay for **190.69.156.11** from 0 to 5 due to max_successful_tryno increase to 5
Completed SYN Stealth Scan at 02:13, 39.67s elapsed (1000 total ports)
Initiating Service scan at 02:13

Scanning 5 services on www.idsn.gov.co (**190.69.156.11**)
Completed Service scan at 02:13, 17.37s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.idsn.gov.co (**190.69.156.11)**
Retrying OS detection (try #2) against www.idsn.gov.co (**190.69.156.11**)
Initiating Traceroute at 02:13
Completed Traceroute at 02:13, 3.02s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 02:13
Completed Parallel DNS resolution of 8 hosts. at 02:13, 6.66s elapsed
NSE: Script scanning **190.69.156.11.**
Initiating NSE at 02:13

```
Completed NSE at 02:14, 40.41s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Nmap scan report for www.idsn.gov.co (190.69.156.11)
Host is up (0.14s latency).
Not shown: 989 closed ports
PORT STATE SERVICE VERSION
21/tcp   open   ftp              Pure-FTPd
22/tcp   open   ssh              OpenSSH 6.0p1 Debian 4 (protocol 2.0)
| ssh-hostkey:
|   1024 d1:89:c8:df:59:c8:f0:81:fb:76:a4:81:a4:ca:97:fc (DSA)
|   2048 88:dd:bf:17:9b:0a:95:a6:32:23:5a:5a:b6:e7:ae:64 (RSA)
|_  256 27:81:b2:1f:ee:5a:d8:09:b6:16:23:71:7b:39:9c:03 (ECDSA)
80/tcp   open   http             Apache httpd 2.2.22 ((Debian))
|_http-favicon: Unknown favicon MD5: A376B20E57F7F45CD0D378A50944AF9F
|_http-generator: Joomla! - Open Source Content Management
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 16 disallowed entries (15 shown)
| /joomla/administrator/ /administrator/ /cache/ /cli/
| /components/ /images/ /includes/ /installation/ /language/
|_/libraries/ /logs/ /media/ /modules/ /plugins/ /templates/
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: ..:: Instituto Departamental de Salud de Nari\xC3\xB1o - IDSN ::.. -...
111/tcp  open  rpcbind          2-4 (RPC #100000)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open  ssl/http          Apache httpd 2.2.22
| http-methods:
|_  Supported Methods: GET
|_http-server-header: Apache/2.2.22 (Debian)
| ssl-cert: Subject: commonName=linuxdb
| Issuer: commonName=linuxdb
| Public Key type: rsa
| Public Key bits: 2048
```

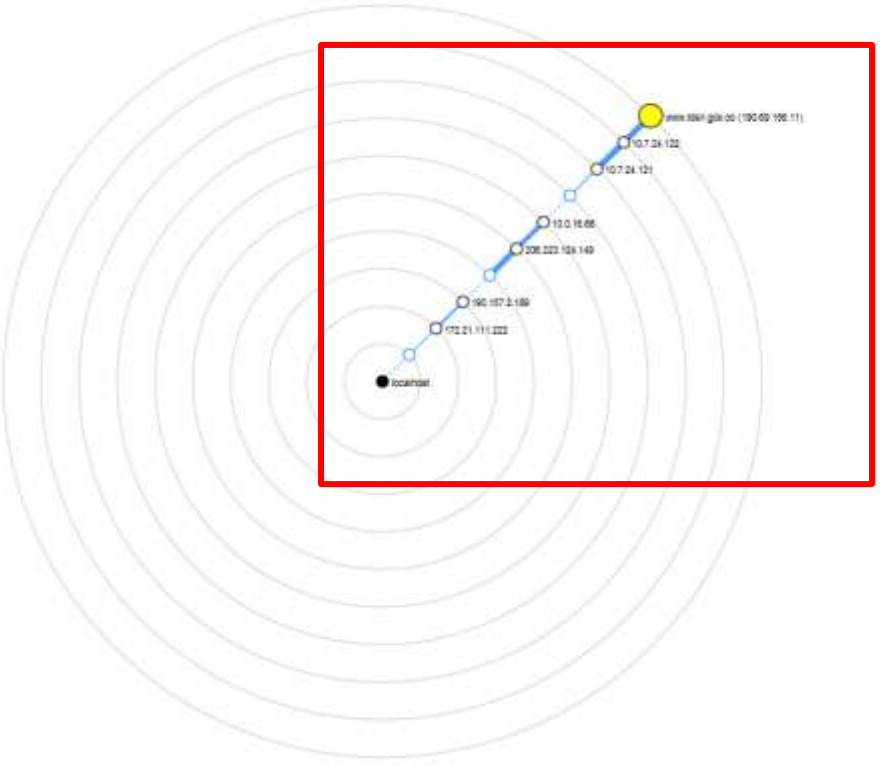
```
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-08-28T17:20:25
| Not valid after:  2023-08-26T17:20:25
| MD5:   f653 5b5a f0f9 d75e b80a 7e96 bd39 f159
```

```
|_SHA-1: ede8 ad74 fa8b a15a 0646 52a2 28cd 9158 b6ef 9523
|_ssl-date: 2016-05-06T07:39:31+00:00; +25m40s from scanner time.
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
4444/tcp filtered krb524
6129/tcp filtered unknown
Aggressive OS guesses: Linux 3.2 - 3.8 (96%), Linux 2.6.32 - 2.6.39 (94%), Linux 2.6.32 -
3.0 (93%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 3.0 or 3.5 (92%), Linux
3.11 - 4.1 (92%), Linux 3.8 (91%), WatchGuard Fireware 11.8 (91%), Linux 3.1 - 3.2 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.547 days (since Mon May  2 13:06:45 2016)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOP RTT       ADDRESS
1   445.23 ms Dynamic-IP-181550761.cable.net.co (181.55.76.1)
2   40.75 ms  172.21.111.202
3   138.23 ms Static-IP-1901572189.cable.net.co (190.157.2.189)
4   ...
5   165.61 ms telecom-nap.ccit.org.co (206.223.124.149)
6   74.51 ms  10.0.16.66
7   ...
8   153.56 ms 10.7.24.121
9   153.37 ms 10.7.24.122
10  128.64 ms 190.69.156.11

NSE: Script Post-scanning.
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.08 seconds
           Raw packets sent: 1401 (63.728KB) | Rcvd: 1245 (52.430KB)
```

Figura 11 Topología IDSN



Fuente: Autor

En la figura 11 se muestra la topología del IDSN, la cual se obtuvo mediante la aplicación de la prueba de Zenmap.

7.3.4 Prueba con la herramienta TheHarvester

TheHarvester es una herramienta de tipo consola que se encuentra en la suite Kali Linux versión 2016.1, sirve para reunir de mensajes de correo electrónico, subdominios, hosts, nombres de empleados, puertos abiertos y las banderas de diferentes fuentes públicas como los motores de búsqueda, los servidores de claves PGP y base de datos.

Para ejecutar esta esta herramienta se ejecuta desde la terminal:

```
usr/bin/theharvester,
```

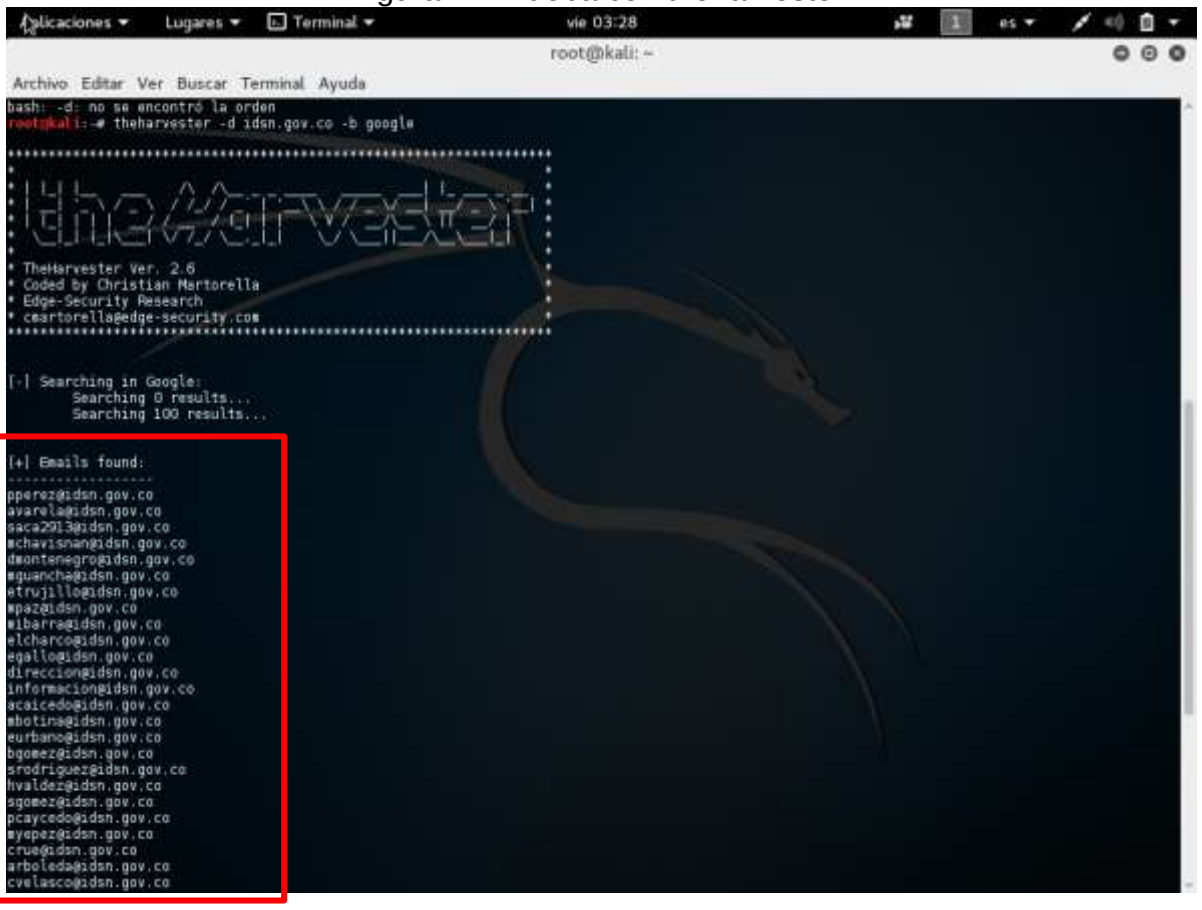
Se la realiza desde consola porque no posee interfaz grafica

Luego se ejecuta el siguiente comando

theharvester -d idsn.gov.co -b google

La fig. Muestra los siguientes resultados: correo institucional encontrado y los servidores donde se alojan

Figura 12 Prueba con theharvester



Fuente: Autor

Informe de *Harvester* a continuación donde muestra se muestra los correos encontrados

```
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
[+] Emails found:
------------------
```

pperez@idsn.gov.co
avarela@idsn.gov.co
saca2913@idsn.gov.co
mchavisnan@idsn.gov.co
dmontenegro@idsn.gov.co
mguancha@idsn.gov.co
etrujillo@idsn.gov.co
mpaz@idsn.gov.co
mibarra@idsn.gov.co
elcharco@idsn.gov.co
egallo@idsn.gov.co
direccion@idsn.gov.co
informacion@idsn.gov.co
acaicedo@idsn.gov.co
mbotina@idsn.gov.co
eurbano@idsn.gov.co
bgomez@idsn.gov.co
srodriguez@idsn.gov.co
hvaldez@idsn.gov.co
sgomez@idsn.gov.co
pcaycedo@idsn.gov.co
myepez@idsn.gov.co
crue@idsn.gov.co
arboleda@idsn.gov.co
cvelasco@idsn.gov.co
yrivera@idsn.gov.co
mguerrero@idsn.gov.co
aarteaga@idsn.gov.co
rivera@idsn.gov.co
ipiales@idsn.gov.co
lparedes@idsn.gov.co
cceron@idsn.gov.co
soniagomezl@idsn.gov.co

[-] Resolving hostnames IPs...

