ANÁLISIS DE LOS RESULTADOS DE ETHICAL HACKING PARA EL CONTROL DE VULNERABILIDADES DE LA BASE DE DATOS TAO ESQUEMA SERVICIOS DE ALCALDÍA DE IBAGUÉ

CLAUDIA LORENA RESTREPO ANGEL
EDWIN GEOVANNY SANCHEZ JARAMILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2018

ANÁLISIS DE LOS RESULTADOS DE ETHICAL HACKING PARA EL CONTROL DE VULNERABILIDADES DE LA BASE DE DATOS TAO ESQUEMA SERVICIOS DE ALCALDÍA DE IBAGUÉ

CLAUDIA LORENA RESTREPO ANGEL
EDWIN GEOVANNY SANCHEZ JARAMILLO

Investigación Aplicada

Director: Martin Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
IBAGUÉ
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Ibagué, 31 mayo de 2018

Dedicatoria

CLAUDIA LORENA RESTREPO ANGEL

Dedico este proyecto a Dios, a mis padres y a mi hermano que me apoyan todo el tiempo.
A mis compañeros de oficina que son un gran apoyo moral durante el tiempo que se realizó este proyecto.

EDWIN GEOVANNY SÁNCHEZ JARAMILLO

A mi Dios que todo lo puede y el que me da fuerzas para avanzar, a mis padres, esposa e hijo que me apoyan en el camino de la vida, a los tutores que nos orientan, a los compañeros y amigos de siempre, mil gracias.

AGRADECIMIENTOS

Los autores de este proyecto expresan sus más sinceros agradecimientos a:

Las directivas de la Universidad Nacional Abierta y a Distancia UNAD por brindar caminos y alternativas para poder prepararnos en esta disciplina tan importante como la seguridad informática.

Al Director del proyecto ingeniero Martin Cancelado, quien acompañó y dirigió el proceso de consolidación del proyecto.

Al tutor Salomón González quien estuvo atento brindando asesoría en el armado del proyecto y complementarios.

A los compañeros que desde el ambiente virtual nos acompañaron el proceso, muchas gracias.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

INTRODUCCIÓN

Las computadoras de cualquier sistema informático son vulnerables a ataques de *Crackers* o *hackers* que son capaces de ingresar al sistema borrando información, modificándola o robándola poniendo en peligro su integridad y haciendo perder a las organizaciones la confianza dentro y fuera de ella. Es por eso que se hace imprescindible saber si estos sistemas y redes de datos están protegidos contra intrusiones.

El *Ethical Hacking* presenta herramientas para hacer hackeo ético explotando las vulnerabilidades existentes en el sistema haciendo test de intrusión evaluando así la seguridad para nuestro caso a las bases de datos.

La seguridad informática dentro de una organización requiere de metodologías y procedimientos que garanticen la integridad, confidencialidad y disponibilidad de la información, es ahí donde los servicios de *Ethical Hacking* entran a evidenciar que vulnerabilidades tienen los sistemas y así ayudar a las organizaciones a tomar correctivos necesarios tendientes a cerrar las puertas, donde los *hackers* pueden hacer daño. Dentro de las tácticas que utiliza se encuentran la ingeniería social, herramientas de *hacking* y uso de *Metasploit* (para vulnerar y entrar a las áreas críticas de los sistemas de la organización).

Las pruebas de penetración hacen parte del proceso de gestión de riesgos organizacionales, mediante el cual se identifican y se abordan sistemáticamente los riesgos; es ahí donde las organizaciones se dan realmente cuenta de que tanto pueden llegar a ser vulneradas y qué acciones tomar ante una intrusión no autorizada. Un activo es algo que usted valora; Una amenaza es algo que puede afectar su activo; Una vulnerabilidad es algo que aumenta la probabilidad de que ocurra la amenaza; Y un control es algo que mejorará la situación, al prevenir, detectar o de otra manera reducir el impacto de una amenaza. Por ejemplo: un activo podría ser un archivo de gestión documental; Una amenaza, podría ser un incendio; Una vulnerabilidad, sería almacenar que un corto circuito por tomas eléctricos cercanos al archivo; Y un control, podría ser la instalación de un extintor de incendios.

Los procedimientos que se realizaran con *Ethical Hacking* dejaran como resultado un documento con un listado de vulnerabilidades del sistema de la base de datos

igualmente las recomendaciones a seguir para que sean aplicadas por el personal de seguridad informática de la entidad en mención.

1. DESCRIPCIÓN DEL PROBLEMA

La gran mayoría de entidades estatales, presenta un alto índice de vulnerabilidades en cuanto a seguridad informática en sus infraestructuras tecnológicas internas, redes, bases de datos, aplicativos, teniendo en cuenta la información como principal activo y el insumo para cumplir la misión de servir a la comunidad y efectuar las metas en sus planes de desarrollo, caso puntual el de las bases de datos donde se ven vulneradas por intrusiones no autorizadas produciendo perdida de datos, integridad de la información y confianza al interior y exterior de la entidad, esto también se ocasiona por factores como:

- Deficiencias de conocimiento técnico en materia de seguridad informática, por parte de los líderes de TI de la organización.

- Falta de liderazgo por parte del grupo TI de la entidad.

- Falta de apropiación de técnicas encaminadas a la detección y corrección de intrusiones a los sistemas de la organización.

- Asignación de Presupuestos insuficientes para la implementación de medidas que protejan el entorno digital de la organización y asignación de presupuesto para actualización de licenciamiento a nivel de software de bases de datos en los servidores de aplicaciones.

- Falta de controles en la implementación, divulgación y actualización de las políticas de seguridad.

- Falta de log de auditoria en las bases de datos.

Se pretendería entonces articular las estrategias de gobierno en línea en el sentido de apropiar metodologías que pretendan asegurar y conservar la privacidad de la información contenida en el esquema estudiado de base de datos; permitiendo así tener un modelo acorde a las necesidades que mejore los niveles de seguridad, que evidencie los avances del país en la materia y que permita identificar las infraestructuras críticas y mejorar la respuesta ante las amenazas que afectan la seguridad digital.

La Alcaldía Municipal de Ibagué, corresponde a una entidad territorial del estado, ubicada en calle 9 número 2-59 sede principal, posee una infraestructura tecnológica a nivel de servidores ubicados en el *Datacenter* central, una base de datos local en Oracle llamada Aplicativo Tao y el esquema de servicios de mantenimiento técnico a la institución, siendo esta materia de estudio del presente proyecto.

TAO es desarrollo de software propio de la organización y cuenta con el personal de ingenieros de soporte a la base de datos en todos sus esquemas. El esquema servicios maneja la base de datos del registro de los servicios que llegan a la Dirección de informática asignándole un número de servicio y un técnico que realiza la obra. Igualmente se registran los datos del equipo al cual se le realiza el servicio (marca, Serial, tipo de dispositivo, placa de inventario, funcionario peticionario, Numero de oficio de la solicitud, entre otros).

El aplicativo cuenta con más de 15 años de adquirido y de funcionamiento, presentando deficiencias en su seguridad y preexistiendo ataques al sistema, comprometiendo su confidencialidad, integridad y disponibilidad. Lo anterior, por falta de aplicar políticas de seguridad encaminadas a la detección profunda de las vulnerabilidades en la plataforma y en la aplicación de procedimientos idóneos que contrarresten los ataques internos y externos a la base de datos, ya que, el uso del código pudo haber sido vulnerado y modificado, por lo que no se han actualizado sus procedimientos de uso y seguridad.

Como es una plataforma que maneja elementos de inventario, no cuenta con la interfaz con la unidad de almacén quien hace el control de los elementos de cómputo y que realiza este control con otra plataforma tecnológica, haciendo que sean independientes los dos software, razón por la cual es necesario integrar las dos en una misma plataforma y actualizarla a un esquema más robusto y seguro.

Con respecto a la políticas de seguridad de la entidad, deben ser reestructuradas y bajar al detalle, debido al crecimiento de la cantidad de aplicaciones en los servidores se han desactualizado dichas políticas y no se podría establecer directrices claras dentro de las cuales estén el control de amenazas de acceso no autorizados a través de metodología de "*Ethical Hacking*" se puede blindar la vulnerabilidad al ejercer control en la forma como están ingresando indebidamente, minimizando el riesgo de pérdida de información y disponibilidad de la misma.

1.1. FORMULACIÓN DEL PROBLEMA

¿Cómo emplear la herramienta Ethical Hacking, para prever los ataques de intrusos, mediante el uso de metodologías para esquema de servicios de la base de datos Tao?

2. OBJETIVO GENERAL

Emplear técnicas de Ethical Hacking, mediante el uso metodologías, en el esquema de Servicios, para prever los ataques de intrusos en la Base de Datos TAO de la Alcaldía de Ibagué.

2.1. OBJETIVOS ESPECÍFICOS

- Establecer la metodología y/o herramientas para el desarrollo del Ethical hacking.
- Efectuar revisión del estado de la base de datos respecto a sus log de auditoria y estado del servidor.
- Determinar el estado de seguridad de la base de datos.
- Estudiar y justificar el uso de herramientas de seguridad para la base de datos.
- Realizar el cronograma de testeo a la base de datos con el software escogido.
- Documentar las posibles fallas y controles a implementar en la gestión de la seguridad de las bases de datos.

3. JUSTIFICACIÓN

El crecimiento constante de la tecnología a nivel mundial ha hecho que las organizaciones adopten cada vez más herramientas tecnológicas, para la salvaguarda y gestión de los activos informáticos. Apoyados en normas de seguridad de la información y procedimientos TI se logra que estos activos se protejan, ya que su disponibilidad los hace vulnerables a ataques al interior y exterior de la organización.

La alcaldía de Ibagué como organización del estado puede apoyarse en los lineamientos de gobierno en línea en lo que se refiere a la adopción de prácticas que suministren requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de seguridad y Privacidad de la Información –MSPI de la estrategia de Gobierno en línea –GEL.[1]

El objetivo de los diagnósticos que se hagan en cuanto a determinar el nivel de seguridad y privacidad de la información y de los sistemas de información es permitir llevar a cabo el desarrollo de un plan de seguridad y privacidad de la información que logre mitigar el riesgo, realizando controles, haciendo seguimiento a los mismos y generando ajustes y mejoras continuas a estos procesos.[2]

Para el caso de las bases de datos, estas pueden ser vulneradas internamente por medio de intrusión, vulnerando el código e indisponiendo así la integridad y disponibilidad de la información haciendo débil la entidad en cuanto a la presentación de informes pues la información que se presenta al usuario final no cumple con los requerimientos mínimos para el normal desarrollo de sus actividades.

Las herramientas de "*Ethical Hacking*" son un gran aliado en la búsqueda de vulnerabilidades y fallas de seguridad en los sistemas informáticos, mediante ataques en un ambiente controlado con su respectiva planificación, reconocimiento, ataque y resultado; todo esto con autorización de la entidad.

---

[1] (Estrategia Gobierno en Línea, Seguridad y Privacidad de la Información. [En línea]. 2016, Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

[2] (MANUAL, Estrategia Gobierno en Línea. [En Línea]. 2015, Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/propertyvalues-7751_archivo_pdf_manual.pdf)

No obstante, aunque las Entidades Estatales también son objeto de ataques no se ha creado la conciencia de proteger los activos de información y poco se invierte en seguridad, ya que se centran los esfuerzos en el cumplimiento de la misión propia de la Entidades sin prever que la pérdida de información conlleva a ser objeto de investigaciones y sanciones

Por esto se hace necesario la ejecución de herramienta de "*Ethical hacking*" en bases de datos en la alcaldía Municipal de Ibagué a la base de datos de Servicios técnicos, para así asegurar en gran medida los tres pilares de la información, integridad, disponibilidad y confidencialidad.

4. MARCO REFRENCIAL

4.1. MARCO TEÓRICO

Ethical hacking es una serie de herramientas y técnicas que nos muestra las vulnerabilidades en los sistemas informáticos. De acuerdo al análisis realizado a los resultados obtenidos mediante la aplicación de estas herramientas, se puede proponer varias medidas de seguridad para la disminución de riesgos informáticos[3].

Haciendo una revisión a los antecedentes o historia del Ethical Hacking, encontramos que la primera máquina considerada como máquina hacking ética, es El "bombe", el cual era un dispositivo electromecánico que fue utilizado durante la segunda guerra mundial por los británicos para descifrar mensajes en alemán. [4]

En el año 1960 Por primera vez los expertos en seguridad discutieron la posibilidad de la “penetración” de la computadora, teniendo como referencia pruebas al azar realizadas por profesionales.

La fuerza Aérea de los estados Unidos fue pionera en esta técnica de rastreo, es así como en 1971 contrató a James Anderson para hacer rastrear su sistema. En este año surge el primer “equipo tigre” (tigerteam), los cuales eran técnicos especialistas conformados para rastrear posibles fuentes de fallas en el Subsistema de nave espacial. Así mismo en el año 1974 llevó a cabo las primeras prácticas de hacking ético para verificar la seguridad del Sistema Operativo Multics. .[5]

La Marina Estadounidense también se acoge a esta práctica y en el año 1984 El comandante Richard Marcinko, construye y lidera un equipo cuyo objetivo es

[3] (UNAM, Universidad Nacional Autónoma de México. [En línea]. 2011, Disponible en: https://www.seguridad.unam.mx/historico/documento/index.html-id=7)

[4] (ISSUU, Actividad integradora luis angel us brito. [En Línea]. 2017, Disponible en: https://issuu.com/iudy/docs/actividad_integradora_luis_angel_us)

[5] (Trustware. Inforgraphic: A time of 15 key dates in ethical hacking history. [En línea]. 2013, Disponible en: https://www.trustwave.com/trustednews/2013/09/infographic-timeline-15-key-dates-ethical-hacking-history/)

identificar vulnerabilidades de las bases navales frente a la amenaza de terrorismo.[6]

La primera publicación de Hacker y para Hackers fue la revista electrónica Phrack publicada el 17/11/1985, la revista está disponible para contribuciones tanto de hacker como de profesionales en seguridad informática.

En el año 1986 Estados Unidos considera que ciertas metodologías de hacking ético son ilegales si no existe un acuerdo contractual y expide normatividad al respecto.

Posteriormente en el año 1995 Dan farmer y wietse venema liberan SATAN (Security Analysis Tool for Auditig Networks), que es una herramienta de seguridad que fue diseñada para ayudar a los administradores de sistemas de información y redes para escanear vulnerabilidades de forma automatizada e informar problemas relacionados con la red. SATAN se convierte en una herramienta muy popular de hacking.[7]

En el año 1999 la seguridad de software y sistemas de información se convierte en una prioridad, la cual se ve materializada con el lanzamiento de Windows 98 de Microsoft, configurándose en una bandera en contra de la piratería informática.

Se avanza en la práctica del ethical hacking en el año 2003 cuando el proyecto de seguridad de aplicaciones web abierta (OWASP) publica la primera guía de pruebas de OWASP, diseñada para orientar las mejores prácticas en las pruebas de penetración.[8]

En el año 2009 se lanzó el PTES (estándar de ejecución de pruebas de penetración), Este proporciona a las empresas una guía para hacer pruebas de

[6] (Trustware. Inforgraphic: A time of 15 key dates in ethical hacking history. [En línea]. 2013, Disponible en: https://www.trustwave.com/trustednews/2013/09/infographic-timeline-15-key-dates-ethical-hacking-history/)

[7] (Trustware. Inforgraphic: A time of 15 key dates in ethical hacking history. [En línea]. 2013, Disponible en: https://www.trustwave.com/trustednews/2013/09/infographic-timeline-15-key-dates-ethical-hacking-history/)

[8] (Trustware. Inforgraphic: A time of 15 key dates in ethical hacking history. [En línea]. 2013, Disponible en: https://www.trustwave.com/trustednews/2013/09/infographic-timeline-15-key-dates-ethical-hacking-history/)

intrusión real, la recolección de información, análisis de amenazas y vulnerabilidades, e informes.

A partir del año 2013 la seguridad de la información ha sido prioridad para las Empresas por lo que cada vez se invierten mayores recursos en este tema, oportunidad que es aprovechada por los ejecutivos de seguridad para hacer del uso de servicios de pruebas de penetración una actividad rentable en contra de la piratería. [9].[10]

El Hacking ético es una práctica de prevención que consiste en hacer pruebas a los sistemas de información, redes y dispositivos a fin de encontrar vulnerabilidades, con el fin de reportarlas y de esta manera establecer mecanismos, políticas y controles que permitan administrar los riesgos a los cuales están expuestos los activos de información.

La mayoría de las Empresas, en especial Entidades Financieras han optado por hacer uso de la práctica de *Ethical Hacking*, para evitar ser víctimas de ataque cibernéticos que ponen en riesgo la continuidad del negocio.

El proyecto de investigación de la Universidad de Ocaña en el 2014 (PLAN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA BIBLIOTECA ARGEMIRO BAYONA DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, MEDIANTE LA APLICACIÓN DE LA NORMA ISO 27001 Y TÉCNICAS DE ETHICAL HACKING), elaborado por LEONARD DAVID LOBO PARRA, JESÚS ANDRÉS OVALLOS OVALLOS y ANA MARIA SIERRA GÓMEZ[11], fue planteado como investigación descriptiva, en el que optaron por la técnica de observación estructurada, y aplicaron entre otras técnicas de levantamiento de información el *pentesting* y análisis forense, lo cual permitió

[9] (SlideShare. The History of Ethical Hacking and Penetration Testing. [En línea]. 2015. Disponible en: https://es.slideshare.net/installCore/install-core-history-of-ethical-hacking-and-penetration-testing)

[10] (Trustware. Inforgraphic: A time of 15 key dates in ethical hacking history. [En línea]. 2013, Disponible en: https://www.trustwave.com/trustednews/2013/09/infographic-timeline-15-key-dates-ethical-hacking-history/)

[11] (LOBO PARRA Leonard David, Tesis. Plan de gestión de la seguridad de la información de la biblioteca Argemiro Bayona de la universidad francisco de paula Santander Ocaña, mediante la aplicación de la norma ISO 27001 y técnicas de ethical hacking. Ocaña Santander, 2012.Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/325/1/25095.pdf)

identificar vulnerabilidades y realizar un diagnóstico claro para establecer e implementar políticas de seguridad, controles y lineamientos que permitirán a la Entidad prever ser objeto de ataques de intrusos, cumpliendo de esta manera con el objetivo del proyecto de grado.

En la revista especializada en seguridad de la información red seguridad, el director técnico del área de seguridad tic de *sidertia solutios*, Juan Luis García Rambla, en su artículo denominado "*hacking*' ético profesional, una necesidad ineludible para empresas y organizaciones"[12], expresa que la auditoría de seguridad o hacking ético debería efectuarse por lo menos una vez año, de tal forma que las Empresas que aplican esta técnica, puedan conocer la evolución del sistema de seguridad, la eficacia de los procedimientos y determinar si la inversión en seguridad es apropiada o no, de tal forma que se tomen correctivos de manera oportuna.

Así mismo Emanuel Abraham, quien se desempeña como *Ethical Hacker* de la empresa *Security Solutions & Education* (SSE), representantes para Colombia del consejo Internacional de Comercio Electrónico[13], considera que el hacker informático puede ser un estudiante curioso o un criminal peligroso. La diferencia es que el *ethical hacker* busca proteger la información mediante la penetración a los sistemas de información con permisos de los propietarios de la misma, e identifican las vulnerabilidades para determinar medidas preventivas, mientras que el propósito del de sombrero negro es vulnerar sistemas sin permisos, hacer daños, destruir o robar información.

El portavoz de la compañía de software de seguridad ESET, Josep Albors, ha explicado que los hackers éticos no se limitan a reaccionar ante las amenazas, sino que son proactivos y diseñan defensas anticipándose a los intrusos, pero para ello se debe conocer hacia donde apuntan dichas amenazas, por lo que se

[12] (GARCÍA RAMBLA, Juan Luis. 'Hacking' ético profesional, una necesidad ineludible para empresas y organizaciones. En: Red seguridad. [En línea]. Disponible en: http://www.redseguridad.com/opinion/articulos/hacking-etico-profesional-una-necesidad-ineludible-para-empresas-y-organizaciones)

[13] (ENTER.CO. El Hacking ético y su importancia para las empresas. [En línea]. 2014. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/)

justifica realizar intrusiones autorizadas o prácticas de penetración en los sistemas de información, con fines preventivos.[14]

En Colombia la referencia más representativa con respecto al tema de Hacking últimamente ha estado ligada a escándalos de índole político, recordemos la operación del CTI a la fachada militar de inteligencia informática, Andrómeda, el 24/01/2014[15]. A partir de ese evento ha quedado en el entender de la gente que el hacker es algo delictivo, maligno, por lo que se considera que es necesario tener claridad en la diferencia que existe entre el hacker y el hacker ético.

El Ministerio de las TIC en la guía Seguridad y Privacidad de la Información, propone la aplicación del hacking ético para detectar vulnerabilidades de direcciones IP, producto de la valoración de servicios críticos para las Entidades del Estado[16], como estrategia para implementar mecanismos de seguridad dentro del componente Gobierno en Línea.

Dentro del hacking ético se pueden realizar pruebas de pentesting dentro de esas pruebas se encuentran caja negra, caja gris y caja blanca. Las pruebas pentesting están catalogadas como la forma más viable de medir la seguridad de los sistemas de información, ya que utiliza herramientas similares o iguales a las que utiliza un atacante, con la diferencia que se realiza en un ambiente controlado y la finalidad es encontrar fallas de seguridad y arreglarlas para evitar intrusión no autorizada.

- **Pruebas de Penetración Caja Blanca.** Es el informe más sencillo de hacer ya que se le suministra toda la información necesaria al que va a realizar las pruebas información como tipos de sistemas, cantidad de equipos conectados,

[14] 20 MINUTOS .EFE Los Hackers Éticos, el peor enemigo de los ciberdelincuentes.[En línea].2011. Disponible en (http://www.20minutos.es/noticia/1108742/0/hacker/etico/campus/#xtor=AD-15&xts=467263)

[15] QUEVEDO HERNANADEZ, Norbey. De Andrómeda a los 'hackers'. En: El Espectador [En línea]. 17-05-2014. Disponible en: https://www.elespectador.com/noticias/investigacion/de-andromeda-los-hackers-articulo-492933

[16] (MINTIC. Guía de aseguramiento del Protocolo OPv6. En: Estrategia Gobierno en Línea. [En Línea]. 2017, Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf)

estructura de la red, servidores, contraseñas, etc.[17] Cabe resaltar que esta información que se entrega para realizar el proceso se ejecuta desde dentro de la entidad, perdiendo así dificultad el proceso de acceso al sistema.

