ANALISIS Y DIAGNOSTICO DE LA SEGURIDAD INFORMATICA DE INDEPORTES BOYACA

ANA MARIA RODRIGUEZ CARRILLO
53070244

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2014

ANALISIS Y DIAGNOSTICO DE LA SEGURIDAD INFORMATICA DE INDEPORTES BOYACA

ANA MARIA RODRIGUEZ CARRILLO
53070244

Trabajo de grado como requisito para optar el título de Especialista En Seguridad informática

Ingeniero
SERGIO CONTRERAS
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2014

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Tunja, 06 de Octubre de 2014.

DEDICATORIA

El presente trabajo es dedicado en primera instancia a Dios quien día a día bendice mi profesión y me ayuda con cada uno de los retos que se me presentan a lo largo del camino de mi vida.

A mi fiel compañero, amigo, cómplice y esposo, quien es la ayuda idónea diaria y mi fortaleza constante para seguir en el camino del conocimiento, quien no deja que me rinda y me apoya incondicionalmente para que día a día logre ser mejor persona.

A mis familiares y compañeros de trabajo, por todo su amor, confianza y apoyo incondicional, a nuestros compañeros y profesores gracias por la amistad, la comprensión, los conocimientos y dedicación a lo largo de todo este camino recorrido que empieza a dar indudablemente los primeros frutos que celebramos.

AGRADECIMIENTOS

La vida está llena de metas y retos, que por lo general van de la mano con grandes sacrificios, por eso hoy podemos decir que gracias a Dios y nuestras familias esta meta se ha cumplido y seguramente vendrá muchas metas que harán parte de nuestro gran triunfo personal como familiar.

El autor del presente trabajo agradece a Indeportes Boyacá, por permitirme realizar este proyecto de investigación y brindarme la confianza y apoyo necesario en el desarrollo de este proyecto de grado.

El autor del presente trabajo agradece a la Educación a Distancia en cabeza de la Universidad Nacional Abierta y a Distancia “UNAD”, por brindar la oportunidad de ser parte de dicha alma Mater y recibir tan excelentes conocimientos.

TABLA DE CONTENIDO

pág.

TABLA DE CUADROS

Pag.

TABLA DE ILUSTRACIONES

Pág.

INTRODUCCIÓN

En la actualidad Colombia cuenta con una amplia gama de Empresas que ofrecen diferentes bienes y servicios; muchas de estas empresas ofrecen los mismos servicios pero las diferencian algunos factores tales como: precio, calidad, atención al cliente, agilidad, servicio, entre otros. Teniendo en cuenta este nivel de competencia, lo que buscan las empresas es estar a la vanguardia de la tecnología con el fin de mantenerse en el mercado y desarrollarse como Empresa.

Las compañías buscan innovar en valor por medio de la tecnología para tener un aliado interno que les permita desarrollar sus actividades y obtener un crecimiento sostenible que les facilite seguir compitiendo en un mercado globalizado, cada vez más competitivo y con mayores exigencias por parte de los clientes

Día a día y en busca de mejorar la prestación de sus servicios las Empresas han implementado soluciones tecnológicas con el fin de ampliar sus mercados sin importar el lugar de ubicación de las personas, lo que conlleva a que aparezcan nuevos servicios como: información a través de la web, call center especializados, transacciones bancarias en línea, entre otros, llegando así ha obtener y capturar información de interés tanto para la empresa responsable de cada una de las transacciones como de personas malintencionadas que pueden hacer un mal uso de la información, ya que en ocasiones algunas empresas no tienen el especial cuidado en el tratamiento de la misma o simplemente no ha implementado un método seguro para el manejo de la información.

Hoy por hoy las personas y las organizaciones, buscan que los procesos sean agiles, rápidos y eficientes pero ante todo que sean seguros, se vive en un mundo donde lo que menos hay es tiempo, razón por la cual y en su necesidad de agilizar sus compromisos utilizan su información personal y privada de manera inadecuada lo que hace que las empresas busquen de cualquier medida

garantizar que sus clientes tengan confianza en las implementaciones tecnológica usadas por las Empresas haciendo un mayor énfasis en la seguridad que deben tener los usuarios en el momento de acceder a algunas de ellas.

Se debe tener en cuenta que las implementaciones tecnológicas invertidas en cada empresa son de alto costo y lo que ellas buscan es que las personas agilicen cada una de sus transacciones de manera oportuna y que sean utilizadas adecuadamente ya que si las mismas son inutilizadas generarían un deterioro al patrimonio de la empresa, por ende es necesario que las implementaciones tecnológicas lleven consigo la carga de la seguridad de la información con el fin de lograr prestar un buen servicio a los clientes y generar en ellos la confianza necesaria para seguir utilizándolas de lo contrario toda la inversión se perdería.

Ahora bien, lo que se pretende con la presente investigación, es determinar las vulnerabilidades presentes, en este caso INDEPORTES BOYACA con el manejo de la información y en este sentido sugerir o proponer mecanismos que mejoren la seguridad informática de la entidad para así optimizar su inversión en el área tecnológica.

1. PROBLEMA DE INVESTIGACIÓN

1.1DESCRIPCIÓN

El Instituto Departamental del deporte de Boyacá INDEPORTES BOYACA, en procura de su misión, ha implementado las tecnologías de información según las necesidades presentadas tales como páginas web, correos institucionales, bases de datos, software de contabilidad entre otros, lo que ha llevado a realizar inversiones en servidores, cableado estructurado, licencias, etc, todos estos ubicados de acuerdo a las dependencias responsables de su uso; en la actualidad INDEPORTES BOYACA maneja aproximadamente 200 empleados, con esta actualización informática, muchos de los procesos que se llevaban de manera manual han sufrido el cambio a la sistematización teniendo el constante miedo entre los funcionarios de la entidad la pérdida o filtración de la información, por lo anterior se hace necesario realizar un estudio de seguridad informática a la entidad con el fin de establecer si la información cuenta con una seguridad optima que cumpla a cabalidad los tres pilares básicos de la información y así generar confiabilidad a los funcionarios de dicha entidad y clientes externos que suministran y procesan información privilegiada que permita medir los resultados y tomar decisiones respecto a la misión del instituto.

Razón por la cual el personal del área misional, estratégica, de apoyo y de evaluación se preguntan qué tan segura y tan confiable es la información que se maneja a través de la red y cuales pudieran llegar a ser las posibles soluciones que puedan evitar la pérdida de información en el instituto teniendo en cuenta que no existe mecanismos de control eficaces que protejan la información que se maneja en Indeportes Boyacá.

1.2 FORMULACIÓN

¿Cómo determinar, detectar las posibles pérdidas o fraudes de información a través de las aplicaciones y elementos informáticos empleados en Indeportes Boyacá mediante pruebas de Hacking ético basadas en la metodología PHVA (Planear, Hacer, Verificar y Actuar) que permitan buscar una posible solución que mitigue el riesgo, aumente la confianza hacia el cliente, mejore la productividad, seguridad y eficiencia de los usuarios que utilizan los medios informáticos en Indeportes Boyacá?

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

El Proyecto es Análisis y diagnóstico de la Seguridad Informática de Indeportes Boyacá desde la implementación que tiene en infraestructura tecnológicas y aplicativos de uso de la entidad.

El proyecto resaltará las posibles deficiencias encontradas en la infraestructura tecnológica y aplicativos de Indeportes Boyacá.

El análisis de resultados permitirá tomar decisiones desde el punto de vista tecnológico en procura del mejoramiento de la seguridad de la información.

2.2 LIMITACIONES

- El Análisis y diagnóstico de la Seguridad Informática de Indeportes Boyacá se realizará en las instalaciones de Indeportes Boyacá.

- El análisis se realizará desde el punto de vista tecnológico.

- Las conclusiones y recomendaciones se le harán al Gerente de Indeportes Boyacá quien tomará la decisión de implementarlas o no.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Determinar el nivel de seguridad informática que existe en INDEPORTES BOYACA, mediante pruebas de hacking ético con el fin de establecer los posibles correctivos pertinentes en el tratamiento de la información de acuerdo a los tres pilares que esta maneja.

3.2OBJETIVOS ESPECÍFICOS

- Identificar cada uno de los Recursos que se desean proteger en Indeportes Boyacá.

- Realizar análisis de la seguridad informática a cada uno de los sistemas informáticos que se manejan en Indeportes Boyacá.

- Realizar las respectivas recomendaciones en la implementación tecnológica que permita mejorar la seguridad informática al interior de INDEPORTES BOYACA.

4. JUSTIFICACIÓN

La información es uno de los principales activos de todas y cada una de las empresas, sin importar la forma y el tratamiento que se les dé, con el paso de los años y en busca de optimizar cada uno de los procesos tanto en tiempo como en orden las personas comenzaron a implementar en cada una de las empresas la sistematización, consiguiendo efectivamente minimizar tiempos en cada una de las actividades que se realizan tanto en el interior como en el exterior de las empresas, partiendo de este punto y con el ánimo de satisfacer a los clientes por medio de la innovación y haciendo uso del aprovechamiento de los recursos tecnológicos cada una de estas empresas ha llegado al punto incluso de ofrecer sus trámites y servicios corporativos en línea, es decir, a través de su portal o página de internet, o incluso dentro de la misma organización implementar redes para compartir en forma directa los archivos que se manejen, teniendo que colocar su principal activo como lo es la información en un lugar de fácil acceso con el fin de cumplir con el objetivo de innovación e impacto tecnológico. Pero así como avanzan las empresas en el fortalecimiento de su seguridad informática, existen también personas que se dedican al estudio del robo o modificación de la información ya sea por intereses personales o fines lucrativos. Teniendo en cuenta lo anterior, y estando la información al alcance de los clientes como de algunos funcionarios, es necesario verificar que la misma se esté tratando con todas las medidas de seguridad como si se mantuvieran en una caja fuerte y constantemente vigilada, ahora bien, es de conocimiento que los datos que se manejan en cada una de las empresas son de tal importancia que son la base fundamental de su funcionamiento y es necesario garantizar esta seguridad de tal forma que se genere confianza y autenticidad.

En la actualidad INDEPORTES BOYACA, cuenta con servicios tecnológicos dentro y fuera de la institución, tales como páginas web, correos corporativos,

además utiliza bases de datos en cada uno de sus programas, software contable y archivos de importancia que son la base fundamental para el cumplimiento de su misión y que con la implementación de las tecnologías han tenido que sufrir algunos cambios para lograr optimizar el trabajo de la institución, no obstante nunca se ha realizado un análisis sobre la seguridad informática que se maneja en el instituto, por lo cual no se puede garantizar si el manejo de la información es el más adecuado o si por el contrario la información cumple con los tres pilares de la información que son: confidencialidad, integridad y disponibilidad, beneficiando en últimas a los diferentes clientes que utilizan los servicios ofrecidos por la entidad.

5. MARCO DE REFERENCIA

5.1 ANTECEDENTES TEMÁTICOS DE LA INVESTIGACIÓN FUNDAMENTOS, PROYECTOS Y TENDENCIAS

Para cumplir con el objeto de la investigación, es indispensable recorrer la historia frente a los diversos avances tecnológicos que ha implementado el hombre para mejorar su calidad de vida y cuáles han sido sus principales inconvenientes presentados con el desarrollo de estos, en especial con el tratamiento de la seguridad de la información y protección de datos.

Se le llama seguridad de la información a todo lo que conlleve a proteger y salvaguardar la información de todos y cada uno de los peligros que esta tenga al asecho con el fin de que la misma cumpla con ciertos requisitos, tales como: confidencialidad, disponibilidad e integridad, no diferente a la seguridad informática ya que lo que esta última busca es la misma seguridad pero en medios informáticos, de allí se desprende que los humanos desde los inicios de la historia hayan buscado diferentes métodos para la protección de la información quien desde ese mismo instante toma diferentes dimensiones dependiendo el contexto en el que trabaje, es así como desde la historia del hombre podemos encontrar que este ha tratado de esconder cierto tipo de información respecto a los demás hombres utilizando este aspecto en ventajas que serían usadas en un tiempo determinado, es así como en la antigüedad surgen las bibliotecas, lugares donde se podían resguardar la información para transmitirla y así evitar que otros la obtuvieran[1].

[1]Contreras N. (2011). Enfoque de la Seguridad de la información, Instituto Tecnológico Nacional de Argentina.

Una de las primeras muestras de protección de la información la encontramos en el Sun Tzue en el arte de la guerra y se vuelve a señalar con Nicolás Maquiavelo con su obra el príncipe, donde señalan la importancia de la información sobre sus adversarios[2], es tan así que después de la creación del lenguaje podemos observar que la información encuentra un tipo de seguridad en la Antigua Grecia con la creación de los primeros intentos criptográficos tales como la escítala quien usa el cifrado de transposición, luego para la época de los Romanos, Julio Cesar utilizaba un lenguaje de cifrado para referirse a sus comandantes.[3]

Llegado el auge de las computadoras hacía finales de los años 80, James P Anderson integrante de las fuerzas armadas norteamericanas publica uno de los primeros textos que habla sobre la seguridad en los computadores.[4]

Algunos estudios se realizan durante los años siguientes hasta que en 1980 James P. Anderson escribe "Computer Security Threat Monitoring and Surveillance"[5], es dónde se da comienzo para detección de intrusos en sistemas de computadores principalmente mediante la consultas de ficheros de log.

Entre 1984 y 1996, Dening y Neumann desarrollan el primer modelo de IDS denominado IDES (Intrusion Detection Expert System) basado en reglas. A partir de este momento, se han ido proponiendo y creando nuevos sistemas de detección de intrusos hasta obtener una separación clara entre los sistemas que

---

[2] Contreras N. (2011). Enfoque de la Seguridad de la información, Instituto Tecnológico Nacional de Argentina.

[3] Seguridad Informática, Claudio López, 2012.

[4]Bruneau, G. (2001). The History and Evolution of Intrusion Detection. http://www.sans.org/reading_room/whitepapers/detection/history-evolution-intrusion

[5] Anderson, J. P. (1980). Computer Security Threat Monitoring and Surveillance. http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf.

efectúan la detección dentro de los ordenadores y aquellos que la efectúan en el tráfico que circula por la red. [6]

A lo largo de la historia y con el uso de las computadoras se han detectado los siguientes ataques informáticos más relevantes en el transcurso de la historia:

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

9. Febrero de 2002: Adrian Lamo Vs. The New York Times: El señor Lamo ha hecho noticia en estos días por ser uno de los hackers soldados responsables de la filtración de los más de 400 mil cables diplomáticos de WikiLeaks. Sin embargo, hace ya casi una década, Adrian Lamo -apodado como "The Homeless Hacker"- se hizo conocido por la intrusión en los servidores de compañías como The New York Times, la cadena de tiendas Kinko's, Starbucks y Lexis-Nexis, provocando daños por aproximadamente 300 mil dólares.