[+] Hosts found in search engines:

190.69.156.11:intranet.idsn.gov.co
190.69.156.11:ssyreproductiva.idsn.gov.co

```
190.69.156.11:www.idsn.gov.co
190.69.156.11:smental.idsn.gov.co
190.69.156.11:cop.idsn.gov.co
190.69.156.11:aiepi.idsn.gov.co
190.69.156.14:sisa.idsn.gov.co
190.69.156.11:old.idsn.gov.co
190.69.156.14:Sisa.idsn.gov.co
190.69.156.11:Ssyreproductiva.idsn.gov.co
190.66.23.131:mail.idsn.gov.co
root@kali:~#
```

7.3.5 Prueba de escaneo de puerto con la herramienta en línea a través de la página https://incloak.es/ports/

Esta herramienta permite realizar un escaneo de puertos en línea.

Figura 13 Escaneo de puertos en Línea

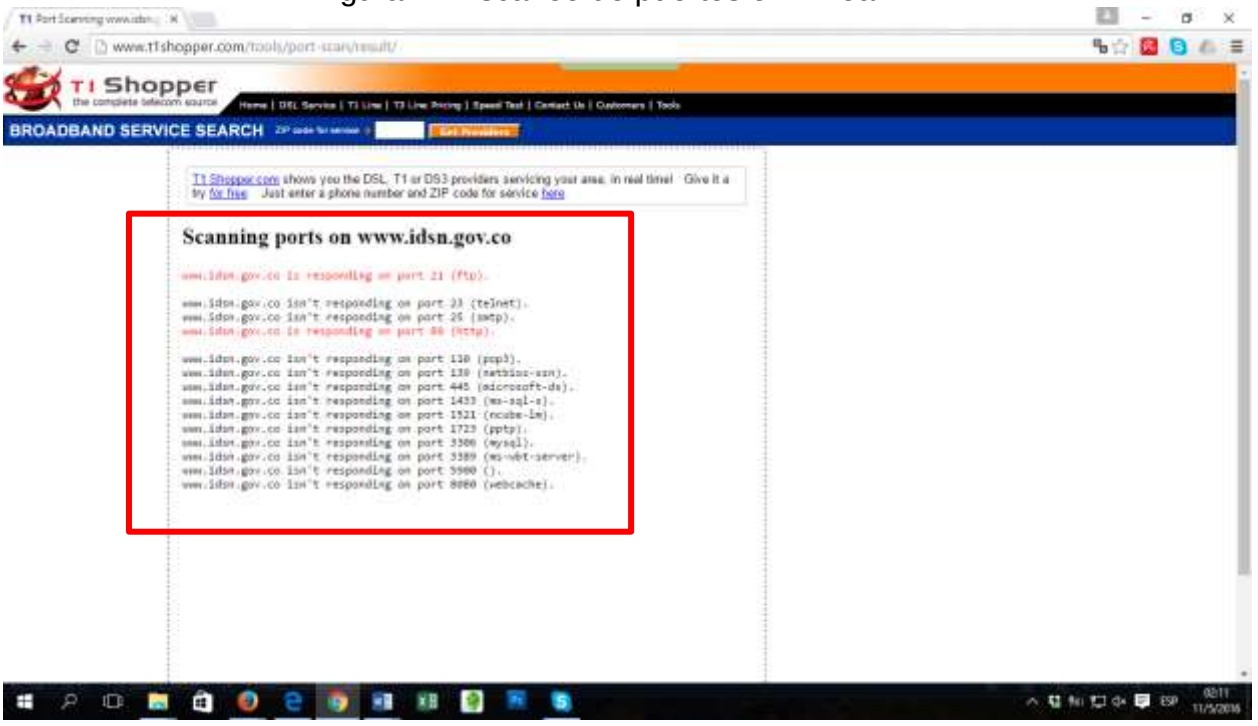
Fuente: Autor

```
Not shown: 995 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
443/tcp open  https
```

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds

7.3.6 Prueba de escaneo de puerto con la herramienta en línea a través de la página http://www.t1shopper.com/tools/port-scan/result/

Figura 14 Escaneo de puertos en Línea



Fuente: Autor

Scanning ports on www.idsn.gov.co

www.idsn.gov.co is responding on port 21 (ftp).

www.idsn.gov.co isn't responding on port 23 (telnet).
www.idsn.gov.co isn't responding on port 25 (smtp).
www.idsn.gov.co is responding on port 80 (http).

www.idsn.gov.co isn't responding on port 110 (pop3).
www.idsn.gov.co isn't responding on port 139 (netbios-ssn).
www.idsn.gov.co isn't responding on port 445 (microsoft-ds).
www.idsn.gov.co isn't responding on port 1433 (ms-sql-s).
www.idsn.gov.co isn't responding on port 1521 (ncube-lm).
www.idsn.gov.co isn't responding on port 1723 (pptp).
www.idsn.gov.co isn't responding on port 3306 (mysql).
www.idsn.gov.co isn't responding on port 3389 (ms-wbt-server).

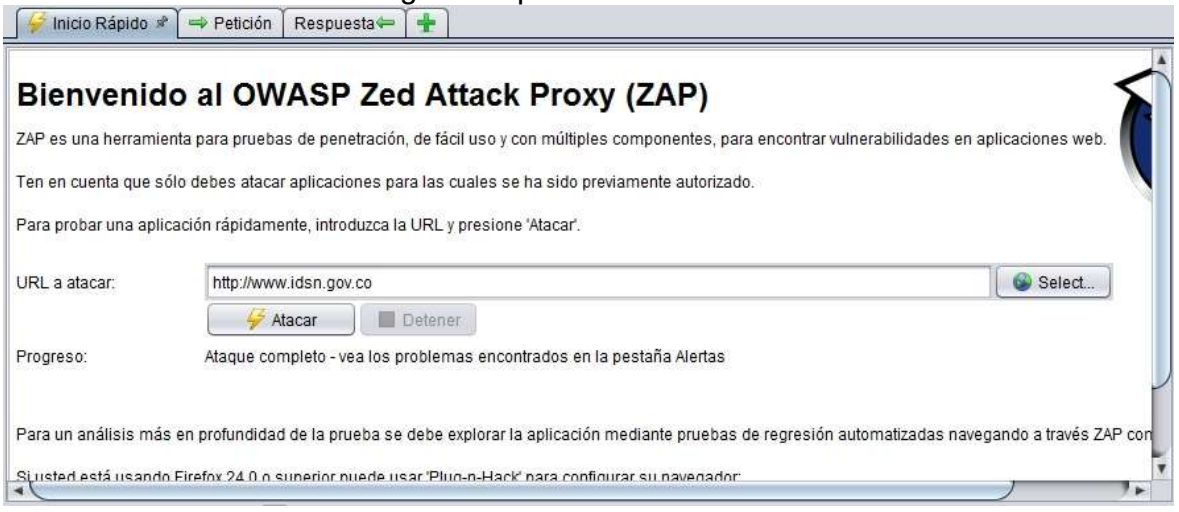
www.idsn.gov.co isn't responding on port 5900 ().
www.idsn.gov.co isn't responding on port 8080 (webcache).

7.3.7 Prueba de escaneo de Vulnerabilidades mediante la herramienta OSWAP Zed Attack

La OWASP Zed Ataque Proxy (ZAP) es una herramienta para realizar pruebas de penetración y para encontrar vulnerabilidades en aplicaciones web. Está diseñado para ser utilizado por personas con una amplia experiencia en seguridad y, es ideal para los desarrolladores, además es muy útil para conformar un kit de herramienta de pruebas de intrusión[6].

Lo primero que se debe hacer para iniciar la prueba es ingresar la URL del sitio a evaluar.

Figura 15 prueba con OWASP

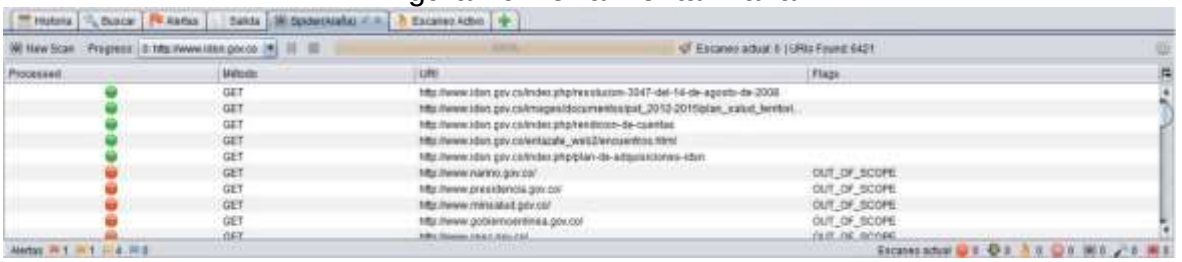


Fuente: Autor

La herramienta Spider (Araña), analiza todos los directorios contenidos en la pagina, mandando peticiones GET

6 http://tools.kali.org/web-applications/zaproxy

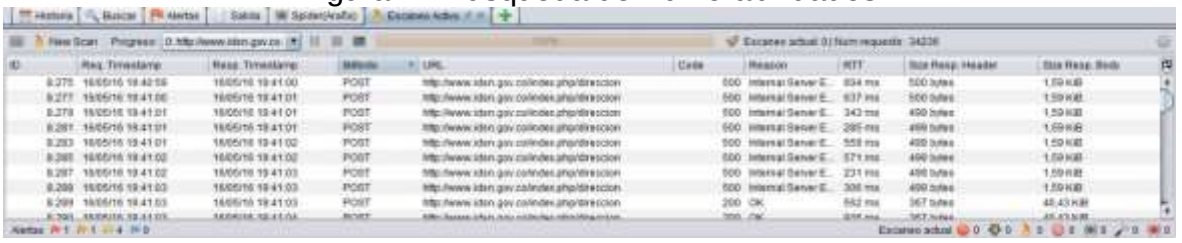
Figura 16 Herramienta Araña



Fuente: Autor

Una vez finalizado el escaneo de directorios, se procede a las respuestas obtenidas por Spider, con la herramienta Escaneo Activo, buscando vulnerabilidades en el sitio