- **Pruebas de Penetración Caja Negra.** En este proceso no se suministra ningún tipo de información al ejecutor de las pruebas, teniendo así un informe de cuan vulnerable es nuestro sistema y teniendo el mínimo de personas y/o usuarios informados de las pruebas una mayor veracidad en los resultados de los ataques. Este tipo de penetración es más costosa por lo que se trabaja sin información previa, pero garantiza la efectividad de los resultados que se irán documentando.
- **Pruebas de Penetración Caja Gris.** Este tipo de método es la combinación de las dos cajas anteriores se trata de dar información parcial no toda del sistema a estudiar, es precisa utilizarla cuando se quiere atacar una parte o un proceso especifico en un sistema de datos.[18]

Nessus es un software de escaneo de vulnerabilidades, utiliza el *Nessusd*, que realiza escaneo en el dispositivo donde se ejecuta, y *Nessus*, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. En modo normal *Nessus* es un software que escanea los puertos con nmap, es bastante útil a la hora de escanear puertos para detectar los que se encuentran abiertos y luego ejecutar *exploits* para atacarlos.[19]

Nmap es un Software de código abierto que se utiliza para realizar rastreo de puertos. Está escrito originalmente por Gordon Lyon. El desarrollo se encuentra hoy a cargo de una comunidad. Se usa para evaluar la seguridad de sistemas

[17] A.Esaú. Tutorial Hacking: Razones para realizar un Pentesting a nuestra empresa. [En Línea] 2015. Disponible en (https://openwebinars.net/blog/Tutorial-hacking-razones-para-realizar-un-pentesting-a-nuestra-empresa/)

[18] BALOCH Rafay.Ethical Hacking and Penetration testing Guide.2014. Disponible en (https://books.google.es/books?id=fKfNBQAAQBAJ&lpg=PP1&ots=SbHCMk4aZJ&dq=ethical%20hacking%20database%20how%20work&lr&hl=es&pg=PA282#v=onepage&q=ethical%20hacking%20database%20how%20work&f=false)

[19] HIGHSEC. Instalación de NESSUS. [En línea] 2013. Disponible en: http://highsec.es/wp-content/uploads/2013/11/Nessus.pdf

informáticos. Igualmente posee varias funciones para sondear redes, incluyendo detección de equipos, servicios y sistemas operativos.[20]

4.2. MARCO CONCEPTUAL

Para el desarrollo del proyecto se medirán variables que están directamente involucradas con vulnerabilidades, amenazas y riesgos de la seguridad de la información, en cuanto a su Disponibilidad, integridad y Confidencialidad específicamente en el diagnóstico de las vulnerabilidades del esquema de servicios de la base de datos de Tao Alcaldía de Ibagué. A continuación, se describe algunos conceptos en el marco del *Ethical Hacking* a bases de datos:

Base de Datos: una base de datos es una unidad que nos permite guardar y acceder a la información debidamente agrupada y estructurada.

Ethical Hacking: hace referencia en aplicación de hacking autorizado a un sistema informático para fines legales y defensivos.

Amenaza: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización" .[21]

Riesgo: "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias" [22]

Vulnerabilidad: "Debilidad de un activo o control que puede ser explotada por una o más amenazas."[23]

---

[20] WIKIPEDIA. Nmap. [En línea]. Disponible en: https://es.wikipedia.org/wiki/Nmap

[21] (ORACLE, Oracle Enterprise Manager 11g. [En línea]. 2016, Disponible en: http://www.oracle.com/technetwork/es/oem/grid-control/overview/index.html)

[22] (ISO 27000.es, El portal de ISO 27001 en Español. Glosario. Riesgo. [En línea]. 2016, Disponible en: http://www.iso27000.es/glosario.html)

[23] (ISO 27000.es, El portal de ISO 27001 en Español. Glosario. Vulnerabilidad. [En línea]. 2016, Disponible en: http://www.iso27000.es/glosario.html)

Confidencialidad: “Debilidad de un activo o control que puede ser explotada por una o más amenazas”[24]

Disponibilidad: “Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.”[25]

Integridad: “Propiedad de la información relativa a su exactitud y completitud”. [26]

Auditoria: “Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000) “[27]

Control: “Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.”[28]

[24] (ISO 27000.es, El portal de ISO 27001 en Español. Glosario. Confidencialidad. [En línea].2016, Disponible en: http://www.iso27000.es/glosario.html)

[25] (ISO 27000.es, El portal de ISO 27001 en Español. Glosario. Disponibilidad. [En línea]. 2016, Disponible en: http://www.iso27000.es/glosario.html)

[26] (ISO 27000.es, El portal de ISO 27001 en Español. Glosario. Integridad. [En línea]. 2016, Disponible en: http://www.iso27000.es/glosario.html)

[27] (GOBIERNO EN LÍNEA. Modelo de Seguridad y Privacidad de la Información. Glosario. Auditoria. [En línea] 2016, Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

[28] (GOBIERNO EN LÍNEA. Modelo de Seguridad y Privacidad de la Información. Glosario. Control. [En línea] 2016, Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

4.3. MARCO LEGAL

La ley 1273 de 2009 del congreso de la republica habla de la clasificación de los delitos informáticos. Dentro de los artículos más relevantes de la ley se encuentran los siguientes: [29]

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

> Artículo 269 A: Acceso abusivo a un Sistema informático. Quien incurra en acceder a un sistema informático sin autorización aun estando el protegido violando la seguridad del mismo incurrirá en una pena de prisión de cuarenta y ocho a noventa y seis meses y una multa entre 100 y 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegitima de sistema informático o red de telecomunicación. El que incurra en la obstaculización del funcionamiento de un sistema informático, al acceso los datos informáticos o a una red de telecomunicaciones incurre en una penalización de cuarenta y ocho a noventa y seis meses de prisión y en una multa de 100 a 1000 salarios mínimos legales vigentes. -Artículo 269C: Interceptación Datos Informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

> Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

> - Artículo 269E: Uso de Software Malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o

[29] ALCALDIA MAYOR DE BOGOTÁ. Ley 1273 de 2009 Nivel Nacional. [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

5. METODOLOGÍA DE INVESTIGACIÓN

5.1. ALCANCE O DELIMITACIÓN

Las herramientas de Ethical Hacking serán ejecutadas en la base de datos de Tao esquema servicios de la organización Alcaldía de Ibagué, mientras se entregue el documento final con el informe de las falencias de seguridad y los controles que se pueden aplicar para salvaguardar los datos.

- **Delimitación Población y muestra**

Población: Alcaldía de Ibagué
Muestra: Usuarios recurrentes Aplicativo TAO
Aplicativo Tao- Esquema de servicios de mantenimiento y archivo histórico

- **Técnicas De Análisis Y Procesamiento De Datos**

- Entrevistas
- Descripciones de procesos
- Gráficas
- Tabulación
- Prueba y Error

- **Metodología del Desarrollo**

La metodología de desarrollo va a contar con los siguientes pasos:

1. Identificar junto con los usuarios responsables de la formulación de las políticas de seguridad de la información los requerimientos, para la actualización de las mismas.

2. Identificar los principales ataques a la base de datos, causas, consecuencias, activos impactados.

3. Identificar y documentar los requerimientos de hardware y software para la implementación de herramientas y técnicas de *Ethical Hacking* al esquema servicios base de datos TAO.

4. Proponer diversas plataformas o herramientas para la detección de vulnerabilidades a la base de datos y solucionar problemas de *hackeo* y robo de datos.

5. Realizar una implementación de herramientas y técnicas de *Ethical Hacking* con software descargado de la web que nos permita lo siguiente:

    - Identificar inyección de código malicioso en la base de datos esquema servicios.
    - Realizar intrusión autorizada para identificar puertas abiertas y vulnerabilidades de la base de datos.
    - Documentación sobre las vulnerabilidades encontradas con las herramientas *Ethical hacking* utilizadas.
    - Realizar pruebas de ataque con distintas herramientas para identificar y clasificar con cada una de ellas opciones seguras para proteger el código.
    - Tomar decisiones en cuanto a actualización de software instalado en servidores y reglas de seguridad sobre firewall que afecten la seguridad de la base de datos en el esquema estudiado.

Corresponde a investigación aplicada o tecnológica, el cual tiene por objeto comparar la teoría, con los hechos de la realidad: a problemas, circunstancias y características concretas, con resultados generalmente inmediatos. Ésta se fundamenta en los resultados de una investigación básica

Según el nivel de medición y análisis de la información: se realizará una **investigación descriptiva y confirmatoria.** De una parte se describirán los aspectos más importantes del objeto del estudio, para el caso concreto ataques informáticos al esquema de servicios de la base de datos TAO de la Alcaldía de Ibagué utilizando *Ethical Hacking*, con el objetivo de identificar las diferentes casusas, y otros sucesos como horas, fechas, objetivo del ataque, tipos de ataque y las posibles consecuencias que impactan el activo de información en mención de la entidad de esta manera se contextualizara la problemática sucedida y se podrá sugerir alternativas de solución. De otra parte la

investigación también nos puede confirmar hechos que intenta explicar el por qué se están generando el problema que se estudia.

Mediante el método no experimental, utilizando encuestas exploratorias ver anexo (B, C y D) con el objeto de obtener más información sobre cómo prevenir ataques informáticos y la implementación de técnicas *ETHICAL HACKING*, el tipo de encuesta a aplicar será Longitudinales. (Secciones transversales sucesivas): este diseño se utiliza para el estudio de cambios o de evolución en los fenómenos de interés. Se entrevista dos o más veces a las mismas muestras de sujetos.

En la metodología y/o herramientas para el desarrollo del *Ethical hacking* se utilizará la técnica de levantamiento de información (entrevista) que será aplicada al jefe de área, a los administradores de la base datos y al usuario final para lograr obtener información que servirá para la investigación de vulnerabilidades de la base de datos Tao esquema servicios.

Dentro de las metodologías más aplicadas para realizar E*thical hacking* se encuentran la *OSSTMM y OWASP*, que encuentran inmersas pruebas de mapeo que pueden ser útiles para determinar vulnerabilidades en este caso al servidor que aloja la base de datos del esquema de servicios TAO. La primera metodología *OSSTMM,* presenta procedimientos de testeo de seguridad y es muy usado en auditorias de seguridad y dentro de sus fases se encuentran: Seguridad de la información, Seguridad de los procesos, Seguridad en las tecnologías de internet, Seguridad en las comunicaciones, Seguridad inalámbrica y Seguridad física.[30]

Por otra parte, OWASP presenta una guía de formas diferentes de encontrar fallos de seguridad en los sistemas y como realizar la comprobación rápida, exacta y eficiente. Está orientada principalmente para tres roles, para desarrolladores con el fin de asegurarse de que están produciendo código seguro, para las personas que realizan pruebas de software para que detecten vulnerabilidades tempranas, reduciendo costos, tiempo y esfuerzo y por ultimo para los especialistas en seguridad para examinar junto con otras técnicas que no queden agujeros de seguridad en las aplicaciones.[31]

[30] DRAGONJAR. OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad [En línea]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

[31] OWASP.ORG. Guía de Pruebas OWASP. [En línea]. 2008, Disponible en: https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

Dentro de los procedimientos que se pueden aplicar son pruebas de *SQL inyection (owasp)*, autenticación, seguridad física, seguridad inalámbrica, seguridad de procesos (*Osstmm).*

Se debe tener en cuenta que de un análisis hecho de acuerdo a las puertas que se encuentran abiertas se deben tomar los correctivos necesarios, por eso debe ser constante la auditoria en todos los procesos que tengan que ver con autenticación actualizaciones, verificación de código, etc. para tener control y cerrar brechas al delincuente. Sin embargo, él tratará por cualquier medio volver a vulnerar la seguridad y más si está obteniendo un beneficio económico, para este caso este beneficio no aplica, pero hace parte de un esquema de una base de datos que, si tiene en su parte tributaria implicaciones, pero no van a ser manera de estudio por su reserva. Dentro del esquema servicios se deben tener en cuenta la revisión de los usuarios de las bases de datos esto con el fin de detener un ataque por medio de un usuario que por ejemplo no pertenezca a la entidad Alcaldía de Ibagué.

Las pruebas *pentesting* a la base de datos constituyen una alternativa importante dentro del proceso de auditoría del esquema de Servicios de la misma. Este proceso va a contar pruebas de caja Gris, donde el auditor o las personas encargadas de realizar las auditorias cuenten con una información parcial del estado de la base de datos y porque el esquema Servicios es una parte dentro de la base de Datos TAO que lo constituyen mas esquemas.

Dentro de las posibilidades que brinda la caja gris al dar parcialmente información al auditor de la base de datos, están que este va a contar con el acceso al servidor, cuyo ingreso es permitido y controlado por el administrador de la Base de datos; y que posteriormente ejecutar herramientas de Ethical hacking para encontrar vulnerabilidades en el servidor.

Se considera que realizar hacking ético debe ser una actividad constante dentro de un esquema de base de datos ya que nos evidencia las vulnerabilidades a las que puede estar expuesta la base de datos y con esto prevenir ataques. Es por ello que se debe trabajar conjuntamente el personal designado para esta labor explotando vulnerabilidades, determinando y analizando los resultados de estas acciones contando con la asesoría y el apoyo del administrador y programadores.

En la identificación y documentación del diagnóstico se debe realizar las pruebas del estado de la base de datos con un equipo de cómputo con las siguientes características:

Tabla 1. Características mínimas de equipo

EQUIPO	CARACTERISTICAS
Equipo de escritorio	Procesador Intel Core i5 Memoria RAM 4 GB Disco Duro 500GB Sistema operativo Windows 7 a 64 bits
Servidor de la base de datos objeto de estudio	Windows server 2003 Dell power edge 1950 Disco Duro 250 GB Memoria RAM 8 GB

Fuente Los autores

Para el proceso de aplicación de herramientas de Ethical hacking se determinó contar con el personal que en la tabla 2 se referencia y se establece que las pruebas las realizaran los dos profesionales en ingeniería de sistemas contando con la asesoría del administrador y el programador asignado.

Tabla 2. Requerimiento personal

PERSONAL	CARACTERISTICAS TECNICAS
Un (1) Funcionario administrador de la Base de Datos	Define la seguridad de la base de datos y gestionan las copias de seguridad y la gestión física de la base de datos.
Un (1) Programador de la base de datos	Encargado de la realización de las aplicaciones de usuario de la base de datos
Dos (2) ingenieros que realizan las pruebas de pentesting y análisis de las vulnerabilidades.	Profesionales en ingeniería de sistemas

Fuente los Autores

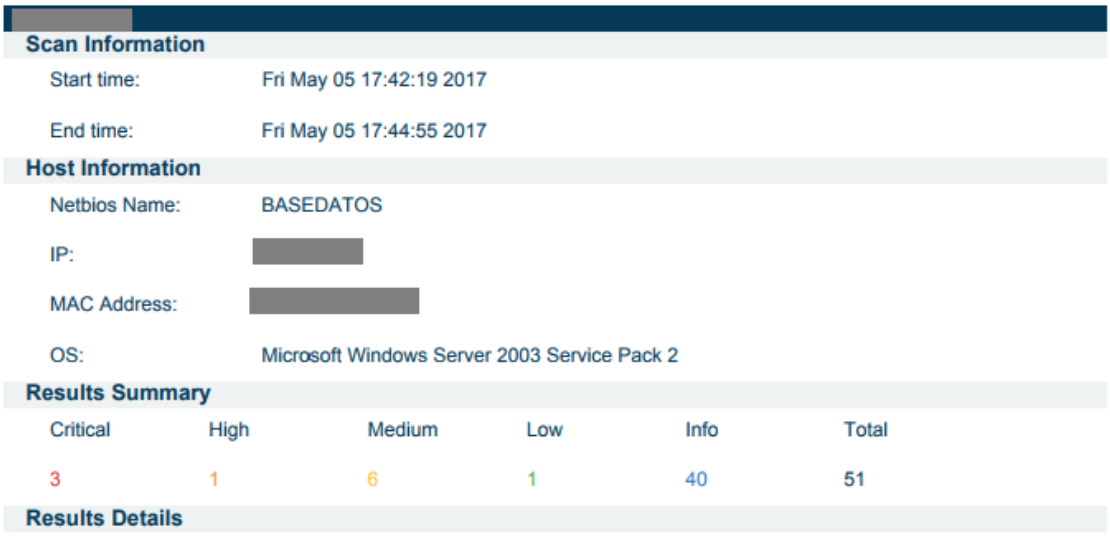
Al realizar la revisión del estado de los log de auditoria de la Base de Datos, se logró determinar que, sí existe una auditoría realizada mediante procedimientos y *triggers*, pero no se está ejecutando la auditoria propia del Gestor de la base de datos Oracle por cuestiones de rendimiento y espacio del servidor.

Para determinar el estado del servidor y de la base de datos se usan las herramientas *Nessus*, comando *NETSTAT y Nmap*.

Con esta herramienta se comprueba la seguridad del servidor y con el escaneo se detectan ciertas vulnerabilidades que al ser solucionadas permiten tener un mejor control de la administración de la base de datos y cierra por decirlo en gran medida puertas al atacante.

En la figura 1. Vemos la ejecución de la herramienta *Nessus* y describe entre otros datos, la fecha en que fue ejecutado, IP ejecutada, sistema operativo y valoración de los resultados

Figura 1. Ejecución de la herramienta *NESSUS* 1

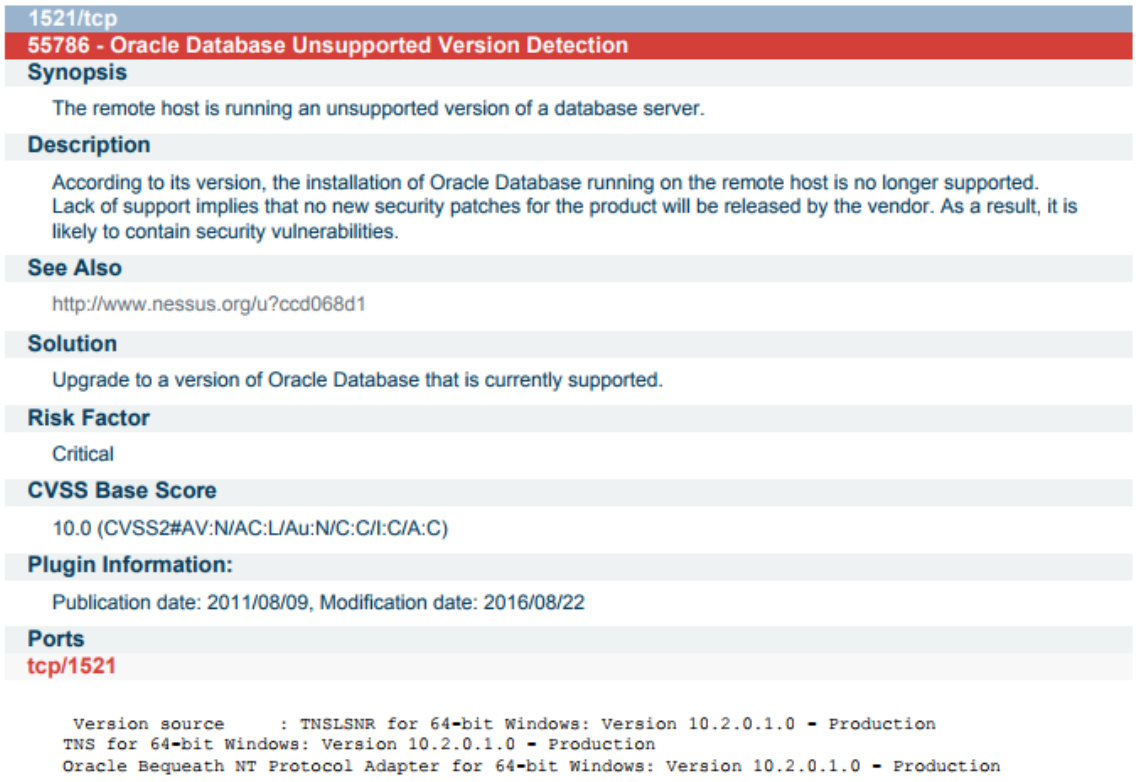


Fuente: Autores

Nota: No se muestran los datos de la dirección Ip ni la dirección MAC del servidor por protección de la confidencialidad de la información.

En la figura 2. Vemos la ejecución de la herramienta *Nessus* y donde se puede ver que está en estado crítico o (en rojo) el puerto 1521, que es el puerto de escucha del Oracle.

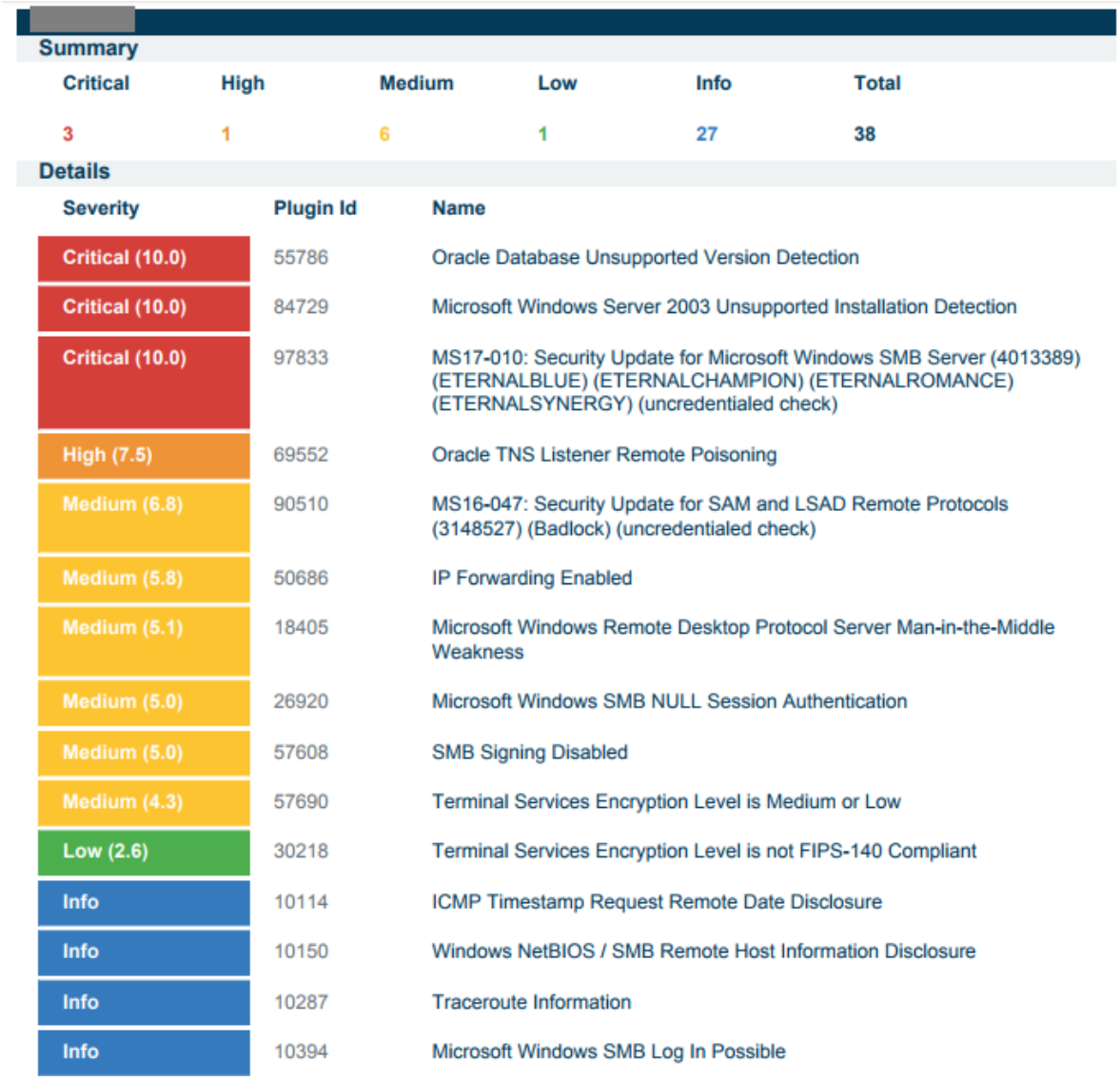
Figura 2. Ejecución de la herramienta NESSUS 2



Fuente: Autores.