8. Enero de 2008: Los anónimos contra la cienciología: No todos los ataques anónimos son malintencionados. También existen las causas nobles. Recién comenzando el año 2008, un grupo de Anonymous (que hoy no necesitan mayor presentación), realizaron ataques de denegación de servicio a los servidores de Scientology.org. Su objetivo: Salvar a la gente de la Cienciología impidiendo el lavado de cerebro.

---

[6] Ludovic Mé, C. M. (SSIR 2001). Intrusion detection: A bibliography. http://www.cs.uiuc.edu/class/fa05/cs591han/papers/intrusionbib.pdf.

7. Febrero de 2000: Mafiaboy Vs. Yahoo, CNN, eBay, Dell, & Amazon: Michael Calce, un joven canadiense de sólo 15 años de edad no se anda con chicas. En el año 2000 lanzó el Proyecto Rivolta, cuyo objetivo era botar el sitio web con más tráfico de ese entonces: Yahoo. No contento con eso siguió con CNN, eBay, Dell y Amazon. Su objetivo no era otro que demostrar con cuanta facilidad un niño podía noquear a los gigantes de internet. Fue condenado a donar US$250 (unos 120 mil pesos chilenos) a caridad.

6. Noviembre de 2008: Atacante desconocido Vs. Microsoft (y el mundo): Si hay una palabra que causa escalofríos en el mundo de la seguridad informática, esta es Conficker. Desde fines del año 2008 este gusano comenzó a explotar vulnerabilidades en varios de los sistemas operativos de Microsoft. Una vez infectados estos equipos pueden ser controlados como redes masivas dispuestas a atacar a quien sea. Conficker ha infectado a millones de computadores en todo el mundo y se dice que incluso puede ser una amenaza de nivel militar.

5. Agosto de 1999: Jonathan James vs. Departamento de Defensa de Estados Unidos Jonathan James es uno de los hackers más famosos de la historia. En 1999 entró en los computadores de la Agencia de reducción de Amenazas interceptando miles de mensajes confidenciales, contraseñas y el software que controlaba toda la vida en la agencia espacial internacional. Tanto fue el daño que la Nasa se vio obligada a apagar sus redes por 3 semanas, en la que invirtió miles de dólares en mejoras de seguridad.

4. Agosto de 2009: Rusia vs. el blogero georgiano "Cyxymu": Ya son cientos de millones los usuarios que cada día dedican una parte de su tiempo a visitar los sitios de redes sociales. Muchos de nosotros recordaremos un día

durante el año pasado en que Facebook y Twitter eran imposibles de navegar. ¿La razón? Un ataque de denegación de servicio por parte de los servicios rusos para intentar silenciar al blogger Cyxymu quien informaba acerca de la difícil situación que se vivía en esos días en la república de Georgia. Paradójicamente este ataque contribuyó a que la situación de la ex república soviética fuera conocida en todo el mundo.

3. Marzo de 1999: David L. Smith vs. Microsoft Word y Outlook: En 1999, el residente del estado de New Jersey David L. Smith le regaló a una stripper en Florida el regalo definitivo: un virus informático bautizado con su nombre. Utilizando una cuenta robada del servicio AOL, Smith publica un documento de Word infectado con el virus "Melissa" en uno de los grupos de discusión más concurridos de la red. El virus se propagó rápidamente vía correo electrónico afectando a millones de computadores que utilizaban Outlook, provocando más deUS$80 millones de dólares en daños.

2. Julio de 2009: Atacante desconocido vs. Estados Unidos y Corea del Sur: Durante tres días, los sitios web de uno de los diarios más importantes de Corea del Sur, de una importante cadena de subastas, un banco, del presidente, de la Casa Blanca, el Pentágono y las ejército de Corea -por sólo nombrar a algunos pocos- fueron víctimas de un ataque masivo de denegación de servicio (DDoS), a través de una red de bots de más de 166 mil computadores controlados supuestamente desde Corea del Norte a través del famoso gusano Mydoom, por lo que el origen nunca fue comprobado.

1. Noviembre de 1998: Robert Tappan Morris contra el mundo: Robert Tappan Morris creó un monstruo. En 1988, mientras era estudiante de posgrado en la universidad de Cornell, diseñó un gusano capaz de autoreplicarse y le asignó una misión: determinar el tamaño de Internet. Sin

embargo, el experimento escapó de su control, infectando miles de computadores por mucho tiempo, con un costo de millones de dólares en daños. Morris enfrentó cargos por este accidental crimen y fue condenado a pagar con US$10.000 y 400 horas de trabajo comunitario. El código fuente de este archivo se encuentra guardado en un disquete de 3.5" y se puede visitar en el Museo de Ciencias de la ciudad de Boston.[7]

Teniendo en cuenta los antecedentes mencionados con anterioridad y no siendo estos ajenos a ninguna empresa o tipo de información, se hace necesario mantener bajo todas las circunstancias un sistema seguro que cumpla con los aspectos de confiabilidad, integridad y disponibilidad, es decir que cumplan con que la información que se encuentre dentro del sistema sea accedida única y exclusivamente por usuarios que tienen autorización y que los mismos serán utilizados para uso exclusivo del cumplimiento de la misión de la Empresa y no la tendrá a disposición otras entidades que cumplan con los mismos objetivos, razón por la cual este estudio se enmarca dentro de la seguridad de la empresa ya que si su información en alguno de los procesos es alterada perdería validez y confianza ante los usuarios, es por esto que se debe tener un trato especial de la información dentro y fuera respecto a las redes o medios que se use para transmitir la misma.

Ahora bien, no solo los datos deben tener especial cuidado en su transportación o publicación sino que es necesario determinar también el nivel de seguridad en la parte física como en la no tangible, llámese físico a todo lo que se considera como hardware, es decir todo lo que se puede ver y tocar y que unidos forman nuestro computador y el nivel de seguridad frente al acceso a estos equipos, tales como claves, permisos de autenticación entre otros. En la actualidad hay miles de estadísticas tales como la publicada en el año 2000 por el Instituto de Seguridad

[7] González Y, Castaño W., (2012), Fundamentos de la Seguridad de la Información, UNAD.

computacional y el FBI, donde se muestra que el 70% de los ataques informáticos ocurren dentro de la misma organización ya que no se cuenta con políticas de seguridad interna.

5.2 HERRAMIENTAS DE ANALISIS Y DE VULNERABILIDAD.

Se debe partir del concepto de vulnerabilidad para poder dar énfasis en las herramientas que existen en la actualidad y que han ayudado a identificar vulnerabilidades de seguridad informática.

- *Vulnerabilidad: En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.*[8]

Dentro de las herramientas existentes más utilizadas para detectar vulnerabilidades informáticas se tienen las siguientes:

- *“ Nessus: Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.*

[8] Texto Recuperado de la pagina web
http://www.alegsa.com.ar/Dic/vulnerabilidad.php#sthash.rqq7Yc4k.dpuf

- *Ethereal: Oliendo el pegamento que mantiene a Internet unida. Ethereal es un analizador de protocolos de red para Unix y Windows, y es libre {free}. Nos permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que queramos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.*

- *Netcat: La navaja multiuso para redes. Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad del tipo "back-end" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta rica en características, útil para depurar {debug} y explorar, ya que puede crear casi cualquier tipo de conexión que podamos necesitar y tiene muchas habilidades incluidas.*

- *Hping2: Una utilidad de observación {probe} para redes similar a ping pero con esteroides. hping2 ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.*

- *DSniff: Un juego de poderosas herramientas de auditoría y pruebas de penetración de redes. Este popular y bien diseñado set hecho por Dug*

Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante -- por ej. debido al uso de switches {"layer-2 switches"}. sshmitm y webmitm implementan ataques del tipo monkey-in-the-middle activos hacia sesiones redirigidas de SSH y HTTPS abusando de relaciones {"bindings"} débiles en sistemas con una infraestructura de llaves públicas {PKI} improvisados.

- *Ettercap: Por si acaso todavía pensemos que usar switches en las LANs nos da mucha seguridad extra. Ettercap es un interceptor/sniffer/registrador para LANs con ethernet basado en terminales {terminal-based}. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También es posible la inyección de datos en una conexión establecida y filtrado al vuelo {"on the fly"} y aun manteniendo la conexión sincronizada. Muchos modos de sniffing fueron implementados para darnos un set poderoso y completo de sniffing. También soporta plugins. Tiene la habilidad para comprobar si estamos en una LAN con switches o no, y de identificar huellas de sistemas operativos {OS fingerprints} para dejarnos conocer la geometría de la LAN.*

- *John the Ripper: Un extraordinariamente poderoso, flexible y rápido cracker de hashes de passwords multi-plataforma. John the Ripper es un cracker de passwords rápido, actualmente disponible para muchos sabores de Unix (11 son oficialmente soportados, sin contar arquitecturas diferentes), DOS, Win32, BeOs, y OpenVMS. Su propósito principal es detectar passwords de Unix débiles. Soporta varios tipos de hashes de password de crypt(3) que son comúnmente encontrados en varios sabores de Unix, así como también AFS de Kerberos y las "LM hashes" de Windows NT/2000/XP. Otros varios*

tipos de hashes se pueden agregar con algunos parches que contribuyen algunos desarrolladores.

- *OpenSSH / SSH: Una manera segura de acceder a computadoras remotas. Un reemplazo seguro para rlogin/rsh/rcp. OpenSSH deriva de la versión de ssh de OpenBSD, que a su vez deriva del código de ssh pero de tiempos anteriores a que la licencia de ssh se cambiara por una no libre. ssh (secure shell) es un programa para loggearse en una máquina remota y para ejecutar comandos en una máquina remota. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables {"untrusted hosts"} sobre una red insegura. También se pueden redirigir conexiones de X11 y puertos arbitrarios de TCP/IP sobre este canal seguro. La intención de esta herramienta es la de reemplazar a `rlogin', `rsh' y `rcp', y puede ser usada para proveer de `rdist', y `rsync' sobre una canal de comunicación seguro. Hay que notar que la versión del siguiente link a SSH.com cuesta dinero para algunos usos, mientras que OpenSSH es siempre de uso libre. Los usuarios de Windows quizás quieran el cliente de SSH libre PuTTYo la linda versión para terminal {"terminal-based port"} de OpenSSH que viene con Cygwin.*

- *Tripwire: El abuelo de las herramientas de comprobación de integridad de archivos. Un comprobador de integridad de archivos y directorios. Tripwire es una herramienta que ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema (por ej. diariamente), Tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo.*

- *Nikto: Un escáner de web de mayor amplitud. Nikto es un escáner de servidores de web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de 200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker.*

- *Kismet: Un poderoso sniffer para redes inalámbricas. Kismet es un sniffer y disecador de redes 802.11b. Es capaz de "sniffear" utilizando la mayoría de las placas inalámbricas; de detectar bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP; listar equipos de Cisco por medio del "Cisco Discovery Protocol"; registrar paquetes criptográficamente débiles y de generar archivos de registro compatibles con los de ethereal y tcpdump. También incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes. La versión para Windows está todavía en etapas preliminares. Es por eso que quien lo necesite quizás quiera darle una mirada a Netstumbler si tiene algún problema.*

- *SuperScan: El escáner de TCP para Windows de Foundstone. Un escáner de puertos de TCP, pinger y resolvedor de nombres {"hostname resolver"} basado en connect(). Viene sin el código fuente. Puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP especificados. También puede conectarse a cualquier puerto abierto descubierto utilizando aplicaciones "ayudantes" especificadas por el usuario (e.g. Telnet, Explorador de Web, FTP).*

- *Netfilter: El filtro/firewall de paquetes del kernel Linux actual. Netfilter es un poderoso filtro de paquetes el cual es implementado en el kernel Linux estándar. La herramienta iptables es utilizada para la configuración. Actualmente soporta filtrado de paquetes stateless o statefull,*

y todos los diferentes tipos de NAT (Network Address Translation) y modificación de paquetes {"packet mangling"}. Para plataformas no Linux, podemos verpf (OpenBSD), ipfilter (muchas otras variantes de UNIX), o incluso el firewall personal Zone Alarm (Windows).

- *Network Stumbler: Sniffer gratuito de 802.11 para Windows. Netstumbler es la más conocida herramienta para Windows utilizada para encontrar "access points" inalámbricos abiertos ("wardriving"). También distribuyen una versión para WinCE para PDAs y similares llamada Ministumbler. Esta herramienta es actualmente gratis pero sólo para Windows y no incluye el código fuente. Se hace notar que "El autor se reserva el derecho de cambiar este acuerdo de licencia a gusto, sin previo aviso." Los usuarios de UNIX (y usuarios de Windows avanzados) quizás quieran darle una mirada a Kismet.*

- *AirSnort: Herramienta de crackeo del cifrado WEP de 802.11. AirSnort es una herramienta para LANs inalámbricas (WLAN) que recupera las llaves de cifrado. Fue desarrollada por el Shmoo Group y opera monitoreando pasivamente las transmisiones, computando la llave de cifrado cuando suficientes paquetes han sido recolectados. La versión para Windows es todavía demasiado preliminar.*

- *NBTScan: Recolecta información de NetBIOS de redes de Windows. NBTscan es un programa que escanea redes IP en busca de información de nombres de NetBIOS. Envía pedidos de "status" de NetBIOS a cada dirección en un rango provisto por el usuario y lista la información recibida de manera humanamente legible. Por cada host que responde, se lista su dirección, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina {"logged in"} , y dirección de MAC.*

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

- *XProbe2: herramienta de identificación de sistemas operativos {"OS fingerprinting"} activa. XProbe es una herramienta que sirve para determinar el sistema operativo de un host remoto. Logran esto utilizando algunas de las mismas técnicas que Nmap al igual que muchas ideas diferentes. Xprobe siempre ha enfatizado el protocolo ICMP en su enfoque de identificación {fingerprinting}.*

- *NGrep: Muestra y busca paquetes. ngrep se esfuerza por proveer de la mayoría de características comunes del "grep" de GNU, aplicándolas a la capa de network ({"network layer"} del modelo de referencia OSI). ngrep es consciente de la presencia de pcap y permite usar expresiones regulares que concuerden con el "payload" (o sea la carga, el cuerpo y _no_ los encabezados) de los paquetes. Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interfaces nulas {"null interfaces"}, y comprende la lógica de un filtro "bpf" de la misma manera que herramientas más comunes de sniffing como tcpdump y snoop.*

- *Perl / Python: Lenguajes de scripting de propósito general para múltiples plataformas {portables}. Aunque en esta página hay disponibles varias herramientas de seguridad enlatadas, es importante tener la habilidad de escribir las nuestras(o modificar las existentes) cuando necesitemos algo más a medida. Perl y Python hacen que sea muy fácil escribir scripts rápidos y portables para comprobar, abusar {exploit}, o incluso arreglar*

sistemas, Archivos como CPAN están llenos de módulos tales como Net: RawIP e implementaciones de protocolos para facilitar nuestras tareas.