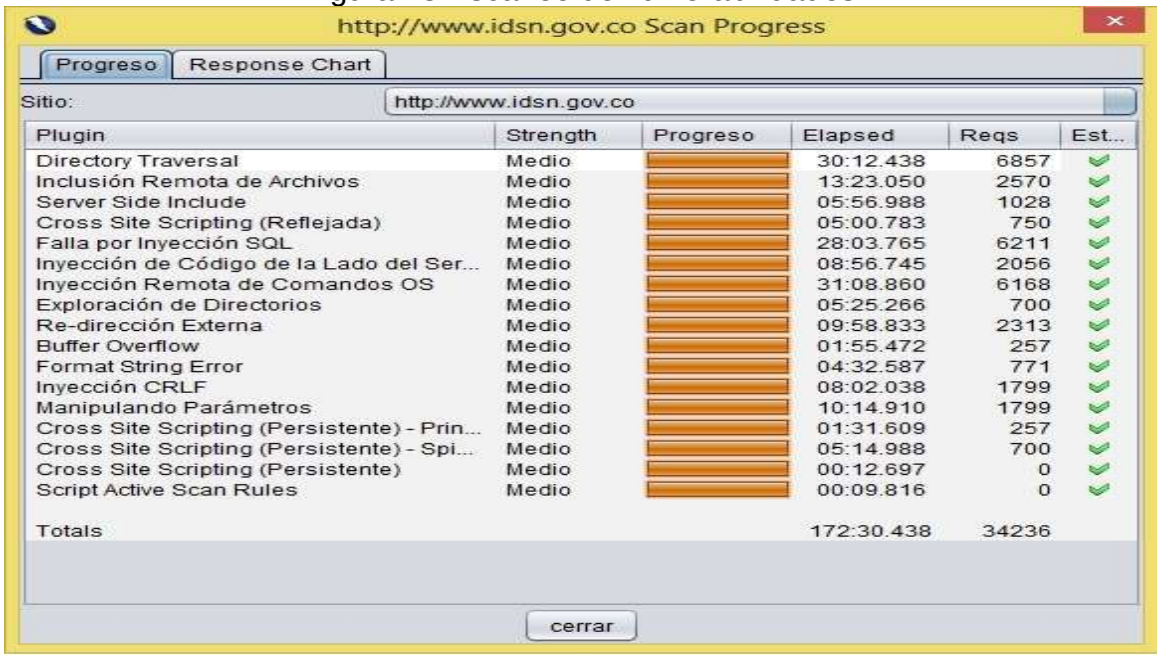
Figura 17 Búsqueda de Vulnerabilidades



Fuente: Autor

Se escanean las vulnerabilidades encontradas en la pagina

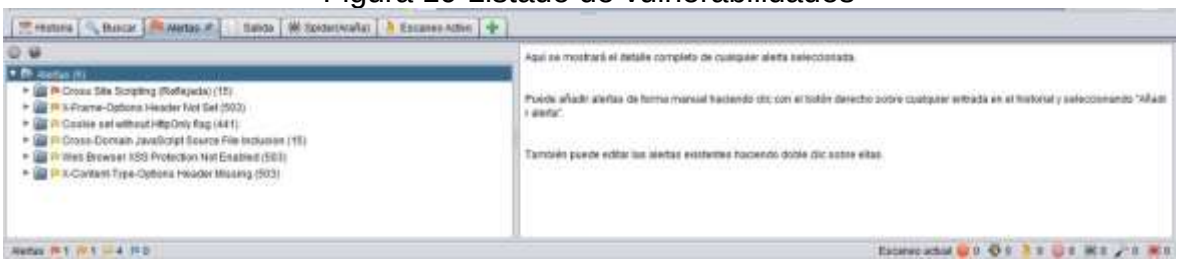
Figura 18 Escaneo de vulnerabilidades



Fuente: Autor

Se muestran las vulnerabilidades encontradas en la página;
Bandera Roja: Riesgo Alto
Bandera Naranja: Riesgo Medio
Bandera Amarilla: Riesgo Bajo

Figura 19 Listado de vulnerabilidades

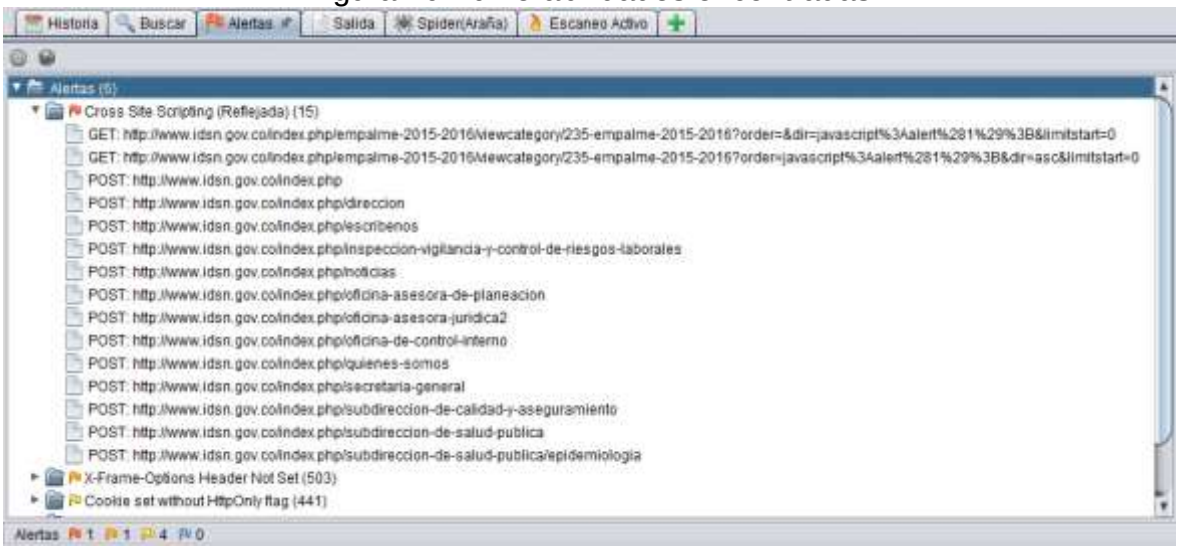


Fuente: Autor

Se describe las paginas vulnerables a Cross-site scripting (Reflejada) de Riesgo Alto en la página del IDSN

Para el caso del IDSN, 1 de Riesgo Alto, 1 de Riesgo Medio y 4 de Riesgo Bajo

Figura 20 Vulnerabilidades encontradas



Fuente: Autor

7.3.8 Prueba de Inyección SQL mediante la herramienta SQLMAP Inyección SQL

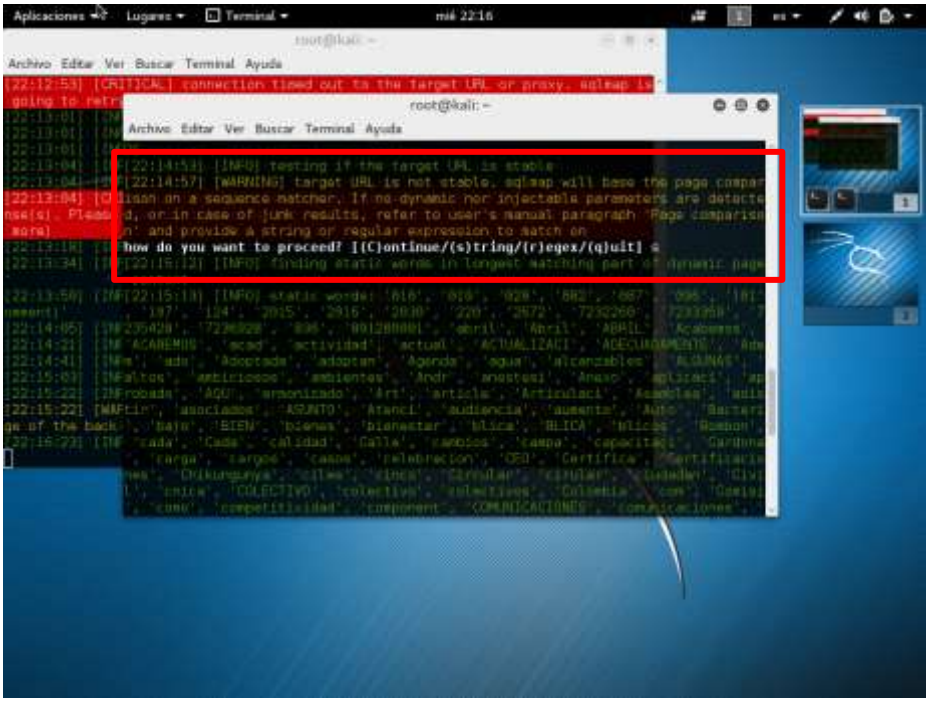
A través de los resultados generados por OWASP ZAP, se obtuvieron los siguientes DORKS para analizar una posible intrusión por Inyección SQL

Tabla 11 Vulnerabilidades encontradas

Punto a evaluar	Vulnerable/No Vulnerable
http://www.idsn.gov.co/index.php?start=12	No vulnerable
http://www.idsn.gov.co/index.php?start=24	No vulnerable
http://www.idsn.gov.co/index.php?start=36	VULNERABLE
http://www.idsn.gov.co/index.php?start=48	No Vulnerable
http://www.idsn.gov.co/index.php?start=60	No vulnerable
http://www.idsn.gov.co/index.php?start=72	No Vulnerable
http://www.idsn.gov.co/index.php?start=84	No Vulnerable
http://www.idsn.gov.co/index.php?start=96	No Vulnerable
http://www.idsn.gov.co/index.php?start=108	No Vulnerable

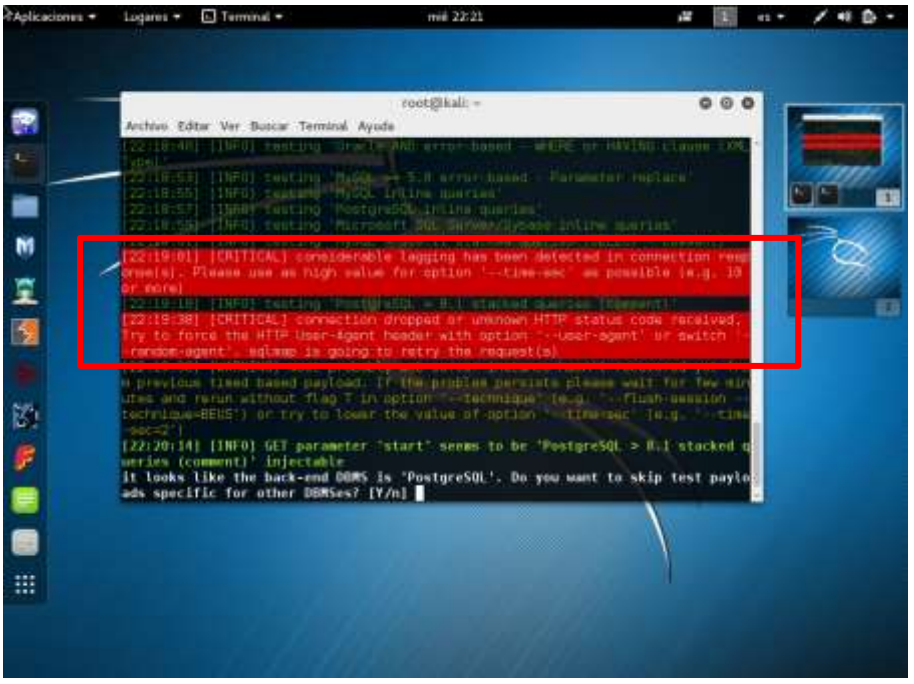
Fuente: Autor

Figura 22 sqlmap –u http://www.idsn.gov.co/index.php?start=36 –dbs



Fuente: Autor

Figura 22 sqlmap –u http://www.idsn.gov.co/index.php?start=36 –dbs



Fuente: Autor

7.4 Análisis y Gestión de Riesgos

El análisis de riesgos informáticos es un método, el cual tiene una serie de etapas, entre las cuales están la identificación de activos informáticos, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, también como su probabilidad de ocurrencia y el efecto de su impacto, con el fin de determinar los controles más adecuados para aceptar, mitigar, trasladar o evitar la ocurrencia del riesgo encontrado.