En la figura 3, se puede ver el informe de ejecución de la herramienta NESSUS, donde se puede observar en colores el nivel de criticidad de las vulnerabilidades encontrada por la herramienta. Lo que se encuentra en rojo es crítico, en amarillo es alto, en naranja es medio, en verde es bajo y en azul es información del sistema.

Figura 3. Informe de la Ejecución de la herramienta NESSUS



Summary

Critical	High	Medium	Low	Info	Total
3	1	6	1	27	38

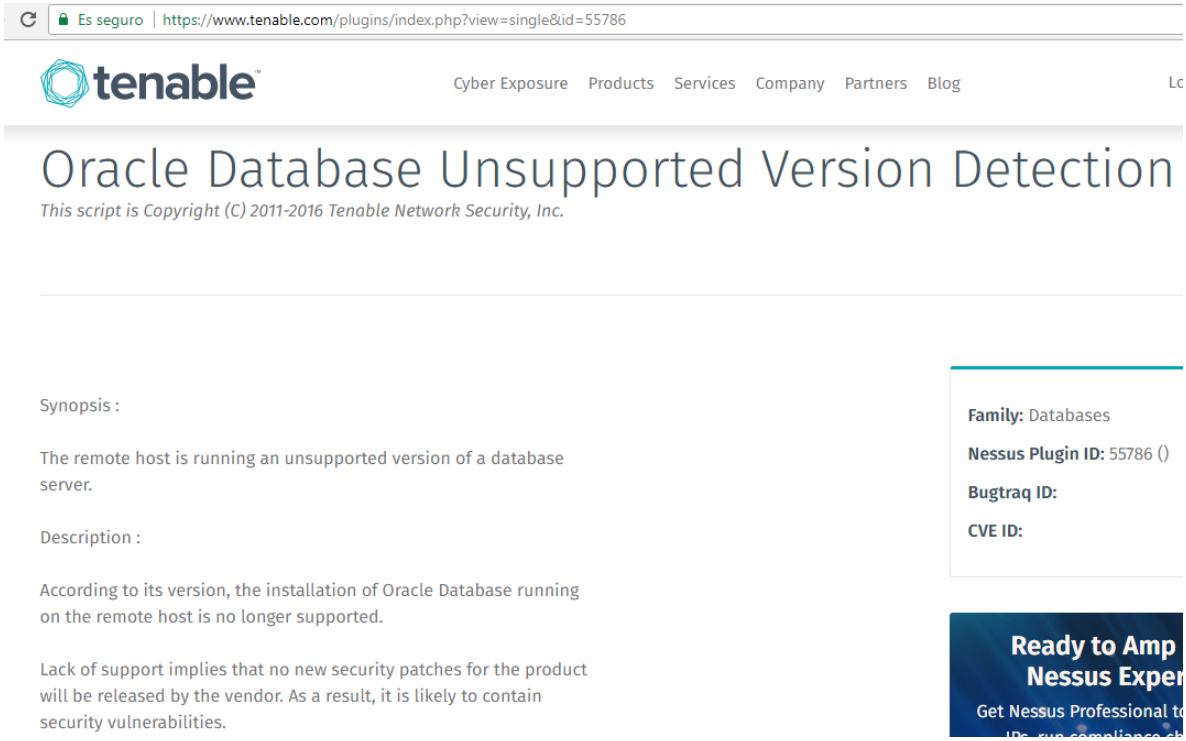
Details

Severity	Plugin Id	Name
Critical (10.0)	55786	Oracle Database Unsupported Version Detection
Critical (10.0)	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)
High (7.5)	69552	Oracle TNS Listener Remote Poisoning
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.8)	50686	IP Forwarding Enabled
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible

Fuente: Autores

En el anterior reporte se dio clic en el campo Plugin id 55786 ya que se encuentra en estado crítico. Este enlace nos lleva a la información que se puede observar en la figura 4, donde nos muestran la vulnerabilidad, descripción y la posible solución.

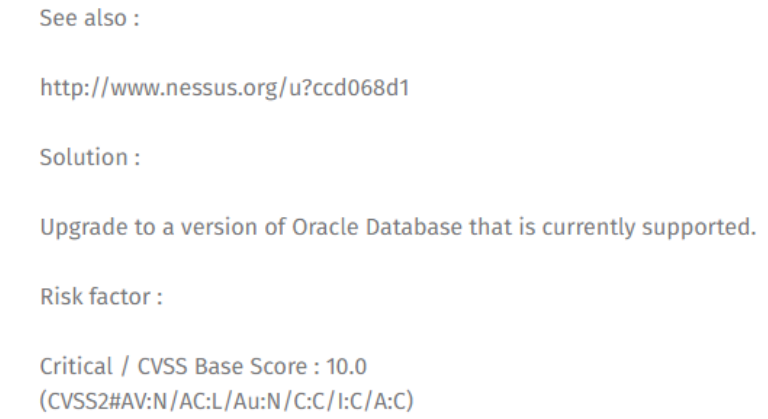
Figura 4. Estado de la vulnerabilidad



Fuente: Autores

En la figura 5 podemos observar la posible solución a la vulnerabilidad encontrada con anterioridad.

Figura 5. Estado de la vulnerabilidad y posible solución



Fuente: Autores

Como se puede observar en la figura 4, el nombre de la vulnerabilidad es "Detección de la versión no compatible de la base de Oracle*", dicha herramienta nos despliega la siguiente información:*
Sinopsis:

el host remoto ejecuta una versión no compatible de un servidor de base de datos.

Descripción:

según su versión, la instalación de *Oracle Database* que se ejecuta en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

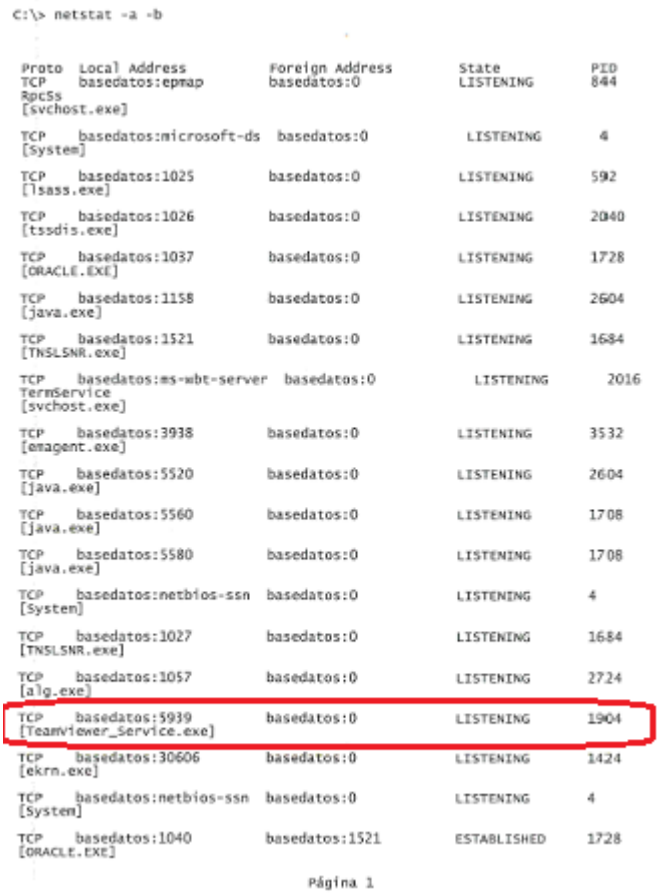
Actualice a una versión de la base de datos Oracle que actualmente es compatible.

Como parte del ejercicio para determinar puertas abiertas se logró establecer autorización para realizar actividades dentro del servidor que aloja el esquema de servicios de la base de datos Tao, para luego determinar las acciones correctivas de acuerdo a lo que se encontró.

Se realiza un análisis sobre los puertos abiertos en el servidor donde se encuentra el aplicativo de servicios y se encuentra que *teamviewer* no solo se encuentra activo, sino una conexión establecida, por lo tanto, alguien se encuentra en acceso remoto a tal servidor.

Lo anterior se logra con el comando NETSTAT, como se puede observar en la figura 6. Cuando t*eamviewer* se encuentra instalado, pero nadie se encuentra conectado, se muestra en estado LISTENING.
En cambio, cuando se está ejecutando se muestra ESTABLISHED
TCP basedatos:3257 server5015.teamviewer.com:5939 ESTABLISHED

Figura 6. Informe ejecución comando NETSTAT



```
C:\> netstat -a -b

  Proto  Local Address          Foreign Address        State           PID
  TCP    basedatos:epmap        basedatos:0            LISTENING       844
  RpcSs
  [svchost.exe]
  TCP    basedatos:microsoft-ds  basedatos:0           LISTENING       4
  [System]
  TCP    basedatos:1025         basedatos:0            LISTENING       592
  [lsass.exe]
  TCP    basedatos:1026         basedatos:0            LISTENING       2040
  [tssdis.exe]
  TCP    basedatos:1037         basedatos:0            LISTENING       1728
  [ORACLE.EXE]
  TCP    basedatos:1158         basedatos:0            LISTENING       2604
  [java.exe]
  TCP    basedatos:1521         basedatos:0            LISTENING       1684
  [TNSLSNR.exe]
  TCP    basedatos:ms-wbt-server  basedatos:0          LISTENING       2016
  TermService
  [svchost.exe]
  TCP    basedatos:3938         basedatos:0            LISTENING       3532
  [emagent.exe]
  TCP    basedatos:5520         basedatos:0            LISTENING       2604
  [java.exe]
  TCP    basedatos:5560         basedatos:0            LISTENING       1708
  [java.exe]
  TCP    basedatos:5580         basedatos:0            LISTENING       1708
  [java.exe]
  TCP    basedatos:netbios-ssn  basedatos:0            LISTENING       4
  [System]
  TCP    basedatos:1027         basedatos:0            LISTENING       1684
  [TNSLSNR.exe]
  TCP    basedatos:1057         basedatos:0            LISTENING       2724
  [alg.exe]
  TCP    basedatos:5939         basedatos:0            LISTENING       1904
  [TeamViewer_Service.exe]
  TCP    basedatos:30606        basedatos:0            LISTENING       1424
  [ekrn.exe]
  TCP    basedatos:netbios-ssn  basedatos:0            LISTENING       4
  [System]
  TCP    basedatos:1040         basedatos:1521         ESTABLISHED     1728
  [ORACLE.EXE]

                                  Página 1
```

Fuente: Autores

Es importante considerar que tener activo el servicio de teamviewer dentro de un servidor es muy perjudicial, ya que este se convierte en una puerta abierta para el atacante, aunque parezca una herramienta que acorte desplazamiento de una maquina a otra, también se convierte en una amenaza latente a la seguridad de la base de datos.

Dentro de las actividades se procede entonces a eliminar la aplicación Teamviewer y a cerrar el puerto 50105.teamviewer, ejecutando línea de comando netstat –a-b-o, y se verifica que el puerto se encuentre cerrado.

En la imagen anterior el resultado del comando Netstat-a-b, se puede visualizar los puertos abiertos.

Netstat-a-b-o
La opción –a, muestra todas las conexiones activas upd y tcp
La opción –b, muestra el nombre del ejecutable que esta usuando el puerto
La opción –o, muestra el process ID

Para encontrar la ruta del ejecutable, podemos usar:
Wmic process where “name=java.exe” get processID, ExecutablePatth

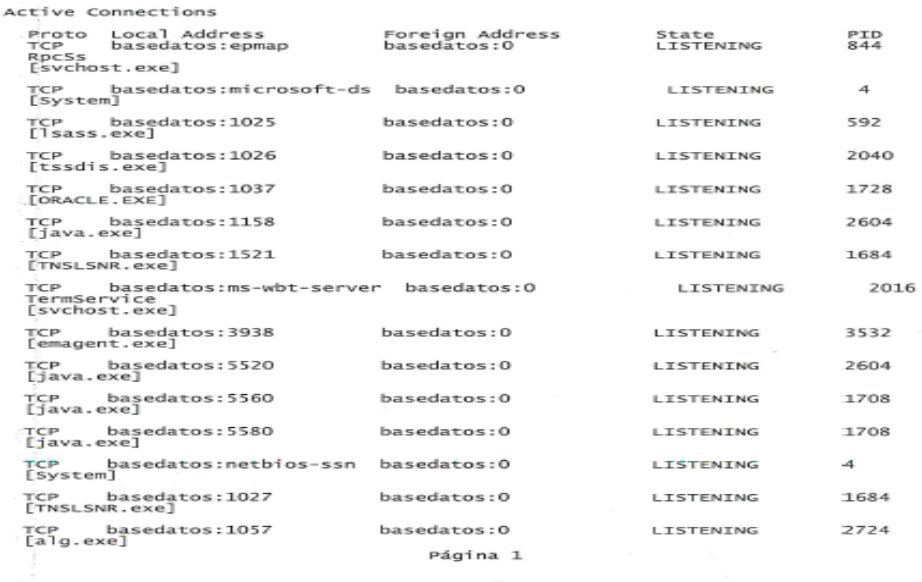
En el caso de los puertos abiertos encontramos que en la maquina local es el que se encuentra en la columna “local Address”, después de basedatos.por ejemplo en la primera línea que vemos listada se encuentra basedatos:epmap, eso quiere decir que el puerto 135 está abierto, dado que epmap corresponde al puerto 135 (cuando el puerto tiene asociado un protocolo conocido, en algunos casos se imprime el nombre del protocolo en vez del puerto, por ejemplo en el caso del puerto 80, puede verse impreso http en vez de 80).

Para cerrar un puerto en Windows 2003 con RRAS, podemos usar
http://www.adminsehow.com/2010/04/block-port-25-in-routing-and-remote-access-ras-to-prevent-spam/ (procedimiento para hacerlo)

Si se tiene un servidor VPN ejecutándose en *Windows* utilizando el enrutamiento y el acceso remoto, algunos de los usuarios pueden abusar de su servicio VPN al enviar correos electrónicos no deseados desde su IP. para evitarlo, debe bloquear el puerto saliente 25 (SMTP).

En las siguientes figuras 7 y 8 se puede observar que no aparece el servicio del *Teamviewer.*

Figura 7. Informe ejecución comando NETSTAT después de cerrar el puerto 1

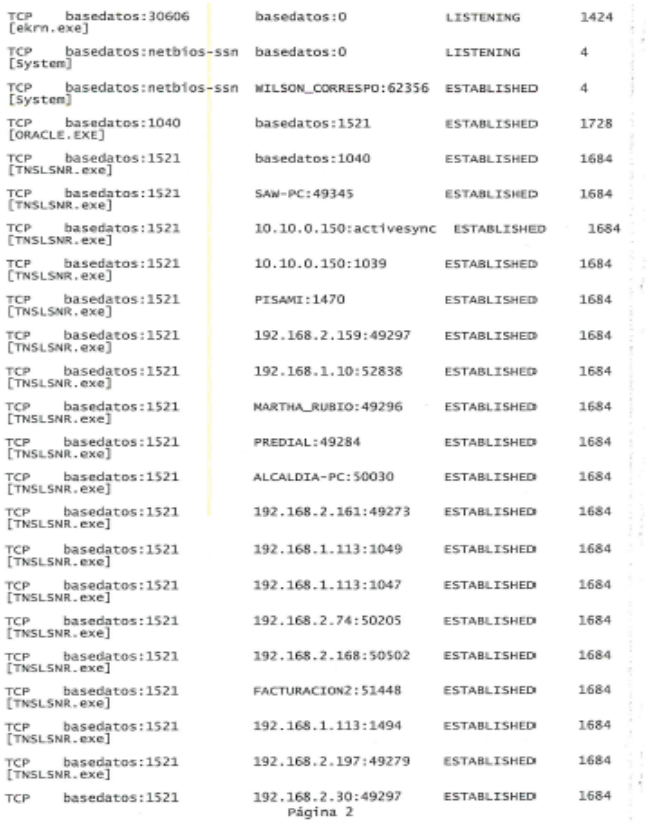


```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    basedatos:epmap        basedatos:0            LISTENING       844
  RpcSs
  [svchost.exe]
  TCP    basedatos:microsoft-ds  basedatos:0           LISTENING       4
  [System]
  TCP    basedatos:1025         basedatos:0            LISTENING       592
  [lsass.exe]
  TCP    basedatos:1026         basedatos:0            LISTENING       2040
  [tssdis.exe]
  TCP    basedatos:1037         basedatos:0            LISTENING       1728
  [ORACLE.EXE]
  TCP    basedatos:1158         basedatos:0            LISTENING       2604
  [java.exe]
  TCP    basedatos:1521         basedatos:0            LISTENING       1684
  [TNSLSNR.exe]
  TCP    basedatos:ms-wbt-server  basedatos:0          LISTENING       2016
  TermService
  [svchost.exe]
  TCP    basedatos:3938         basedatos:0            LISTENING       3532
  [emagent.exe]
  TCP    basedatos:5520         basedatos:0            LISTENING       2604
  [java.exe]
  TCP    basedatos:5560         basedatos:0            LISTENING       1708
  [java.exe]
  TCP    basedatos:5580         basedatos:0            LISTENING       1708
  [java.exe]
  TCP    basedatos:netbios-ssn  basedatos:0            LISTENING       4
  [System]
  TCP    basedatos:1027         basedatos:0            LISTENING       1684
  [TNSLSNR.exe]
  TCP    basedatos:1057         basedatos:0            LISTENING       2724
  [alg.exe]
                                    Página 1
```

Fuente autores

Figura 8. Informe ejecución comando NETSTAT después de cerrar el puerto 2



```
  TCP    basedatos:30606        basedatos:0            LISTENING       1424
  [ekrn.exe]
  TCP    basedatos:netbios-ssn  basedatos:0            LISTENING       4
  [System]
  TCP    basedatos:netbios-ssn  WILSON_CORRESPO:62356  ESTABLISHED     4
  [System]
  TCP    basedatos:1040         basedatos:1521         ESTABLISHED     1728
  [ORACLE.EXE]
  TCP    basedatos:1521         basedatos:1040         ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         SAW-PC:49345           ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         10.10.0.150:activesync ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         10.10.0.150:1039       ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         PISAMI:1470            ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.159:49297    ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.1.10:52838     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         MARTHA_RUBIO:49296     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         PREDIAL:49284          ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         ALCALDIA-PC:50030      ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.161:49273    ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.1.113:1049     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.1.113:1047     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.74:50205     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.168:50502    ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         FACTURACION2:51448     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.1.113:1494     ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.197:49279    ESTABLISHED     1684
  [TNSLSNR.exe]
  TCP    basedatos:1521         192.168.2.30:49297     ESTABLISHED     1684
                                    Página 2
```

Fuente: autores

Existen dos tipos de reglas, inbound y outbound. Inbound se refiere a una regla que bloquea el tráfico hacia afuera de nuestra máquina.
Outbound se refiere a una regla que no deja salir tráfico de nuestra máquina.

Cada una de estas reglas puede tener un puerto fuente y otro de destino. Por ejemplo, si creamos una regla inbound con el puerto de destino 80, y el puerto fuente 45, significa que nuestro firewall no va a dejar entrar trafico si una maquina lo intente enviar a nuestro puerto 80, desde su puerto 45.
Lo anterior seguirá permitiendo que nos manden tráfico a nuestro puerto 80, siempre y cuando el que lo envía no lo haga desde el puerto 45, entonces para generalizar a que se bloquee así provenga desde cualquier puerto siempre y cuando lo intente mandar a nuestro puerto 80, en el puerto fuente asignamos el valor de 0.

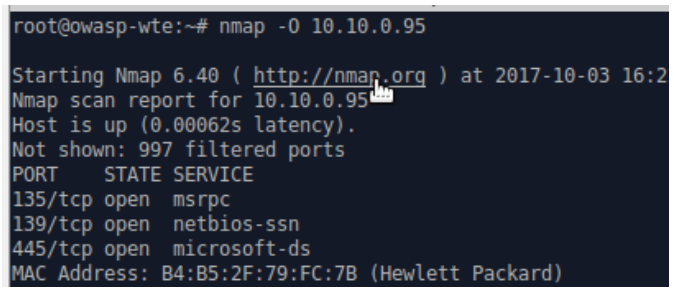
Ahora, supongamos que ahora queremos que desde nuestra maquina no se pueda usar http. Para eso creamos una regla outbound, con el puerto fuente igual a 0 (para que no importe desde que puerto tratemos de salir nos bloquee) y con el puerto de destino 80.

Antes de realizar las acciones de cerrar los puertos se debe verificar en el servidor de pruebas para verificar que ocurre.

Para realizar el proceso de ingreso al servidor donde se encuentra alojada la base de datos y su esquema de estudio “Servicios”, se proyectó inicialmente usar una base datos de pruebas llamada TAO en un motor de bases de datos Oracle. Por problemas técnicos en el servidor y de dicha base se optó por instalar el Oracle Express 10 G.