- *OpenSSL: La más célebre biblioteca de cifrado para SSL/TLS. El proyecto OpenSSL es un esfuerzo de cooperación para desarrollar un set de herramientas robusto, de nivel comercial, completo en características, y "Open Source" implementando los protocolos "Capa de sockets seguros" {"Secure Sockets Layer"} (SSL v2/v3) y "Seguridad en la Capa de Transporte" {"Transport Layer Security"} (TLS v1) así como también una biblioteca de cifrado de propósito general potente. El proyecto es administrado por una comunidad de voluntarios a lo ancho del mundo que utilizan Internet para comunicarse, planear, y desarrollar el set de herramientas OpenSSL y su documentación relacionada.*

  - NTop: Un monitor de uso de tráfico de red. Ntop muestra el uso de la red en una manera similar a lo que hace top por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

- *Nemesis: Inyección de paquetes simplificada. El Proyecto Nemesis está diseñado para ser una pila de IP ("IP stack") humana, portable y basada en línea de comandos para UNIX/Linux. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell. Si Nemesis es de nuestro agrado, quizás queramos mirar hping2. Se complementan mutuamente bastante bien.*

- *LSOF: List Open Files (Listar archivos abiertos).Esta herramienta forense y de diagnóstico específica de Unix lista información acerca de cualquiera archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.*

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

- *Brutus: Un cracker de autenticación de fuerza bruta para redes. Este cracker sólo para Windows se lanza sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más.*

- *Fragroute: La peor pesadilla de los IDS.Fragroute intercepta, modifica, y reescribe el tráfico de salida, implementando la mayoría de los ataques descriptos en el "IDS Evasion paper" de Secure Networks. Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operaciones más en todos los paquetes salientes destinados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico. Esta herramienta fue escrita de buena fe para ayudar en el ensayo de sistemas de detección de intrusión, firewalls, y comportamiento básico de implementaciones de TCP/IP. Al igual que Dsniff y Libdnet, esta excelente herramienta fue escrita por Dug Song.*

- *THC-Hydra: Cracker de autenticación de red paralelizado. Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada {login} por red, incluyendo FTP, POP3, IMAP, Netbios, Telnet, HTTP Auth, LDAP, NNTP, VNC, ICQ, Socks5, PCNFS, y más. Incluye soporte para SSL y aparentemente es ahora parte de Nessus. Al igual que Amap, esta versión es de la gente de THC.*

- *Bactrack: Herramienta diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática."*[9]

Teniendo en cuenta lo anterior se hace necesario utilizar herramientas que ayuden a identificar las vulnerabilidades informáticas que se presentan alrededor de las Empresas, una de estas herramientas es Bactrack que es una distribución libre GNU/LINUX que se encuentra diseñada para la auditoria de Seguridad informática[10] en general, esta herramienta ha evolucionado y esto lo ha demostrado en las versiones emitidas a la comunidad de manera gratuita, en la actualidad se encuentra vigente Backtrack5R3, quien trae consigo una serie de herramientas que son de fácil uso, además es la herramienta que ocupa el puesto 32 en la famosa lista "Top 100 Network Security Tools" del año 2006[11]

Esta herramienta es de fácil acceso a todo público además se puede actualizar de manera rápida ya que es una herramienta que cuenta con la mayor base de datos de colección de herramientas en seguridad informática que abarca desde pruebas

[9] Texto Recuperado de la pagina web http://insecure.org/tools/tools-es.html.

[10] Texto Recuperado de la pagina web http://www.backtrack-linux.org/

[11] Texto Recuperado de la pagina web http://www.backtrack-linux.org/

de penetración hasta explotación de servidores.[12], razón por la cual se empleo esta herramienta como principal apoyo en la elaboración de este proyecto, en primera medida por su eficiencia, su facilidad en el uso de cada una de las herramientas, además de la ventaja de ser un software libre que cuenta con una comunidad que realiza bastantes tutoriales y en segundo lugar porque en el transcurso de la especialización fue la herramienta que se utilizó en los diferentes ataques, es decir que es donde mayor pericia ejerce el autor.

[12]Texto Recuperado de la pagina web http://www.backtrack-linux.org/

5.3 MARCO CONTEXTUAL, INSTITUCIONAL

INDEPORTES BOYACÁ, es un establecimiento público, descentralizado del orden departamental con autonomía administrativa, patrimonio propio, personería jurídica, creado mediante ordenanza No. 016 de 2001 de la Asamblea de Boyacá.

Ofrece la oportunidad de un desarrollo integral del ser humano mediante servicios y productos tales como:

- Deporte formativo.
- Deporte Profesional
- Deporte Universitario
- Deporte asociado
- Ciencias Aplicadas al deporte
- Deporte social Comunitario
- Asistencia técnica y administrativa a los municipios y demás entidades del sistema nacional del deporte en la jurisdicción, a través de talleres, seminarios, cursos, conferencias y convenios.

- Financiamiento de proyectos a entidades territoriales del departamento encaminados al fomento de la práctica de la educación física, el deporte, la recreación y el aprovechamiento del tiempo libre, mediante convenios interinstitucionales, obras de infraestructura y eventos deportivos.

El principal producto es la calidad de vida de la comunidad y los deportistas de alto nivel competitivo.

Cuadro 1. Clientes y partes interesadas.

CLIENTES	PRODUCTOS
Instituciones educativas, escuelas de formación deportiva, clubes deportivos y ligas deportivas, entes deportivos municipales, deportistas, comunidad indígena y población Boyacense.	Deporte, Plan Departamental de Recreación, Programa Departamental de Capacitaciones, Plan Departamental de Educación Física, Construcción, mejoramiento y adecuación de escenarios deportivos departamentales, Elaboración de Proyectos de construcción, mejoramiento o adecuación de escenarios deportivos del instituto.
PARTES INTERESADAS	**PRODUCTOS**
NACIONALES	
Ministerio de Educación Nacional	Informes cumplimiento de políticas.
Coldeportes	Informes adopción de políticas, planes y programas.
Contraloría General de la República.	Informes estadísticas fiscales (SIDEF)
Consejo Asesor del gobierno Nacional y Territorial en materia de Control Interno.	Informa avance del Sistema de Control Interno.
DIAN	Pago de Impuestos.
Contaduría General de la Nación.	Información Financiera.
DEPARTAMENTALES	
Gobernación de Boyacá.	Informes Financieros (presupuesto, tesorería, racionalización del gasto público).
	Informes de Gestión (Avances Plan de Desarrollo y Plan de Acción).
Asamblea de Boyacá	Informes de Gestión
Contraloría General de Boyacá	Rendición de Cuentas.
Ministerio Público - Procuraduría Regional.	Informe de Procesos Disciplinarios.
MUNICIPALES	
Alcaldía Mayor de Tunja.	Pago Impuesto de Industria y Comercio.
	Pago de Impuesto Predial.

Fuente: Indeportes Boyacá.

Cuadro 2. Indeportes opera a través de programas, proyectos y productos

PROGRAMAS	PROYECTOS	PRODUCTO
Deporte formativo	Festivales Escolares	Deporte
	Juegos Intercolegiados	
	Escuelas de Formación Deportiva	
	Juegos Departamentales	
	Organización del Festival Departamental de Escuelas de Formación Deportiva	
Deporte comunitario	Juegos Campesinos	
	Juegos de las Provincias	
	Juegos de las Comunidades Indígenas	
	APRODEP	
	Juegos Comunales	
Deporte asociado	Juegos Nacionales	
	Apoyo a Ligas Deportivas	
	Grupo Científico Metodológico	
	Alto Rendimiento	
	Ciencias Aplicadas al Deporte	
Recreación y Actividad Física	Coordinación y Seguimiento a la ejecución del Plan Departamental de Recreación y Actividad Física “Boyacá Activa y Feliz”	Recreación y Actividad Física
Programa Departamental de Capacitaciones	Capacitación	Capacitación
Construcción, mejoramiento y adecuación de escenarios deportivos	Construcción, mejoramiento y adecuación de escenarios deportivos.	Construcción, mejoramiento y adecuación de escenarios deportivos Departamentales.
		Elaboración de proyectos de construcción, mejoramiento o adecuación de escenarios deportivos del Instituto.
Educación Física	Plan Departamental de Educación Física	Educación Física

Fuente: Indeportes Boyacá.

Su estructura orgánica es la siguiente:

Ilustración 1. Organigrama de Indeportes Boyacá

Fuente: Indeportes Boyacá.

Algunas de sus Funciones

- Estimular la participación comunitaria y la integración funcional en los términos de la constitución política, la ley 181 de 1995 y las demás normas que lo regulen.
- Coordinar y desarrollar programas, actividades que permitan fomentar la práctica del deporte, la recreación del aprovechamiento del tiempo libre en el territorio departamental.
- Prestar asistencia técnica y administrativa a los municipios y a las demás entidades del sistema nacional de deporte en el territorio de su jurisdicción.
- Proponer y aprobar en lo de su competencia el plan departamental para el desarrollo del deporte, la recreación y el aprovechamiento del tiempo libre.

- Participar en la elaboración y ejecución de programas de cofinanciación de la construcción, ampliación y mejoramiento de las instalaciones deportivas de los municipios
- Promover, difundir y fomentar la práctica de la educación física, el deporte y la recreación en el territorio departamental.
- Cooperar con los municipios y las entidades deportivas y recreativas en la promoción y difusión de la actividad física, el deporte y la recreación y atender a su financiamiento de acuerdo con los planes y programas que aquellos presenten
- Fomentar la recreación en sus diferentes expresiones como la deportiva, el turismo, social y de aprovechamiento del tiempo libre.
- Programar actividades del deporte formativo y comunitario, eventos deportivos en todos los niveles de educación formal y no formal.
- Promover la educación extraescolar en materia de recreación.
- Ejercer funciones de coordinación como subsidiaridad y concurrencia relacionadas con las competencias municipales en materia de deporte y recreación.
- Celebrar con personas naturales o jurídicas de derecho público y privado los contratos necesarios para la realización de trabajos acordes con el objeto del instituto.
- Actuar como instancia de intermediación entre la nación y los municipios.[13]

Misión.

Fomento, coordinación, promoción y apoyo de la práctica del deporte, la educación física, la recreación y el aprovechamiento del tiempo libre, en el departamento de Boyacá a través de la adopción de políticas, programas y proyectos establecidos por el Gobierno Nacional y Departamental.

---

[13] **Fuente:** Tomado del proyecto de modernización y estudio técnico año 2005, "Legislación Deportiva ley 181 de 1995. Decretos leyes y sus decretos reglamentarios.

Nota: Para concordancia con los requisitos de la norma, se utiliza como nomenclatura los numerales de la misma.

Visión.

INDEPORTES BOYACÁ será para el año 2015 una entidad reconocida a nivel nacional, por su liderazgo y excelencia en el fomento de la práctica deportiva, recreativa y física de la población boyacense y la consecución de altos logros deportivos en el contexto departamental, nacional e internacional.

Objetivos Institucionales.

- Desarrollar tecnológicamente y de manera integral la institución para lograr una entidad más eficiente.
- Dotar al instituto de una estructura organizacional ágil, dinámica, centrada en procesos, y con un sistema de información que facilite el logro de sus objetivos.
- Crear una cultura de servicio al cliente que garantice el seguimiento de su satisfacción.
- Mantener un sistema administrativo, que base sus decisiones en índices de gestión.
- Garantizar un talento humano con claro sentido de pertenencia a la institución, comprometido con el logro de los objetivos organizacionales.[14]

[14] **Fuente:** Tomado de los documentos privados de INDEPORTES BOYACA.

5.3 MARCO LEGAL O NORMATIVO

5.3.1 Normatividad Internacional.

- **Estándar RFC2196**

El Estándar RFC2196 es usado en la práctica de la seguridad de la información. Entre las características de la seguridad de la información, según el RFC2196, se tienen las siguientes:

Se debe poder poner en práctica mediante procedimientos descritos de administración de sistemas, publicación de guías sobre el uso aceptable de los recursos informáticos o por medio de otros métodos prácticos apropiados, debe poder implantarse, debe obligar al cumplimiento de las acciones relacionadas mediante herramientas de seguridad, tiene que detectar fugas o errores; debe definir claramente las áreas de responsabilidad de los usuarios, administradores y dirección, y tener un uso responsable para toda situación posible.

El RFC 2196, llamado “Site Security Handbook” es un manual de seguridad que puede ser utilizado como estándar para establecer Políticas de Seguridad. Este manual fue escrito por varios autores y fue publicado en Septiembre de1997, y a pesar de tener varios años, por sus contenidos y la temática que trata es un documento vigente y valido en el área de la Seguridad Informática.
Este documento trata entre otros, los siguientes temas:

Políticas de Seguridad
1. Que es una Política de Seguridad y porque es necesaria.
2. Que es lo que hace que una Política de Seguridad sea buena.
3. Manteniendo la Política Flexible.

Arquitectura de Red y de Servicios

1. Configuración de Red y de Servicios.
2. Firewalls.

Servicios y Procedimientos de Seguridad

1. Autentificación
2. Confidencialidad.
3. Integridad.
4. Autorización.
5. Acceso
6. Auditoria

Gestión de Incidentes de Seguridad

1. Notificación y puntos de contacto
2. Identificando un Incidente
3. Gestión de un Incidente
4. Consecuencias de un Incidente
5. Responsabilidades.

- **Estándar IT Baseline Protection Manual**

El IT Baseline Protection Manual presenta un conjunto de recomendaciones de seguridad, establecidas por la Agencia Federal Alemana para la Seguridad en Tecnología de la Información.