7.4.1 Catalogación activos de red

Inicialmente se hace la catalogación de la tabla de los activos de la red de datos y la clasificación de seguridad que se darán a cada uno de los activos de información:

Tabla 12. Clasificaciones de seguridad

Clasificación Cualitativa	Descripción
Sensitiva	El compromiso de la información podría dañar los intereses de los usuarios y terceros.

En confianza	El compromiso de la información podría perjudicar la privacidad de los usuarios y terceros.
Publica no clasificada	El compromiso de la información afecta la imagen de la entidad.
Top Secret	El compromiso de la información podría dañar los intereses de la organización de manera grave.
Secreta	El compromiso de la información podría dañar los intereses de la organización de manera seria.
Confidencial	El compromiso de la información podría dañar los intereses de la organización de manera significativa.
Restringida	El compromiso de la información podría dañar los intereses de la organización de manera adversa.

Fuente: Autor

Tabla 13. Escala de valoración de rango porcentual de impacto en los activos

Porcentaje	Criterio
90%-100%	Muy alto
75%-89%	Alto
50%-74%	Medio
20%-49%	Bajo
0%-19%	Muy bajo

Fuente: Autor

Tabla 14. Clasificación de activos de información

INVENTARIO DE ACTIVOS						
Tipos de activos	**Nombre de activos área de informática**	**Clasificación de la información**	**Criticidad**			
			Conf.	**Integ**	**Disp.**	**Promedio**
Información [INF]	[INF] Base de datos ORACLE	Confidencial	100%	100%	100%	100%
	[INF] Documentos Físicos (Manuales de usuario, Correspondencia…	Confidencial	80%	60%	60%	67%
Software [SW]	[SW] Linux Debían	Confidencial	100%	100%	100%	100%

INVENTARIO DE ACTIVOS						
	[SW] WINDOWS Server 2010	Confidencial	100%	100%	100%	100%
	[SW] F - Security	Secreta	100%	100%	100%	100%
Hardware [HW]	[HW] Servidor de base de datos	Restringida	100%	100%	100%	100%
	[HW] Servidor de aplicaciones	Restringida	100%	100%	100%	100%
	[HW] Servidor de correo	Restringida	100%	100%	100%	100%
	[HW] Servidor de dominio	Restringida	100%	100%	100%	100%
	[HW] Servidor de Archivos	Restringida	100%	100%	100%	100%
	[HW] Servidor Web	Restringida	100%	100%	100%	100%
	[HW] Servidor proxy	Restringida	80%	80%	100%	87%
Red [COM]	[COM] Switches	Restringida	90%	100%	100%	97%
	[COM] Unidad NAS – Backup		100%	100%	100%	100%
	[COM] UPS tripplite	Sensitiva	80%	80%	100%	87%
	[COM] Cableado	Sensitiva	80%	80%	100%	87%

Fuente: Autor

Tabla 15. Tipos de activos de información

TIPO DE ACTIVO	DESCRIPCIÓN
[INF] Información	
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos propios o contratados, etc.
[HW] Hardware / Equipos informáticos	Son activos o bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluye las instalaciones dedicadas como también los servicios de comunicaciones contratados a terceros.

Fuente: Autor

7.4.2 Tabla de Amenazas

Tabla 16. Tabla de Amenazas

Ítem	Tipo de Amenaza	Descripción
A001	Desastres Naturales [N]	Se incluyen: [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales
A002	De origen Industrial [I]	Se incluyen: [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación mecánica [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales

Ítem	Tipo de Amenaza	Descripción
		[I.10] Degradación de los soportes de almacenamiento de la información [I.11] Emanaciones electromagnéticas
A003	Errores y fallos no intencionados [E]	Se incluyen: [E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.8] Difusión de software dañino [E.9] Errores de re-encaminamiento [E.10] Errores de secuencia [E.14] Fugas de información [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.28] Indisponibilidad del personal

Ítem	Tipo de Amenaza	Descripción
A004	Ataques intencionados [A]	Se incluyen: [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Fuente: Autor

7.4.3 Tabla de Vulnerabilidades

Tabla 17. Tabla de Vulnerabilidades

ID	Vulnerabilidad	Dominio	Tipo de Amenaza
R001	No existen procedimientos de autorización para determinar quién accede a las redes y servicios de red.	A9. Control de Acceso	Errores y fallos no intencionados [E] [E.7] Deficiencias en la organización
R002	No existen medios para acceder a redes y servicios de red como VPN.	A9. Control de Acceso	Errores y fallos no intencionados [E] [E.4] Errores de configuración [E.7] Deficiencias en la organización
R003	No existen herramientas para el monitoreo del uso de servicios de red.	A9. Control de Acceso	Errores y fallos no intencionados [E] [E.21] Errores de mantenimiento / actualización de programas (software)
R004	No existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.	A9. Control de Acceso	Errores y fallos no intencionados [E] [E.7] Deficiencias en la organización
R005	No se establecen las responsabilidades y procedimientos para la gestión de equipos de redes.	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal
R006	No existen controles para proteger los sistemas y aplicaciones conectados.	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E]

ID	Vulnerabilidad	Dominio	Tipo de Amenaza
			[E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización
R007	No existe responsabilidad operacional de las redes y de las operaciones de cómputo	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal
R008	No se coordinan las actividades de gestión para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.2] Errores del administrador [E.7] Deficiencias en la organización
R009	No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red.	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software)
R010	No se definen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.2] Errores del administrador

ID	Vulnerabilidad	Dominio	Tipo de Amenaza
	conexión de seguridad y de red		[E.7] Deficiencias en la organización
R011	No existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario	A 13 Seguridad de las Comunicaciones	Errores y fallos no intencionados [E] [E.2] Errores del administrador [E.7] Deficiencias en la organización

Fuente: Autor

7.4.4 Análisis de Riesgos

El análisis de riesgos informáticos es un método, el cual tiene una serie de etapas, entre las cuales están la identificación de activos informáticos, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, también como su probabilidad de ocurrencia y el efecto de su impacto, con el fin de determinar los controles más adecuados para aceptar, mitigar, trasladar o evitar la ocurrencia del riesgo encontrado.

Para en análisis de riesgos, los hallazgos o vulnerabilidades encontradas tanto en las pruebas como en las inspecciones realizadas al IDSN, se realizan valoraciones tanto cuantitativas como cualitativas, donde en primer lugar se da una valoración al riesgo y posteriormente se realiza el cálculo de este. Por último se obtiene el riesgo evaluado donde se clasifican los de mayor criticidad con el fin de mitigar su impacto en la organización.

Calculo del Riesgo

- Valoración del Riesgo: La valoración de los riesgos encontrados se determinara por la siguiente escala, siendo de 1 a 6 considerado como Bajo, de 8 a 9, Medio y de 12 a 16 como riesgo Alto:

Tabla 18 Valoración del Riesgo

Escala	Valoración del Riesgo
1 – 6	BAJO
8 – 9	MEDIO
12 – 16	ALTO

Fuente: Autor

- Calculo de Análisis de Riesgos

Probabilidad: es la posibilidad que la amenaza ocurra. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 la máxima que se materialice la amenaza.

Impacto: es el efecto que produce la amenaza. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 las máxima que afecte el recurso.

El riesgo total, se calcula de acuerdo a la probabilidad por el impacto:

Evaluación del Riesgo = Probabilidad * Impacto

- Riesgo Evaluado

Se evalúan los hallazgos tanto en las pruebas de penetración como en los cuestionarios realizados en el IDSN.

Matriz de Riesgos

Se identifican los riesgos previamente evaluados en una matriz con el fin de clasificar aquellos de mayor criticidad.

7.4.4.1 Análisis de Riesgos A9. Control de Acceso

Tabla 19 Análisis de Riesgos A9

Tipo de Activo	No	Vulnerabilidad	Probabilidad	Impacto	Evaluación Riesgo
[COM]	R001	No existen procedimientos de autorización para determinar quién accede a las redes y servicios de red.	4	4	**16**

Tipo de Activo	No	Vulnerabilidad	Probabilidad	Impacto	Evaluación Riesgo
[COM]	R002	No existen medios para acceder a redes y servicios de red como VPN.	2	3	**6**
[SW]	R003	No existen herramientas para el monitoreo del uso de servicios de red.	4	3	**12**
[HW]	R004	No existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.	3	4	**12**

Fuente: Autor

Matriz de Riesgos A9. Control de Acceso

Tabla 20 Matriz de Riesgos A9

PROBABILIDAD	**4**			**R003, R004**	**R001**
	3				
	2			**R002**	
	1				
		1	**2**	**3**	**4**
		IMPACTO			

Fuente: Autor

7.4.4.2 Análisis de Riesgos A13. Seguridad en las Telecomunicaciones

Tabla 21 Análisis de Riesgos A13

Tipo de Activo	No	Vulnerabilidad	Probabilidad	Impacto	Evaluación Riesgo
[HW]	R005	No se establecen las responsabilidades y procedimientos para la gestión de equipos de redes.	4	4	**16**
[IN]	R006	No existen controles para proteger los sistemas y aplicaciones conectados.	3	4	**12**
[IN]	R007	No existe responsabilidad operacional de las redes y de las operaciones de cómputo	2	3	**6**
[IN]	R008	No se coordinan las actividades de gestión para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.	4	4	**16**
[SW]	R009	No existe tecnología aplicada a la	3	4	**12**

Tipo de Activo	No	Vulnerabilidad	Probabilidad	Impacto	Evaluación Riesgo
		seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red.			
[COM]	R010	No se definen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red	2	4	**8**
[COM]	R011	No existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario	3	4	**12**

Fuente: Autor

Matriz de Riesgos A13. Seguridad en las Telecomunicaciones

Tabla 22 Matriz de Riesgos A13

PROBABILI	**4**				**R005, R008**
	3				**R006, R009, R11**
	2			**R007**	**R010**

D A D	**1**				
		1	**2**	**3**	**4**
	IMPACTO				

Fuente: Autor

7.4.5 Análisis de Riesgos

Para en análisis de riesgos, los hallazgos o vulnerabilidades encontradas tanto en las pruebas como en las inspecciones realizadas al IDSN, se realizan valoraciones tanto cuantitativas como cualitativas, donde en primer lugar se da una valoración al riesgo y posteriormente se realiza el cálculo de este. Por último se obtiene el riesgo evaluado donde se clasifican los de mayor criticidad con el fin de mitigar su impacto en la organización.

7.4.5.1 Calculo del Riesgo

- Valoración del Riesgo: La valoración de los riesgos encontrados se determinara por la siguiente escala, siendo de 1 a 6 considerado como Bajo, de 8 a 9, Medio y de 12 a 16 como riesgo Alto:

Tabla 23 Valoración del Riesgo

Escala	Valoración del Riesgo
1 – 6	BAJO
8 – 9	MEDIO
12 – 16	ALTO

Fuente: Autor

- Calculo de Análisis de Riesgos

Probabilidad: es la posibilidad que la amenaza ocurra. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 la máxima que se materialice la amenaza.

Impacto: es el efecto que produce la amenaza. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 las máxima que afecte el recurso.