Se optó por montar el gestor de base de datos Oracle Express 10 G, en el cual se importó el esquema servicios que se encontraba en un backup reciente.
Se creó el usuario SERVICIOS el cual sería el propietario del esquema.
Se crearon los Tablespace correspondientes.
Se importó el archivo servicios.DMP.
Se ejecuta la herramienta NMAP como se observa en la figura 9, en un sistema operativo Ubuntu. Esta una herramienta se basa en hacer pruebas de escaneo donde nos muestra el estado de puertos y servicios en un Equipo.
En nuestra primera prueba ejecutamos el comando nmap –O 10.10.0.95

Figura 9. Pantallazo ejecución nmap con el comando O



Fuente: Autores

El servidor es un pc personal, esta consulta nos da una salida así:

1. Latencia del Equipo
2. Puertos, estado del puerto y el servicio.
3. Dirección MAC
4. Sistema Operativo y su versión.

En la figura 10 podemos visualizar un nmap hecho específicamente al puerto 1521 (Oracle Listener). Como se puede visualizar el puerto está en estado Filtered (Filtrado) que puede suceder ya que el equipo tiene instalado un firewall.

Figura 10. Pantallazo ejecución nmap con el comando –p

Fuente: Autores

El estado de la base de datos de tao y su esquema de servicios, actualmente se encuentra de la siguiente manera:

- No se encuentra documentado los objetos de la base de datos ni sus relaciones de manera actualizada.

- Puertos que se encontraron abiertos que ponían en riesgo la seguridad de la base de datos.
- No se encuentra habilitada la auditoria propia del gestor de la base de datos por cuestiones físicas del servidor que aloja.
- La versión del gestor de base de datos no tiene soporte, esta desactualizada.
- Las copias de seguridad del esquema de la base de datos se realizan diariamente por medio de una programación hecha por el administrador de la base de datos en los horarios más acordes para no interrumpir el desempeño de la misma

En el estudio y justificación del uso de herramientas de seguridad, se propone hacer el filtrado MAC de los equipos de cómputo que acceden al servidor y base de datos que aloja al esquema servicios. realizar pruebas de penetración para identificar puertos abiertos, pruebas de inyección de código sql, todo ello para obtener información de la forma como se puede alterar en un momento determinado la información y datos que reposan en la base de datos del esquema de servicios que tiene la información de los requerimientos que se hacen a diario las actividades de mantenimiento correctivo y preventivo de equipos de cómputo (impresoras, Desktop, laptop, scanner) y que sirven para llevar un recorrido a una hoja de vida del equipo y todas sus intervenciones de tipo técnico.

Los cronogramas de las pruebas de testeo se realizaron de acuerdo a las fechas establecidas en el cronograma de actividades utilizando las herramientas Nessus, Nmap y el comando *Netstat.*

Se documentan las posibles fallas y controles a implementar de acuerdo a las vulnerabilidades encontradas. Se recomiendan lo siguiente:

- Revisión periódica y depuración de los puertos abiertos, sus servicios.
- Realizar la adquisición y configuraciones del firewall de la base de datos
- Actualización de la versión del sistema de gestor de la base de datos Oracle.
- Documentar toda la información correspondiente a los objetos y sus relaciones dentro de la base datos.
- Activación de la auditoria propia del sistema gestor de la base de datos.
- Tener plan de continuidad del negocio en caso de que la base de datos sufra un daño ya sea por daño físico del servidor, software o por algún evento que afecte el servicio.

6. RESULTADOS ESPERADOS

Actualización de software en servidores y dispositivos que interactúan con la base de datos en estudio. De acuerdo a las vulnerabilidades detectadas con ethical hacking a la base de datos, recomendar a la dirección herramientas de hardware y/o software para prevenir futuros ataques. Implementación de firewall para bases de datos.

Para la consolidación de resultados esperados de acuerdo a la metodología aplicada se identificaron los activos presentes en la entidad que administra la base de datos y el esquema materia de estudio (servicios).

IDENTIFICACIÓN DE ACTIVOS

Los activos de información se identificaron según la clasificación de la metodología Magerit de la tabla No.1 (Jesús, 2012)9

Tabla.3 Clasificación de los activos Informáticos

Los Activos de Magerit se clasifican
1.-[s] Servicios
2.-[D] Datos/Información
3.-[SW] Aplicaciones (Software)
4.-[HW] Equipos Informáticos (Hardware)
5.-[COM] Redes de comunicaciones
6.-[SI] Soportes de información
7.- [AUX] Equipamiento auxiliar
8.-[L] Instalaciones
9.-[P] Personal

Cuadro 1. Clasificación de los activos informáticos de la Alcaldía Municipal de Ibagué.

[S] SERVICIOS	• [email] Correo electrónico
	• [www]Portal web
	• [www] Intranet
[SW] APLICACIONES	• [Sistema Operativo] (Linux Centos 6 y 7, Windows Server2003, Windows XP, Siete, Ocho
	• [Gestor Base Datos] Oracle 10G, Mysql
	• [Software]Software antivirus Karpesky
	• [OFFICE] en sus diferentes versiones estándar (2003, 2007, 2010, 2013 y 2016]
[SW]APLICACIONES	• [www]Aplicaciones web ERP PISAMI (Hoja Vida, Nomina, Pqr, Correspondencia, Industria y Comercio, Otros Impuestos, Cobro Coactivo, Tesorería, Presupuesto, Contabilidad y Contratación)
	• [www] Portal Servicios
	• [exe] SOFTCON (Control procesos Judiciales
	• [exe] GCI (Manejo de Inventarios)
	• [exe] Tao (Impuesto Predial)
[HW] EQUIPOS INFORMÁTICOS	• [app]Servidores web
	• [dbms]Servidor de base de datos y Aplicacion
	• [app]Equipos virtuales
	• [mid]Medios de Impresión
	• [mid]Computadores de escritorio
	• [firewall]Firewalls
	• [mid]router
[COM]REDES DE COMUNICACIONES	• [lan]Red LAN
	• [vpn]Red privada virtual
	• [internet]Internet
[SI]SOPORTES DE INFORMACIÓN	• [app]Sistema de gestión de proyectos, servidores de prueba, de producción y de Backup, donde se encuentra alojado el código fuente, las pruebas, y copias de respaldo.
[AUX] EQUIPAMIENTO AUXILIAR	• [UPS]Sistema de alimentación ininterrumpida
	• [cabling]Cableado de datos • [furniture] Mobiliario Rack • [AC] Aire Acondicionado
[P] Personal	[ui] Usuarios Internos [ue] Usuarios Externos [Adm] Administradores de sistemas

	[Dba] Administradores de Bases de Datos
[D] Datos	[VR] Datos Vitales Base de Datos Subsistema Financiero, Gestión Documental, Subsistema Tributario, Susbsistema Gerencial y Administrativo, de correos, portal web, Intranet [Source] Codigo Fuente [Test]Datos de Prueba [ADM] Datos Administración, Políticas de seguridad

VALORACIÓN CUALITATIVA DE LOS ACTIVOS.

MAGERITH, es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y las comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos. (Información, 2012)

Para la valoración de activos se ha determinado el análisis de las dimensiones indicadas en la siguiente tabla.

Cuadro 2. Dimensiones de Seguridad

DIMENSIÓN DE SEGURIDAD	NOMENCLATURA	DEFINICIÓN
DISPONIBILIDAD	**D**	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
INTEGRIDAD	**I**	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
CONFIDENCIALIDAD	**C**	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

AUTENTICIDAD	**A**	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
TRAZABILIDAD	**T**	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Fuente: El Autor

Cuadro 3. Niveles de valoración de activos informáticos

Nivel	Descripción
MA	Muy Alto
A	Alto
M	Medio
B	Bajo
MB	Muy Bajo

Fuente: El autor

Cuadro 4. Identificación de Activos y Dimensiones de Seguridad

ACTIVOS	DIMENSIONES				
	D	**I**	**C**	**A**	**T**
[HW] EQUIPOS INFORMÁTICOS					
[app] Servidores web	MA	MA	MA	MA	MA
[dbms]Servidor de base de datos y Aplicación	MA	MA	MA	MA	MA
[app] Equipos virtuales	MA	MA	MA	MA	MA
[mid] Medios de Impresión	A	A	A	A	A
[mid]Computadores de escritorio	A	A	A	A	A
[firewall]Firewalls	A			M	M
[mid]router	M			M	M
[D] Datos	**D**	**I**	**C**	**A**	**T**
[VR] Datos Vitales Base de Datos Subsistema Financiero, Gestión Documental, Subsistema Tributario, Subsistema Gerencial y Administrativo,		A	A		

de correos, portal web, Intranet					
[Source] Codigo Fuente	A	A	A	A	A
[Test]Datos de Prueba		A	A	A	A
[ADM] Datos Administración, Políticas de seguridad	A	A	A	A	A
[COM]REDES DE COMUNICACIONES	**D**	**I**	**C**	**A**	**T**
[lan]Red LAN	M			M	M
[vpn]Red privada virtual	M			M	M
[internet]Internet	M			M	M
[SW]APLICACIONES	**D**	**I**	**C**	**A**	**T**
[Sistema Operativo] (Linux Centos 6 y 7, [Sistema Operativo] (Linux Centos 6 y 7, Windows Server2003, Windows XP, Siete, Ocho.M		A	A	A	A
					M
[Software]Software antivirus Karpesky					M
[OFFICE] en sus diferentes versiones estándar (2003, 2007, 2010, 2013 y 2016]					M
[www]Aplicaciones web ERP PISAMI		A	A	A	A
[[www] Portal Servicios					M
[exe] SOFTCON (Control procesos Judiciales					M
[exe] GCI (Manejo de Inventarios)					M
[exe] Tao (Impuesto Predial)		A	A	A	A
[P] Personal	**D**	**I**	**C**	**A**	**T**
[ui] Usuarios Internos			M		
[ue] Usuarios Externos			M		

[Adm] Administradores de sistemas			M		
[Dba] Administradores de Bases de Datos			M		
[S] SERVICIOS	D	I	C	A	T
[email] Correo electrónico		A	A	A	A
[www]Portal web		A	A	A	A
[www] Intranet		A	A	A	A
[S] SOPORTE DE INFOMRACIÓN	D	I	C	A	T
[disk] discos	A	A	A	A	A
[S] EQUIPAMENTO AUXILIAR	D	I	C	A	T
[ups] Sistema de alimentación interrumpida	M			M	MA
[ac] Equipos de climatización	A				A

Fuente: El autor.

Cuadro 5. Criterios de Valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

De acuerdo a MAGERIT V3 libro 2 Catalogo de elementos (3.0, 2012)

Cuadro 6. Criterios de valoración 2.

Datos vitales [pub]				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
Datos vitales [pub]	Subsistema Financiero	Información correspondiente a saldos de presupuesto vigencias anteriores y año actual, disponiblidades, registros traslado presupuestales, Terceros, cuentas por pagar, asientos contables, libros auxiliares, libro de balance, libros mayores, cuentas bancarias, saldos, movimientos bancarios, Acuerdos de Pago, Proceso Cobro Coactivo, Proceso en control Fiscal	Confiabilidad	9
			Integridad	9
			Autenticidad	9
			Disponibilidad	8
			Trazabilidad	9
	Subsistema Contratación	Contratos, Pólizas, Supervisores, Interventores informes de interventoría, liquidación contratos	Confiabilidad	9
			Integridad	9
			Autenticidad	9
			Disponibilidad	8
			Trazabilidad	9
	Subsistema Administrativo		Confiabilidad	9
			Integridad	9
			Autenticidad	9
			Disponibilidad	8
			Trazabilidad	9
	Subsistema Tributario	Predios, Negocios comerciales, contribuyentes, estados de pagos, actos administrativos exoneración, excepción,	Confiabilidad	9
			Integridad	9
			Autenticidad	9
			Disponibilidad	8
			Trazabilidad	9

SERVICIOS [S]				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[email] correo electrónico	XXXX@ibague.gov.co	Cuentas de correo producto google con dominio @ibague.gov.co a	Confiabilidad	7
			Integridad	7
			Autenticidad	7
			Disponibilidad	9
			Trazabilidad	6
[www] Portal web	www .ibague.gov.co	portal internet www.ibague.gov.co	Confiabilidad	8
			Integridad	8
			Autenticidad	8
			Disponibilidad	9
			Trazabilidad	8
[www] intranet	www .ibague.gov.co/intranet	Plataforma dispuesta a través del portal www. Ibague.gov.co	Confiabilidad	3
			Integridad	3
			Autenticidad	3
			Disponibilidad	3
			Trazabilidad	3

APLICACIONES [SW]				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[prp]	pisami.ibague.gov.co	[www] Aplicaciones WEB, ERP PISAMI (Hoja Vida, Nomina, Pqr, Correspondencia, Industria y Comercio, Otros Impuestos, Cobro Coactivo, Tesorería, Presupuesto, Contabilidad y Contratación), Tramites en Linea	Confiabilidad	3
			Integridad	8
			Autenticidad	3
			Disponibilidad	9
			Trazabilidad	7
[sub]	Aplicaciones	[exe] aplicaciones SOFTCON, TAO, GCI	Confiabilidad	3
			Integridad	8
			Autenticidad	3
			Disponibilidad	9

			Trazabilidad	8
[os]	Sistemas Operativos Basico	[SO] Sistemas Operativos (Linux Centos 6 y 7, Windows Server2003, Windows XP, Siete, Ocho	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	8
			Trazabilidad	8
[office]	ofimática	[Office], Programa Office en sus diferentes versiones estándar (2003, 2007, 2010, 2013 y 2016]	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2
[av] Antivirus Kapersky	Antivirus	Kapersky, antivirus libres	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	2
			Trazabilidad	2
[exe]	GESTOR BASE DATOS	SQL server, Oracle	Confiabilidad	9
			Integridad	9
			Autenticidad	9
			Disponibilidad	9
			Trazabilidad	9

Equipamiento informático [HW]				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[host]	Grandes equipos	Servidores web (linux)	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2
[host]	Grandes equipos	Servidor de base de datos (sql Tramties sectoriales portal www.ibague.gov.co) (ORACLE, ERP -	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9

		PISAMI Y TAO)	Trazabilidad	2
[peripheral] periféricos	[print] medios de impresión (6)	Medios de Impresión	Confiabilidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	2
			Trazabilidad	0
[vhost] equipo virtual	Equipos Virtuales	Virtual vox y Vitware	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2
[host]	Grandes equipos	Servidores de aplicación (TAO - Modulo Pedial) (ERP - PISAMI)	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2
[firewall]	cortafuegos	Firewalls	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	8
			Trazabilidad	2
[router]	encaminadores	Routers	Confiabilidad	2
			Integridad	2
			Autenticidad	2

			Disponibilidad	9
			Trazabilidad	2
[pc]	informática personal (3)	Computadores de escritorio	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	2
			Trazabilidad	2

REDES COMUNICACIONES [LAN] red local				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[COM]	[LAN]	Redes Cableado Estructurado	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2
	[Internet]	Internet	Confiabilidad	2
			Integridad	2
			Autenticidad	2
			Disponibilidad	9
			Trazabilidad	2

[Media] Soportes de información				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[Media]	[disk] discos	Sistema de gestión de proyectos donde se encuentra alojado el código fuente, backups, pruebas.	Confiabilidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	0
			Trazabilidad	0

[AUX] EQUIMAMENTO AUXILIAR

Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[ups]	sistemas de alimentación ininterrumpida	UPS Nicomar, APC (20, 10) KVA	Confiabilidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	8
			Trazabilidad	0
[ac]	equipos de climatización	Aire acondicionado	Confiabilidad	0
			Integridad	0
			Autenticidad	0
			Disponibilidad	8
			Trazabilidad	0

[P] Personal				
Nombre grupo de activo MAGERIT	Código Activo de acuerdo a la entidad	Nombre activo de acuerdo a la entidad	Dimensión de Seguridad	Criterio
[ui]	usuarios internos	Funcionarios de planta y contrato	Confiabilidad	1
			Integridad	1
			Autenticidad	1
			Disponibilidad	5
			Trazabilidad	1
[ue]	usuarios externos	Contribuyentes, entidades externas como bancos, proveedores, entidades de control	Confiabilidad	2
			Integridad	2
			Autenticidad	5
			Disponibilidad	2
			Trazabilidad	2
[adm]	administradores de sistemas	Administrador Sistemas	Confiabilidad	3
			Integridad	3
			Autenticidad	3
			Disponibilidad	6
			Trazabilidad	4
[dba]	administradores de BBDD	DBA Oracle, SQL	Confiabilidad	6
			Integridad	6
			Autenticidad	6
			Disponibilidad	6
			Trazabilidad	6

VALORACION DE LAS AMENAZAS

Se realiza la valoración de las amenazas de los activos de la organización y dentro de los cuales están incluidos los activos que tienen que ver con la base del estudio el esquema de servicios que está dentro de una base de datos que pertenece a una aplicación, que usa equipamento (equipos y servidores), que está dentro de una red que comparte datos y que está administrada y manejada por personal del área de sistemas y por los usuarios finales

Cuadro 7**.** Escala de rango de frecuencia de amenaza

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Cuadro 8. Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	Valor cuantitativo
Muy alto	100%

Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Cuadro 9. Impacto en los Activos de Información

Datos vitales [pub]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
DATOS	Datos vitales Bases de Datos(subsistema Financiero: Disponibilidades, registros, pagos, movimientos bancos, libros auxiliares y terceros) Subsistema Contratación (terceros, contratos, valores, pagos, pólizas) Subsistema Administrativo (empleados, pagos nomina, retenciones, novedades de vacaciones, licencias, encargos, licencias) Subsistema Tributario (Contribuyentes, predios, negocios, historial de pagos)	[E15]Manipulación de la información	10		20			
		[E19]Divulgación de la información	10			20		
		[A15] Modificación de la información	10		20			
		[E8]Difusión de Software dañino	5	5	5	5		
		[E20]Vulnerabilidades de los programas	10			20		
		[A7]Uso no previsto	10	20	20	20		
		[E21]Errores de mantenimiento/actualización de programas	5	20	20			
	Código fuente	[E15]Manipulación de la información	10		20			
		[E20]Vulnerabilidades de los programas	10			20		
		[A7]Uso no previsto	10	20	20	20		
		[E21]Errores de mantenimiento/actualización de programas	5	20	20			
	Datos de prueba	[E8]Difusión de Software dañino	5	5	5	5		

		[E20]Vulnerabilidades de los programas	10			20		
		[A7]Uso no previsto	10	20	20	20		
		[E21]Errores de mantenimiento/actualización de programas	5	20	20			
	Datos Administración-Políticas	[E15]Manipulación de la Información	5		5			
		[A7]Uso no previsto	5	20	20	20		

SERVICIOS [S]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
[S]SERVICIOS	[email] correo electrónico	[I8]Fallo de servicios de comunicaciones (internet)	5	50				
		[E2]Errores del administrador	10	5		20		20
		[E19]Divulgación de la información	70		50		50	50
		[A5]Suplantación de identidad del usuario	5		10		10	10
	[www] Portal web	[A11]Acceso no autorizado	10		100		100	
		[I6]Corte del suministro eléctrico	70	70				
		[I8]Fallo de servicios de internet	5	50				
		[E4]Errores de configuración	50		20	20		20
		[A.4] Manipulación de la configuración	10	20	20	20		
		[E2]Errores del administrador	10	10		20		20
	[www] Intranet	[A11]Acceso no autorizado	5		10		10	10
		[I6]Corte del suministro eléctrico	70	70				
		[I8]Fallo de servicios de comunicaciones (internet)	50	50				
		[E4]Errores de configuración	50		20	20		20
		[E2]Errores del administrador	10	10	10	10		

APLICACIONES [SW]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
APLICACIONES	[www] Aplicaciones WEB, ERP PISAMI (Hoja Vida, Nomina, Pqr, Correspondencia, Industria y Comercio, Otros Impuestos, Cobro Coactivo, Tesorería, Presupuesto, Contabilidad y Contratación), Tramites en Linea	[A.4] Manipulación de la configuración	10	20	20	20		
		[A.5] Suplantación de la identidad del usuario	5		10	10	10	
		[A.6] Abuso de privilegios de acceso	10	20	50	50		
		[A.8] Difusión de software dañino	5	5	5	5		
		[A11]Acceso no autorizado	5		10	10		
		[A.15] Modificación deliberada de la información	10		5			
		[E.1] Errores de usuarios	50	20	20	20		
		[E4]Errores de configuración	50		20			
		[E15]Manipulación de la información	10		50	50		50
		[I6]Corte del suministro eléctrico	70	70				
		[E.21] Errores de mantenimiento / actualización de programas (software)	50	50	50			
		[I8]Fallo de servicios de internet	5	100				
	[exe] aplicaciones SOFTCON, TAO, GCI	[A11]Acceso no autorizado	5		10		10	10
		[E.1] Errores de usuarios	50	20	20	20		
		[E.21] Errores de mantenimiento / actualización de programas (software)	50	50	50			
		[E4]Errores de configuración	50		20			
		[A.4] Manipulación de la configuración	50		20	20		20
		[A.6] Abuso de privilegios de acceso	10	20	50	50		

		[E15]Manipulación de la información	10		75	75		75
	[SO] Sistemas Operativos (Linux Centos 6 y 7, Windows Server2003, Windows XP, Siete, Ocho	[I5]Avería de origen físico o lógico	5					
		[E2]Errores del administrador	10	20		20		20
		[E4]Errores de configuración	50		20			
		[E8]Difusión de Software dañino	50	50	50	50		
	[Office], Programa Office en sus diferentes versiones estándar (2003, 2007, 2010, 2013 y 2016]	[I5]Avería de origen físico o lógico	5	50				
		[I10]Degradación de los soportes de almacenamiento de la información	5	100				
		[E1]Errores de los usuarios	50	50	20	20		
		[E4]Errores de configuración	50		20			
	[av] Antivirus Kapersky	[I5]Avería de origen físico o lógico	5	50				
		[E4]Errores de configuración	50		20			
	[exe] Gestor de Base Datos	[I5]Avería de origen físico o lógico	5	50				
		[I10]Degradación de los soportes de almacenamiento de la información	5	100				
		[E4]Errores de configuración	50		20			
		[E15]Manipulación de la información						
		[A.4] Manipulación de la configuración	10		20	20		20
		[E2]Errores del administrador	10	10	20	20		
		[E21]Errores de mantenimiento/actualización de programas	10	5	5			

EQUIPAMIENTO INFORMÁTICO [HW]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T