Este estándar plantea en forma detallada aspectos de seguridad en ámbitos relacionados con aspectos generales (organizacionales, gestión humana,

criptografía, manejo de virus, entre otros); infraestructura, (edificaciones, redes wifi); sistemas (Windows, novell, unix); redes (cortafuegos, módems), y aplicaciones (correo electrónico, manejo de la web, bases de datos, aplicativos)

- **Estándar ISO 27001**

Este es el nuevo estándar oficial. Su título completo en realidad es BS 7799-2:2005 (ISO/IEC 27001:2005). También fue preparado por el JTC 1 y en el subcomité SC 27, IT Security Techniques. La versión que se considerará es la primera edición, de fecha 15 de octubre de 2005.El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son:

- ISO/IEC 27000 Fundamentals and vocabulary.
- ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005).Publicado el 15 de octubre del 2005.
- ISO/IEC 27002 Code of practice for information security management.
- Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005.
- ISO/IEC 27003 ISMS implementation guidance (en desarrollo).
- ISO/IEC 27004 Information security management measurement (en desarrollo).
- ISO/IEC 27005 Information security risk management (basado en ISO/IEC 13335MICTS Part 2 e incorporado a éste; en desarrollo).
- El ISO-27001:2005 es aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. Presentar al ISO-27001:2005 como estándar de facto genera la posibilidad de tener un estándar mejorado y más robusto en el trayecto de la historia; los entes que aplican estos procedimientos para garantizar la seguridad e integridad de la información mejorarán considerablemente el estándar, luego de haber hecho las pruebas y haber tenido la experiencia.

Los demás estándares establecidos, como el alemán, basado en el IT Baseline Protection Manual, y las recomendaciones de la IEFT con su RFC2196, constituyen orientaciones y guías para usuarios que deseen implementar gestión en la seguridad de la información; sin embargo, queda demostrado que el estándar de ISO es el más adoptado por las empresas porque es más flexible y se acopla mejor a los procesos que normalmente se llevan a cabo en las organizaciones; ISO es el estándar de facto en la gerencia de la integridad de la información.

- **Estándar ISO/IEC 17799 (denominado también como ISO 27002)**

Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.

- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Cumplimiento
- Gestión de Continuidad del Negocio.

- **Estándar ISO/IEC 27000:2009**

Es parte de una familia en crecimiento de Estándares para Sistemas de Administración de Seguridad de la información (ISMS), las “series ISO/IEC 27000” ISO/IEC 27000 es un estándar internacional titulado “Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario”

El estándar fue desarrollado por el sub-comité 27 (SC27) del primer Comité Técnico Conjunto (JTC1), de la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission)ISO/IEC 27000 provee:

- Una vista general a la introducción de los estándares de la familia ISO/IEC 27000.
- Un glosario o vocabulario de términos fundamentales usados a lo largo de toda la familia ISO/IEC 27000.

La Seguridad de la Información, como muchos otros temas técnicos, está desarrollando una compleja red de terminología. Relativamente pocos autores se toman el trabajo de definir con precisión lo que ellos quieren decir, un enfoque que es inaceptable en el campo de los estándares, porque puede potencialmente llevar a la confusión y a la devaluación de la evaluación formal y la certificación.

El alcance de ISO/IEC 27000 es “especificar los principios fundamentales, conceptos y vocabulario para la serie de documentos ISO/IEC 27000”ISO/IEC 27000 contiene, en otras palabras: una vista general de los estándares ISO/IEC 27000, mostrando cómo son usados colectivamente para planear, implementar, certificar, y operar un Sistema de Administración de Seguridad de la información, con una introducción básica a la Seguridad de la Información, administración de riesgos, y sistemas de gestión, definiciones cuidadosamente redactadas para temas relacionados con seguridad de la información.

ISO/IEC 27000 es similar a otros vocabularios y definiciones y con suerte se convertirá en una referencia generalmente aceptada para términos relacionados con seguridad de la información entre ésta profesión.

- **Estándar ISO/IEC 18028-2:2006**

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

COMMON CRITERIA: El Criterio Común para la Evaluación de la Seguridad en Tecnologías de la Información (abreviado como Criterio Común o CC), es un estándar internacional (ISO/IEC 15408), para la certificación de la seguridad en computadores. Está actualmente en la versión 3.1.

El Criterio Común es un marco de trabajo en el cual los usuarios de sistemas computacionales pueden especificar sus requerimientos funcionales de seguridad y de garantía, para que los vendedores puedan implementar y/o hacer

reclamaciones acerca de los atributos de seguridad de sus productos, y los laboratorios de prueba pueden evaluar los productos para determinar si en realidad satisfacen las reclamaciones.

En otras palabras, el Criterio Común provee garantía de que los procesos de especificación, implementación y evaluación de la seguridad de un producto de cómputo hayan sido conducidos en una forma rigurosa y estandarizada. Consta de tres partes:

PARTE 1: Introducción y modelo general
PARTE 2: Componentes funcionales de la Seguridad
PARTE 3: Componentes para la garantía de la Seguridad

- **Estándar ISO/IEC 21827:2008:**

INFORMATION TECHNOLOGY- SECURITY TECHNIQUES- SYSTEMS SECURITY ENGINEERING- CAPABILITY MATURITY MODEL (SSE-CMM)

ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827) es un estándar internacional basado en el Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas, desarrollado por la Asociación Internacional de Ingeniería de Seguridad de la Información (ISSEA).

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

industria. El modelo es una métrica estándar para las prácticas de la ingeniería de seguridad, que cubre lo siguiente:

- Ciclos de vida del proyecto, incluyendo actividades de desarrollo, operación, mantenimiento y desmantelamiento.
- Cubre todos los ámbitos de la organización, incluyendo actividades de gestión, organizacionales y de ingeniería.
- Interacciones concurrentes con otras disciplinas, como software y hardware de sistemas, recurso humano, pruebas de ingeniería, gestión de sistemas, operación y mantenimiento.

5.3.2Normatividad Nacional.

- **Ley 1273 el 2009**

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

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

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

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

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

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

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

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

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente

el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.

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

CAPITULO II:
De los atentados informáticos y otras infracciones

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

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio

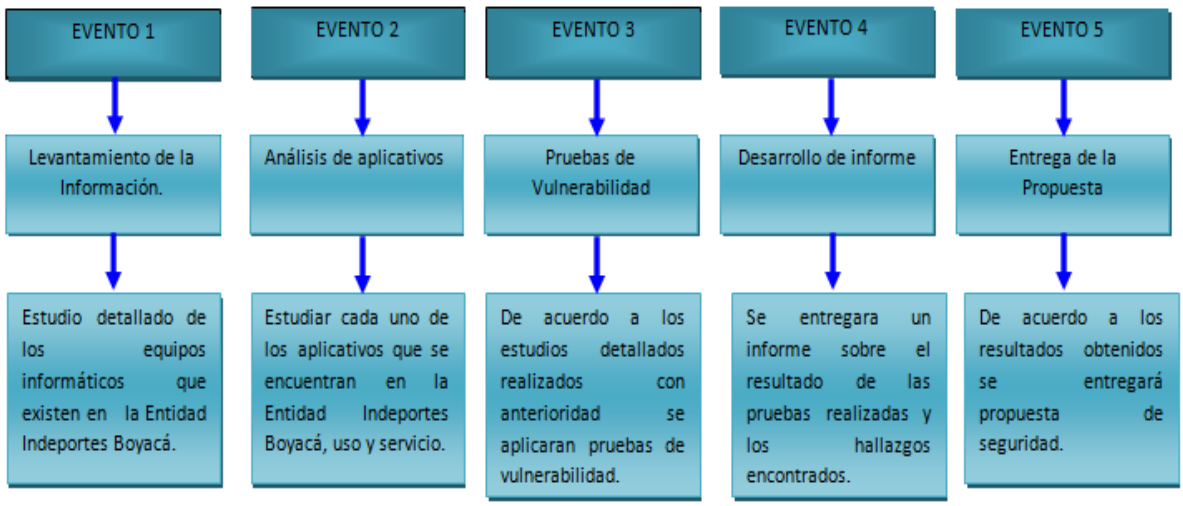
semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.[15]

[15] Osorio Cristian, (2011), wikispaces, Recuperado de: http://seguridadinformaticaufps.wikispaces.com/Normatividad+en+la+Seguridad+Inform%C3%A1tica

6. MÉTODO DE INVESTIGACIÓN

El presente trabajo estará dividido en 5 eventos los cuales se desarrollarán en respectivo orden de acuerdo con el objetivo propuesto para este proyecto de grado, así:

Ilustración 2. Eventos



Fuente. Autor

- **Evento 1: Levantamiento de la Información:** En este paso lo que se va a realizar es el estudio de la organización general de INDEPORTES BOYACA, este levantamiento es sobre la infraestructura sistemática y la comunicación que tienen las diferentes dependencias, se revisarán los tipos de conexiones y conectividad disponibles y accesibles.

- **Evento 2: Análisis de Aplicativos:** Teniendo en cuenta que INDEPORTES BOYACA, es una entidad descentralizada pero que hace parte estructural de la Gobernación de Boyacá está maneja sus recursos

propios, pero dentro de su ejecución debe mostrar balance de las arcas monetarias de las que está haciendo uso, por esta razón es indispensable revisar los aplicativos que manejan cada una de las dependencias, con el fin de establecer que tipos de comunicaciones tienen, accesos, permisos entre otros.

- **Evento 3: Pruebas de Vulnerabilidad:** Ya teniendo acceso a la información de la entidad y analizados cada uno de los componentes que hacen parte del manejo sistémico de la información se realizarán pruebas de hacking ético con el fin de determinar el nivel de seguridad informática que tienen cada uno de estos elementos**.**

- **Evento 4: Desarrollo del Informe:** teniendo los resultados del Hacking ético, se procederá a la realización del informe que será presentado al Director de la entidad como al Director del curso para que sean revisados los resultados y se determine el nivel de seguridad informática al que está expuesto la entidad INDEPORTES BOYACA.

- **Evento 5: Entrega de la Propuesta:** Teniendo en cuenta el análisis de resultados arrojados con el hacking ético practicado se sugerirán correcciones para garantizar un mayor índice de seguridad informática en la entidad INDEPORTES BOYACA.

7. ANÁLISIS DE LA INFORMACIÓN

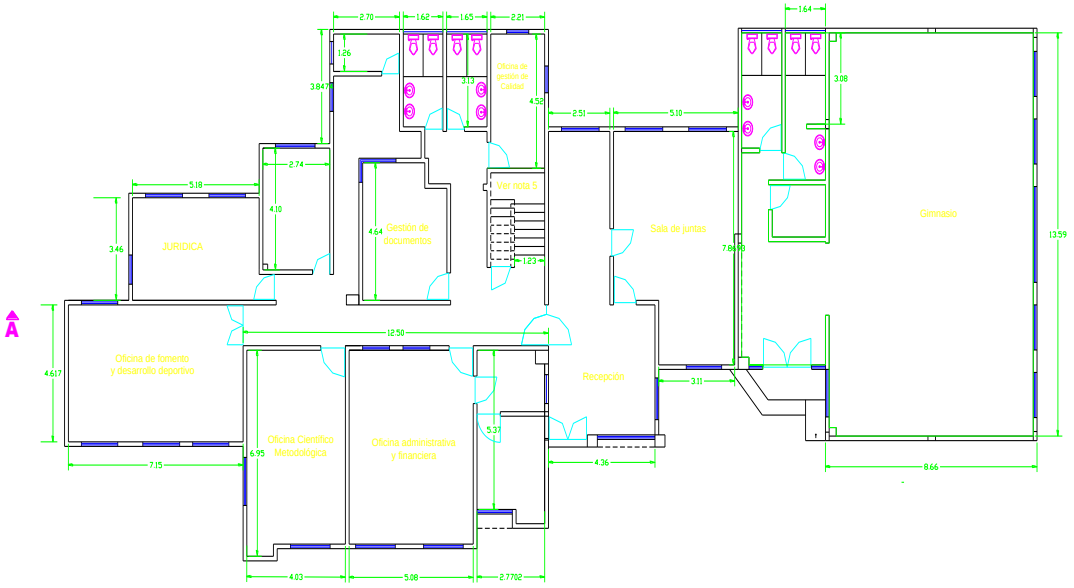
7.1 LEVANTAMIENTO DE INFORMACIÓN

La casa del deporte de INDEPORTES BOYACA, cuenta con una infraestructura modular de 2 pisos, donde se ubican todas y cada de las dependencias intervinientes en el cumplimiento de la misión y cuenta con un personal Activo mínimo diario de 40 personas aproximadamente, quienes hacen uso de los recursos ofrecidos por la entidad en cumplimiento de su Misión.

Estructura Física:

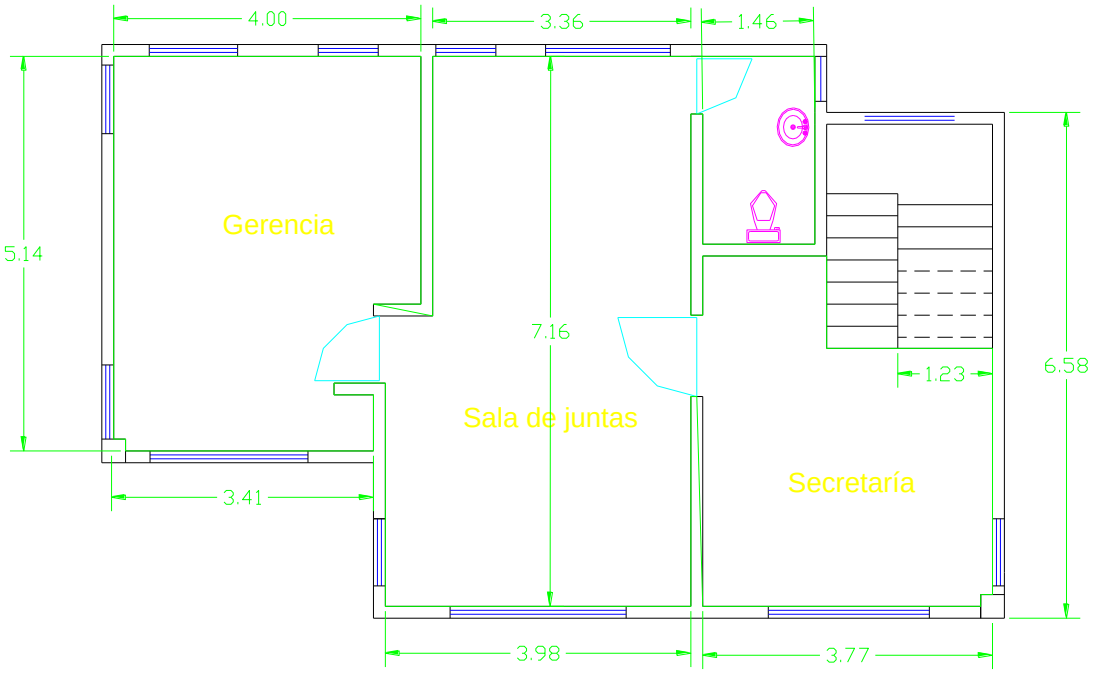
La casa del deporte cuenta con las siguientes dependencias ubicadas de la siguiente manera: Segundo piso: Gerencia, Secretaría de Gerencia y sala de Reunión de Gerencia; Primer piso: Oficina Jurídica, Oficina de Dirección Administrativa y Financiera, Oficina de Dirección de Fomento y Desarrollo Deportivo; Oficina de Infraestructura; Oficina de Metodólogos; Oficina de Prensa y Comunicaciones; Oficina de Almacén; Oficina de Gestión Documental; Oficina de Contabilidad; Oficina de Talento Humano; Oficina de Control Interno; Oficina de Tesorería; Oficina de Radicación; Oficina de Archivo; Oficina de Calidad y Sistemas; Oficina de Escuelas de Formación; Recepción y Gimnasio.