El riesgo total, se calcula de acuerdo a la probabilidad por el impacto:

Evaluación del Riesgo = Probabilidad * Impacto

- Riesgo Evaluado

Se evalúan los hallazgos tanto en las pruebas de penetración como en los cuestionarios realizados en el IDSN.

Tabla 24. Cuadro Resumen de Riesgos

Recurso	**No**	**Vulnerabilidad**	**Amenaza**	**Riesgo**	**Probabilidad**	**Impacto**	**Evaluación Riesgo**
Software	R001	No existe tecnología aplicada a la seguridad de servicios de red como autenticación, criptografía y controles de conexión	Ausencia de tecnologías de seguridad	Ataques informáticos	3	4	**12**
	R002	Vulnerabilidad por Cross Site Scripting	Inyección de código malicioso	Denegación de Servicios (DoS)	4	4	**16**
	R003	Vulnerabilidad por Cross Domain JavaScript	Inyección de código malicioso	Inyección SQL	4	4	**16**
	R004	Los servicios web no incluyen la cabecera X-Frame options	Servicios web vulnerables	Ataques Clickjacking	2	3	**6**
	R005	Los servicios web no incluyen la cabecera X-Content-Type	Servicios web vulnerables	Sniffing	1	3	**3**
Hardware	R006	No existen responsabilidades y procedimientos para la	Deterioro de los equipos de redes	Afecta la disponibilidad y rendimiento de la red	3	4	**12**

Recurso	No	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Evaluación Riesgo
		gestión de equipos de redes					
	R007	Escaso mantenimiento de los equipos de red	Deterioro de los equipos de redes	Daño de equipos	3	3	**9**
	R008	Los equipos de red no cumplen con las especificaciones de los fabricantes	Mal funcionamiento de los equipos de red	Afecta la disponibilidad y rendimiento de la red	3	3	**9**
	R009	Los cables de energía eléctrica no están separados de los cables de telecomunicaciones.	Mal funcionamiento de las instalaciones de cableado	Afecta el correcto funcionamiento de los cableados	4	3	**12**
Comunicaciones	R010	Puertos Abiertos	Ataques a puertos abiertos con herramientas de explotación	Acceso a los servicios de información	3	4	**12**
	R011	Falta de procedimientos de autorización de acceso a la red y servicios de red	Acceso de personal no autorizado	Robo y perdida de la información	3	4	**12**
	R012	No se especifican medios para acceder a la red y servicios de red	Accesos remotos a la red	Robo y perdida de la información	3	4	**12**

Recurso	No	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Evaluación Riesgo
	R013	No hay monitoreo del uso de los servicios de la red	Ataques informáticos	Acceso y robo de la información. Suplantación de identidad.	2	4	**8**
	R014	No existen controles de acceso físico o lógico para el aislamiento de aplicaciones	Acceso no autorizado a la información	Alteración de la integridad de los datos	2	4	**8**
	R015	No se separan responsabilidades operacionales de redes con las operaciones de computo	Uso inadecuado de las operaciones de red y de las operaciones de computo	Controles de acceso a operaciones de red y de computo	2	2	**4**
	R016	No existen controles para proteger los sistemas y aplicaciones instaladas	Ataque informáticos	Robo y perdida de la información	4	4	**16**
	R017	No hay respaldo de la administración para implementación de los controles de gestión para optimizar el servicio de procesamiento de la información.	Escasa o nula implementación de las políticas y procedimientos de seguridad	Sistema de red vulnerable	4	4	**16**

Recurso	No	Vulnerabilidad	Amenaza	Riesgo	Probabilidad	Impacto	Evaluación Riesgo
	R018	No existen procedimientos técnicos que permitan garantizar la conexión segura de los servicios de red	Al no garantizar una conexión segura, los servicios de red son vulnerables y no son confiables	Sistema de red vulnerable Pérdida y robo de la información.	3	4	**12**
	R019	No existen procedimientos para restringir el acceso a servicios o aplicaciones de la red	Acceso no autorizado a la información	Robo y perdida de la información	3	4	**12**

Fuente: Autor

7.4.5.2 Matriz de Riesgos

A continuación se identifican los riesgos previamente evaluados en una matriz con el fin de clasificar aquellos de mayor criticidad.

Tabla 25. Identificación de los Riesgos

PROBABILIDAD	**4**			**R009**	**R002, R003, R016, R017**
	3			**R007, R008**	**R001, R006, R010, R011, R012, R018, R019**
	2		**R015**		**R013, R014**
	1			**R004, R005**	
		1	**2**	**3**	**4**
	IMPACTO				

Fuente: Autor

8. RESULTADOS DE LA AUDITORÍA

8.1 Tablas de hallazgos

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **R002**

ÁREA	EVALUACIÓN	D	M	A

FORMATO DE HALLAZGOS

REFERENCIA DOCUMENTOS	PREGUNTA

Descripción de Hallazgo – No Conformidad :
Vulnerabilidad por Cross Site Scripting

Riesgo – Evaluación Causa / Efecto :
Denegación de Servicios (DoS), la página presenta vectores de ataque expuestos a Cross Site Scripting, el cual envía código con secuencia de órdenes a sitios cruzados. La multitud peticiones puede ocasionar que se genere un denegación de servicios (DoS), afectando la disponibilidad del sistema.

Recomendaciones, Acción Correctiva :
Corregir los errores de diseño de las aplicaciones web. Realizar pruebas de aceptación para prevenir las fallas y huecos de seguridad.

Evidencias :
Los vectores de ataque se pueden evidenciar en el informe HTML realizado con la herramienta OWASP-ZAP

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **R003**

ÁREA	EVALUACIÓN	D	M	A

FORMATO DE HALLAZGOS

REFERENCIA DOCUMENTOS	PREGUNTA

Descripción de Hallazgo – No Conformidad :
Vulnerabilidad por Cross Domain JavaScript

Riesgo – Evaluación Causa / Efecto :
Se encontraron vectores de ataque que son vulnerables a inyección de código malicioso, como inserción de código JavaScript y órdenes de sentencias SQL presentes en la página web del IDSN

Recomendaciones, Acción Correctiva :
Implementar captchas o validaciones de petición de usuarios. Crear limitaciones y reglas en los formularios como en las entradas de texto y entradas de contraseñas. Impedir la entrada de código malicioso reemplazando los caracteres especiales por los equivalentes textuales.

Evidencias :
Se realizó la evaluación de cada uno de los vectores de ataque (DORKS) encontrados con el testeo de la página con la herramienta OWASP-ZAP. Las pruebas de inyección SQL se la realizo con la herramienta SQLmap

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **R0016**

ÁREA	EVALUACIÓN	D	M	A

FORMATO DE HALLAZGOS

REFERENCIA DOCUMENTOS	PREGUNTA

Descripción de Hallazgo – No Conformidad :
No existen controles para proteger los sistemas y aplicaciones instaladas además no existe un manual donde se implemente procedimientos y policías para la seguridad informática en el IDSN.

Riesgo – Evaluación Causa / Efecto :
Ataque informáticos y robo y perdida de la información

Recomendaciones, Acción Correctiva :
Establecer políticas en cuanto al uso de herramientas que garanticen la seguridad en los sistemas y aplicaciones instaladas. Implementar un manual de procedimientos y políticas de seguridad informática avalado y aprobado por la dirección del IDSN.

Evidencias :
A través de las entrevistas y listas de chequeo realizadas al coordinador de la oficina de sistemas del IDSN se determinó que no existe documentación acerca de políticas y procedimientos de Seguridad Informática.

Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **R0017**

ÁREA	EVALUACIÓN	D	M	A

FORMATO DE HALLAZGOS

REFERENCIA DOCUMENTOS	PREGUNTA

Descripción de Hallazgo – No Conformidad :
No hay respaldo de la administración para implementación de los controles de gestión para optimizar el servicio de procesamiento de la información.

Riesgo – Evaluación Causa / Efecto :
Escasa o nula implementación de las políticas y procedimientos de seguridad

Recomendaciones, Acción Correctiva :
Exigir la implementación de un sistema de control de seguridad de la información a la administración ya que la red del IDSN se considera vulnerable y está expuesta a distintos ataques informáticos.

Evidencias :
A través de las entrevistas y listas de chequeo realizadas al coordinador de la oficina de sistemas del IDSN se determinó que no existe apoyo por parte de la administración para implementar un documento políticas y procedimientos de Seguridad Informática.

8.2 Gestión de Riesgos

Los riesgos de mayor criticidad clasificados previamente en la matriz, son aquellos que necesitan ser mitigados de manera inmediata. Para ellos, se establece un control de mitigación con el fin de corregir su impacto sobre la organización.

Tabla 26. Gestión de Riesgos

Recurso	No	Riesgo	Control de Mitigación
Software	R001	Ataques informáticos	Implementar tecnologías de seguridad informática tales como herramientas criptográficas y de seguridad de red que permitan establecer un sistema que garantice la confiabilidad de los servicios de la organización.
	R002	Denegación de Servicios (DoS)	Corregir los errores de diseño de las aplicaciones web. Realizar pruebas de aceptación para prevenir las fallas y huecos de seguridad.

Recurso	No	Riesgo	Control de Mitigación
	R003	Inyección SQL	Implementar captchas o validaciones de petición de usuarios. Crear limitaciones y reglas en los formularios como en las entradas de texto y entradas de contraseñas. Impedir la entrada de código malicioso reemplazando los caracteres especiales por los equivalentes textuales.
Hardware	R006	Afecta la disponibilidad y rendimiento de la red	Se debe implementar revisiones periódicas de mantenimiento preventivo a los equipos de redes
	R007	Daño de equipos	Se debe implementar revisiones periódicas de mantenimiento preventivo a los equipos de redes
	R008	Afecta la disponibilidad y rendimiento de la red	La organización debe contar con un proveedor d confiable para la adquisición de equipos y garantizar el correcto funcionamiento de estos.
	R009	Afecta el correcto funcionamiento de los cableados	Establecer políticas de cableado en cuanto a su ubicación, mantenimiento, seguridad y disponibilidad.
Comunicaciones	R010	Acceso a los servicios de información	Se recomienda realizar el cierre de puertos para que los servicios no se vean afectados, sobre todo en los puertos: 22 que corresponde al servicio ssh, se puede ver comprometida la integridad de la información 139 que corresponde el servicio netbios, el cual se considera de riesgo alto

Recurso	No	Riesgo	Control de Mitigación
			111 que corresponde al proceso rpcbind que contiene la información de todos los servicios activos Otros puertos como el 445 y el 593 se consideran también de riesgo alto por encontrase expuestos.
	R011	Robo y perdida de la información	Establecer políticas de control de acceso a la red y sus servicios
	R012	Robo y perdida de la información	Establecer una VPN para evitar los accesos remotos a los sistemas de información del IDSN
	R013	Acceso y robo de la información. Suplantación de identidad.	Establecer una política para el uso de herramientas de monitoreo de red; herramientas de escaneo y mapeo de red, control de tráfico de red, herramientas de seguridad que eviten ataques informáticos como pishing, detección de código malicioso, sniffing, Spoofing, etc. Verificar periódicamente el estado de la red de datos del instituto para comprobar que se cumplan las normas recomendadas en cuanto a su seguridad.
	R014	Alteración de la integridad de los datos	Establecer una política de control de acceso en cuanto a los privilegios de uso de las aplicaciones.
	R016	Robo y perdida de la información	Establecer políticas en cuanto al uso de herramientas que garanticen la seguridad en los

Recurso	No	Riesgo	Control de Mitigación
			sistemas y aplicaciones instaladas.
	R017	Sistema de red vulnerable	Exigir la implementación de un sistema de control de seguridad de la información a la administración ya que la red del IDSN se considera vulnerable y está expuesta a distintos ataques informáticos.
	R018	Sistema de red vulnerable Pérdida y robo de la información.	Realizar un manual de procedimientos para garantizar la seguridad de los servicios de red en el IDSN.
	R019	Robo y perdida de la información	Establecer una política de control de acceso en cuanto uso de servicios o aplicaciones de la red.