EQUIPOS INFORMÁTICOS	Servidores web (linux)	[I1]Fuego	5	5				
		[N*]Desastres naturales	5	5				
		[I.3]Contaminación Mecanica	5	20				
		[I5]Avería de origen físico o lógico	10	100				
		[I6]Corte del suministro eléctrico	75	75				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	5				
		[A.3] Manipulación de los registros de actividad (log)	5	5				5
		[A.4] Manipulación de la configuración	10	20	20	20		
		[A.6] Abuso de privilegios de acceso	10	20	50	50		
		[A.11] Acceso no autorizado	10	5	5			
		[A24]Denegación del servicio	50	50				
		[I10]Degradación de los soportes de almacenamiento de la información	20	100				
	Servidor de base de datos (sql Tramties sectoriales portal www.ibague.gov.co) (ORACLE, ERP - PISAMI Y TAO)	[I1]Fuego	5	100				
		[N*]Desastres naturales	5	100				
		[I.3]Contaminación Medioambiental	5	20				
		[I5]Avería de origen físico o lógico	5	100				
		[I6]Corte del suministro eléctrico	75	75				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	20				
		[A24]Denegación del servicio	50	50				
		[I10]Degradación de los soportes de almacenamiento de la información	5	20				
		[E2]Errores del administrador	50	50	50	50		

		[E21]Errores de mantenimiento/actualización de programas	50	50				
		[A11]Acceso no autorizado	50	20			20	
		[A8]Difusión de software dañino	10	20	20	20		
		[E15]Manipulación de la información	10		50	50		50
		[E4]Errores de configuración	10		20			
		[I8]Fallo de servicios de internet	5	100				
	Medios de Impresión	[I1]Fuego	5	50				
		[I5]Avería de origen físico o lógico	50	50				
	Equipos Virtuales	[I1]Fuego	5	100				
		[I5]Avería de origen físico o lógico	5	100				
		[I6]Corte del suministro eléctrico	75	75				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[A24]Denegación del servicio	50	50				
		[A11]Acceso no autorizado	10	20			20	
		[E2]Errores del administrador	50	50	50	50		
		[E4]Errores de configuración	50		20			
		[E21]Errores de mantenimiento/actualización de programas	10	5	5			
		[A4]Manipulación de la configuración	10	20	20	20		
	Servidores de aplicación (TAO - Modulo Pedial) (ERP - PISAMI)	[I1]Fuego	5	100				
		[I5]Avería de origen físico o lógico	5	100				

		[I6]Corte del suministro eléctrico	75	75				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	20				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[I10]Degradación de los soportes de almacenamiento de la información	5	20				
		[E2]Errores del administrador	50	50	50	50		
		[E4]Errores de configuración	50		20			
		[E21]Errores de mantenimiento/actualización de programas	50	50				
		[E23]Errores de mantenimiento/actualización de equipos	50	50				
		[E24]Caída del sistema por agotamiento físico de recursos	50	75				
		[A4]Manipulación de la configuración	10	20	20	20		
		[A25]Perdida de equipos						
	Firewalls	[I1]Fuego	5	100				
		[I6]Corte del suministro eléctrico	70	75				
		[I5]Avería de origen físico o lógico	5	100				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	20				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[E2]Errores del administrador	10	20	20	20		
		[E4]Errores de configuración	5		20			
		[E23]Errores de mantenimiento/actualización de equipos	5	20				
	Computadores de	[I1]Fuego	5	100				

	escritorio	[I5]Avería de origen físico o lógico	50	20				
		[N2]Daños por agua	10	20				
		[N*]Desastres naturales	5	100				
		[E1]Errores de los usuarios	5	5				
		[E4]Errores de configuración	5	5				
		[A8]Difusión de software dañino	10	20	20	20		
		[E23]Errores de mantenimiento/actualización de equipos	10	5				
		[A25]Perdida de equipos	10	20		20		
		[A4]Manipulación de la configuración	5	5	5	5		
		[E24]Caída del sistema por agotamiento físico de recursos	10	75				
	Router	[I1]Fuego	5	100				
		[I6]Corte del suministro eléctrico	70	75				
		[I5]Avería de origen físico o lógico	5	100				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	20				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[E2]Errores del administrador	10	20	20	20		
		[E4]Errores de configuración	5		20			
		[E23]Errores de mantenimiento/actualización de equipos	5	20				

REDES COMUNICACIONES [LAN] red local

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
REDES DE COMUNICACIONES	Red LAN	[I1]Fuego	5	100				
		[I6]Corte del suministro eléctrico	70	75				
		[I7]Condiciones inadecuadas de temperatura o humedad	5	20				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[E2]Errores del administrador	10	20	20	20		
		[E4]Errores de configuración	5		20			
		[E23]Errores de mantenimiento/actualización de equipos	5	20				
		[E9]Errores de [re-]encaminamiento	5			5		
		[E10]Errores de secuencia	5		5			
	Internet	[I6]Corte del suministro eléctrico	70	75				
		[I8]Fallo de servicios de comunicaciones	10	100				
		[E24]Caída del sistema por agotamiento físico de recursos	10	20				
		[A4]Manipulación de la configuración	5	5	5	5		

SOPORTES DE INFORMACIÓN [Media]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
SOPORTES DE INFORMACIÓN	Sistema de gestión de proyectos donde se encuentra alojado el código fuente,	[I1]Fuego	5	100				
		[I5]Avería de origen físico o lógico	5	100				

	backups, pruebas.	[I6]Corte del suministro eléctrico	70	75				
		[I8]Fallo de servicios de comunicaciones	10	20				
		[I10]Degradación de los soportes de almacenamiento de la información	5	5				
		[E2]Errores del administrador	10	20	20	20		
		[E4]Errores de configuración	10	20				
		[E21]Errores de mantenimiento/actualización de programas	10			20		
		[E24]Caída del sistema por agotamiento físico de recursos	10	20				
		[E8]Difusión de software dañino	5	5	5	5		
		[E20]Vulnerabilidades de los programas	10			20		

EQUIMAMENTO AUXILIAR [AUX]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
EQUIPAMIENTO AUXILIAR	Fuentes de alimentación ininterrumpida	[A5]Daños por Fuego	10	5				
		[N2]Daños por agua	5	5				
		[N*]Desastres naturales	5	100				
		[I5]Avería de origen físico o lógico	20	5				
		[E23]Errores de mantenimiento/actualización de equipos	50	5				
		[I.3]Contaminación Medioambiental	20	5				
		[I7]Condiciones inadecuadas de temperatura o humedad	50	5				
	Aire acondicionado	[I7]Condiciones inadecuadas de temperatura o humedad	5	5				
		[I.3]Contaminación Medioambiental	5	5				
		[I5]Avería de origen físico o lógico	10	20				

		[I6]Corte del suministro eléctrico	70	75				
		[N2]Daños por agua	5	5				

Personal [P]

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	PROBABILIDAD				
				D	I	C	A	T
PERSONAL	Usuarios Internos	[E19]Divulgación de la información	50			50		
		[A30]Ingeniería social	5	20	20	20		
		[E28.1]Enfermedad	5	20				
		[E28.2]Huelga	5	5				
		[A29.2]Ataques desde el interior	5		5			5
	Usuario Externo	[A11]Acceso no autorizado	10		20	20		
		[A30]Ingeniería social	5	20	20	20		
	Administradores de sistemas	[E19]Divulgación de la información	10			20		
		[A30]Ingeniería social	5	20	20	20		
		[E28.1]Enfermedad	10	20				
	Administradores de bases de datos	[E19]Divulgación de la información	10			20		
		[A30]Ingeniería social	5	20	20	20		
		[E28.1]Enfermedad	10	20				

VALORACIÓN DEL RIESGO

Estimación del Impacto

El segundo dato necesario para la valoración del impacto es la "Degradación", el cual nos indica que tan perjudicado resulta el [valor del] activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas:

- 90% a 100%: Degradación muy considerable del activo
- 25% a 89%: Degradación medianamente considerable del activo
- 1% a 24%: Degradación poco considerable del activo

8, Muy alto, Daño muy grave

Se valora muy alto los servidores. Ya ha sucedido que en ocasiones anteriores el solo hecho de que no hay disponibilidad de esos se afecta el funcionamiento completo de la Cede central, el hardware está expuesto a diferentes tipos de amenazas sobre todo físicas. Por lo que el nivel de los servidores es muy alto y el estimado de degradación de 90% - 100%.

En la siguiente tabla el valor del impacto si se materializa las amenazas identificadas con anterioridad, es 8 Desastroso (Impacta fuertemente en la operatividad de los procesos).

IMPACTO		Degradación		
		1%	50 %	**100 %**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos. Mayor (5): Impacta en la operatividad de los procesos.
Moderado (3): Impacta en la operatividad del macro proceso. Menor (2): Impacta en la operatividad del proceso.
Insignificante (1): Impacta levemente en la operatividad del proceso

ACTIVO TI	**EQUIPAMIENTO INFORMÁTICO [HW]**	
Administrador	Administrador Sala Servidores	
Degradación	100%	
Impacto	8	Desastroso
Tipo	Hardware	

Cuadro 10. Valoración del riesgo

Activo	Tipo de Amenaza	Descripción Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
							3.83	Intolerable
				Frecuencia (F)		R	NR	
Servidores web (linux, Servidor de base de datos (sql Tramites sectoriales portal www.ibague.gov.co) (ORACLE, ERP - PISAMI Y TAO)) En total son 3 servidores	Desastres naturales	[N*]Desastres naturales	La Sala de servidores está ubicada en edificación antigua que no cumple con los parámetros antisísmicos.	Raro	1	**8**	3	Intolerable
		[I1]Fuego	La Sala de servidores cuenta con un extinto Solkaflan tipo 123	Muy baja	2	**16**	4	Extremo
		[I.3]Contaminación Mecánica	La sala de servidores está expuesta a polvo y vibraciones	Raro	1	**8**	3	Intolerable
		[I5]Avería de origen físico o lógico	No existen servidores tipo backup que garanticen el funcionamiento de la plataforma en caso de una falla técnica que presente algunos de los servidores en los que se encuentren instaladas los gestores de las bases de datos.	Muy baja	2	**16**	4	Extremo
		[I6]Corte del suministro eléctrico	Además de lo anterior la energía es un servicio muy deficiente y constante las caídas de luz de todo el edificio, la autonomía de las UPS , destinada a la granja de servidores es aproximadamente 45 minutos, por lo que al transcurrir este tiempo la indisponibilidad del servicio del portal se genera.	Baja	3	**24**	4	Extremo

		[I7]Condiciones inadecuadas de temperatura o humedad	El cuarto de Servidores cuenta con aire acondicionado , en caso de periodo largo de ininterrupción de energía puede generar calentamiento el cuarto de servidores	Baja	3	**24**	4	Extremo
		[I10]Degradación de los soportes de almacenamiento de la información	No existen servidores tipo backup que garanticen el funcionamiento de la plataforma en caso de una falla técnica que presente algunos de los servidores en los que se encuentre instaladas los gestores de las bases de datos.	Muy baja	2	**16**	4	Extremo
	Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	Existe un solo funcionario con conocimiento en instalación y configuración de base de datos Oracle. Para los demás gestores (SQL, Firebire entre otros) no existe funcionarios de perfil técnico con experiencia en instalación y configuración, situación que conlleva a la entidad a cometer errores. Falta del cumplimiento de la política de seguridad (definición de claves robustas, presamos de usuarios. Falta de monitoreo de la acciones realizadas por usuarios en la BD por usuarios con exceso de privilegios	Raro	1	**16**	4	Extremo
		[A.4] Manipulación de la configuración		Muy baja	2	**16**	4	Extremo
		[A.6] Abuso de privilegios de acceso		Muy baja	2	**16**	4	Extremo
		[A.11] Acceso no autorizado	Falta del cumplimiento de la política de seguridad (definición de claves robustas, prestamos de usuarios. Falta de monitoreo de la acciones realizadas por usuarios en la BD por usuarios con exceso de privilegios. Además de	Muy baja	2	**16**	4	Extremo

			la jackeo por inyección de código SQL, donde logran obtener la contraseñas y nombres de usuarios.					
		[A24]Denegación del servicio	Como se expuso anterior los pocos conocimientos técnicos en la configuración de manejadores de base de datos, hace que se realicen configuraciones inadecuadas que hacen las maquinas realicen reprocesos, aunado a esto la ejecución de software que se encuentra optimizado.	Muy baja	2	**16**	4	Extremo

VERIFICAR LOS CONTROLES INFORMÁTICOS APLICANDO LISTAS DE CHEQUEO DE ACUERDO A LA NORMA ISO/IEC 27002

Cuadro11. Lista de Chequeo Alcaldía de Ibagué

Ítem	Dominio	Objetivo de Control	Controles	Pregunta existencia control	Si	No	Observación
1	A.5.Políticas de seguridad	A.5.1. Directrices de la Dirección en seguridad de la información	A.5.1.1. Políticas para la seguridad de la información	¿Cuenta la Alcaldía de Ibagué, con un conjunto de políticas para la seguridad de la información?	Si		Parcialmente, Documento Socializado pero no todos los funcionarios asisten a los talleres de capacitación, reinducción y socialización sin embargo el documento se encuentra publicado en el portal de la de la entidad
			A.5.1.2. Revisión de las políticas para seguridad de la información	¿Existe un plan de revisión y cumplimiento de las políticas de la seguridad de la información?	Si		Mediante el procedimiento de actualización de políticas públicas dispuestos por la Secretaria de Planeación, la dirección de Informática, actualiza la directriz que por alguna eventualidad o cambio normativo modifique la política. Además de lo anterior se hace seguimiento mediante proceso de revisión y auditoria por parte de la Oficina de Control Interno de la
2	A.6. Aspectos organizativos de la SI	A.6.1. Organización interna	A.6.1.1. Roles y responsabilidades para la seguridad de la información	¿Existe en la organización un equipo líder del proceso de seguridad informática?	Si		Secretaria Planeación Municipal, responsable de proceso de gestión de políticas públicas y la secretaria ejecutora del

							proceso al que corresponda el sector, para este caso, Secretaria Administrativa Dirección de Informática
			A.6.1.2. Separación de deberes	¿Se realiza seguimiento a las tareas asignadas al equipo encargado?		No	
			A.6.1.3. Contacto con las autoridades	¿Cuenta la entidad con procedimientos claros y los canales de comunicación para informar novedades como perdidas de equipos? hardware o pérdida o alteración de datos	Si		Director Grupo Informática, Director Recursos Físicos, Almacenista, Secretario Administrativa, Secretario Responsable Proceso
			A.6.1.4. Contacto con grupos de interés especial	¿Se realizar asignación de responsabilidades para la seguridad de la información?	Si		Manual de funciones y por actos administrativos para la Administración de las BD
			A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existe contacto con las autoridades?	Si		Parcialmente, Cada vez que se detectan anomalías de fraudes, se da traslado a las autoridades mediante denuncia penal.
		A.6.2. Dispositivos para movilidad y teletrabajo	A.6.2.1. Política para dispositivos móviles	¿La empresa tiene una política de uso de dispositivos para movilidad?	No		
			A.6.2.2. Teletrabajo	¿La empresa implementa el teletrabajo?		No	
3	A.7. Seguridad ligada a los recursos humanos	A.7.1. Antes de la contratación	A.7.1.1. Selección	¿La entidad realiza verificación de antecedentes laborales, judiciales, penales?	Si		Cumple parcialmente, se verifica antecedentes disciplinarios, penales pero no se verifican las referencias laborales para confirmar si la idoneidad de la persona. Es situación es una generalidad en toda la entidad.
			A.7.1.2. Términos y condiciones del empleo	¿ El manual de funciones de los empleados de planta y en la minutas contractuales, están contempladas como función o obligación contractual las responsabilidades del servidor público en cuanto a la seguridad la información?		No	
		A.7.2. Durante la contratación	A.7.2.1. Responsabilidad de la dirección	¿Se encuentra contratado un profesional específicamente para la realización del tema?	Si		Cumple parcialmente, en la actualidad hay profesional especializado en seguridad de la información, revisando los documentos, procedimientos y realizando levantamiento de información con el objetivo de actualizar las políticas de seguridad de la Alcaldía de Ibagué.

			A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	¿Cuenta la Alcaldía de Ibagué, con procedimientos de capacitación a servidores públicos y estos contienen actividades precisas sobre seguridad de la información?	Si		..
				¿Realiza la Alcaldía de Ibagué, capacitación y reinducción a los funcionarios en temas de seguridad de la información?	Si		Parcialmente, en al ejecución de los procesos de capacitación (inducción y reinducción) a los funcionarios y contratistas se les explica sobre la exigencia de la aplicación de las políticas de seguridad en cuanto a la gestión de privilegios en las aplicaciones, manejos de clave de acceso, amenazas y riesgos de sistemas de seguridad de la información en la Alcaldía de Ibagué
			A.7.2.3. Proceso disciplinario	¿Se realizan socializaciones para actualizar a los empleados en los diferentes cambios generados?	Si		Parcialmente, aunque el proceso esta reglado por la ley, no se tiene un reglamentación específica para que los empleados conozcan el riesgo en el que pueden incurrir cuando se llegase a realizar una acción que este tipificada como un delito informático
		A.7.3. Terminación o cambio de puesto de trabajo	A.7.3.1. Terminación o cambio de responsabilidades de empleo	¿Se tienen definidos las responsabilidades y deberes de seguridad de la información una vez el empleado termine su contratación o se le realice un cambio de puesto?	Si		En la Alcaldía de Ibagué, una vez se termine el contrato, los supervisores informan a la dirección de Informática, sobre el tiempo de duración del contrato y el sistema controla este periodo. Para los empleados de plata la dirección de personal informa sobre la novedad a la dirección de Informática.
4	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.1. Inventario de activos	¿Se cuenta con un inventario de activos actualizado?	Si		
			A.8.1.2. Propiedad de los activos	¿Se cuenta con un procedimiento para la solicitud de algún equipo faltante y necesario para el desempeño?	Si		Esta solicitud la hacen a través de comunicación interna directamente por el responsable de la dirección recursos físicos Almacén. Quien elabora plan de compra anual.
			A.8.1.3. Uso aceptable de los activos	¿Los funcionarios de la Alcaldía de Ibagué, hacen buen uso de los activos informáticos?		No	Muchas veces por descuidos como dejarlos encendidos toda la noche o fines de semana estos se queman, a no protegerlos en el manejo de los elementos de computador
			A.8.1.4. Devolución de activos	¿Los empleados de la Alcaldía de Ibagué, al ser traslados, removidos o por terminación del contrato hacen devolución de los	Si		Todos los activos físicos, son entregados mediante tarjetas de responsabilidad y descargados mediante acta documental. En cuanto a la información, estos hacen entrega de la serie documental

				activos?			en medio magnético y la suspensión de los privilegios de acceso a los aplicativos.
		A.8.2. Clasificación de la información	A.8.2.1. Clasificación de la información	¿Cuenta la Alcaldía con sistema de inventario que permita la identificación de los equipos y la propiedad?	Si		Todo esta inventariado y se controla a través del software de inventario
			A.8.2.2. Etiquetado de la información	¿Se tienen implementado un procedimiento para el etiquetado de la información?		No	
			A.8.2.3. Manejo de activos	¿Se manejan los activos de acuerdo al procedimiento implementado?	SI		Parcialmente, para todos los elementos tangibles, se debe contar con ingreso al sistema de inventario, los intangibles como licencias también se registran, pero las base de datos y su información como tal no se encuentran ni registradas ni valoradas
5	A.9. Control de Acceso	A.9.1. Requisitos de negocio para el control de accesos	A.9.1.1. Política de control de acceso	¿Se tiene control sobre el acceso a LAN por parte personas internas a la Entidad?	Si		Para el acceso a LAN las redes se cuentan con un subneteo, especifico por sedes, el acceso a las aplicaciones se hace través de un sistema de gestión de seguridad UTM
			A.9.1.2. Política sobre el uso de los servicios de red	¿La empresa posee una política de control de accesos?	Si		
				¿Se tiene control sobre los accesos a LAN por parte personas externas a la Alcaldía?	Si		No está permitido
		A.9.2. Gestión de acceso de usuario	A.9.2.1. Registro y cancelación del registro de usuarios	¿Se lleva un control sobre los usuarios de los sistemas de información?	Si		El control de acceso de algunos de los aplicativos se hace por Sistema Operativo y aplicación, otros solo por aplicación pero cualquiera de los anteriores se hace autenticación.
			A.9.2.2. Suministro de acceso a usuarios	¿Se tiene un reporte de los procesos realizados por cada usuario en los Sistemas de información?	Si		Modulo auditoria
			A.9.2.3. Gestión de derechos de acceso privilegiado	¿La Alcaldía de Ibagué, gestiona el registro de ingresos, actualización e inactivación de usuarios?	Si		A través de módulos de Administración de Aplicación de los diferentes aplicativos. Previo cumplimiento de la política para asignación de privilegios de acceso.
			A.9.2.4. Gestión de información de autenticación secreta de usuarios	¿Cuenta la Alcaldía de Ibagué, con procedimiento que identifique los diferentes niveles de seguridad de acceso a las herramientas o sistemas de información?	Si		El ERP – PISAMI, cuentan con módulos de seguridad donde se existen un rolles de consulta, inserción, actualización y borrado sobre los objetos de la BD, los cuales a través de privilegios son concedidos a un usuario. Como se mencionó anteriormente el ERP-PISAMI,

							a través de un módulo de Administración se configura el acceso del usuario de acuerdo a los privilegios requeridos y autorizado por el responsable del proceso de información. Existen otros aplicativos no integrados al ERP que también cuenta con módulo de administración y se aplica la misma política.
			A.9.2.5. Revisión de los derechos de acceso de usuarios	¿Se realiza monitoreo permanente de los logs de acceso a las diferentes herramientas o sistemas de información?		No	
			A.9.2.6. Retiro o ajuste de los derechos de acceso	¿Se realiza una revisión periódica de los derechos de acceso, realizando de esta manera la eliminación de los usuarios que ya no trabajan en la empresa?	Si		Esta función se realiza de manera permanente
		A.9.3. Responsabilidad de los usuarios	A.9.3.1. Uso de la información de autenticación secreta	¿Los usuarios cumplen a cabalidad con el buen uso de la información secreta (No divulgación)?	Si		La información que maneja la entidad en gran medida está clasificada como publica.
		A.9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1. Restricción de acceso de la información	¿Los aplicativos cuentan con niveles de control para despliego de información con relación a cada usuario?	Si		La información que maneja la entidad en gran medida está clasificada como publica. Sin embargo de acuerdo al perfil del usuario puede, este consultar, modificar o insertara información
			A.9.4.2. Procedimiento de ingreso seguro	¿Se cuenta con la asignación de contraseñas para el acceso a la información?	Si		El acceso a la plataforma se hace por medio de autenticación de usuarios
			A.9.4.3. Sistema de gestión de contraseñas	¿Se cuenta con un administrador de la base de datos y el código de aplicaciones?	Si		
			A.9.4.4. Uso de programas utilitarios privilegiados	¿La empresa hace uso de herramientas de administración de sistemas?	Si		
			A.9.4.5. Control de acceso a códigos fuente de programas	¿Se tiene definido los roles de las personas que tienen acceso al código fuente y se encuentra esta información en lugares seguros?	Si		La entidad cuenta con datacenter y este tiene equipos servidores de desarrollo, pruebas, base datos y aplicaciones, de acuerdo a esto están configurados los acceso dependiendo el tipo de usuario (desarrolladores, ingenieros soporte, administrador sistema y usuarios de los aplicativos)
6	A.10. Criptografía	A.10.1. Controles	A.10.1.1. Política sobre el uso de	¿Se tiene una política sobre el uso de		No	