Ilustración 3. Planta Primer piso.



Fuente: Indeportes Boyacá.

Ilustración 4. Planta Segundo Piso.



Fuente: Indeportes Boyacá.

Sistemas de Información:

Indeportes Boyacá, en cumplimiento de su Misión tiene el uso de un solo sistema de información que es el contable; este almacena el presupuesto de la entidad, junto con toda la contabilidad manejada por la Empresa, datos de egresos, ingresos, personal entre otros.

Los demás funcionarios manejan información de cada uno de sus deberes, pero no utilizan sistema o software especializado para tal fin sino que su manejo se da especialmente con herramientas ofimáticas.

Hardware:

En cuanto a Hardware, INDEPORTES BOYACA, cuenta con 1 servidor donde se almacena única y exclusivamente el sistema de Información contable, un modem, un router de movistar, el cual trae la seguridad por defecto, 2 Switch marca encoré y tplink, adicional 10 equipos propios con las siguientes características

- 2 equipos de mesa todo en uno Marca Lenovo, procesador CoreI5, 1 Tera de Disco Duro, memoria Ram de 4 gigas, sistema Operativo Windows 7.
- 1 equipo de mesa marca HP, procesador CoreI3, 500 GB de Disco Duro, Memoria Ram 2 gigas, sistema operativo Windows 7.
- 1 equipo de mesa Sony Vaio todo en 1, procesador Pentiun Inside, 500 gigas de Disco Duro, Memoria Ram 2 gigas, Sistema operativo Windows 7.
- 2Computador portátil Toshiba L745 – SP4251LL, cargador.
- 1 Computador HPCOMPAQ 8200 Elite W/7 /CPU / MOUSE / MONITOR.
- 1 Computador HP Pro/3400 Intel Core W/7, memoria Ram de 2 Gigas, Disco Duro 500 Gigas.

- 1 Computador HP Pro 3400, procesador Intel CoreI3 W/7, Ram de 2 Gigas, Disco Duro 500 Gigas.

SERVIDOR:

- 1 Equipo de mesa marca HP, procesador CoreI7, 1 Tera de Disco Duro, Memoria Ram de 4 Gigas , sistema operativo Windows 7.

Software:

En la actualidad no se encuentra ningún tipo de software registrado, la mayoría de los equipos utilizan software gratuitos y algunos sin licencia, a continuación encontrarán una tabla con la descripción de software instalado en cada uno de los equipos, no se describen los equipos de acuerdo a la privacidad de información que maneja la entidad.

Cuadro 3. Características de Software

Equipos	Software Instalado	Dependencia
1	Equipo Portátil. Sistema Operativo Windows 8, Office Suite 2010, antivirus Avast.	Gerencia
1	Equipo de Mesa. Sistema Operativo Windows 7, Office 2010, antivirus Avast.	Secretaria de Gerencia
5	Equipos de Mesa. Sistema Operativo Windows 7, Office 2007, antivirus Avast, Software Contable Flash.	Tesorería y Administrativa
5	Equipos de Mesa. Sistema Operativo Windows 7, Office 2007, antivirus Avast,	Sistemas
7	Equipos de Mesa. Sistema Operativo Windows 7, Office 2007, antivirus Avast,	Jurídica

12	Equipos de Mesa. Sistema Operativo Windows 7, Office 2007, antivirus Avast,	Fomento
10	Equipos de Mesa. Sistema Operativo Windows 7, Office 2007, antivirus Avast,	Gimnasio, recepción y otras

Fuente. Autor

Red

Indeportes Boyacá cuenta con una estructura de red cableada e inalámbrica, la cual abarca todas y cada una de las dependencias, teniendo en cuenta que la red cableada no tiene los suficientes puertos para el número de personas que trabaja constantemente en la entidad se tuvo que adaptar la red inalámbrica como solución a la problemática de conexión.

La red cableada presenta las siguientes características:

En el área de secretaría encontramos el router principal junto con dos switch, ellos son los responsables de distribuir tanto la red cableada como la red inalámbrica.

La red cableada aunque tiene una estructura de canaleta, se puede observar que la misma está expuesta a daños y a una depreciación más rápida.

La canaleta que se encuentra en el área de gerencia esta sin terminar, los cables se salen y no representa un orden.

Se observa también un switch que va conectado directamente al equipo servidor, el switch no se encuentra protegido sino que está a la intemperie.

Se observa que la mayor parte de la canaleta se encuentra afectada por la humedad lo que hace que la misma no esté adherida a la pared sino que se encuentra en el piso.

Existe otro switch que se encuentra en el piso de una de las oficinas, el mismo se encuentra ubicado debajo de un escritorio se observan todos y cada uno de los cables de manera desordenada y en el piso, ya que como se dijo anteriormente la canaleta no está adherida a la pared por causa de la humedad.

De otro lado se observa canaleta aérea pero no se encuentra completa hay partes que se observan los cables que lleva, es decir de donde salen y para donde van.

7.2. ANALISIS DE APLICATIVOS

La casa del Deporte Indeportes Boyacá, en la actualidad cuenta con un solo aplicativo, su nombre es FLASH, este aplicativo es de tipo contable y financiero, es el encargado de almacenar el presupuesto, los activos de la entidad, el presupuesto, la nomina y la contabilidad de la entidad, es decir, es el encargado de llevar a cabo todo y cada uno de los procesos administrativos desde el inicio de la causación del presupuesto, hasta cada uno de los datos de los contratistas y personal de planta, pagos entre otros; este aplicativo esta compuesto por un servidor quien es el encargado de almacenar toda la información de las 5 terminales.

Todos y cada uno de los equipos cuenta con el software basico para trabajo de oficina como lo son las herramientas office tanto 2007 como 2010, el 98% de los sistemas operativos es Windows Siete y el 2% Windows 8, los equipos en su totalidad se encuentran en buenas condiciones, todos y cada uno de los equipos cuentan con antivirus instalado como lo es Avast en su versión 4.7.7, es decir, sus

bases de datos de antivirus se encuentran desactualizadas, por ende no estan haciendo ningún efecto en cuanto a seguridad, por otro lado los equipos que se encuentran conectados a la red por cable estos tienen un direccionamiento ip mientras que los de la inhalambrica no. La conexión de estos equipos se hace mediante disco compartido, no existe un control de acceso ni de cambios, cabe anotar que en este documento y por motivos de seguridad no se pueden nombrar las licencias de los equipos.

7.3 PRUEBAS DE VULNERABILIDAD

Estructura Física:

La casa del deporte en cuanto a la estructura física cuenta con seguridad de tipo privada las 24 horas del día quienes son los encargados del cuidado de todas y cada una de las oficinas y elementos pertenecientes a la casa del deporte, se observa mediante prueba física que los elementos de la entidad no están lo suficientemente custodiados ya que ni al ingreso ni a la salida de la entidad se cuenta con una revisión continúa de las pertenencias que se sacan de la misma; se realiza la prueba sacando en el bolso de mano un switch de marca encoré ubicado en la oficina de Fomento, se puede sacar de la entidad sin ningún problema, el switch vuelve a ingresar pasado dos horas y tampoco se revisa el ingreso al lugar. Por lo cual se detalla una falta alta de seguridad física porque no se tiene control de acceso como de salidas de la infraestructura del lugar, no existen cámaras de seguridad ni sensores que identifiquen elementos tanto de entrada y salida, solo existe un celador en la entrada principal pero no hace revisión de ingreso o salidas.

De igual forma se observa que la parte de infraestructura del primer piso se encuentra con bastantes zonas humedas, lo que hace que el deterioro de la red alambrica sea prematuro.

Ilustración 5 Humedad en canaleta

Fuente: Autor.

RED

Indeportes Boyacá cuenta con 3 redes inalambricas quienes se desprenden de un solo punto y son las responsables de repartir la señal en toda la casa del Deporte, estas redes se caracterizan por su nombre que tiene alución a la entidad.

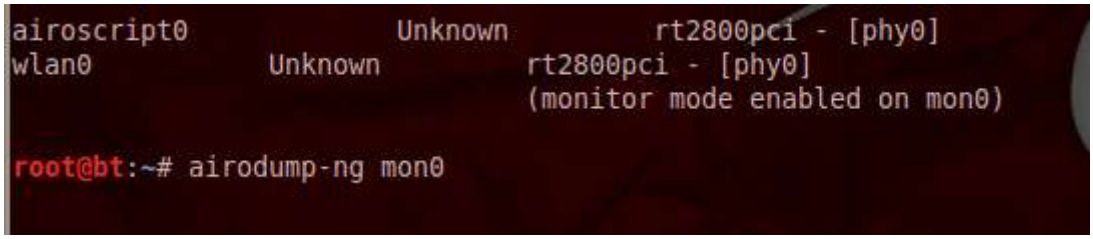
Todas y cada una de las redes poseen contraseña, las mismas no se encuentran ocultas sino que están en un radio de 30 metros aproximadamente disponibles a cualquier conexión de red inalambrica.

Teniendo en cuenta que cada una de las redes tienen contraseña lo que se comienza a realizar es revisar si se puede vulnerar alguna de ellas para tener acceso a las redes.

Ataque 1: Contraseñas de Red. Se hace necesario detectar la seguridad de las claves de red para tener acceso en primer lugar al servicio de internet. Para esto se utiliza el sistema operativo Bactrack.

Abrimos una ventana de comandos y vamos a mirar las interfaces de red presente en el equipo, para esto se usa el comando airmon-ng

Ilustración 6 Airmon.ng



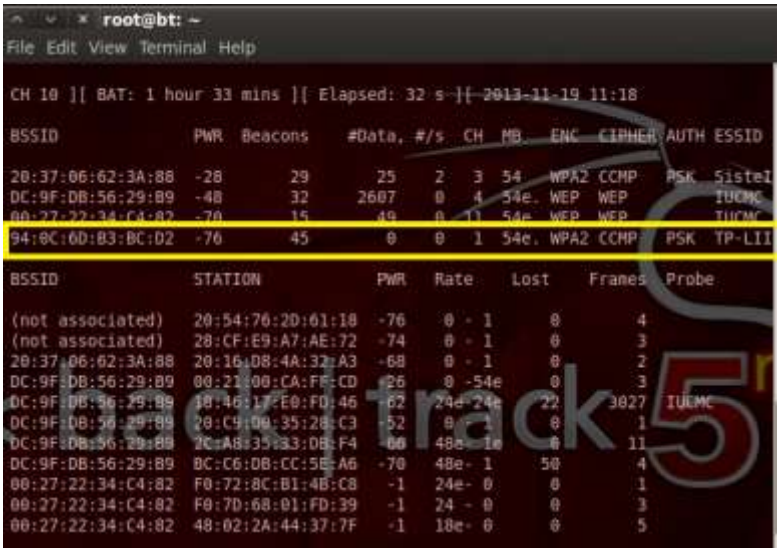
Fuente: Autor.

Ilustración 7 Vista de Red

Fuente: Autor.

Con el comando airodump-ng mon0 empezamos la captura. Y ya tenemos la dirección MAC del Acces point al que vamos a acceder.

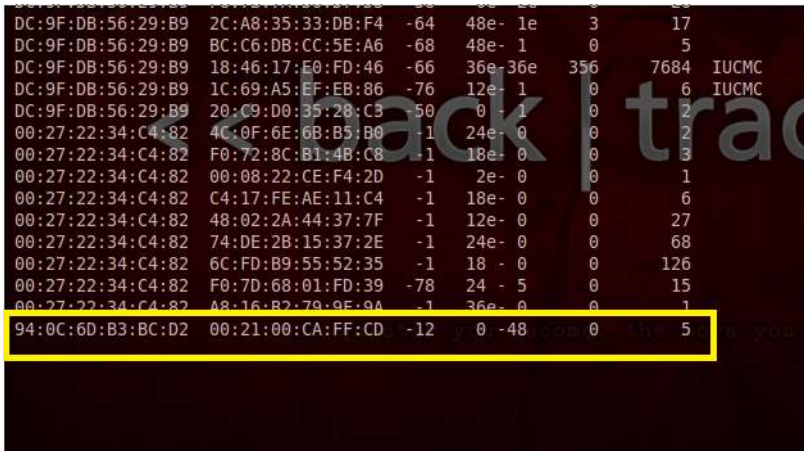
Ilustración 8 Dirección MAC



Fuente: Autor.

Seguidamente procedemos a descubrir la MAC de los equipos conectado a ese acces point detectado.

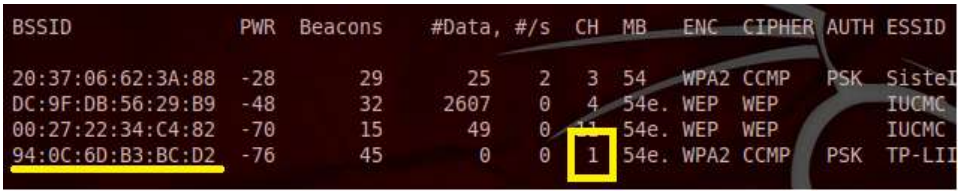
Ilustración 9Acces Point



Fuente: Autor.

Además de esto necesitamos conocer el canal por la que se está llevando a cabo la comunicación.

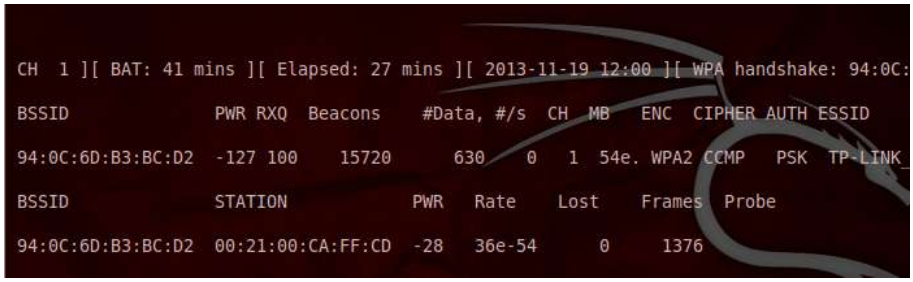
Ilustración 10 Canal de Comunicación



Fuente: Autor.