Fuente: Autor

Es muy importante la implementación de estas políticas con el fin de garantizar la integridad, confidencialidad, disponibilidad de la información. Por lo tanto es necesario comprometerse con lo siguiente:

a) Asegurar que se establezca la política y los objetivos de la seguridad de la información y que estos sean viables con la dirección estratégica de la organización.

b) Asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización.

c) Asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles.

d) Comunicar la importancia de una gestión de la seguridad de la información eficiente y de conformidad con los requisitos del SGSI.

e) Asegurar y supervisar que el SGSI logre los resultados previstos.

f) Promover la mejora continua del SGSI y apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a las áreas de responsabilidad.

8.2.1 Valoración de riesgos de la seguridad de la información

La oficina de sistemas del IDSN, debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que permita:

a) Establecer y mantener los criterios de riesgos y de aceptación de la misma.

b) Asegurar que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables.

c) Aplicar el proceso de valoración de riesgos de la seguridad de la información para Identificar riesgos asociados a la perdida de la confidencialidad, integridad y disponibilidad, al igual que a los dueños de los mismos.

d) Analizar y evaluar los riesgos para priorizar los que mayor impacto puedan ocasionar para el área de informática de la Cooperativa.

8.2.2 Plan de tratamiento de riesgos

Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario dar un tratamiento. Las opciones posibles para el tratamiento del riesgo deberían incluir:

- Aplicación de los controles apropiados para reducir el riesgo.
- Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política respectiva para la seguridad de la información.
- Evitación de los riesgos al no permitir acciones que pudieran hacer que estos se presentaran.

- Transferencia de riesgos asociados a otras partes.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se encuentran descritos anteriormente y se deben implementar adecuadamente.

8.3 INFORME GENERAL DE AUDITORÍA

San Juan de Pasto, 29 de mayo de 2016

Ingeniero:
GUSTAVO CUELLAR
Coordinador Oficina de Sistemas
IDSN
Ciudad

Por medio de la presente, se remite a usted el Informe Final de la auditoría de sistemas practicada a la red de datos del Instituto Departamental de Salud de Nariño, que se realizó el periodo comprendido entre febrero de 2016 a mayo de 2016 como resultado de nuestro trabajo de grado para optar el título de especialista en Seguridad Informática.

La revisión comprendió la evaluación de la seguridad de la red del Instituto Departamental de Salud de Nariño (IDSN).

En el citado informe encontrará las políticas y procedimientos a las cuales se llegó como resultado después de la aplicación de las técnicas y procedimientos de auditoría de sistemas.

A continuación, se muestran los resultados obtenidos en la auditoría y recomendaciones generales de los procesos que fueron evaluados, teniendo en cuenta que algunos de los riesgos ya fueron corregidos durante el transcurso de la auditoría

Riesgos encontrados:

- Existen varios puertos abiertos.
- No se bloquean páginas de uso no institucional.
- No se cuenta con políticas de seguridad actualizadas para la red.
- La clave de Wifi es pública y esta publica en sitios visibles.
- No se cuenta con protecciones antimalware.
- No se cuenta con planes de contingencia para el reemplazo del personal que administra red en caso de ausencia en caso de falta del personal clave en la parte de Redes de datos, O el proceso no está documentado

- Existe un inventario actualizado del hardware de comunicaciones, pero no se encuentra documentado.
- No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware de la red de datos.
- No se lleva una bitácora con el registro de inconvenientes con la prestación de los servicios de red que presta el IDSN.

Recomendaciones:

- Implementar los procedimientos planteados para la seguridad de la red
- Implementar controles que permitan restringir el accesos a sitios web de uso no institucional
- Implementar políticas de seguridad para la red de datos
- Restringir y controlar el acceso a la red Wifi y cambiar las claves de todas las redes Wifi del IDSN.
- Implementar controles encaminados a la protección antimalware
- Tener planes de contingencia para el reemplazo del personal clave que administra la red de datos del IDSN, para evitar contingencias al momento de faltar el personal clave.
- Actualizar el inventario de los equipos de red.
- Implementar simulacros con los planes de contingencia con el fin de estar preparados para evitar problemas a futuro.
- Implementar una bitácora con el registro de inconvenientes en la prestación d los servicios de red.

Quedamos de Usted para cualquier aclaración al respecto.

Cordialmente,

_____ _____

Javier Mesías Narváez **Diego Rosero Almeida**

9. CONCLUSIONES

- La realización de la auditoría permitió determinar amenazas, vulnerabilidades y riesgos que pueden atentar contra la seguridad de la información, lo cual permitió proporcionar políticas y controles para mitigar dichos eventos adversos.

- Determinar los riesgos a los cuales está este expuesto el IDSN, permitió establecer los procedimientos necesarios para garantizar los niveles de confidencialidad, integridad y disponibilidad de la información.

- Las políticas y procedimientos de seguridad formuladas para la red del IDSN, las cuales están consignadas en este documento, permitirán implantar nuevos controles y mejorar los controles existentes para proteger y mantener la seguridad de la información que actualmente se maneja en el área de sistemas.

- Después de haber realizado este trabajo de auditoría, donde se formularon políticas y procedimientos para la red del IDSN, es importante contar con el apoyo de la Dirección y de la Oficina de Sistemas del IDSN, para que se implementen en un futuro las recomendaciones plateadas.

10. RECOMENDACIONES

- Se deben implementar las políticas y procedimientos para la seguridad de red del IDSN, con el fin de mantener la seguridad de la información, teniendo en cuenta que la información, es el activo más importante que tiene el IDSN.

- Cuando se realice la implementación de los controles para la red del IDSN, consignados en este documento, estos deben ser acatadas por el personal de la oficina de sistemas y todo el personal que tenga injerencia sobre la red, en caso contrario se deben aplicar las sanciones del caso, de acuerdo al impacto que se cause sobre los activos de información.

- Se debe controlar y restringir el acceso a todas las redes Wifi del IDSN, a personal ajeno a la institución, esto con el fin de evitar el acceso de personal no autorizado, previniendo de esta manera las congestiones del tráfico de red y posibles intrusiones.

- Es importante contar con los medios necesarios para identificar las vulnerabilidades amenazas y riesgos a los cuales pueda estar expuesta la red de IDSN, teniendo en cuenta que se puede aprovechar estas debilidades para afectar la confidencialidad, integridad y disponibilidad de la información.

- Es importante realizar capacitaciones por parte de la Dirección del IDSN, a todo el personal tanto a los funcionarios de planta como los de contrato, en materia de seguridad informática con el fin de crear una conciencia de protección del activo más importante para la empresa y de esta manera mantener su integridad, disponibilidad y confidencialidad.

- Para las aplicaciones de desarrollo propio del IDSN, se recomienda validar la fase de desarrollo del software, con el fin de realizar un diagnóstico temprano y oportuno de vulnerabilidades.

Bibliografía

ANTONIO ÁNGEL RAMOS VARÓN, CARLOS A BARBERO MUÑOZ., JUAN MANUEL GONZÁLEZ CAÑAS, FERNANDO RAMOS PICOUTO, Seguridad Perimetral, Monitorización y Ataques en Redes. Mundo Hacker, 1a Ed., RA-MA Editorial, Colombia, 2015.

Artículo 5: WIFI. La comunicación inalámbrica Internet: <http://www.aulaclic.es/articulos/wifi.html.>

Auditoría aplicada a la seguridad en redes de computadores, Internet: <http://www.monografias.com/trabajos10/auap/auap.shtml>

Auditoría Informática, Internet: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

BOGOTÁ. UNIVERSIDAD NACIONAL DE COLOMBIA. Guía para elaboración de políticas de seguridad [en línea]. [Consultado el 17 de abril de 2015]. Disponible en Internet: http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf.

Clasificación de los tipos de auditoría, Internet: <http://myblog-bilky.blogspot.com/>

COSTAS SANTOS JESÚS, Seguridad informática, 1ª Ed, Editorial RA – MA, Ediciones de la U, Bogotá, 2001

ECHENIQUE GARCÍA JOSÉ A. Auditoría en Informática. 2ª Ed., Editorial Mc Graw Hill, México: 2001.

ECHENIQUE GARCÍA JOSÉ A. Auditoría en informática. 5a Editorial Mc GRAW-HILL. México D.F: 2001.

El portal de ISO 27001 en español. Internet http://www.iso27000.es/

GAMINO JHONATAN. Proceso de Penetration Testing [en línea]. [Consultado el 22 de abril de 2015]. Disponible en Internet: <https://www.academia.edu/7168943/1.-Penetration testing.

Las Nuevas Versiones de las normas ISO 27001 e ISO 27002, Internet: http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf

Ley 1273 de 2009 en PDF Internet: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Norma ISO 270001, Resumen en PDF. Internet: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

PIATTINI MARIO, DEL PESO EMILIO. Auditoría en informática. Un enfoque práctico. 2ª Ed, Alfaomega /RA-MA, México D.F: 2001.
Sistemas de Gestión Seguridad de la Información, Internet: <http://sgsi-iso27001.blogspot.com.co/search/label/ISO%2027005>.

SOLARTE, FRANCISCO N J, Auditoría Informática y de Sistemas, Internet: <http://auditordesistemas.blogspot.com.co/>.

SOLARTE, FRANCISCO N J, GUSTIN LÓPEZ ENITH ENILSE HERNÁNDEZ REVELO RICARDO JAVIER. Manual de Procedimientos para llevar a la práctica la auditoría informática. Colombia: Editorial CESMAG, 2012.

VEITES GÓMEZ ÁLVARO. Auditoría de Seguridad Informática. Editorial Ediciones. Colombia: 2013.

ANEXOS

Por motivos de seguridad de la información, no se anexaron documentos e informes de pruebas estos anexos se entregaran en medio magnético.

Anexo A Listas de chequeo ISO 27001

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 9 Control de Acceso
Subdominio A 9.1.2

OBJETIVO:

Verificar el control A 9.1.2 Acceso a redes y a servicios en red, de acuerdo a la norma ISO 27001:2013

Control

Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

NOMBRE	CARGO
Gustavo Cuéllar De los Ríos	Administrador Red de Datos

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Ítem	Si	No
¿Qué redes y que servicios de red tiene el acceso el usuario autorizado?	✓	
¿Los procedimientos de autorización para determinar a quién se permite acceder a las redes y servicios de red?		✓
¿Los controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?	✓	
¿Los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		✓
¿Los requisitos de autenticación de usuarios para acceder a diversos servicios de red?	✓	
¿El monitoreo del uso de servicios de red?		✓

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 9 Control de Acceso
Subdominio A 9.4.1

OBJETIVO:

Verificar el control A 9.4.1 Restricción de acceso a la información, de acuerdo a la norma ISO 27001:2013

Control

El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

NOMBRE	CARGO
Gustavo Cuéllar De los Ríos	Administrador Red de Datos

Se cuenta con los siguientes requisitos de restricción de acceso:

Ítem	Si	No
¿Menús para controlar acceso a la funcionalidad de las aplicaciones?	✓	
¿Control de los datos a los que puede tener acceso un usuario particular?	✓	
¿Control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?	✓	
¿Control de los derechos de acceso de otras aplicaciones?	✓	
¿Limitación de la información contenida en las salidas?	✓	
¿Controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?		✓

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones
Subdominio A 13.1.1

OBJETIVO:

Verificar el control A 13.1.1 Controles de redes, de acuerdo a la norma ISO 27001:2013

Control

Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.