		criptográficos	controles criptográficos	controles criptográficos para la protección de la información?			
			A.10.1.2. Gestión de llaves	¿Se tiene una política con la cual se conoce el uso, protección y tiempo de vida de las llaves criptográficas?		No	
7	A.11. Seguridad física y del entorno	A.11.1. Áreas seguras	A.11.1.1 Perímetro de seguridad física	¿Los servidores y puntos de conexión se encuentran ubicados en un lugar seguro?	SI		Datacenter
			A.11.1.2. Controles físicos de entrada	¿Las entradas a los lugares prohibidos se encuentran con algún mecanismo de seguridad, por ejemplo biométricos?		No	
			A.11.1.3. Seguridad de oficinas, recintos e instalaciones	¿Las oficinas, recintos e instalaciones cuentan con algún tipo de seguridad? Por ejemplo Vigilantes, cámaras.	Si		Cumple parcialmente La ubicación del datacenter, esta resguardada con chapas de seguridad y acceso restringido
			A.11.1.4. Protección contra amenazas externas y ambientales	¿El lugar donde se encuentran los servidores cuenta con las medidas de seguridad apropiadas (Extintores, aire acondicionado, entre otros)?	Si		Cuenta con aire acondicionado y extintor
			A.11.1.5. Trabajo en áreas seguras	¿Se tiene establecido un procedimiento que indique como se debe realizar el trabajo en las áreas seguras?		No	
			A.11.1.6. Áreas de despacho y carga	¿El lugar donde se realiza el despacho y carga de herramientas (computadores, teclados, entre otros), cuenta con medidas de seguridad?	Si		Taller independiente de la oficina de informática
		A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	¿La infraestructura eléctrica se encuentra bien instalada y sin riesgos?	Si		La infraestructura eléctrica que energizan computadores, se hace a través del sistema cableado estructurado el cual se encuentra protegido por sistema de Energía ininterrumpida
			A.11.2.2. Servicios de suministro	¿Los equipos informáticos y accesos de red, están seguros?	Si		Todos los armarios se encuentran protegidos con chapas de seguridad.
			A.11.2.3. Seguridad del cableado	¿Se realiza mantenimiento a los equipos periódicamente?	Si		
			A.11.2.4. Mantenimiento de equipos	¿Se cuenta con puestos de trabajos agradables y seguros?		No	La distribución del espacio es reducida, sabiendo que existen varias entidades como la Contraloría, Concejo, Personería y la Alcaldía en el misma edificación.
			A.11.2.5. Retiro de activos	¿Cuándo se va a realizar un cambio de	Si		La instalación la realiza un técnico de la dirección de

				algún computador a otro puesto de trabajo, se tiene un conducto regular para realizar dicho proceso?			informática
			A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Cuándo un activo es retirado de las dependencias de la Administración Municipal, este cuenta con las medidas de seguridad en caso de tener pérdida?	Si		Todos los activos están protegidos con una póliza global contra todo daño.
			A.11.2.7. Disposición segura o reutilización de equipos	¿Se realiza un backup y limpieza de los equipos de cómputo antes de entregarlo a otra persona?	Si		De acuerdo a las políticas la información, se realizan los Backus a las base de datos que se encuentran en custodia por parte del grupo Informática, los archivos tipo texto, hojas de cálculo los custodia cada responsable del proceso de información, sin embargo la oficina de informática apoya el procedimiento de copia o Bakcup de ser necesario
			A.11.2.8. Equipos de usuario desatendidos	¿Los equipos que no tienen personal asignado se les da una protección adecuada?	Si		Se encuentran en custodia por el Almacén de la entidad.
			A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se tiene una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	No		
8	A.12. Seguridad en las operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Procedimientos de operación documentados	¿Cuenta la Alcaldía de Ibagué, con manual de procedimientos de operación y se ponen a disposición de los usuarios?	Si		En las secciones de inducción y reinducción a los funcionarios, se enseñan los objetivos y alcance del manual de operaciones como también donde está publicado y como acceder a la información en el portal web de la Alcaldía de Ibagué
			A.12.1.2. Gestión de cambios	¿Se tiene un procedimiento de gestión de cambios en el área de desarrollo de los aplicativos?	SI		Cumple parcialmente, se llevan documentos como actas de trabajo y después de la entrega de los módulos en operación, los cambios al software se hacen todos por escrito y por solicitud del responsable del proceso de información
			A.12.1.3. Gestión de capacidad	¿Se monitorean de manera permanente el comportamiento de los recursos de los equipos tipo servidores de la Alcaldía de Ibagué?	Si		
			A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación	¿Se cuenta y aplican procedimientos de desarrollo, pruebas y producción separados?	Si		La Alcaldía de Ibagué, a través de la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fase (Análisis y Diseño, Desarrollo, Migración,

							Pruebas, Ajuste, Puesta en Operación, y Estabilización) cada fase tiene un esquema de base de datos independiente o compartido dependiendo el alcance de la etapa en la Implementación de software,
		A.12.2. Protección contra códigos maliciosos	A.12.2.1. Controles contra códigos maliciosos	¿Tiene la Alcaldía de Ibagué, un software tipo antivirus activo en todos los equipos de cómputo?	SI		Cumple parcialmente, existen algunos equipos que por obsolescencia en su hardware, no es compatible con la versión de antivirus que dispone la entidad, por lo que toca recurrir a programas free que protejan el equipo de computo
				¿Tiene la Alcaldía de Ibagué, un software tipo antivirus activo en todos los equipos tipo servidor?	SI		
				¿Se realizan monitoreo en prevención a ataques que se generan al sistema?		No	Cuando sucede el ataque se revisa la situación y se tomas acciones correctivas
		A.12.3. Copias de seguridad	A.12.3.1. Respaldo de información	¿Se realizan periódicamente copias de seguridad de la información?	Si		Copias a diario, en la nube y servidor de copia
		A.12.4. Registro y seguimiento	A.12.4.1. Registro de eventos	¿Se realiza revisión periódica de los logs de las diferentes herramientas con el fin de verificar las fallas y eventos de seguridad de la información?		No	
			A.12.4.2. Protección de la información de registro	¿Se tiene un control de acceso no autorizado, con el fin de proteger la información de algún tipo de modificación?	Si		Solo acceden los usuarios autorizados, mediante la asignación de privilegios de conexión y acceso a la base de datos y después el usuario mediante procedimientos de autenticación
			A.12.4.3. Registros del administrador y del operador	¿Las actividades realizadas por los administradores de las diferentes herramientas son monitoreadas?		No	
			A.12.4.4. Sincronización de relojes	¿Los relojes de los equipos de cómputo, servidores y demás sistemas, se encuentran sincronizados?	Si		Cumple parcialmente, servidores si, equipos de escritorio en la mayoría de equipos las opciones de configuración están inhabilitadas solo se pueden realizar por usuario administrado
		A.12.5. Control de software operacional	A.12.5.1. Instalación de software en sistemas operativos	¿Se tiene alguna regla que impida a los usuarios finales realizar la instalación de software?	Si		La directriz es clara son labores de exclusivas de la dirección de informática, sin embargo las opción de reinstalar no está disponible solo la puede realizar el usuario administrador
		A.12.6. Gestión de	A.12.6.1. Gestión de las vulnerabilidades	¿Se realizan pruebas de penetración para		No	

		la vulnerabilidad técnica	técnicas	encontrar vulnerabilidades en los sistemas y así prevenirlas?			
			A.12.6.2. Restricciones sobre la instalación de software	¿Tiene la Alcaldía de Ibagué, procedimientos claros para la instalación del software que se puede realizar en los equipos de cómputo?	Si		La directriz es clara en cuanto a solo se puede instalar programas debidamente licenciados y autorizados, además de la competencia que tiene la dirección de Informática para la instalación de software en los equipos de propiedad de la Administración Central. También se cuenta con el procedimiento administrativo
		A.12.7. Consideraciones sobre auditorias de sistemas de información	A.12.7.1. Información de controles de auditoría de sistemas	¿Cuentan los gestores de base de datos tienen el sistema de auditoria activo?	Si		Sistema auditoria de Oracle
9		A.13.1. Gestión de la seguridad de las redes	A.13.1.1. Controles de redes	¿Se cuenta con IPS (Sistema de Análisis y Tráfico de la red LAN)?		No	
			A.13.1.2. Seguridad de los servicios de red	¿En la empresa existen mecanismos de seguridad asociados a servicios de red?	SI		La entidad tiene un Firewall, el cual filtra tráfico y neutraliza ataques de virus
			A.13.1.3. Separación en las redes	¿Se tiene algún procedimiento sobre el acceso a las redes?	Si		
		A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	¿Se cuenta con protocolos de intercambio de información con externos?	Si		Cumple parcialmente la política existe, pero no tiene definido los controles, sin embargo la entidad toma en cuenta la tabla de clasificación de la información, los medios y la debida autorización del responsable del proceso, antes de genera cualquier tipo de entrega
			A.13.2.2. Acuerdos sobre transferencia de información	¿Se cuenta con servicio de email dentro del dominio de la compañía?	Si		La entidad cuenta con servicio de correo Google, a través de un tercero.
			A.13.2.3. Mensajería electrónica	¿La información contenida en los correos cuenta con mecanismos de seguridad, como por ejemplo antivirus, protección por contraseña?	Si		Todos los correo se manejan con contraseñas independientes y la cuenta está respaldada por google
			A.13.2.4. Acuerdos de confidencialidad o de no divulgación	¿Cuenta la Alcaldía de Ibagué, con acuerdos de confidencialidad?		No	
10	A.14. Adquisición, desarrollo y mantenimiento de sistemas	A.14.1. Requisitos de seguridad de los sistemas de información	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	¿ Garantiza la plataforma tecnológica PISAMI, que se cumplan los criterios de seguridad de la información como: la Confidencialidad, Integridad, Disponibilidad,	Si		Cumple parcialmente, los aplicativos ERP-PISAMI, cuenta con seguridad tanto para el acceso, proceso, y salidas de información, que garantizan la disponibilidad, integridad y confidencialidad de la información.

				Autenticidad de la información almacenada en la BD ?			
			A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	¿Los Trámites y Servicios tipo Web, prestados por la entidad y estos se apoyan por el software PISAMI a nivel de Web, garantizan que los datos estén libre de fraudes, alteraciones o divulgación?.	Si		Cumple parcialmente, aunque la entidad tiene implementado un sistema de seguridad a nivel firewall, hace falta la implementación de mecanismo de seguridad a las bases de datos que protejan la información de ataques de inyección SQL
			A.14.1.3. Protección de transacciones de los servicios de las aplicaciones	¿Se realiza la protección de la información involucrada en las transacciones de los servicios de las aplicaciones, por ejemplo certificados digitales?		No	
		A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.1. Política de desarrollo seguro	Se cuenta con un procedimiento para la solicitud de desarrollo de software	Si		Existe un plan desarrollo de aplicaciones
			A.14.2.2. Procedimientos de control de cambios en sistemas	Se lleva un control de las versiones de las aplicaciones desarrolladas	Si		Cumple parcialmente, se notifica a través de comunicación interna todas las mejoras a los módulos y cuando estas son publicadas y puestas en producción
			A.14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se cuenta con un protocolo para la aplicación de pruebas a los SI desarrollados	Si		La Alcaldía de Ibagué, a través de la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fase (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización) cada fase tiene un esquema de base de datos independiente o compartido dependiendo el alcance de la etapa en la Implementación de software
			A.14.2.4. Restricciones en los cambios a los paquetes software	Se cuenta con un procedimiento para la puesta en producción de un desarrollo en SI	Si		La Alcaldía de Ibagué, a través de la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fases (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización).
			A.14.2.5. Principios de construcción de sistemas seguros	Se tienen en cuenta principios de seguridad en un entorno de desarrollo	Si		Existe una metodología desarrollo de software, (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y

							Estabilización). En la fase de diseño está considerado, para que la producción de software sean incorporados los criterios de seguridad de la información.
			A.14.2.6. Ambiente de desarrollo seguro	¿El lugar en donde se encuentra el código y las aplicaciones desarrolladas es seguro?	Si		El servidor desarrollo también se encuentra protegido por esquema de seguridad tipo Firewall
			A.14.2.7. Desarrollo contratado externamente	¿Cuenta la Alcaldía de Ibagué, con un hosting tercerizado?		No	El hosting es provisto por la misma entidad
			A.14.2.8. Pruebas de seguridad de sistemas	¿Se realizan pruebas de funcionalidad a las aplicaciones desarrolladas?	Si		La Alcaldía de Ibagué, a través de la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fases (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización). La fase de pruebas las realizan los desarrolladores a través de casos o e pruebas o de estudio antes de llevarlos a pruebas con los usuarios finales, procedimiento que es repetitivo hasta que se supere la prueba.
			A.14.2.9. Pruebas de aceptación de sistemas	¿Cuándo se realizan actualizaciones a los desarrollos de aplicaciones, se hacen pruebas de aceptación?	Si		La Alcaldía de Ibagué, a través de la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fases (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización). La fase de ajustes, contempla este tipo de actualizaciones las cuales también aplica las pruebas de caso de estudio o casos.
		A.14.3. Datos de prueba	A.14.3.1. Protección de datos de prueba	¿Cuándo se realizan las pruebas se trabajan con datos falsos?		No	Cuando no existe información contenida en BD, se crean datos de prueba
11	A.15. Relación con los proveedores	A.15.1. Seguridad de la información en las relaciones con los proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	¿Se cuenta con una política de seguridad de la información asociada a terceros?		No	
			A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	¿Se tienen establecidos los requisitos y procedimientos de acceso a las instalaciones por parte de terceros?	Si		
			A.15.1.3. Cadena de suministro de tecnología de información y comunicación	¿Se tiene acuerdos con terceros que incluyan los requisitos para tratar los riesgos de seguridad de la información asociados		No	

				a la cadena de suministro?			
		A.15.2. Gestión de la prestación de servicios con los proveedores	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	¿Se hace un seguimiento de la prestación del servicio de terceros?	SI		Informes de supervisión de ejecución del contrato
			A.15.2.2. Gestión de cambios en los servicios de proveedores	¿Se tiene una gestión de cambios en el suministro de servicios por parte de terceros?	Si		Cumple, en los estudios de previos a los procesos de contratación, Estudios de Mercado se apropian los recursos de acuerdo a la necesidad y a la problemática y experiencias anteriores
12	A.16. Gestión de incidentes en la seguridad de la información	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1. Responsabilidad y procedimientos	¿Se cuenta con un procedimiento para la identificación de un incidente de seguridad de la información?		No	
			A.16.1.2. Reporte de eventos de seguridad de la información	¿Se cuenta con un procedimiento para el reporte de un incidente de seguridad de la información?		No	
			A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se cuenta con un procedimiento para el trámite de un incidente de seguridad de la información?		No	
			A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones de la información	¿Se tiene identificado un responsable para la gestión de los incidentes de seguridad de la información?		No	
			A.16.1.5. Respuesta a incidentes de seguridad de la información	¿Los incidentes informáticos son tratados y solucionados a tiempo?		No	
			A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	¿Se solicitan evidencias de los incidentes de seguridad de información identificados?	Si		Cumple parcialmente, cuando se identifica un hallazgo de fraude, hackeo se realiza análisis archivos log, trazabilidad, copias de seguridad entre otros
			A.16.1.7. Recolección de evidencia	¿Se tiene definido un procedimiento en donde se especifique como debe realizarse la identificación, recolección, adquisición y preservación de información que es tomada como evidencia?		No	
13	A.17. Aspectos de seguridad de la información en la gestión de la continuidad del	A.17.1. Continuidad de la seguridad de la	A.17.1.1. Planificación de la continuidad de la seguridad de la información	¿Se hace seguimiento a la seguridad de la información?		No	

	negocio	información	A.17.1.2. Implementación de la continuidad de la seguridad de la información	¿Se tiene un plan de continuidad?		No	
			A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se realiza regularmente la verificación del plan de continuidad?		No	
		A.17.2. Redundancias	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad?		No	
14	A.18. Cumplimiento	A.18.1. Cumplimiento de requisitos legales y contractuales	A.18.1.1. Identificación de requisitos legales y contractuales	¿Se realizan auditorías internas para verificar el cumplimiento de la norma?	Si		Auditoria de control interno, Mintic
			A.18.1.2. Derechos de propiedad intelectual	¿Se cuenta con mecanismos de protección de la información?	Si		Procedimientos seguridad acceso autorizados, autenticación, a nivel de red y servidores un dispositivo UTM
			A.18.1.3. Protección de registros	¿Se tiene documentado todo el proceso de seguridad y protección de la información?		No	
			A.18.1.4. Privacidad y protección de datos personales	¿Se asegura la privacidad y la protección de la información de datos personales?			
		A.18.2. Revisiones de la seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información	¿Se cumple con las políticas y normas de seguridad?	Si		Cumple parcial están son insuficientes y algunas no tiene el alcance en cuanto a controles y no está cubiertos todos los elementos del sistema de seguridad de la información
			A.18.2.2. Cumplimiento con las políticas y normas de seguridad	¿Se realizan comités de seguridad con los altos directivos en donde se revisen con regularidad el cumplimiento de las políticas de seguridad en todas las áreas?		No	
			A.18.2.3. Revisión del cumplimiento técnico	¿Se realiza revisión periódica de los sistemas con el fin de verificar el cumplimiento de las políticas de seguridad de la información?		No	

DECLARACION DE APLICABILIDAD (SOA)

Cuadro 12. Declaración de aplicabilidad (SOA)

		DECLARACION DE APLICABILIDAD (SOA)								
	Objetivo	**Producir la Declaración de Aplicabilidad (SOA) que contenga los controles necesarios producto de la Matriz de Riesgos establecida y la justificación de las exclusiones de los controles del Anexo A de la norma**								
	Empresa:	**Alcaldía de Ibagué, Sistema de Información ERP PISAMI**								
	OBJETIVO DE CONTROL	**CONTROLES**	**APLICABILIDAD**		**EXCLUSIONES**	**JUSTIFICACION**	RL	OC	BR/ RP	RRA
			SI	**NO**						
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN										
	A 5.1 Directrices de la dirección para la gestión de la seguridad de la información	A 5.1.1 Políticas para la seguridad de la información	X			El control aplica, La Alcaldía de Ibagué, tiene aprobada las Políticas de Seguridad, mediante Decreto 1000-0148 de fecha 06/03/20115, por medio del cual se reglamenta el Manual Operativo y Calidad, donde además de lo anterior dando cumplimiento a la ley 712 de 2014, están publicadas en el portal www.ibague.gov.co. Además de lo anterior a través de los procesos de inducción y reinducción a funcionarios y contratistas, se hace la socialización del cumplimiento de estas directrices. Además de lo anterior en el diseño del software de los módulos que conforman la Plataforma PISAMI, (mediante procedimientos de autenticación de contraseñas, gestión de privilegios de usuarios, soporte de mesa de ayuda, bakup, y acciones de estabilización y mejora de los aplicativos) se implementaron controles y validaciones dando cumplimiento a las políticas de seguridad con que cuenta la entidad.	X		X	
		A 5.1.2 Revisión de las políticas para la seguridad de la información	X			El control se e cumple parcialmente, en cuanto al procedimiento de creación y actualización de políticas, sin embargo el seguimiento con eficiencia se realiza, mediante auditorias de a los procesos de información y procedimientos administrativos apoyados por plataformas tecnológica PISAMI, realizada por la Oficina de control Interno demás entes control. Se observa que no se da cumplimiento estricto al procedimiento en cuanto a la revisión y actualización de las políticas de seguridad	X			

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN										
	A 6.1 Organización interna	A 6.1.1 Roles y responsabilidades para la seguridad de la información	X			El control se cumple, La Secretaria de Planeación Municipal, es la responsable de proceso administrativo de gestión de políticas públicas y las secretarias ejecutoras de los procesos de información al que corresponda, en este caso es la Secretaria Administrativa Dirección de Informática (PROCESO: GESTION DE RECURSOS FISICOS Y TECNOLOGICOS - Código: PROGRT-06)	X			
		A 6.1.2 Separación de deberes		X		El control no se cumple, se observa que las funciones de la administración de a base de datos no están separadas de las funciones de desarrollo y soporte de software.			X	
		A 6.1.5 Seguridad de la información en la gestión de proyectos.		X		Actualmente se encuentran implementadas las políticas de seguridad para la plataforma tecnológica PISAMI			X	
	A.7 SEGURIDAD DE LOS RECURSOS HUMANOS									
	A 7.1 Antes de asumir el empleo	A 7.1.1 Selección	X			Dentro de la lisita de chequeo de requisitos de verifican los antecedentes disciplinarios y judiciales dando cumplimiento a la norma.	X			
		A 7.1.2 Términos y condiciones del empleo	X			En las minutas contractuales, existe una obligación específica que garantiza la confiabilidad de la información.	X			
	A 7.2 Durante la ejecución del empleo	A 7.2.1 Responsabilidad de la dirección	X			Actualmente hay un profesional especializado en seguridad de la información, encargado de revisar los documentos, procedimientos y realizando levantamiento de información con el objetivo de actualizar las políticas de seguridad de la Alcaldía de Ibagué.		X		X
		A 7.2.2 Toma de conciencia, educación, y formación en si	X			La alcaldía de Ibagué cuenta con procedimientos de capacitación a servidores públicos, en estas capacitaciones de socializan las políticas de seguridad y su aplicabilidad.		X		
	A 7.3 Terminación y cambio de empleo	A 7.3.1 Terminación o cambio de responsabilidades de empleo	X			La entidad cuenta con políticas de seguridad con directrices específicas sobre el registro de novedades como (terminación, sesión y traslados de funcionarios a otras dependencias) en aras de garantizar integridad de la información		X		X
	A 8.1 Responsabilidad por los activos	A 8.1.1 Inventario de activos	X			La entidad cuenta con un sistema de inventarios denominada SGI, en el cual se registran todos los activos bienes muebles e inmuebles de propiedad de la entidad.	X			X
	A 8.2 Clasificación de la información	A 8.2.1 Clasificación de la información	X			La entidad cuenta con tabla de valoración de la información, donde se clasifican de acuerdo al tipo de información a la que corresponda: datos públicos, privados, semiprivados y confidenciales.	X			