Haciendo uso del comando airodump-ng –w capture –bssid 94:0c:6d:b3:bc:d2 –c 1 mon0

Ilustración 11 Captura de Paquetes



Fuente: Autor.

Después de varias horas de espera, y realizando inyección por medio de datos de diccionario, obtenemos las claves de la casa del Deporte.

Ilustración 12 Clave de Red

Fuente: Autor.

De esta forma se logran obtener las claves de las 3 redes wifi de Indeportes Boyacá. Se nota bastante simplicidad en las contraseñas encontradas por medio del ataque, no se revelan en este documento por razones de confidencialidad.

Ataque 2: Teniendo en cuenta que la casa del Deporte Indeportes Boyacá cuenta con un solo sistema de Información el cual cuenta con 6 puntos de Red y un Servidor, siendo este el activo de información más importante se procede a realizar un escaneo de puertos, para observar los posibles paquetes y determinar las direcciones ip que se conectan al punto de acceso.

El ataque nuevamente se realizará con la herramienta Backtrack 5R3, y con la ayuda de wireshark, que es una herramienta que se encarga de escanear los puertos de la red en la que ya hemos entrado, se aclara que se revisaron las 3 redes inalambricas inicialmente, además se determina que

el punto de acceso selecciona ip dinámicas tan pronto se inicia la conexión a internet.

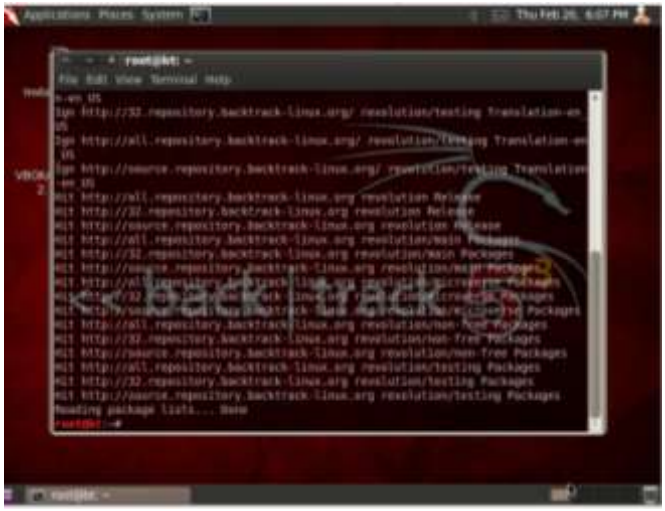
Se inicia el ataque colocando la tarjeta de red en modo promiscuo.

Ilustración 13 Cambio de tarjeta

Fuente: Autor.

Se actualizan repositorios.

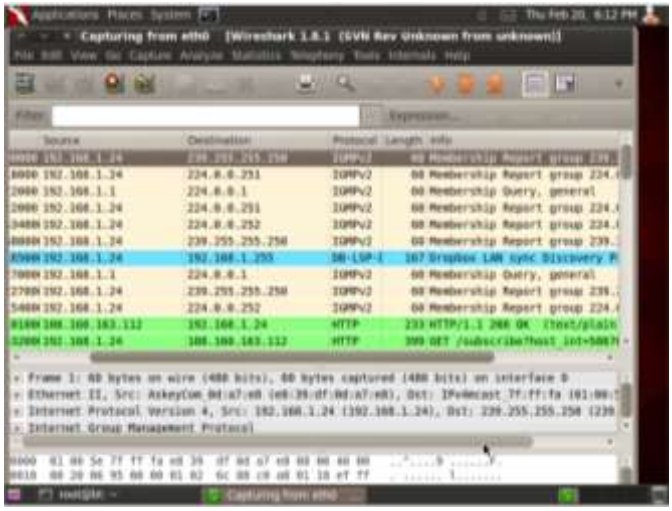
Ilustración 14 Actualización Repositorios



Fuente: Autor.

Se da inicio al escaneo de puertos con la herramienta wiresark.

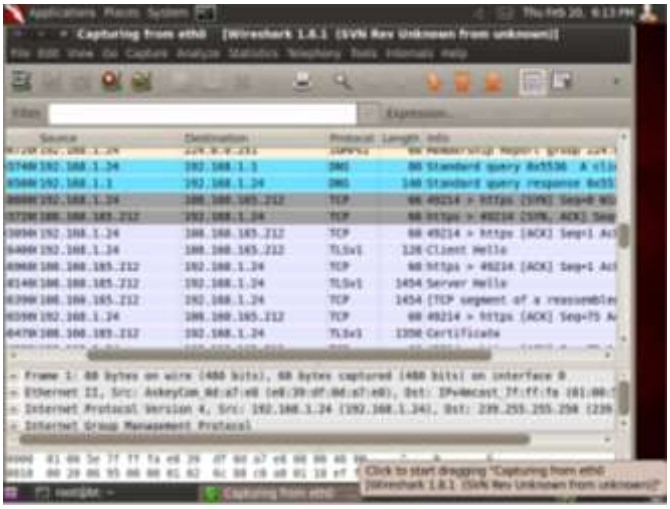
Ilustración 15 Escaneo de Puertos



Fuente: Autor.

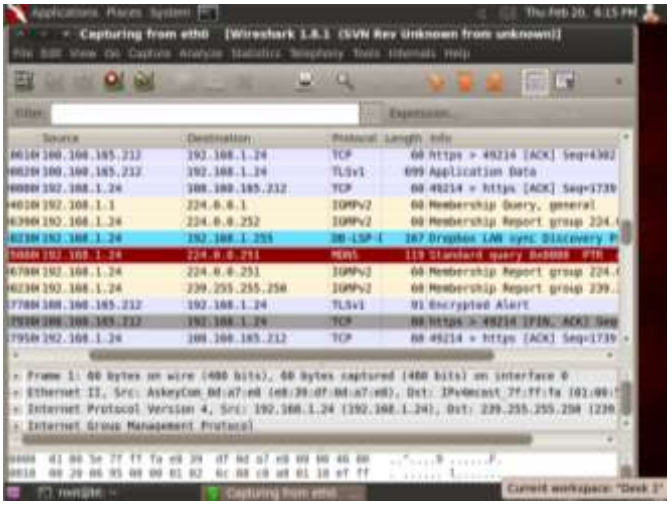
Aquí se pueden observar las conexiones ip que en el momento están conectadas a la red, de donde salen a dónde van los paquetes.

Ilustración 16 Conexiones ip



Fuente: Autor.

Ilustración 17 Conexiones ip

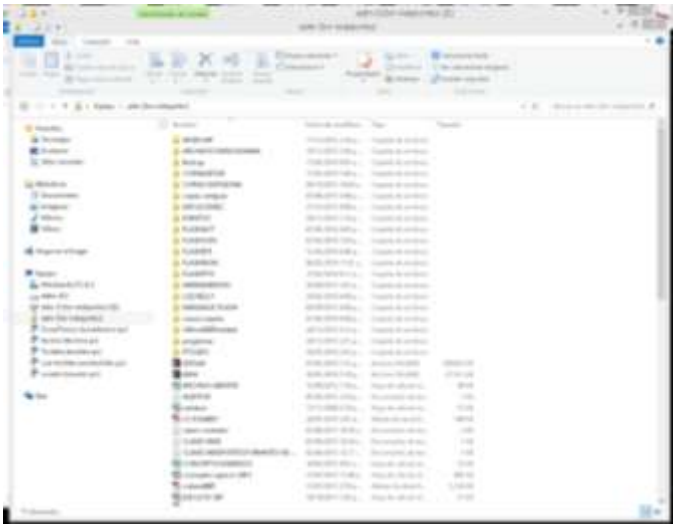


Fuente: Autor.

Se observa que las direcciones ip encontradas o las que más transmiten paquetes son las ip estáticas, es decir las que se encuentran en red con el servidor. Así con estas direcciones ip procedemos a realizar ataque por medio del trafico para que el mismo nos de entradas al servidor, teniendo como resultado acceso a paquetes del mismo.

Ataque 3: Ataque Servidor: Para realizar el ataque al servidor se realiza por medio de la estructura cableada de la entidad, se puede observar que el servidor no posee clave, es decir, no fue necesario practicar algún tipo de ataque ya que los mismos dentro de la estructura de red cableada existe acceso al servidor sin ninguna restricción.

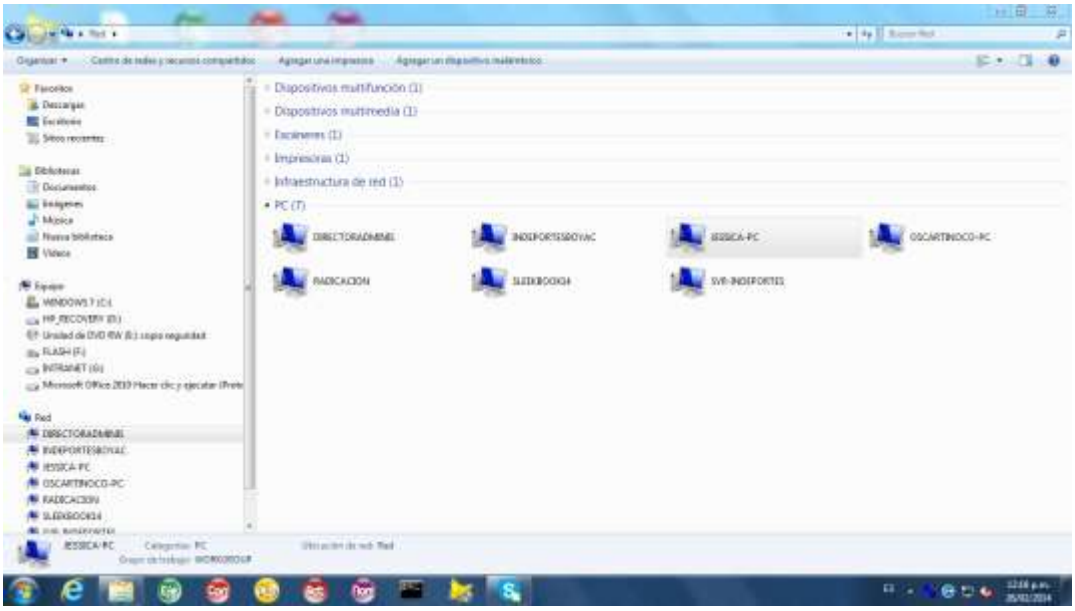
Ilustración 18 Documentos de Servidor



Fuente: Autor.

Ataque 4: Desde el Servidor a PC: Se tiene acceso al servidor y se entra en la red y se encuentran los siguientes equipos de la red.

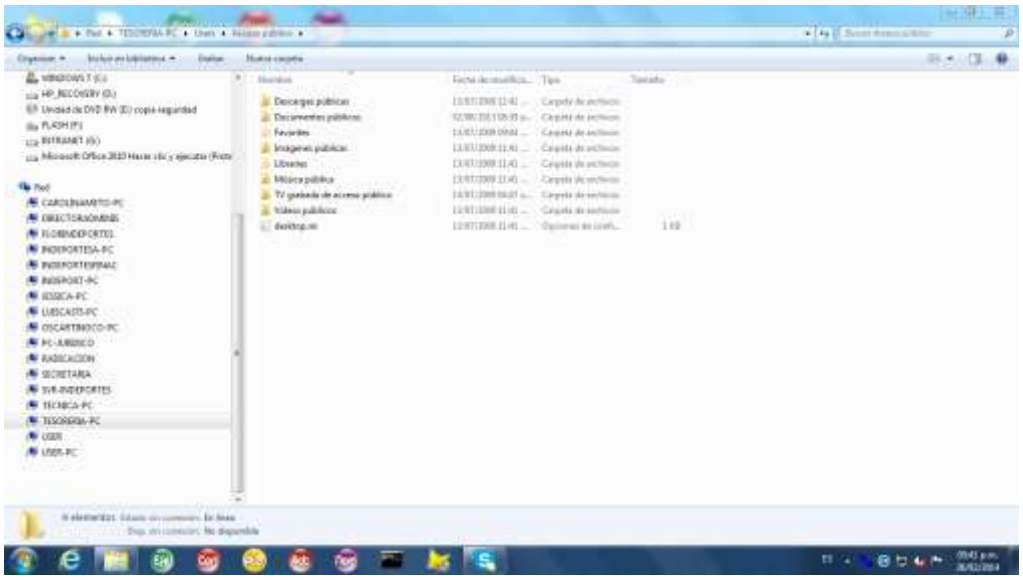
Ilustración 19 Equipos presentes en la Red



Fuente: Autor.

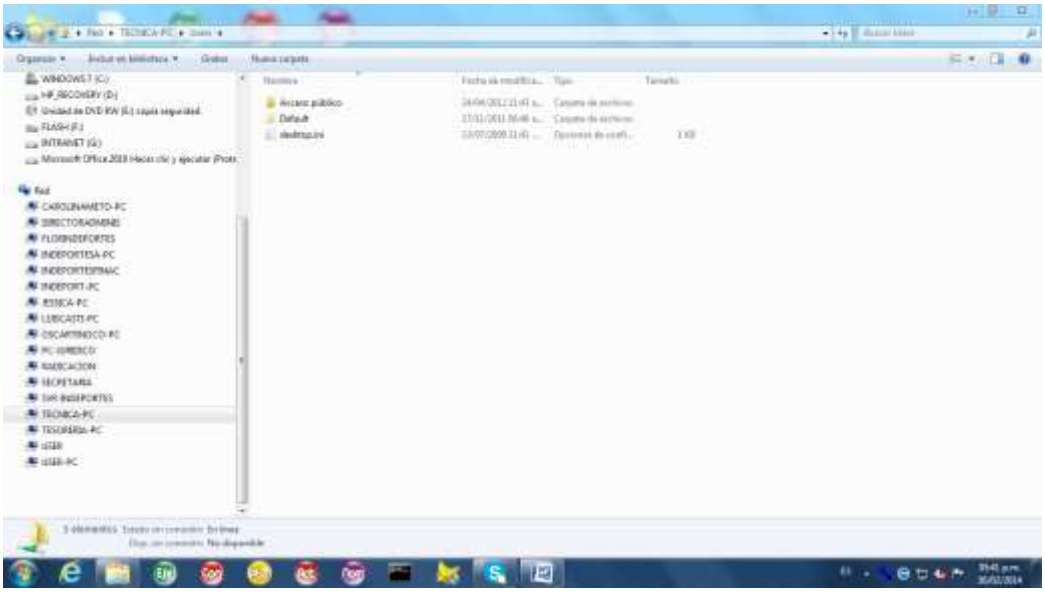
Se observa que se tiene acceso a documentos de personas que se encuentran conectadas a la red, tal como se muestra en las siguientes imágenes.