NOMBRE	CARGO
Gustavo Cuéllar De Los Ríos	Administrador Red de Datos

Se tiene implementado los siguientes controles en la red con el fin de proteger la información:

Ítem	Si	No
Se establecen las responsabilidades y procedimientos para la gestión de equipos de redes?		✓
Se separa la responsabilidad operacional por las redes, de las operaciones de computo?		✓
Se tienen establecido controles especiales para : • salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?	✓	
• para proteger los sistemas y aplicaciones conectados?		✓
• Se cuenta con controles especiales para mantener disponibilidad de los servicios de red y computadores conectados?		
	✓	
Se cuenta con registro (Logging) y el seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?	✓	
Se coordinan las actividades de gestión para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma		✓

coherente a través de la infraestructura de procesamiento de información?				
Los sistemas en la red se autentican?			✓	
Se restringe la conexión de los sistemas a la red?			✓	
Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida	
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado		

UNAD Universidad Nacional Abierta y a Distancia	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DEL INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO**	**REF.** **CRD-01**

ÁREA	D	M	A
Red de Datos			

Lista de chequeo Dominio A 13 Seguridad de las Comunicaciones Subdominio A 13.1.2

OBJETIVO:

Verificar el control **A 13.1.2 13.1.2 Seguridad de los servicios de red**, de acuerdo a la norma ISO 27001:2013

Control

Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

NOMBRE	CARGO
Gustavo Cuéllar De los Ríos	Administrador Red de Datos

Se cuenta con las siguientes características de seguridad en las redes de servicio:

Ítem	Si	No
tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y controles de conexión de red;		✓
Los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;		✓
Los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario		✓

Elaboro por:	Javier Mesías Narváez	Reviso por	Diego Rosero Almeida
Entrevistado	Gustavo Cuellar De los Ríos	Firma del entrevistado	

Anexo B Resumen Analítico RAE.

Título de Documento.	Auditoría a la Seguridad de la Red de Datos del Instituto Departamental de Salud de Nariño
Autor	Mesias Narvaez Javier Orlando Rosero Almeida Diego Fernando
Palabras Claves	Auditoría, información, pruebas de penetración, seguridad,
Descripción En este proyecto de investigación se realizó una auditoría a la seguridad de la red, con el fin de formular unas políticas y procedimientos para la red del Instituto Departamental de Salud de Nariño (IDSN)	
Fuentes Bibliográficas	Echenique García, José Antonio. Auditoría en Informática. 2ª Ed., Editorial Mc Graw Hill, México, 2001. PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed, Alfaomega/RA-MA, México D.F, 2001. ECHENIQUE GARCÍA JOSÉ A., Auditoría en informática, 5a Editorial Mc GRAW-HILL, México D.F., 2001. SOLARTE, FRANCISCO N J, GUSTIN LÓPEZ ENITH ENILSE HERNÁNDEZ REVELO RICARDO JAVIER., Manual de Procedimientos para llevar a la practica la auditoría informática, 1a Ed., Editorial CESMAG, Colombia, 2012. ÁLVARO GÓMEZ VEITES., Auditoría de Seguridad Informática, 1a Ed., Editorial Ediciones de la U, Colombia, 2013. ANTONIO ÁNGEL RAMOS VARÓN, CARLOS A BARBERO MUÑOZ., JUAN MANUEL GONZÁLEZ CAÑAS, FERNANDO RAMOS PICOUTO, Seguridad Perimetral, Monitorización y Ataques en Redes. Mundo Hacker, 1a Ed., RA-MA Editorial, Colombia, 2015. Auditoría Informática y de Sistemas, Internet: <http://auditordesistemas.blogspot.com.co/>.

Sistemas de Gestión Seguridad de la Información, Internet: <http://sgsi-iso27001.blogspot.com.co/search/label/ISO%2027005>.

Las Nuevas Versiones de las normas ISO 27001 e ISO 27002, Internet: <http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf>

BOGOTÁ. UNIVERSIDAD NACIONAL DE COLOMBIA. *Guía para elaboración de políticas de seguridad [en línea]*. [Consultado el 17 de Abril de 2015]. Disponible en Internet: <http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf>

GAMINO, Jonathan. Proceso de Penetration Testing [en línea]. [Consultado el 22 de Abril de 2015]. Disponible en Internet: <https://www.academia.edu/7168943/1.-_Penetration_testing>

Contenido:

Planteamiento del Problema

De acuerdo a la información inicial recogida en el Instituto Departamental de Salud de Nariño (IDSN) y como uno de los usuarios de los sistemas de información del mismo, se ha detectado que se presentan situaciones de infiltración de usuarios no autorizados a la red del IDSN, estas vulneraciones han tenido como resultado cambios de índex de los sistemas de información y negación de servicios del servidor del IDSN, lo cual ocasiona retrasos en el ingreso de la información, no solamente a los clientes internos de los sistemas de información sino que también afecta a los clientes externos del mismo.

Lo anterior se debe a que no existe un sistema de control en la red del IDSN, lo cual ocasiona que se presenten este tipo de intromisiones.

Objetivo General

Establecer un sistema de control adecuado que evite los posibles ataques y reduzca los niveles de vulnerabilidad mediante la aplicación de una auditoría a la seguridad de la red de datos en la red en el Instituto Departamental de Salud de Nariño.

Objetivos Específicos

- Conocer la red de datos del instituto departamental de salud de Nariño para

verificar las vulnerabilidades, riesgos y amenazas existentes, lo que servirá como soporte para determinar el estado actual de la seguridad tanto física como lógica dentro de la institución.

- Elaborar el plan de auditoría donde se incluya el objetivo y alcances, la metodología, los recursos necesarios para llevarla a cabo, diseñar los instrumentos y el plan de pruebas que se ejecutará sobre la red de datos para determinar las causas de los problemas.

- Ejecutar las pruebas y aplicar los instrumentos que permitan evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes, los recursos afectados y las causas que los originan para proponer los controles adecuados para mitigarlos.

- Mostrar los resultados en el informe final para identificar los niveles de madurez en cada dominio evaluado, los hallazgos confirmados, los controles adecuados para establecer las políticas y procedimientos que permitan mitigarlos.

El proyecto trata del tema de auditoría aplicada a la seguridad en redes, donde se aplicara la norma ISO 27001. La metodología que se sigue es la siguiente:

En la primera fase se identifico el estado actual y los componentes de la red de datos del instituto departamental de salud de Nariño, con el fin de verificar las vulnerabilidades, riesgos y amenazas existentes y las actividades desarrolladas fueron, las siguientes:

- Realizar una visita de campo para conocer la infraestructura de la red de datos y el hardware que la soporta.
- Solicitar la documentación de la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos.
- Realizar una entrevistas con el administrador de la red y algunos de los usuarios que permita identificar algunos de los problemas de seguridad en la red de datos.

Para el cumplimiento de la fase dos, cuál era la planeación de la auditoría se desarrollaron las siguientes actividades:

- Determinar los puntos que serán evaluados.
- Identificar y seleccionar los métodos, pruebas y procedimientos necesarios.

Para la realización de la fase tres, la cual consistía en la ejecución de la auditoría se realizaran las siguientes actividades:

- Aplicar las pruebas e instrumentos de recolección de la información seleccionados.
    - Pruebas de intrusión
    - Pruebas de testeo
- Análisis y evaluación de riesgos.
- Organizar los papeles de trabajo de la auditoría

Para presentar los resultados de la auditoría se realizaran las siguientes actividades:

- Realizar la lista de hallazgos y con las causas que los originan.
- Realizar el informe final de auditoría con políticas y procedimientos de seguridad para la red.

Como producto final se entregó el informe con las políticas y controles definidos para la red y los resultados más importantes que se obtuvieron fueron problemas en:

- Control de acceso
- Trafico de red

Metodología

Se realizó una auditoría a la seguridad de la red, para ejecutar este examen consta de cuatro fases se realizó siguiente metodología:

- Etapa 1 (Conocimiento): En esta fase de analizo la red de datos para verificar las vulnerabilidades, riesgos y amenazas existentes.

- Etapa 2 (Planeación): En esta fase se elaboró el plan de auditoría, se diseñó los instrumentos y el plan de pruebas que se ejecutará sobre la red de datos.

- Etapa 3 (Ejecución): En esta fase se ejecutó las pruebas y se aplicó los instrumentos que permitieron evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes.

- Etapa 4 (Resultados): En esta fase final se entregó los resultados obtenidos en el desarrollo de la auditoría y los cuales se consolidaron en el informe final de la auditoría.

Conclusiones

la realización de la auditoría permitió determinar amenazas, vulnerabilidades y riesgos que pueden atentar contra la seguridad de la información, lo cual permitió proporcionar políticas y controles para mitigar dichos eventos adversos.

Determinar los riesgos a los cuales está este expuesto el IDSN, permitió establecer los procedimientos necesarios para garantizar los niveles de confidencialidad, integridad y disponibilidad de la información.

Las políticas y procedimientos de seguridad formuladas para la red del IDSN, las cuales están consignadas en este documento, permitirán implantar nuevos controles y mejorar los controles existentes para proteger y mantener la seguridad de la información que actualmente se maneja en el área de sistemas.

Después de haber realizado este trabajo de auditoría, donde se formularon políticas y procedimientos para la red del IDSN, es importante contar con el apoyo de la Dirección y de la Oficina de Sistemas del IDSN, para que se implementen en un futuro las recomendaciones plateadas.

Recomendaciones.

Entre las principales recomendaciones se encuentran las siguientes:

- Restricción a Páginas Web y Contenidos de uso No Institucional, consístete en restringir el acceso a páginas web de uso no institucional

- Procedimiento de Gestión de Vulnerabilidades consistente en cerrar los puertos en el servidor con el fin de prevenir ataques de negación de servicios e inyecciones SQL.

- Procedimiento para el Aseguramiento de la Red WIFI consistente en Objetivo: restringir las claves de la red WIFI solo al personal autorizado, en caso de solicitar el servicio se debe dejar registro que personas se conectan y se debe tener una red para la conexión temporal y su clave debe ser cambiada periódicamente, la clave de la red Wi fi no debe ser publicada en sitios públicos con el fin de evitar la congestión de la red.