		A 8.2.2 Etiquetado de la información		X		Aunque la entidad cuenta con políticas de manejo y clasificación de la información, no todas, están implementadas a nivel de aplicación, por lo que toda la información suministrada ya sea como dato especifico o por lote (listado, base datos) son solicitadas mediante solicitud al despacho correspondiente y este se encarga de verificar y dar respuesta de acuerdo al tratamiento corresponda el dato requerido.			X	
		A 8.2.3 Manejo de activos	X			Los activos informáticos tangibles (hardware, ups, sistemas de cableado estructurado, impresoras), e inclusive el licenciamiento de software ofimático se gestiona a través del software de control de inventarios SGI. Sin embargo los activos intangibles que corresponden a (bases de datos,), el control y registro se hace a través de transacciones las cuales quedan registrada en archivos tipo Log o historial, la política es no borrar datos (inactivar, si es un dato sensible se ajusta dejando la observación en campos de auditoria).	X		x	
	A.9 CONTROL DE ACCESO									
		A 9.1.1 Política de control de acceso	X			Se han implementado procedimientos técnicos de asignación de IP en la red LAN, permitiendo tener varios segmentos de red por edificios o sedes, de esta manera tienen el control de IP validas con acceso a LAN Además de lo anterior se cuentan con un sistema de gestión de seguridad UTM, que protege la granja de servidores de ataque desde internet. De otra parte todo el acceso a nivel de aplicación se hacen por autenticación de usuarios. Todo lo anterior Dándole aplicabilidad a las políticas de seguridad en lo que tiene que ver con el control todos los accesos			X	X
		A 9.1.2 Política sobre el uso de los servicios de red	X						X	X
	A 9.2 Gestión de acceso de usuarios	A 9.2.1 Registro y cancelación del registro de usuarios	X			Dándole aplicabilidad a la política seguridad todas las novedades de gestión de usuarios y privilegios (registro, cancelación de usuarios) se hace por oficio, suscrito por el responsable del proceso de información. A nivel de aplicación, la Herramienta PISAMI, cuenta con utilidades que permiten realizar la gestionar los requerimientos de los usuarios (activar, inactivar, modificar, asignar privilegios, modificar, retirar).	X		X	
		a 9.2.2 Suministro de acceso de usuarios	X				X		X	
		A 9.2.3 Gestión de derechos de acceso privilegiado	X				X		X	
		A 9.2.4 Gestión de la un. De autenticación secreta de usuarios	X			La plataforma PISAMI, cuentan con módulos de seguridad donde existen roles de consulta, inserción, actualización y borrado sobre los objetos de la BD, los cuales a través de privilegios son concedidos a un usuario. Como se mencionó anteriormente el ERP-PISAMI, a través de un módulo de Administración se configura el acceso del usuario de acuerdo a los privilegios requeridos y autorizado por el responsable del				

						proceso de información. Existen otros aplicativos no integrados al ERP que también cuenta con módulo de administración y se aplica la misma política.				
		A 9.2.5 Revisión de los derechos de acceso de usuarios		X		No existe control automáticos a nivel de aplicación, para que a través o de la validación controle la permanencia de un usuario (término del plazo del contrato o que maneje novedades como (traslados, nombramientos, retiros, comisiones) para que de manera automática no permite el acceso de empleados o funcionarios que ya no están autorizados, todo se hace a través de comunicación interna, una vez se recibe la comunicación se procede a resolver la solicitud en sentido que se haya solicitado.	X		X	X
		A 9.2.6 Retiro o ajuste de los derechos de acceso.	X			La plataforma PISAMI, cuentan con módulos de seguridad donde existen roles de consulta, inserción, actualización y borrado sobre los objetos de la BD, los cuales a través de privilegios son concedidos a un usuario. Como se mencionó anteriormente el ERP-PISAMI, a través de un módulo de Administración se configura el acceso del usuario de acuerdo a los privilegios requeridos y autorizado por el responsable del proceso de información. Existen otros aplicativos no integrados al ERP que también cuenta con módulo de administración y se aplica la misma política.	X		X	
	A 9.3 Responsabilidades de los usuarios	A 9.3.1 Uso de información de autenticación secreta	X			La entidad cuenta con políticas de clasificación de la información en el proceso de gestión documental, en la plataforma tecnológica existe un módulo para gestionar privilegios sobre los usuarios, de esta manera su autoriza el despliegue de la información.	X			
	A 9.4 Control de acceso a sistemas y aplicaciones	A 9.4.1 Restricción de acceso a la información	X			La mayor parte de la información que maneja la entidad está clasificada como publica. Sin embargo a nivel de aplicación y de acuerdo al perfil del usuario, puede este consultar, modificar o insertar información.	X			
		A 9.4.2 Procedimiento de ingreso seguro	X			El acceso a la plataforma se realiza por medio de autenticación de usuarios.			X	X
		A 9.4.3 Sistema de gestión de contraseñas	X			La entidad cuenta con políticas de seguridad donde define claramente, las características de las contraseñas, las cuales deben contener lo mínimo minúsculas y mayúsculas, caracteres, alfanuméricas.			X	
		A 9.4.4 Uso de programas utilitarios privilegiados	X			La entidad cuenta con software ofimático debidamente licenciado y actualizado.	X		X	

		A 9.4.5 Control de acceso a códigos fuente de programas.	X			La Alcaldía de Ibagué, cuenta con un datacenter y tiene equipos servidores de desarrollo, pruebas, base de datos y aplicaciones, de acuerdo a esto están configurados los acceso dependiendo el tipo de usuario (desarrolladores, ingenieros soporte, administrador de sistemas y usuarios de los aplicativos).			X	
	A. 11 SEGURIDAD FISICA Y DEL ENTORNO									
	A 11.1 Áreas seguras	A 11.1.1 Perímetro de seguridad física	X			La entidad cuenta con un espacio datacenter el cual está protegido con puerta de seguridad, chapa de seguridad, aire acondicionado y extintor.			X	X
		A 11.1.2 Controles de acceso físicos		X		No cuenta con sistema biométrico ni cámaras internas.				X
		A 11.1.3 Seguridad de oficinas, recintos e instalaciones	X			La ubicación del datacenter se encuentra resguardada con chapas de seguridad y acceso restringido.			X	X
		A 11.1.4 Protección contra amenazas externas y ambientales	X			La entidad cuenta con un espacio datacenter el cual está protegido con puerta de seguridad, chapa de seguridad, aire acondicionado y extintor.			X	X
	A 11.2 equipos	A 11.2.1 Ubicación y protección de los equipos	X			La infraestructura computacional se encuentra protegida, por energía regulada (el edificio Central y Las Sedes) cuentan sistema de cableado estructurado y ese a su vez se encuentra protegido con sistemas de energía ininterrumpida (UPS)				X
		A 11.2.2 Servicios de suministro	X			Todos los armarios de comunicación están protegidos con chapas de seguridad.				X
		A 11.2.3 Seguridad en el cableado	X			La entidad cuenta con un cableado estructurado certificado categoría 6.				X
		A 11.2.4 Mantenimiento de equipos		X		Los sitios de trabajo son muy reducidos, y existen varias entidades ubicadas en la misma edificación, como la contraloría, concejo, personería y la alcaldía.				
		A 11.2.5 Retiro de activos	X			La instalación es realizada por un técnico de la dirección de informática.				
		A 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	X			En cuanto a seguridad todas las dependencias cuentan con vigilancia de seguridad las 24 horas. Sin embargo todos los activos informáticos tangibles y que estén registrados debidamente en el inventario de bienes muebles e inmuebles esta protegidos con una póliza global contra todo daño. Los demás activos correspondientes a base de datos están, se reguardan mediante copias de seguridad y backup a través de almacenamiento en la nube provista por un tercero.		X		X
		A 11.2.7 Disposición segura o reutilización de equipos	X			De acuerdo a las políticas de la información, se realizan los Backup a las base de datos que se encuentran en custodia por parte del grupo de Informática, los archivos tipo texto, hojas de cálculo los custodia cada responsable del proceso de información, sin embargo la oficina de informática apoya el procedimiento de copia o Backup al ser		X		X

						necesario.				
		A 11.2.8 Equipos de usuario desatendido	X			Se encuentran en custodia por el almacén de la entidad.				X
		A 11.2.9 Política de escritorio limpio y pantalla limpia.		X		La entidad no cuenta con esta política.			X	
	A. 12 SEGURIDAD DE LAS OPERACIONES									
	A 12.1 Procedimientos operacionales y responsabilidades	A 12.1.1 Procedimientos de operación documentados	X			En las secciones de inducción y reinducción, es darle alcance para la aplicabilidad de las políticas de seguridad, teniendo en cuenta que unas de las principales herramientas de trabajo es el ERP PISAMI, además de lo anterior se explica a los funcionarios cuales son los objetivos y alcances del manual de operaciones y también como acceder a la información, trámites y servicios publicados en el portal web de la Alcaldía de Ibagué.				
		A 12.1.2 Gestión de cambios	X			Cumple parcialmente, los cambios, ajustes o nuevos desarrollos de software se realizan por escrito, la dirección de informática, realiza mesas de trabajos técnicas donde deciden si el requerimiento procede y lo comunican generando las acciones pertinentes para cada caso.			X	X
		A 12.1.3 Gestión de capacidad	X			Dentro de los procedimientos administrativos de la dirección de Informática, está el Mantenimiento Preventivo y Correctivo se realiza periódicamente a los equipos tipo servidor, se examinan los eventos de alarmas como alarmas, además de lo anterior cuando presentan fallas se interviene de manera inmediata. Sin embargo es necesario destacar que la monitorización no se realiza de manera permanente.				X
		A 12.1.4. Separación de los ambientes de desarrollo, pruebas y operación	X			La Alcaldía de Ibagué, a través de la dirección de informática, tiene una metodología definida, en el desarrollo de software, tiene procedimientos claros en cada una de las fases (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización) cada fase cuenta con un esquema de base de datos independiente o compartida dependiendo del alcance de la etapa en la Implementación del software,				X

	A 12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos		X		Cumple parcialmente, debido a que hay equipos obsoletos en su hardware, y no son compatibles con la versión de antivirus que dispone la entidad, en varios ocasiones toca recurrir a programas free que protejan el equipo.				X
	A 12.3 Copias de respaldo	A 12.3.1 Respaldo de la información	X			Se realizan Copias de Seguridad con una frecuencia Diaria, se envían a la Nube a través de la plataforma de una entidad externa y además dentro de la entidad se almacenan la información en servidores independientes.		X	X	X
	A 12.4 Registro y seguimiento	A12.4.1 Registro de eventos		X		La dirección de informática tiene la responsabilidad de estar monitoreando los servidores y bases de datos,				X
		A12.4.2 Protección de la información de registro	X			Como se han mencionado en otros controles, solo se tienen acceso los usuarios debidamente autorizados mediante procedimientos de autenticación dispuestos a nivel de aplicación, además de lo anterior mediante la asignación de privilegios de conexión y acceso a la base de datos.			X	X
		A12.4.3 Registros del administrador y del operador		X		Se observa que las actividades de los administradores no son monitoreadas, las de los usuarios finales se registran en archivos de auditoria.				X
	A 12.5 Control de software operacional	A 12.5.1 Instalación de software en sistemas operativos	X			La directriz de la política de seguridad es clara, las lobares de instalación y configuración de sistemas operativos básicos son labores de exclusivas de la dirección de informática, se controla a nivel de equipos por medio de usuario administrador del cual tiene solo acceso la dirección de informática.				X
	A 12.6 Gestión de la vulnerabilidad técnica	A 12.6.1 Gestión de las vulnerabilidades técnicas		X		No se realizan pruebas de Pentest, con herramientas que permitan medir detectar las vulnerabilidades de la plataforma Tecnológica incluyendo PISAMI			X	X
		A 12.6.2 Restricción sobre la instalación de software	X			La directriz de la política de seguridad es clara, las lobares de instalación y configuración de sistemas operativos básicos son labores de exclusivas de la dirección de informática, se controla a nivel de equipos por medio de usuario administrador del cual tiene solo acceso la dirección de informática.				X
	A 12.7 Consideraciones sobre auditorias de sistemas de información	A 12.7.1 Información controles de auditorías de sistemas	X			El ERP PISAMI, cuenta con el gestor de BD Oracle cuenta con sistema de auditoria propia la cual se encuentra habilitada				X
	A. 13 SEGURIDAD DE LAS COMUNICACIONES									
	A 13.1 Gestión de la seguridad de las redes	A 13.1.1 Controles de redes		X		La entidad no cuenta con herramientas de análisis de trafico IPS e IDS			X	X
		A 13.1.2 seguridad de los servicios de red	X			La Alcaldía de Ibagué, cuenta con un Firewall, el cual filtra tráfico y neutraliza a ataques de virus			X	X

		A 13.1.3 separación en las redes	X			Cumple parcialmente, Se han implementado procedimientos técnicos de asignación de IP en la red LAN, permitiendo tener varios segmentos de red por edificios o sedes, de esta manera tienen el control de IP validas con acceso a LAN Además de lo anterior se cuentan con un sistema de gestión de seguridad UTM, que protege la granja de servidores de ataque desde internet. De otra parte todos los accesos a nivel de aplicación se hacen por autenticación de usuarios. Todo lo anterior Dándole aplicabilidad a las políticas de seguridad en lo que tiene que ver con el control todos los accesos				
	A 13.2 Transferencia de información	A 13.2.1 Políticas y procedimientos de transferencia de información	X			Aunque existen una directriz para la transferencia e intercambio de información con algunas entidades externas, la entidad toma en cuenta los controles de las la tablas de clasificación de la información y de acuerdo a eso da el tratamiento, previa autorización del responsable del proceso de información antes de genera cualquier tipo de entrega	X			X
		A 13.2.2 Acuerdos sobre transferencia de información	X				X			X
	A.14 adquisición, desarrollo y mantenimiento de sistemas									
	A 14.1 Requisitos de seguridad de los sistemas de información	A 14.1.1 Análisis y especificación de requisitos de si	X			La plataforma PISAMI, fue desarrollada, para que cumpliera con los objetivos de los pilares de un sistema de seguridad de la información (disponibilidad, integridad, confidencialidad y autenticidad), es así que los diferentes módulos cuenta con seguridad tanto para el acceso, proceso, y salidas de información. De otra parte comparten Base de datos es única permitiendo compartir datos entre los módulos que conforman el ERP-PISAMI.			X	X
		A 14.1.2 seguridad de servicios de las aplicaciones en redes públicas		X		La entidad cuenta un sistema de Gestión de seguridad a nivel firewall, sin embargo, no existe un sistema de seguridad a nivel de base de datos que garanticen la integridad y autenticidad de la información contenida en las bases de datos, contra a taques ataques de inyección SQL			X	X
		A 14.1.3 Protección de transacciones de los servicios de las aplicaciones		X					X	X
	A 14.2 Seguridad en los procesos de desarrollo y soporte	A 14.2.1 Política de desarrollo seguro	X			La entidad cuenta con un procedimiento para la solicitud de ajustes, actualización y nuevos desarrollos de software, además de contar plan estratégico desarrollo de software.			X	
		A 14.2.2 Procedimiento de control de cambios en sistemas	X			La dirección de Informática, lleva un control de las versiones de las aplicaciones desarrolladas, dando cumplimiento al procedimiento administrativo, se notifica a través de comunicación interna todas las mejoras a los módulos y cuando estas son publicadas y puestas en producción			X	X

		A 14.2.3 Revisión técnicas de las aplicaciones después de cambios en la plataforma de operación	X			La entidad cuenta con un protocolo para la aplicación de pruebas a los Sistemas de información desarrollados, la dirección de informática, tiene definido una metodología desarrollo de software la cual tiene procedimientos claros en cada una de las fase (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste, Puesta en Operación, y Estabilización) cada fase tiene un esquema de base de datos independiente o compartido dependiendo el alcance de la etapa en la Implementación de software, además de estar contemplado los niveles de seguridad que garanticen los principios de seguridad de información (Disponibilidad, Confidencialidad, Integridad, Autenticidad)			X	X
		A 14.2.4 Restricciones en los cambios a los paquetes de software	X						X	X
		A 14.2.5 Principios de construcción de los sistemas seguros	X						X	X
		A 14.2.6 Ambiente de desarrollo seguro	X			El equipo servidor donde se encuentra el código fuente de las aplicaciones, hace parte de las aplicaciones que componen la plataforma PISAMI, hace parte de la granja de servidores de propiedad de la Alcaldía de Ibagué, el cual está protegido con medidas de seguridad tanto físicas como de ataques cibernéticos.				X
		A 14.2.7 Desarrollo contratado externamente		X		Aunque todo el software esta patentado a nombre de la Alcaldía de Ibagué, existen unos servicios paralelos que son necesarios para que el software funciones de manera correcta, servicios tales como Hosting, Internet, almacenamiento Nube se encuentran tercer izados a través de aliados tecnológicos.		X		
		A 14.2.8 Pruebas de seguridad de sistemas	X			La Alcaldía de Ibagué a través de la dirección de Informática, realiza pruebas de funcionalidad a cada una de las aplicaciones que conforman el ERP - PISAMI, para tal fin dispone de una metodología para el desarrollo de software la cual tiene procedimientos claros en cada una de las fase de la implementación (Análisis y Diseño, Desarrollo, Migración, Pruebas, Ajuste) pruebas que deben ser lo suficientemente aceptadas tanto por el grupo técnico como para los usuarios finales antes de la Etapa de entrada en Operación y Estabilización. La fase de pruebas las realizan los desarrolladores a través de casos de pruebas o casos de estudio antes de llevarlos a pruebas con los usuarios finales, procedimiento que es repetitivo hasta que se supere la prueba.			X	X
		A 14.2.9 Pruebas de aceptación de sistemas	X						X	X
	A 14.3 datos de prueba	A 14.3.1 Protección de datos de prueba	X			La dirección de Informática, tiene tanto servidores, gestores de base de datos y metodologías de esquemas de prueba, son datos, Cuando no existen información de la BD, se crean datos de prueba			X	X
	A.15 RELACIONES CON LOS PROVEEDORES									

	A. 15.1 Seguridad de la información en las relaciones con los proveedores	A 15.1.1 Política de seguridad de la información para las relaciones con los proveedores		X		NO se cuenta con directrices, tampoco procedimientos para el manejo de los proveedores, el contacto se tienen a través de los supervisores y solo cuando hay un contrato en ejecución.		X		X
		A 15.1.2 tratamiento de la seguridad dentro de los acuerdos con proveedores	X			La entidad tiene establecidos requisitos y procedimientos de acceso a las instalaciones datacenter, que son los mismos que se aplican a funcionarios, una vez se hagan mesas técnicas y se establezcan e identifiquen obligaciones contractuales.		X		X
		A 15.1.3 Cadena de suministro de tecnología de información y comunicación		X		No se tiene tienen directrices de seguridad de la información con terceros que incluyan los requisitos para tratar los riesgos asociados a la cadena de suministro				X
	A 15.2 Gestión de la presentación de servicios con los proveedores	A 15.2.1 Seguimiento y revisión de los servicios de los proveedores	X			El seguimiento a la prestación de servicios prestados por de terceros, se hace través de la supervisores de los contratos.				X
		A 15.2.2 Gestión de cambios en los servicios de los proveedores	X			La entidad garantiza la gestión de cambios de suministro de servicios por parte de terceros, a través de los análisis realizados en los estudios previos, mediante otro si a los contratos de compraventa o suministro de elementos. Además de la apropiación de recursos.	X			X
	A.16 Gestión de incidentes de seguridad de la información	A 16.1.1 Responsabilidades y procedimientos		X		La Alcaldía de Ibagué, a través de la dirección de Informática, no cuenta con procedimientos para la identificación de incidente, evaluación y respuesta de seguridad de la información. Se interviene la situación cada vez que sucede.				X
		A 16.1.2 Reporte de eventos de seguridad de la información		X						X
		A 16.1.3 Reporte de debilidades de seguridad de la información		X						X
		A 16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos		X						X
		A 16.1.5 Respuesta a incidentes de seguridad de la información		X						X
		A 16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	X			Cuando se identifica un hallazgo de fraude, hackeo se realiza análisis archivos log, trazabilidad, copias de seguridad entre otros				X
		A 16.1.7 Recolección de evidencia		X		Cuando se detectan o se intervienen las situaciones, se documentan, y se corrigen.				X

	A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO									
	A 17.1 Continuidad en seguridad de la información	A 17.1.1 Planificación de la continuidad de la seguridad de la información		X		La Administración Municipal, no tiene un plan de seguridad que garantice el cumplimiento de los pilares del sistema de seguridad de la información,	X			X
		A 17.1.2 Implementación de la continuidad de la si		X		La Alcaldía de Ibagué, no tiene planes de continuidad del negocio, en las políticas tampoco hay directrices y los planes de contingencias que tienen son planteados con los componentes mínimos.	X			X
		A 17.1.3 Verificación, revisión y evaluación de la continuidad de la si		X		La Administración Municipal, no tiene un plan de seguridad que garantice el cumplimiento de los pilares del sistema de seguridad de la información,	X			X
	A 17.2 Redundancias	A 17.2.1 Disponibilidad de instalaciones de procesamiento de información		X		La Disponibilidad de las aplicaciones en cuanto planes de continuidad no está garantizada de manera total, existen una medidas contingentes que podrían mitigar de alguna manera un colapso informático	X			X
	A. 18 CUMPLIMIENTO									
	A 18.1 Cumplimiento de requisitos legales y contractuales	A 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	X			La entidad realiza verificaciones a través de auditoria por parte de la oficina de Control Interno, cumplimiento de la norma en los procedimientos implementados en PISAMI y otras auditorias que realiza MINTIC	X			X
		A 18.1.2 Derechos de propiedad intelectual	X			Todos el software que compone el ERP PISAMI, es de propiedad de la Administración Municipal	X			X
		A 18.1.3 Protección de registros		X		La entidad no tiene documentado el proceso de seguridad y protección de la información.				X
		A 18.1.4 Privacidad y protección de información de datos personales		X		La entidad toma en cuenta los controles de las la tablas de clasificación de la información y de acuerdo a eso da el tratamiento, previa autorización del responsable del proceso de información antes de genera cualquier tipo de entrega				X
	A 18.2 Revisiones de seguridad de la información	A 18.2.1 Revisión independiente de la seguridad de la información	X			La entidad tiene contratado un profesional especializado en seguridad informática, se observa que la política no está actualizados no tiene el alcance a aterrizado al contexto de la seguridad del procedimiento en cuanto a controles y no están cubiertos todos los elementos del sistema de seguridad de la información				
		A 18.2.2. Cumplimiento con las políticas y normas de seguridad		X		No se observan el componente directivo en la monitorización de las políticas, no se realizan comités de seguridad con los altos directivos en donde se revisen con regularidad el cumplimiento de las				

						políticas de seguridad en todas las áreas de la Administración,				
		A 18.2.3 Revisión del cumplimiento técnico		X		Los sistemas se ajustan en cuanto a controles de seguridad, cada vez que se detecta una violación o fuga de información, pero la Administración a través de la dirección de Informática, no realiza revisión periódica de los sistemas con el fin de verificar el cumplimiento de las políticas de seguridad de la información.				

7. CRONOGRAMA DE ACTIVIDADES

Figura 11. Cronograma de Actividades.

Nombre de la tarea	Duración	Comienzo	Fin
Proyecto ethical hacking	16 semanas	semana 1	semana 16
1. Identificar junto con los usuarios responsables de la formulación de las políticas de seguridad de la información los requerimientos, para la actualización de las mismas.	4 semanas	1	4
2. Identificar los principales ataques a la red y base de datos, causas, consecuencias, activos impactados.	4 semanas	5	8
3. Identificar y documentar los requerimientos de hardware y software para la implementación de herramientas y técnicas de Ethical Hacking al esquema servicios base de datos TAO.	4 semanas	5	8
4. Proponer diversas plataformas o herramientas para la detección de vulnerabilidades a la base de datos y solucionar problemas de hackeo y robo de datos.	4 semanas	9	12
5. Realizar una implementación de herramientas y técnicas de ethical Hacking con software descargado de la web que nos permita lo siguiente:	4 semanas	13	16
· Identificar inyección de código malicioso en la base de datos esquema servicios.	1 semana	13	14
· Realizar intrusión autorizada para identificar puertas abiertas y vulnerabilidades de la base de datos.	1 semana	14	15
· Documentación sobre las vulnerabilidades que encontradas con las herramientas ethical hacking utilizadas.	1 semana	14	15
· Realizar pruebas de ataque con distintas herramientas para identificar y clasificar con cada una de ellas opciones seguras para proteger el código.	1 semana	15	16
· Tomar decisiones en cuanto a actualización de software instalado en servidores y reglas de seguridad sobre firewall que afecten la seguridad de la base de datos en el esquema estudiado.	1 semana	15	16

Fuente: Autores

Elaborar y entregar al Director del Área un documento como informe, detallando procedimientos ejecutados y pantallazos de los mismos, vía correo electrónico, al finalizar cada una de las actividades.

8. RECOMENDACIONES

- Tener plan de continuidad del negocio en caso de que la base de datos sufra un daño, ya sea por motivos físicos del servidor, software o por algún evento que afecte el servicio.

- Documentar todos los procesos y procedimientos, realizados por el administrador de la base de datos, el administrador de los servidores y el programador. De esta manera se puede tener claro que se hizo en determinado momento y el por qué.

- Realizar revisión periódica y depuración de los puertos abiertos junto con sus servicios.

- Realizar la adquisición y configuraciones del firewall de la base de datos

- Conseguir un servidor con más capacidad para así poder activar la auditoria propia del gestor de la base de datos.

- Actualización de la versión del sistema de gestor de la base de datos Oracle.

- Documentar toda la información correspondiente a los objetos y sus relaciones dentro de la base datos.

- Siguiendo la Norma ISO 27002, se aplicarían los siguientes dominios de dicha norma con los siguientes controles para su efectivo cumplimiento:

Dominio 5. Política de seguridad

- Creación de la Política de seguridad para la Alcaldía Municipal de Ibagué. Las políticas de seguridad de la información estarán contenidas en un documento aprobado por el comité de seguridad de la entidad.

Control: La entidad deberá rendir y mostrar en Gobierno en línea sobre la creación y aprobación de políticas de seguridad de la información.

- Las políticas de seguridad de la información deberán ser evaluadas cada año y actualizadas por el comité de seguridad de la Alcaldía Municipal de Ibagué.
  Control: Por cada revisión de las políticas de seguridad de la información se debe generar un acta.

Dominio 6. Aspectos organizativos de la Seguridad de la Información

- Responsables de la seguridad de la información. Se crea comité de la seguridad conformado por el director del área de sistemas, el experto de la seguridad de la información y delegado del área de control interno. Este comité tendrá las siguientes responsabilidades:
  . Asignación de responsables de la seguridad de la información.
  . Aprobación de las políticas de seguridad.
  . Actualización de las políticas de seguridad de la información.
  . Vigilar por el cumplimiento de las políticas de la seguridad de la información.
  . Verificar que las políticas de seguridad de la información se encuentren publicadas en el portal web de la Alcaldía Municipal de Ibagué como lo pide Gobierno en Línea.
  Control: El acta de cada comité debe quedar publicado en el intranet de la Alcaldía.

Dominio 9. Control de Acceso

- Control de Acceso. Cada actuación realizada por cualquiera de los usuarios, será controlada mediante creación de usuario, contraseñas y privilegios de acceso a los distintos módulos de los aplicativos.
  Control: Para la creación de un usuario en cualquiera de los aplicativos.
  La solicitud debe venir por escrito y firmada por el jefe inmediato.

  Nombre completo del funcionario.
  Dependencia del funcionario.
  Cedula
  Correo electrónico.

Módulos a los que va a tener acceso
En el caso de ser contratista fecha de finalización del contrato
En caso de ser de planta notificar vacaciones.
Tipo de privilegio (Consulta, Facturación, Actualización, Inserción)

- Creación de contraseñas de usuario. La seguridad de las contraseñas de usuario es responsabilidad de cada usuario.
  Control: Cada contraseña es de mínimo 8 caracteres, alfanuméricos, contienen mayúsculas y minúsculas.
  El aplicativo obliga al cambio de contraseñas cada 3 meses. En caso de olvido de contraseña se encuentra el campo recuperar contraseña.

Dominio 11. Seguridad física y del entorno

- Configuración y administración de las redes. La oficina de informática contratará personal capacita para la implementación y seguimiento de las redes en el palacio municipal.
  Control: La dirección de informática es la responsable de la instalación de la configuración de la red y la configuración de controles de seguridad como firewalls y sistemas de detección de intrusos.
- Creación de usuario de administrador en cada equipo de la administración. Cada equipo de cómputo de la administración municipal tendrá usuario administrador con el que se controlará la instalación y el bloqueo del equipo cuando este desatendido.
  Control: la dirección de informática será la responsable de la creación de cada usuario administrador.
  La instalación de software no autorizado o sin licencia será responsabilidad de cada uno de los servidores públicos.

Dominio 12. Seguridad en las operaciones

- Ambiente de pruebas de desarrollo. La dirección de informática será la responsable de definir los estándares y procedimientos para el manejo del ambiente de pruebas y lo que se aprueba para que sea montado al ambiente de producción.
  Control: para subir cualquier cambio al entorno de producción estos deben pasar por el líder de desarrollo para su respectiva verificación.

Toda solicitud de software nuevo debe venir debidamente sustentado junto con su respectiva necesidad.

- Registros de Auditoria. Los sistemas y aplicativos que almacenen y procesen información crítica para la Alcaldía, contarán con registros de auditoria de cada transacción y de cada usuario.
  Control: Los logs de auditoria deben contener información importante como fecha y hora, campo auditado, transacción realizada y usuario.
  El acceso de estos logs de auditoria será solo para los administradores de las bases de datos.

Dominio 14. Adquisición, desarrollo y mantenimiento de sistemas

- Control de cambios. Cada dependencia puede solicitar un cambio en el desarrollo de software debidamente justificado.
  Control: Si la solicitud del cambio solicitado afecta a una o más dependencias esta se debe realizar por escrito.

Dominio 16. Gestión de incidentes en la seguridad de la información

- Reportes de incidentes. La dirección de informática es responsable de reportar a los entes de control o a la oficina de control interno los incidentes ocurridos.
  Control: Cada incidente debe ser reportado y se debe realizar por escrito dejando evidencia del sucedido.

Dominio 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

- Disponibilidad de los servicios. La administración diseñará un plan de contingencia para garantizar la continuidad de negocio.
  Control: La dirección de informática será la responsable de la creación de las copias de seguridad, custodia y almacenamiento.
  Los procesos y procedimientos deben estar debidamente documentados.

Dominio 18. Cumplimiento

- Revisión del cumplimiento de las políticas de seguridad. Los cumplimientos de las políticas de la información son para todos los servidores públicos de la administración municipal sin importar el rango.
  Control: Se informará a los entes de control sobre el no cumplimiento de las políticas.

9. CONCLUSIONES

- Como se pudo evidenciar, las diferentes herramientas para realizar hacking ético son una gran ayuda para disminuir las vulnerabilidades encontradas en las bases de datos y en los servidores que las almacenan.

- La auditoría propia del gestor de la base de datos no está activa por la poca capacidad de almacenamiento y memoria del servidor que la contiene.

- Podemos concluir que la Base de datos objeto de estudio se encuentra en un estado de baja seguridad respecto a la actualización del sistema gestor de la base de datos, ya que este no tiene más soporte por parte del proveedor.

- La prevención y el uso adecuado de herramientas que determinen vulnerabilidades en los esquemas de una base de datos son altamente necesarias en el proceso de gestión pues el software que contiene la base datos puede ser vulnerado y allí las acciones que se realicen son importantes para establecer mecanismos y controles de seguridad haciendo más confiable, disponible y oportuna la información.

- De acuerdo al cronograma realizado en las fechas programadas se pudo evidenciar que existen vulnerabilidades y que se pueden corregir, todo de la mano de la realización de la auditoria y la actualización adecuada del software que contiene la base datos y la instalación como recomendación del firewall de la base datos.

- Los controles en cuanto a nivel de usuarios software y hardware deben llevar la misma línea establecidas en las políticas de seguridad de la organización y se deben tomar en cuenta nuevos controles de acuerdo a lo que se vaya evidenciando con las auditorias y monitoreo constantes de la operación de la base de datos.

10. DIVULGACIÓN

La divulgación del presente proyecto “ANÁLISIS DE LOS RESULTADOS DE ETHICAL HACKING PARA EL CONTROL DE VULNERABILIDADES DE LA BASE DE DATOS TAO ESQUEMA SERVICIOS DE ALCALDÍA DE IBAGUÉ”, se hará a través del repositorio institucional de la Universidad Nacional Abierta y a distancia UNAD. Donde quedara como referencia para consulta.

Cabe aclarar que las recomendaciones se realizaron en base a los resultados obtenidos con las pruebas realizadas.

11. BIBLIOGRAFÍA

Seguridad cultura de prevención para TI No.19 /agosto-septiembre 2013 disponible en (http://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1659/107.pdf?sequence=1&isAllowed=y)

BONILLA VACA, Carolina Isabel. Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la empresa Automekano cía. ltda., de la ciudad de Ambato". 2017 disponible en (http://repositorio.uta.edu.ec/bitstream/123456789/24534/1/Tesis_t1200mbd.pdf)

JARA Héctor, PACHECO Federico. Ethical Hacking 2.0 Buenos aires 2011-2013 disponible en (https://books.google.es/books?hl=es&lr=&id=PkDCIzakkB4C&oi=fnd&pg=PA4&dq=ethical+hacking+a+bases+de+datos&ots=B3B36Pz44s&sig=lxSj5A3RyBXosdOowv7B2QpaROk#v=onepage&q&f=false)

SQLMAP. Herramienta automática de inyección SQL y adquisición de base de datos disponible en (http://sqlmap.org/)

DUARTE Eugenio. Las 50 mejores Herramientas de Ethical Hacking octubre 15 2014 disponible en (http://blog.capacityacademy.com/2014/10/15/las-50-mejores-herramientas-de-ethical-hacking/)

SQLNINJA..Una herramienta de inyección y adquisición de SQL server. Disponible en (http://sqlninja.sourceforge.net/)

LOBO PARRA Leonard David, Tesis. Plan de gestión de la seguridad de la información de la biblioteca Argemiro Bayona de la universidad francisco de paula Santander Ocaña, mediante la aplicación de la norma ISO 27001 y técnicas de ethical hacking. Ocaña Santander, 2012.Disponible en (http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/325/1/25095.pdf)

COELLO SALAS María Gabriela. Proyecto previo a la obtención del título de ingeniero en sistemas informáticos y de computación. Quito, Noviembre 2012. Disponible en (http://bibdigital.epn.edu.ec/bitstream/15000/5736/1/CD-4677.pdf)

CLARKE Justin. SQL Injection Attacks and Defense.2009.Disponible en (https://books.google.es/books?id=KKqiht2IsrcC&lpg=PP1&dq=sqlinjection&hl=es&pg=PA5#v=onepage&q=sqlinjection&f=false)

HACKINGLOOPS. How to hack Database Online Tutorial Part 1- Basics of Database Hacking. Disponible en (https://www.hackingloops.com/how-to-hack-database-online-tutorial-part-1-basics-of-database-hacking/)

BALOCH Rafay.Ethical Hacking and Penetration testing Guide.2014. Disponible en (https://books.google.es/books?id=fKfNBQAAQBAJ&lpg=PP1&ots=SbHCMk4aZJ&dq=ethical%20hacking%20database%20how%20work&lr&hl=es&pg=PA282#v=onepage&q=ethical%20hacking%20database%20how%20work&f=false)

CHANDOLA Sagar. A tour of Ethical Hacking.2014. Disponible en (https://books.google.es/books?id=d_KqBAAAQBAJ&pg=PA56&dq=ethical+hacking+database&hl=es&sa=X&ved=0ahUKEwiOub-GsIHUAhUJKiYKHbjLBmoQ6AEILjAB#v=onepage&q=ethical%20hacking%20database&f=false)

PRAKASH Abhijeet. Hack the world-Ethical Hacking. Disponible en (https://books.google.es/books?id=o62cCgAAQBAJ&lpg=PT269&dq=ethical%20hacking%20database&hl=es&pg=PT269#v=onepage&q=ethical%20hacking%20database&f=false)

MANUAL Estrategia de Gobierno en Línea. Disponible en (http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf)

GANDINI Isabella. Ley de delitos Informáticos en Colombia. Disponible en (http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia).

20 MINUTOS .EFE Los Hackers Éticos, el peor enemigo de los ciberdelincuentes.2011. Disponible en (http://www.20minutos.es/noticia/1108742/0/hacker/etico/campus/#xtor=AD-15&xts=467263)

A.Esaú. Tutorial Hacking: Razones para realizar un Pentesting a nuestra empresa.2015. Disponible en (https://openwebinars.net/blog/Tutorial-hacking-razones-para-realizar-un-pentesting-a-nuestra-empresa/)

DRAGONJAR. Pruebas de penetración (pentest o pententing). Disponible en (https://www.dragonjar.org/pruebas-de-penetracion.xhtml)

ANEXO A. CARTA DE ACEPTACIÓN PROYECTO

Ibagué, 20 de mayo de 2017

Ingeniero
Luis Fernando Zambrano
Director de Proyecto Seguridad Informática
Universidad Nacional Abierta y a Distancia "UNAD" CEAD Ibagué
Grupo 233006_7

Me dirijo a usted en calidad de Director del Grupo de Informática (E) de la Alcaldía de Ibagué, con el fin de autorizar la ejecución del proyecto de investigación aplicada con el título: "ANÁLISIS PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE ETHICAL HACKING PARA EL CONTROL DE VULNERABILIDADES DE LA BASE DE DATOS TAO ESQUEMA SERVICIOS DE ALCALDÍA DE IBAGUÉ", quien tiene como ejecutores a los Ingenieros de Sistemas: Claudia Lorena Restrepo Ángel y Edwin Geovanny Sánchez Jaramillo, dichos funcionarios pertenecen a la planta de personal de la entidad.

En tal sentido manifiesto, la gratitud de nuestra entidad alcaldía por considerarnos para el desarrollo de dicho proyecto que incidirá de manera positiva en la seguridad del esquema de servicios de la base de datos TAO.

Cordialmente,

LUIS ENRIQUE ALVAREZ
DIRECTOR GRUPO DE INFORMATICA (E)
ALCALDIA DE IBAGUE

Fig. 12. Formato Encuesta Funcionario 1

Entidad: Alcaldía de Ibagué	
Dependencia	Grupo de informática
Nombre Encuestado	Monica Patricia Valbuena Hernandez
Rol dentro de la base de datos	Usuario final ___ Administrador _X_ Programador___

Cuestionario

Pregunta	**SI**	**NO**	**N/A**
¿conoce algún archivo de tipo Log donde guarde información de las transacciones que se realizan en la Base de datos?	X		
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado permisos de Administración del servidor?	X		
¿Existe un administrador que lleve el control de los usuarios?	X		
¿Los perfiles de estos usuarios son gestionados por el administrador?	X		
¿Los accesos a las instancias de la Base de Datos son gestionados?	X		
¿Las contraseñas de los usuarios de la Base de Datos se cambian dependiendo de la situación?	X		
¿Se obliga el cambio de la contraseña de forma automática cada tanto tiempo?		X	
¿Se encuentra registro de todos los intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?		X	
¿La base de datos cuenta con un diseño físico y lógico?		X	
¿El diccionario de datos cuenta con un diseño físico y lógico?		X	
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	X		
¿Los datos utilizados en el entorno de desarrollo, son reales?	X		
¿Las copias de seguridad se efectúan diariamente?	X		
¿Las copias de seguridad son encriptados?		X	

¿Se ha realizado el proceso de restauración de las copia de seguridad, para probar que las mismas se encuentren bien hechas?	X		
¿Se establece la frecuencia con la que se hacen la restauración de las copias?		X	
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?		X	
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	X		
¿Se documentan los cambios efectuados?	X		
¿Hay algún procedimiento para dar de activar a un usuario?	X		
¿Hay algún procedimiento para dar de cancelar o eliminara un usuario?	X		
¿Es eliminada la cuenta del usuario en dicho procedimiento?		X	
¿El motor de Base de Datos soporta herramientas de auditoría?	X		
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?		X	
¿Existen los que permitan tener pistas sobre las acciones realizadas sobre los objetos del base de datos?	X		
Documentos probatorios presentados:		X	
TOTAL			

Fig. 13. Formato Encuesta Funcionario 2

Entidad: Alcaldía Municipal Ibagué	
Dependencia	Informatica
Nombre Encuestado	William Barreto
Rol dentro de la base de datos	Usuario final ___ Administrador___ Programador X

Cuestionario

Pregunta	**SI**	**NO**	**N/A**
¿conoce algún archivo de tipo Log donde guarde información de las transacciones que se realizan en la Base de datos?	✓		
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado permisos de Administración del servidor?		✓	
¿Existe un administrador que lleve el control de los usuarios?	✓		
¿Los perfiles de estos usuarios son gestionados por el administrador?	X		
¿Los accesos a las instancias de la Base de Datos son gestionados?	X		
¿Las contraseñas de los usuarios de la Base de Datos se cambian dependiendo de la situación?	✓		
¿Se obliga el cambio de la contraseña de forma automática cada tanto tiempo?		X	
¿Se encuentra registro de todos los intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?	✓		
¿La base de datos cuenta con un diseño físico y lógico?		✓	
¿El diccionario de datos cuenta con un diseño físico y lógico?		✓	
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?	X		
¿Los datos utilizados en el entorno de desarrollo, son reales?	X		
¿Las copias de seguridad se efectúan diariamente?	✓		
¿Las copias de seguridad son encriptados?	✓		

¿Se ha realizado el proceso de restauración de las copia de seguridad, para probar que las mismas se encuentren bien hechas?	X		
¿Se establece la frecuencia con la que se hacen la restauración de las copias?		X	
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?			X
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?		X	
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	X		
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	X		
¿Se documentan los cambios efectuados?	X		
¿Hay algún procedimiento para dar de activar a un usuario?	X		
¿Hay algún procedimiento para dar de cancelar o eliminara un usuario?	X		
¿Es eliminada la cuenta del usuario en dicho procedimiento?	X		
¿El motor de Base de Datos soporta herramientas de auditoría?	X		
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	X		
¿Existen los que permitan tener pistas sobre las acciones realizadas sobre los objetos del base de datos?	X		
Documentos probatorios presentados:			
TOTAL			

Fig. 14. Formato Encuesta Funcionario 3

Entidad: Alcaldía Municipal de Ibagué			
Dependencia	Informática		
Nombre Encuestado	German Suarez		
Rol dentro de la base de datos	Usuario final X Administrador___ Programador___		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿conoce algún archivo de tipo Log donde guarde información de las transacciones que se realizan en la Base de datos?	X		
¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X		
¿Existe algún usuario que no sea el DBA pero que tenga asignado permisos de Administración del servidor?			X
¿Existe un administrador que lleve el control de los usuarios?	X		
¿Los perfiles de estos usuarios son gestionados por el administrador?	X		
¿Los accesos a las instancias de la Base de Datos son gestionados?			X
¿Las contraseñas de los usuarios de la Base de Datos se cambian dependiendo de la situación?	X		
¿Se obliga el cambio de la contraseña de forma automática cada tanto tiempo?		X	
¿Se encuentra registro de todos los intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			X
¿La base de datos cuenta con un diseño físico y lógico?			X
¿El diccionario de datos cuenta con un diseño físico y lógico?			X
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?			X
¿Los datos utilizados en el entorno de desarrollo, son reales?			X
¿Las copias de seguridad se efectúan diariamente?	X		
¿Las copias de seguridad son encriptados?			X

¿Se ha realizado el proceso de restauración de las copia de seguridad, para probar que las mismas se encuentren bien hechas?			X
¿Se establece la frecuencia con la que se hacen la restauración de las copias?			X
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	X		
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?			X
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?			X
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?			X
¿Se documentan los cambios efectuados?			X
¿Hay algún procedimiento para dar de activar a un usuario?	X		
¿Hay algún procedimiento para dar de cancelar o eliminara un usuario?	X		
¿Es eliminada la cuenta del usuario en dicho procedimiento?			X
¿El motor de Base de Datos soporta herramientas de auditoría?			X
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			X
¿Existen los que permitan tener pistas sobre las acciones realizadas sobre los objetos del base de datos?			X
Documentos probatorios presentados:			
TOTAL			

12. RECURSOS NECESARIOS PARA EL DESARROLLO

Cuadro 13. Recursos para el desarrollo

Recursos	Descripción	Presupuesto
Equipo Humano	**El recurso humano no tendrá costo ya que los funcionarios encargados de las actividades serán funcionarios de planta en la entidad.**	$0
Viajes y Salidas de Campo	**Capacitaciones fuera de la ciudad, trabajo de campo interno en la entidad**	$6.000.000
Equipo y Software	**Servidor de la base de datos servidor de aplicaciones y equipos que van a acceder remotamente a la base datos.**	$0
Materiales y Suministros	**Elementos de Papelería y oficina para trabajar y documentar el proyecto**	$2.000.000
Total		$8.000.000