Ilustración 20 Equipos que permiten acceso



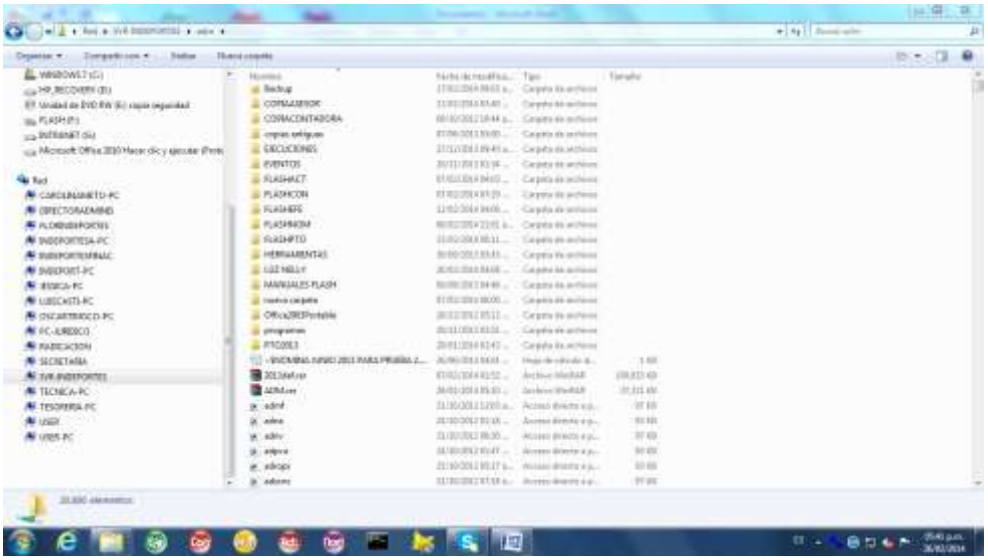
Fuente: Autor.

Ilustración 21Equipos que permiten acceso



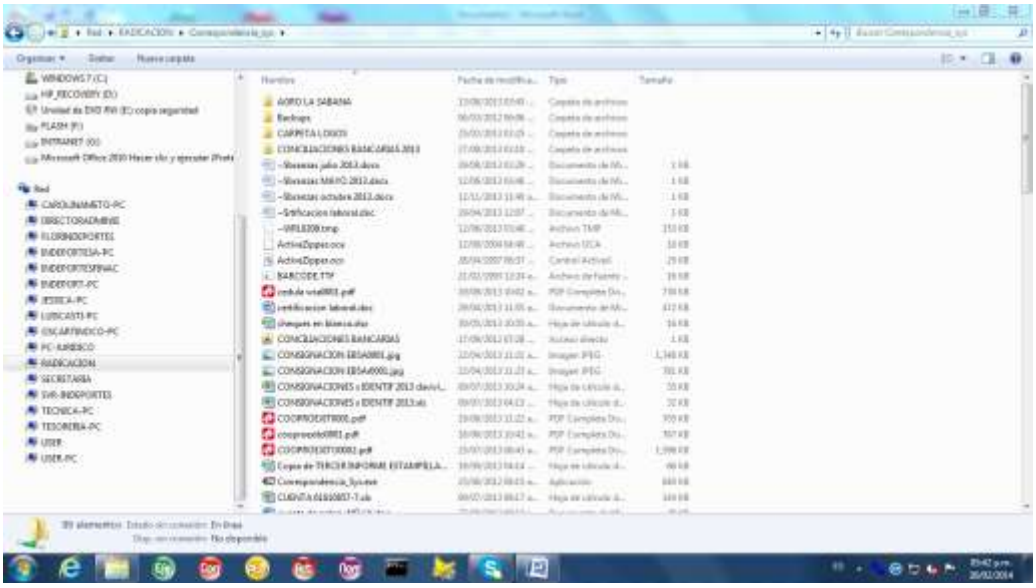
Fuente: Autor.

Ilustración 22Equipos que permiten acceso



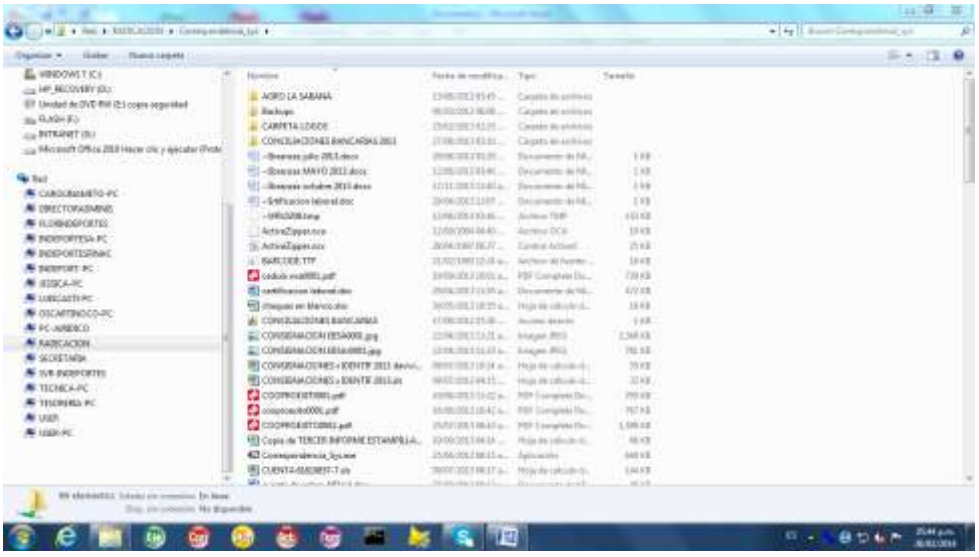
Fuente: Autor.

Ilustración 23Equipos que permiten acceso



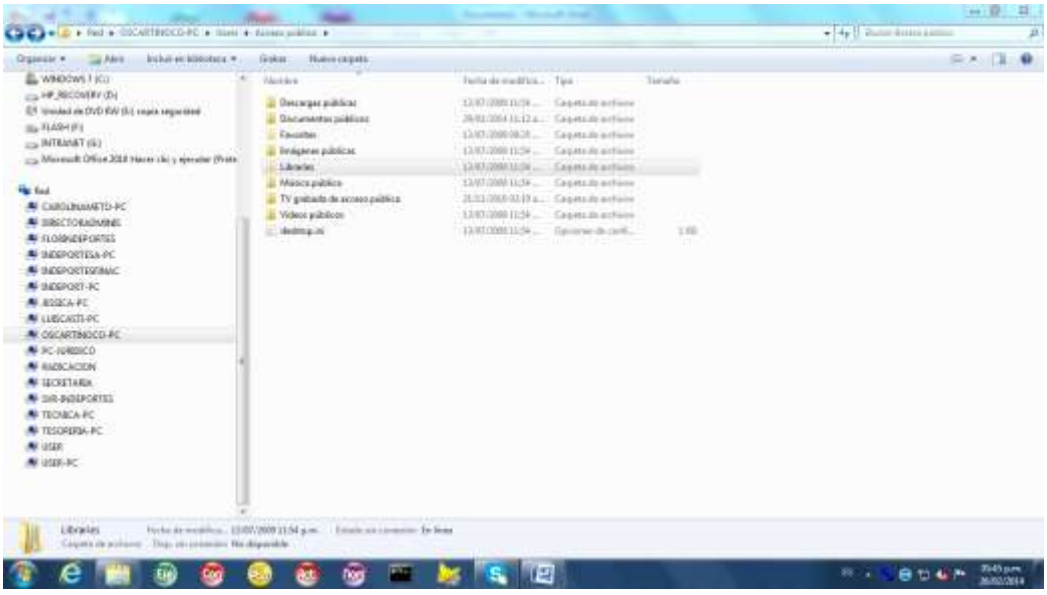
Fuente: Autor.

Ilustración 24Equipos que permiten acceso



Fuente: Autor.

Ilustración 25Equipos que permiten acceso



Fuente: Autor.

Teniendo acceso al servidor se puede constatar que existe un puerto que permanece abierto debido al soporte que debe realizarse mediante conexión remota, generando así cambios en la información sin tener un control de cambios activo.

7.4 MANEJO DE LA INFORMACIÓN – DIAGNOSTICO SITUACIÓN ACTUAL

En la actualidad Indeportes Boyacá tiene un manejo de información paralelo, de acuerdo a cada uno de los procesos que siguen para el cumplimiento de su misión, estos procesos los generan todos y cada uno de los usuarios que hacen parte de la entidad de manera individual.

No existe restricción alguna en cuanto a la disponibilidad de la información y aunque cada funcionario sabe que debe hacer, como manipular la información, la entidad no se queda con copia de esta y mucho menos con un control de cambios,

además que los backups son responsabilidad de las personas que manipulan la información y no existe seguridad en que ellos estén realizando este proceso de manera periódica lo que indica que se está presentando un riesgo latente con la información, sumándole a lo anterior la no restricción de descargas o paginas cuyos contenidos pueden tener software malicioso que nuevamente va a poner en estado de alto riesgo la información que se tiene.

La información se encuentra en constante peligro ya que la mayoría de los documentos carece de contraseñas tal como lo específica la norma de seguridad NTC 5411-1:2006, además que el tratamiento de la información no tiene definido un Sistema de Gestión de Seguridad Informática como lo indica la norma NTC ISO/IEC 27001. Cada usuario dispone de su información sin tener un orden o restricción, además que los equipos se encuentran altamente vulnerables teniendo en cuenta que utilizan el servidor como medio de dispersión de archivos, lo que hace que cualquier usuario que ingrese a la red tenga acceso a esos documentos, no tienen un tratamiento adecuado de la información sino que solo la almacenan en equipos, memorias, impresiones etc, pero no cumplen con la confidencialidad ni la disponibilidad.

La información está en riesgo por lo que no hay un esquema de tratamiento como lo indica la norma NTC ISO/IEC 2700, es decir no cumple con el modelo estándar PHVA.

Se puede apreciar que desde cualquier equipo conectado a la red podemos ingresar a otro y hacer uso o manejo de la información, no existe respaldo de documentos ya que no hay un control de Backups o un control de cambios lo que conlleva a que la información no se hace confiable teniendo en cuenta que cualquier usuario que este dentro de la red puede realizar modificaciones, además que no existe restricción de acceso a los equipos lo que se puede verificar mediante acceso de estos.

7.5 DESARROLLO DEL INFORME

Teniendo en cuenta lo observado se puede determinar las siguientes falencias comprobadas en el desarrollo de la práctica de seguridad informática en cuanto a la entidad de INDEPORTES BOYACÁ.

- **Estructura Física:** En cuanto a la estructura física, Indeportes Boyacá no cuenta con una seguridad adecuada que me garantice el cuidado y la no perdida de elementos relevantes para el buen funcionamiento infraestructura empresarial en cuestiones de hardware puesto que los mismos no tienen un control en el acceso o salida de los mismos ni hay garantías reales de no perdida de elementos siendo la única señal un ticket de Indeportes Boyacá que puede ser fácilmente desprendible.

- **Red Inalámbrica:** Dentro de la red inalámbrica se pueden observar 3 tipos de red con nombres de la entidad, según las pruebas de hacking se determinó que las contraseñas cumplen un nivel de seguridad mínimo ya que las mismas tienen asociación a la entidad y no cumple con los requisitos exigidos para obtener una contraseña indescifrable.

  Adicional de lo anterior la conexión a la red inalámbrica se realiza mediante ingreso de contraseña y se asigna IP por defecto, lo que genera un descontrol en la red ya que no se puede determinar con seguridad el número de equipos conectados y el volumen de información que manejan.

  Se cuenta con un router que trae configurada la seguridad por defecto, pero que la misma es deficiente y no es aplicable de manera manual sino que trae su predeterminación sin opción o posibilidad a cambios.

- **Red cableada:** Se encuentra que la red cableada tampoco tiene un direccionamiento ip fijo sino que el mismo lo toma predeterminado, esto no sucede en todas las conexiones, ya que los equipos de administrativos y las personas que manejan el paquete contable si tienen dirección ip fijas debido a la necesidad del programa. Es así como cuando un equipo diferente al de la entidad es conectado por medio de la red cableada, fácilmente tiene acceso por medio de la misma red a los documentos del servidor, teniendo permisos de eliminación, modificación, inserción dentro de la red, lo que genera el no cumplimiento de los 3 pilares de la información y se pone en riesgo la información que maneja el equipo contable de la entidad.

- **Backups:** Se determina que única y exclusivamente se realizan backups al sistema contable o financiero FLASH y este se realiza cada 15 días por el Ingeniero de Sistemas de la entidad; pero el resto de información manejada por las personas de planta como los contratistas no existe backup alguno, ya que en apariencia cada uno de ellos debe responder por su copia de respaldo lo que no le garantiza a la entidad que la información esté disponible cuando se necesite sino que dependa de terceros, adicional no se puede tener una información confiable porque no se manejan controles de cambios ni comparativos que nos puedan servir de ayuda en el momento de confrontar cierto tipo de información.

- **Antivirus:** En la actualidad no se cuenta con licencia de antivirus, sino que el mismo es de tipo gratuito para todos y cada uno de los equipos de los funcionarios de la entidad.

- **Firewall:** Solo en algunos equipos que son la gran minoría existe corta fuegos, los demás carecen del mismo, dejando desprotegido tanto el equipo como la red.

- **Restricción de Paginas:** No existe ningún tipo de restricción a páginas, los usuarios tienen acceso a cualquier tipo de navegación sin importar la seguridad que las mismas representen para la entidad.

- **Descargas:** No existe algún tipo de restricción en cuanto a descargas e instalación de software en los equipos que maneja la entidad, lo que hace que la mayoría de los equipos contenga caballos troyanos, gusanos, espías y cualquier tipo de virus que puede afectar tanto al equipo como a la red.

- **Traslado de la Información:** La entidad tiene activo todos y cada uno de los periféricos de traslado de información como lo son: puertos USB, unidades de CD/DVD, entre otros.

- **Seguridad de Equipos:** Se puede constatar en cada uno de los equipos que solo algunos cuentan con contraseñas de acceso que son en su gran minoría los demás carecen de la misma, presentándose así un problema de seguridad en cuanto a la información.