Anexo C Resultados de Pruebas Efectuadas Durante la Auditoría

Prueba con protocolo Whois

Domain Name: IDSN.GOV.CO
Domain ID: D611023-CO
Sponsoring Registrar: .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID: 111111
Registrar URL (registration services): www.cointernet.com.co
Domain Status: clientTransferProhibited
Variant: IDSN.GOV.CO
Registrant ID: 7324-REG
Registrant Name: INSTITUTO DEPARTAMENTAL DE SALUD DE NARINO
Registrant Organization: INSTITUTO DEPARTAMENTAL DE SALUD DE NARINO
Registrant Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Registrant City: PASTO
Registrant State/Province: Nariño
Registrant Postal Code: 57
Registrant Country: Colombia
Registrant Country Code: CO
Registrant Phone Number: +92.7236928
Registrant Email: gustavo.cuellar@hotmail.com
Administrative Contact ID: 7324-ADMIN
Administrative Contact Name: GUSTAVO CUELLAR DE LOS RIOS
Administrative Contact Organization: IDSN
Administrative Contact Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Administrative Contact City: PASTO
Administrative Contact State/Province: Nariño
Administrative Contact Postal Code: 57
Administrative Contact Country: Colombia
Administrative Contact Country Code: CO
Administrative Contact Phone Number: +92.7236928
Administrative Contact Email: gcuellar100@gmail.com
Billing Contact ID: 7324-BILLING
Billing Contact Name: DIRECTOR
Billing Contact Organization: IDSN
Billing Contact Address1: CRA.29 CLLS.14 Y 15 PLAZOLETA BOMBONA
Billing Contact City: PASTO

Billing Contact State/Province: Nariño
Billing Contact Postal Code: 57
Billing Contact Country: Colombia
Billing Contact Country Code: CO
Billing Contact Phone Number: +92.7236928
Billing Contact Email: gcuellar@idsn.gov.co
Technical Contact ID: 7324-TECH
Technical Contact Name: gustavo cuellar de los rios
Technical Contact Address1: CRA 29 CLLS 14 Y 15 PLAZOLETA BOMBONA
Technical Contact City: pasto
Technical Contact Country: Colombia
Technical Contact Country Code: CO
Technical Contact Phone Number: +571.0000000
Technical Contact Email: gcuellar@idsn.gov.co
Name Server: NS.COMPUTRONIX.COM.CO
Name Server: NS.IDSN.GOV.CO
Created by Registrar: NEULEVELCSR
Last Updated by Registrar: .CO INTERNET S.A.S.
Domain Registration Date: Wed Jun 09 00:00:00 GMT 1999
Domain Expiration Date: Mon Jun 08 23:59:59 GMT 2020
Domain Last Updated Date: Tue Jun 09 10:15:02 GMT 2015
DNSSEC: false

Prueba con Zenmap

Starting Nmap 7.01 (https://nmap.org) at 2016-05-06 02:12 COT
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating NSE at 02:12
Completed NSE at 02:12, 0.00s elapsed
Initiating Ping Scan at 02:12
Scanning www.idsn.gov.co (**190.69.156.11**) [4 ports]
Completed Ping Scan at 02:12, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:12
Completed Parallel DNS resolution of 1 host. at 02:12, 0.28s elapsed
Initiating SYN Stealth Scan at 02:12
Scanning www.idsn.gov.co (**190.69.156.11**) [1000 ports]
Discovered open port 21/tcp on **190.69.156.11**
Discovered open port 111/tcp on **190.69.156.11**
Discovered open port 22/tcp on **190.69.156.11**
Discovered open port 443/tcp on **190.69.156.11**
Discovered open port 80/tcp on **190.69.156.11**
Increasing send delay for **190.69.156.11** from 0 to 5 due to max_successful_tryno increase to 5
Completed SYN Stealth Scan at 02:13, 39.67s elapsed (1000 total ports)
Initiating Service scan at 02:13

Scanning 5 services on www.idsn.gov.co (**190.69.156.11**)
Completed Service scan at 02:13, 17.37s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.idsn.gov.co (**190.69.156.11)**
Retrying OS detection (try #2) against www.idsn.gov.co (**190.69.156.11**)
Initiating Traceroute at 02:13
Completed Traceroute at 02:13, 3.02s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 02:13
Completed Parallel DNS resolution of 8 hosts. at 02:13, 6.66s elapsed
NSE: Script scanning **190.69.156.11.**
Initiating NSE at 02:13
Completed NSE at 02:14, 40.41s elapsed
Initiating NSE at 02:14

```
Completed NSE at 02:14, 0.00s elapsed
Nmap scan report for www.idsn.gov.co (190.69.156.11)
Host is up (0.14s latency).
Not shown: 989 closed ports
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         Pure-FTPd
22/tcp   open     ssh         OpenSSH 6.0p1 Debian 4 (protocol 2.0)
| ssh-hostkey:
|   1024 d1:89:c8:df:59:c8:f0:81:fb:76:a4:81:a4:ca:97:fc (DSA)
|   2048 88:dd:bf:17:9b:0a:95:a6:32:23:5a:5a:b6:e7:ae:64 (RSA)
|_  256 27:81:b2:1f:ee:5a:d8:09:b6:16:23:71:7b:39:9c:03 (ECDSA)
80/tcp   open     http        Apache httpd 2.2.22 ((Debian))
|_http-favicon: Unknown favicon MD5: A376B20E57F7F45CD0D378A50944AF9F
|_http-generator: Joomla! - Open Source Content Management
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 16 disallowed entries (15 shown)
| /joomla/administrator/ /administrator/ /cache/ /cli/
| /components/ /images/ /includes/ /installation/ /language/
|_/libraries/ /logs/ /media/ /modules/ /plugins/ /templates/
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: ..:: Instituto Departamental de Salud de Nari\xC3\xB1o - IDSN ::.. -...
111/tcp  open     rpcbind     2-4 (RPC #100000)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/http    Apache httpd 2.2.22
| http-methods:
|_  Supported Methods: GET
|_http-server-header: Apache/2.2.22 (Debian)
| ssl-cert: Subject: commonName=linuxdb
| Issuer: commonName=linuxdb
| Public Key type: rsa
| Public Key bits: 2048
```

```
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-08-28T17:20:25
| Not valid after:  2023-08-26T17:20:25
| MD5:   f653 5b5a f0f9 d75e b80a 7e96 bd39 f159
|_SHA-1: ede8 ad74 fa8b a15a 0646 52a2 28cd 9158 b6ef 9523
```

|_ssl-date: 2016-05-06T07:39:31+00:00; +25m40s from scanner time.
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
4444/tcp filtered krb524
6129/tcp filtered unknown
Aggressive OS guesses: Linux 3.2 - 3.8 (96%), Linux 2.6.32 - 2.6.39 (94%), Linux 2.6.32 - 3.0 (93%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 3.0 or 3.5 (92%), Linux 3.11 - 4.1 (92%), Linux 3.8 (91%), WatchGuard Fireware 11.8 (91%), Linux 3.1 - 3.2 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.547 days (since Mon May 2 13:06:45 2016)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOP RTT   ADDRESS
1   445.23 ms Dynamic-IP-181550761.cable.net.co (**181.55.76.1**)
2   40.75 ms 172.21.111.202
3   138.23 ms Static-IP-1901572189.cable.net.co (**190.157.2.189**)
4   ...
5   165.61 ms telecom-nap.ccit.org.co (**206.223.124.149**)
6   74.51 ms 10.0.16.66
7   ...
8   153.56 ms 10.7.24.121
9   153.37 ms 10.7.24.122
10 128.64 ms 190.69.156.11

NSE: Script Post-scanning.
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.08 seconds
        Raw packets sent: 1401 (63.728KB) | Rcvd: 1245 (52.430KB)

Prueba con theharvester

```
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
[+] Emails found:
------------------
pperez@idsn.gov.co
avarela@idsn.gov.co
saca2913@idsn.gov.co
mchavisnan@idsn.gov.co
dmontenegro@idsn.gov.co
mguancha@idsn.gov.co
etrujillo@idsn.gov.co
mpaz@idsn.gov.co
mibarra@idsn.gov.co
elcharco@idsn.gov.co
egallo@idsn.gov.co
direccion@idsn.gov.co
informacion@idsn.gov.co
acaicedo@idsn.gov.co
mbotina@idsn.gov.co
eurbano@idsn.gov.co
bgomez@idsn.gov.co
srodriguez@idsn.gov.co
hvaldez@idsn.gov.co
sgomez@idsn.gov.co
pcaycedo@idsn.gov.co
myepez@idsn.gov.co
crue@idsn.gov.co
arboleda@idsn.gov.co
cvelasco@idsn.gov.co
yrivera@idsn.gov.co
mguerrero@idsn.gov.co
aarteaga@idsn.gov.co
rivera@idsn.gov.co
ipiales@idsn.gov.co
lparedes@idsn.gov.co
```

cceron@idsn.gov.co
soniagomezl@idsn.gov.co

[-] Resolving hostnames IPs...

[+] Hosts found in search engines:

190.69.156.11:intranet.idsn.gov.co
190.69.156.11:ssyreproductiva.idsn.gov.co
190.69.156.11:www.idsn.gov.co
190.69.156.11:smental.idsn.gov.co
190.69.156.11:cop.idsn.gov.co
190.69.156.11:aiepi.idsn.gov.co
190.69.156.14:sisa.idsn.gov.co
190.69.156.11:old.idsn.gov.co
190.69.156.14:Sisa.idsn.gov.co
190.69.156.11:Ssyreproductiva.idsn.gov.co
190.66.23.131:mail.idsn.gov.co
root@kali:~#

Prueba de escaneo de puerto con la herramienta en línea a través de la pagina
https://incloak.es/ports/

```
Not shown: 995 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
443/tcp open  https
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

Prueba de escaneo de puerto con la herramienta en línea a través de la página http://www.t1shopper.com/tools/port-scan/result/

Scanning ports on www.idsn.gov.co

www.idsn.gov.co is responding on port 21 (ftp).

www.idsn.gov.co isn't responding on port 23 (telnet).
www.idsn.gov.co isn't responding on port 25 (smtp).
www.idsn.gov.co is responding on port 80 (http).

www.idsn.gov.co isn't responding on port 110 (pop3).
www.idsn.gov.co isn't responding on port 139 (netbios-ssn).
www.idsn.gov.co isn't responding on port 445 (microsoft-ds).
www.idsn.gov.co isn't responding on port 1433 (ms-sql-s).
www.idsn.gov.co isn't responding on port 1521 (ncube-lm).
www.idsn.gov.co isn't responding on port 1723 (pptp).
www.idsn.gov.co isn't responding on port 3306 (mysql).
www.idsn.gov.co isn't responding on port 3389 (ms-wbt-server).
www.idsn.gov.co isn't responding on port 5900 ().
www.idsn.gov.co isn't responding on port 8080 (webcache).

Prueba de Inyección SQL mediante la herramienta SQLMAP

Inyección SQL

A través de los resultados generados por OWASP ZAP, se obtuvieron los siguientes DORKS para analizar una posible intrusión por Inyección SQL

Tabla Vulnerabilidades encontradas

Punto a evaluar	Vulnerable/No Vulnerable
http://www.idsn.gov.co/index.php?start=12	No vulnerable
http://www.idsn.gov.co/index.php?start=24	No vulnerable
http://www.idsn.gov.co/index.php?start=36	VULNERABLE
http://www.idsn.gov.co/index.php?start=48	No Vulnerable
http://www.idsn.gov.co/index.php?start=60	No vulnerable
http://www.idsn.gov.co/index.php?start=72	No Vulnerable
http://www.idsn.gov.co/index.php?start=84	No Vulnerable
http://www.idsn.gov.co/index.php?start=96	No Vulnerable
http://www.idsn.gov.co/index.php?start=108	No Vulnerable

Fuente: Autor