  El servidor se mantiene las 24 horas encendido y no posee ups para mitigar o controlar daños en caso de caídas de luz, adicional se observa que existe el puerto 80:80 que se encuentra abierto y disponible y es susceptible a realizar cualquier tipo de cambios relevantes de la información.

- **Seguridad en Usuarios:** Los usuarios de Indeportes Boyacá tienen manipulación diaria de la información, es decir ellos modifican la información de acuerdo a los parámetros de la entidad sin tener un control de cambios que pueda evitar un posible daño a la información, además que los mismos tienen red abierta lo que les permite realizar descargas que en un momento dado pueden ocasionar daños al equipo teniendo como

resultado la perdida de la información o en otros casos traslado de la información puesto que los correos no institucionales se encuentran activos lo que permite que los mismos lleven la información a través de la web o memorias USB ya que sus puertos también se encuentran habilitados y sin ningún tipo de restricción.

7.6. PROPUESTA DE SEGURIDAD

Teniendo en cuenta la información encontrada en el transcurso de análisis y pruebas realizadas a la entidad se pueden dar las siguientes sugerencias frente a los problemas encontrados de la siguiente manera:

- **Estructura Física:** Se sugiere verificación de cada una de las Entradas y salidas de las personas que ingresan a la entidad para corroborar cada uno de los ingresos y salidas de los elementos físicos de la entidad con el fin de asegurar que los mismos no corran peligro en cuanto a la pérdida o cambio.

- **Red:** Mantener instalado herramientas que permitan que el servicio de SSH (ataques de fuerza) sea optimo ya que así disminuimos la probabilidad de ser atacados por uno de estos.

- **Red Inalámbrica:** Las contraseñas deben cumplir los requisitos de seguridad que son los siguientes: mínimo 8 caracteres que contengan, letras, números, combinación de minúsculas y mayúsculas y un carácter simbólico, esto con el fin de no ser víctima de robos de contraseñas.

  Se recomienda ocultar cada una de las redes inalámbricas para que los dispositivos que contengan señal wifi no detecten la red y se abstengan de ingresar a ella de forma fraudulenta.

La contraseña debe tener un nivel de encriptación de tal forma que no sea observable los caracteres reales sino que los mismos tengan proceso de encripción ya sea en números o letras.

Teniendo en cuenta que no existe un control en la red en cuanto al número de usuarios que se encuentran conectados se sugiere realizar la inversión de un radio y un rack para que se puedan todas y cada una de las redes inalámbricas conectar mediante dirección ip estática, para así poder controlar los accesos a la red.

Se recomienda realizar inversión en router que deje programar manualmente la seguridad de la red, para que así la misma sea controlada por el administrador y no por un tercero.

- **Red cableada:** Se recomienda direccionar toda la red cableada mediante direcciones ip estáticas para tener control sobre cada uno de los equipos que ingresan a la red.

  Cada uno de los equipos debe tener seguridad en la red, es decir que no tenga opción de compartir documentos si no son necesarios, pero de serlos debe crear un usuario con contraseña para acceder a los mismos, de tal manera que si se presentan cambios se tenga la certeza que fueron realizados por personas autorizadas para esto.

- **Backups:** Se sugiere que los Backups del sistema contable se realicen diariamente y en horas no laborales pero los mismos no se deben almacenar en el mismo servidor sino que se tendrá un servidor o disco alterno para esas copias de seguridad; de igual forma se deben realizar copias de seguridad a los contratistas cada mes, esto con el fin de que la entidad cuente con la información que requiera sin disponer directamente

del encargado de la misma; con esto se contribuye a realizar revisiones y controles de cambios

- **Antivirus:** No se recomienda la utilización de antivirus gratuitos ya que en su gran mayoría traen encriptados virus que pueden contaminar el equipo y que generalmente se activan tan pronto se acaba el periodo de prueba; es por esto que se recomienda que se compre licencia de antivirus renovable cada año para así garantizar la seguridad en cada uno de los PC.

- **Firewall:** Se recomienda instalar el firewall en todos y cada uno de los equipos que se encuentren activos en la entidad y que sea compatible con el antivirus instalado para que no vayan a surgir bloqueos por permisos.

- **Restricción de Paginas**: Es necesario realizar el proceso de restricción de páginas, en primera media con el fin de no dejar puertas abiertas en las redes que puedan ocasionar daños a nuestra información; y en segundo lugar para no congestionar y cargar la red con temporales inutilizados.

- **Descargas:** Es necesario restringir las descargas sobre todo si se trata de software, ya que los mismos pueden tener ataques maliciosos que hacen que se pierda la información y ataquen el sistema operativo causando pérdidas incontables y daños irreparables; además se evita el uso de software ilegal.

- **Traslado de la Información:** Debido al cuidado que debe tener la información es necesario desactivar los periféricos de traslado de la información con el fin de proteger la información y evitar que la misma sufra filtraciones indeseadas.

- **Seguridad de Equipos:** Es necesario crear contraseñas a cada uno de los usuarios de los equipos siguiendo las normas de seguridad en contraseñas.

- Se recomienda apagar el servidor ya que puede sufrir un calentamiento simultáneo o deterioro anticipado de sus componentes.

- Se debe filtrar el puerto 80:80 de tal manera que se prevengan ataques externos al servidor de Indeportes Boyacá.

- Se debe Ejecutar el Proxy, de esta manera se van a filtrar todos y cada uno de los paquetes que vayan a causar algún tipo de daño en la red, se recomienda el uso de squid.

- Se hace necesario poner en marcha el uso del RAID (Redundant Array Of Inexpensive Disk), esto con el fin de proteger la información de posibles fallas técnicas.

- Cada equipo debe tener ups de mínimo 10 minutos de duración, para que tanto al software como al hardware garanticen una duración larga y no se tengan contratiempos.

- Se recomienda la realización de auditorías cada trimestre o semestre para prevenir cualquier tipo de daño en los servidores o posibles ataques a la información.

- **Seguridad en Usuarios:** Se hace necesario que se efectué un control de cambios en el área contable de la entidad de tal forma que si ocurre un error se pueda restablecer el documento a un estado anterior.

- Se debe aplicar seguridad de descargas a la red por parte de los usuarios para que así evitemos que por desconocimiento dañen la información que se tiene en cada uno de los equipos.

- Es necesario inhabilitar correos personales en la entidad para que no se efectúe traslado de información.

- Es necesario inhabilitar las entradas y salidas de USB o CD / DVD para que los usuarios no trasladen la información de querer hacerlo deben contar con un permiso.

7.7. PRESUPUESTO

Teniendo en cuenta los estudios, observaciones, conclusiones y recomendaciones de este proyecto a continuación se relaciona el presupuesto que se necesita para mejorar la seguridad informática de INDEPORTES BOYACÁ.

Cuadro 4. Presupuesto Implementación Seguridad Informática Física

PRESUPUESTO			
CANTIDAD	**DESCRIPCIÓN**	**VALOR UNITARIO**	**VALOR TOTAL**
2	Servidores Proliant con las siguientes características: 2 Procesador Intel Pentium, con 2 núcleos cada procesador, form Factor, con 4 salidas de fuente de alimentación y 4 ranuras de expansión. Estos serán necesarios para el manejo del software contable y la intranet	$ 1.740.990	$ 3.481.980
2	Rollos de cable de red tipo 6, ya que puede transmitir datos hasta de 1 Gbps en una frecuencia de 250 Mhz	$ 606.400	$ 1.212.800
2	router de banda dual preferiblemente tp-link	$ 309.000	$ 618.000
1	Repetidor de señal Cisco Linksys Re 1000	$ 205.000	$ 205.000
1	Rack con mínimo 54 UR	$ 930.000	$ 930.000
12	Licencias de sistema operativo Windows 7equipos de mesa	$ 170.000	$ 2.040.000

3	Licencia de antivirus por un año karpesky por 4 equipos	$ 179.000	$ 537.000
12	Licencias de Office 2013	$ 270.000	$ 3.240.000
2	Ingenieros de Sistemas, mano de obra.	$ 3.000.000	$ 6.000.000
1	Firewall para Windows compatible con PC del presupuesto.	$ 300.000	$ 3000.000
1	Gasto de improviso	$ 1.000.000	$ 1.000.000
1	Profesional Categoría 5 en Ingeniería de Sistemas Especialista en seguridad Informática. (Un mes)	$4.311.000	$4.311.000
	TOTAL	**$ 13.021.390**	**$ 23.875.780**

Fuente. Autor

7.8. CRONOGRAMA

A continuación se relaciona el cronograma de implementación de seguridad física en INDEPORTES BOYACA.

Cuadro 5. Cronograma de Implementación Seguridad Física

ACTIVIDAD	MES 1				MES DOS			
	1	2	3	4	1	2	3	4
Consultoría de análisis de vulnerabilidades								
Compra de implementos								
Implementación de Servidores								
Implementación de Cableado								
Instalación de Router y pruebas de seguridad								
Instalación de Rack y prueba de Seguridad								
Implementación de equipos con Sistemas de Seguridad, Office, antivirus y licencias								
Pruebas de Vulnerabilidad a la red								
Pruebas de vulnerabilidad o hardering a los equipos								
Verificación de funcionamiento de seguridad								
Entrega Final								

Fuente. Autor.

8. CONCLUSIONES Y RECOMENDACIONES

El presente trabajo permitió detectar las falencias de seguridad informática presentadas en la entidad Indeportes Boyacá y a la vez entregar una propuesta para la implementación y mejoramiento de seguridad informática de la entidad mencionada de tal manera que permanezca en el tiempo y mejore la seguridad de la información cumpliendo a cabalidad con los tres pilares informáticos.

Se recomendó Implementar una política de seguridad informática en cuanto al manejo que se le debe dar a la información y al cuidado de la misma, esto con el fin de garantizar el cumplimiento de la misión y visión de la entidad, como lo estipula la norma NTC ISO/IEC 2700, en cuanto a la implementación del modelo PHVA y el tratamiento del riesgo que lo determina el numeral 4 de la presente norma con el sistema de Gestión de Seguridad Informática.

Se recomendó Implementar la norma de seguridad ISO 27002, cuyo objetivo es preservar la confidencialidad de la información cumpliendo los estándares de seguridad, integridad y disponibilidad de la información y sus activos asociados y fragmentado en once secciones, para garantizar que la información se maneje de forma segura a través de los dispositivos con los que cuenta INDEPORTES BOYACA.

Se recomendó capacitar a los usuarios de la entidad en las buenas prácticas del manejo y tratamiento de la información en cuanto a los riesgos de gestión de la Información tal cual lo dispone la Norma NTC ISO 27001 4.2.2. Literal B.

El servidor de la entidad es uno de los principales componentes de la entidad ya que allí se encuentra almacenada la información más relevante de la empresa, es por esto que se hace necesario implementar un plan de auditoría constante con el

fin de garantizar el correcto funcionamiento, este plan debe estar alineado con la norma ISO 27001, aquí se podrán implementar controles específicos donde los usuarios implementen medidas de seguridad con el manejo de las herramientas tecnologías que en la actualidad maneja y tienen a disposición INDEPORTES BOYACA.

La utilización de usuario y contraseñas garantizan cada una de las actividades realizadas por una persona y se hace necesaria para realizar un debido control de cambios tal como lo establece la norma NTC 5411-1:2006, numeral 4 Literal c.

En necesario el uso de herramientas que permitan la administración de la red tal como radios y racks y accesos por plataforma para controlar el número de usuarios registrados y conectados a la red y tener el control sobre la información que se maneja para que no se presenten filtros de información diferente a la manejada por la entidad.

Es necesario utilizar la herramienta firewall ya que esta protege la información en gran medida, porque su función es permitir o negar acceso a la red de acuerdo con los permisos otorgados por el administrador.

Es necesario usar antivirus licenciado para prevenir propagación de virus que puedan causar daños a la información, ya que esto evita en gran medida la intrusión tanto de troyanos como espías que quieran realizar modificación o eliminación de la información.

El uso de Backups previene la pérdida de información en las entidades, es por esto que se hace necesario realizar un cronograma mensual dependiendo cada uno de los riesgos de la información con el fin de custodiar la información por si llegara a suceder algún tipo de daño.

El bloqueo de páginas de internet y descargas hace que la red sea más eficiente y que los funcionarios rindan más en las tareas correspondientes y a su cargo, por esto es necesario realizar el respectivo bloqueo para evitar descargas o acceso a páginas que ocasionen daño, perdida o modificación a la información, esto se realizará mediante bloqueo en el router principal.

Para la corrección de los problemas presentados se recomendó la adquisición de los siguientes componentes:

- 2 Servidores Proliant con las siguientes características: 2 Procesador Intel Pentium, con 2 núcleos cada procesador, form Factor, con 4 salidas de fuente de alimentación y 4 ranuras de expansión. Estos serán necesarios para el manejo del software contable y la intranet.
- Instalación de cable de red tipo 6, ya que puede transmitir datos hasta de 1 Gbps en una frecuencia de 250 Mhz.
- 2 router de banda dual preferiblemente tp-link.
- 1 Repetidor de señal Cisco Linksys Re 1000.
- 1 Rack con mínimo 54 UR.
- 1 Firewall de compatibilidad con los equipos aquí presupuestados

9. BIBLIOGRAFÍA

ICONTEC. Norma técnica colombiana 1486. Documentación, presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C. 2008. 42 p.

ICONTEC. Norma técnica colombiana 5613.Referencias Bibliográficas. Contenido, Forma y Escritura. Bogotá D.C. 2008. 38 p.

ICONTEC. Norma técnica colombiana 4490. Referencias Documentales para Fuentes de Información Electrónicas. Bogotá D.C. 1998. 27 p.

EL CONGRESO DE COLOMBIA. Ley 1273 de 2009, Código Penal "De la Protección de la información y de los datos. Bogotá D.C. 1993. Capítulos I y II, Arts. 269A, 269B, 269C y s.s.

Gómez, M., Aparicio, A., Ortega, A., Camacho, M., Rondón, J., Rocha, M., Torres. P., Salgado, M, & Nieto, C (2011). La investigación Ciencias en la Escuela de Básicas, Tecnología e Ingeniería. Bogotá. Unad.

Contreras N. (2011). Enfoque de la Seguridad de la información, Instituto Tecnológico Nacional de Argentina.

Bruneau, G. (2001). The history and evolution of Intrusion Detection. http://www.sans.org/reading_room/whitepapers/detection/history-evolution-intrusion.

Ludovic Mé, C. M. (SSIR 2001). Intrusion detection: A bibliography. http://www.cs.uiuc.edu/class/fa05/cs591han/papers/intrusionbib.pdf.

Anderson, J. P. (1980). Computer Security Threat Monitoring and Surveillance. http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf.