DISEÑO DE UN PLAN ESTRATEGICO PARA LA SEGURIDAD DE LA INFORMACIÓN TRIBUTARIA EN UNA ENTIDAD PUBLICA

ALEXA MILENA RODRIGUEZ PINTO
ROSALBA ROZO CABALLERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.- IBAGUÉ
2015

DISEÑO DE UN PLAN ESTRATEGICO PARA LA SEGURIDAD DE LA INFORMACIÓN TRIBUTARIA EN UNA ENTIDAD PUBLICA

ALEXA MILENA RODRIGUEZ PINTO
ROSALBA ROZO CABALLERO

Trabajo de grado para optar al título de Especialista en Seguridad informática

Director de Proyecto:
Ingeniero Daniel Andrés Guzmán Arévalo
M.Sc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.- IBAGUÉ
2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____
JURADO

_____
JURADO

Bogotá D. C – Ibagué, 24 de Septiembre de 2015

AGRADECIMIENTOS

Los autores expresan sus agradecimientos:

Al Ingeniero JOHN FREDDY QUINTERO, líder de la especialización y jurado del proyecto.

Al Ingeniero Alejandro Méndez González, Líder Zonal de la Escuela de Ciencias Básicas, Tecnología e Ingeniería Caed Ibagué.

Al Ingeniero Salomón González García, Gestor de Informática en Computadores para Educar.

Al Ingeniero José Miguel Herrán Suárez, Líder Nacional Tecnología en Desarrollo del Software.

Ingeniero Daniel Andrés Guzmán Arévalo, Magister en Software Libre, Especialista en Teleinformática.

A la ingeniera Gloria Alejandra Rubio Vanegas, Especialista en Teleinformática.

A todos aquellos por su constante apoyo y sus valiosas orientaciones.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

Gráfica No. 16: ¿Conoce las responsabilidades que tiene como empleado de los bienes y servicios informáticos para cumplir las Políticas y Estándares de Seguridad en las bases de datos?

Gráfica No. 17: ¿Una vez Diseñadas las herramientas de seguridad en la organización, usted recomendaría dar algún tipo de asesoría o capacitación junto con el manual de uso, de cómo funciona la herramienta de administración de seguridad informática?

Gráfica No. 18: Los equipos o activos críticos de información y proceso, ¿están ubicados en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el administrador del área?

Gráfica No. 19: ¿Las estaciones o terminales de trabajo, con procesamientos críticos cuentan con medios de almacenamientos extraíbles?

Gráfica No. 20: ¿Se permite la utilización de correos electrónicos personales y el fácil acceso a páginas de internet en la organización?

Gráfica No. 21: ¿Al terminar una sesión de trabajo en las estaciones, evita dejar encendido el equipo?

Gráfica No. 22: ¿La longitud mínima de caracteres permisibles en su contraseña se establece?

Gráfica No. 23: ¿Se cumplen con los requisitos legales o reglamentarios y las obligaciones contractuales de seguridad?

Gráfica No. 24: ¿Todo el software comercial que utiliza la organización está legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias?

LISTAS DE IMÁGENES

Pág.

LISTAS DE ANEXOS

GLOSARIO

SEGURIDAD INFORMÁTICA: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante

ENTIDAD PUBLICA: Se entiende a toda organización del Estado, con Personería jurídica de Derecho Público, creada por norma expresa en el que se le confiere mandato a través del cual ejerce funciones dentro del marco de sus competencias y atribuciones, mediante la administración de recursos públicos, para contribuir a la satisfacción de las necesidades y expectativas de la sociedad, y como tal está sujeta al control, fiscalización y rendición de cuentas.

INFORMACIÓN TRIBUTARIA: Es el mecanismo de identificación, ubicación y clasificación de los contribuyentes del Impuesto predial, Industria y Comercio, Avisos y Tableros.

OBLIGACIÓN TRIBUTARIA: es el vínculo que se establece por ley entre el acreedor (el Estado) y el deudor tributario (las personas físicas o jurídicas) y cuyo objetivo es el cumplimiento de la prestación tributaria. Por tratarse de una obligación, puede ser exigida de manera coactiva.

IMPUESTOS: es una clase de tributo (obligaciones generalmente pecuniarias en favor del acreedor tributario) regido por derecho público.

IMPUESTO PREDIAL: es aquel tributo que se aplica al valor de los predios urbanos y rústicos.

IMPUESTO DE INDUSTRIA Y COMERCIO: Es el gravamen establecido sobre las actividades industriales, comerciales y de servicios, a favor de cada uno de los distritos y municipios donde ellas se desarrollan, según la liquidación privada

SUJETO ACTIVO: Es aquel que tiene la potestad para exigir el pago de tributos. La Constitución determina que tal potestad recae en el Estado y, en su extensión, en las comunidades autónomas y las corporaciones locales.

SUJETO PASIVO: s aquella persona física o jurídica obligada al cumplimiento de las obligaciones tributarias, puede ser como contribuyente o como responsable.

AMENAZA: hecho que puede producir un daño provocado por un evento natural o antrópico

VULNERABILIDAD: es la incapacidad de resistencia cuando se presenta un fenómeno amenazante o la incapacidad para reponerse después de que ha

ocurrido un desastre. Por ejemplo, las personas que viven en la planicie son más vulnerables ante las inundaciones que los que viven en lugares más altos.

NTC-ISO-IEC27001: es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

ESTRATEGIAS: es un plan que especifica una serie de pasos o de conceptos nucleares que tienen como fin la consecución de un determinado objetivo.

POLÍTICAS DE SEGURIDAD: son el instrumento que adopta la empresa para definir las reglas de comportamiento aceptables. La seguridad de la información y el modo de tratarla no es una excepción. En las siguientes líneas se avanza en los contenidos deseables de dichas políticas y cómo le afectan como trabajador.

RESUMEN

El éxito en el recaudo de los tributos de un municipio o país, depende que la información prevista para su liquidación se encuentre en buen estado, de ahí la necesidad de proteger dicho recurso.

Al realizar un análisis de riesgo se puede evidenciar que los eventos adversos se deben a deficiencias en las políticas de seguridad existentes, imprudencia por parte de los funcionarios, falta de estrategia de la entidad, falta de cultura de seguridad informática y de la prevención de riesgos y su capacidad para aprender de los errores.

Con el objetivo de blindar las bases de datos y proteger los recursos de un municipio, se diseña un plan estratégico para resguardar la información tributaria de cualquier amenaza que pueda ser vulnerable. Este plan consta del fortalecimientos de las políticas de seguridad en las bases de datos, vistas desde diferentes aspectos y que su éxito dependerá del cumplimiento de las fases señaladas.

Índice de Términos- Seguridad informática, Impuestos, Tributos, Vulnerabilidad, Estrategias, NTC-ISO-IEC 2700, Políticas

INTRODUCCIÓN

Hoy en día, la informática se ha convertido en un factor importante en la vida de una empresa, la cantidad de información que actualmente se maneja, hace que el tratamiento automático en las bases de datos sea realmente útil y necesario. En la actualidad los sistemas de información están basados en computadoras que son objetos de gran consideración en la toma de decisiones oportunas, confiables y efectivas en cuanto a técnicas de planificación, programación y administración con el fin de garantizar su éxito, limitar el riesgo, reducir costos y aumentar las ganancias.

La información que se maneja tanto al interior de una organización como hacia el exterior de la misma está expuesta a un gran número de riesgos, los cuales tienen un impacto variable en los atributos de seguridad en las bases de datos: confidencialidad, integridad y disponibilidad. En la actualidad, el principal reto está en entender los riesgos específicos para cada entorno de negocios en particular y también entender, o incluso medir, el impacto que estos riesgos tienen sobre la seguridad en las bases de datos.

Debido a esta razón, nace en las entidades públicas la idea de implementar nuevos sistemas de información para fortalecer las políticas de uso, velando para que se administren eficientemente los procedimientos que se desempeñan.

El Diseño de un plan estratégico que garantice la seguridad de la información tributaria está conformado por procesos donde se evalúan y administran los riesgos apoyados en políticas y estándares que cubran las necesidades de las entidades públicas en materia de seguridad.

Este proyecto se estructurara en base a criterios que permiten resaltar el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades en la seguridad de las bases de datos, tales como:

- ✓ Infraestructura de la Seguridad en las bases de datos
- ✓ Responsabilidad de los Activos de Información
- ✓ Seguridad personal
- ✓ Seguridad física y Ambiental
- ✓ Control de Acceso
- ✓ Lineamientos legales

1. FORMULACIÓN DEL PROBLEMA

1.1 DESCRIPCION

La seguridad informática ha adquirido gran auge dada la aparición de nuevas amenazas en los sistemas informáticos. Los sistemas pueden ser vulnerables y quizás, no se es consciente de lo que un ataque tanto interno como externo puede afectar a una entidad responsable de los recursos del estado.

El uso de los sistemas de información como la principal herramienta para el manejo de los datos, la interoperabilidad de los sistemas operativos, la necesidad de estar en red para compartir los recursos informáticos y el rotación contante de funcionares responsables de los procesos, ha provocado que las entidades públicas sean el objetivo de personas que se las ingenian para lucrar, hacer daño o causar perjuicios.

Por lo anterior se hace necesario invertir el capital económico y humano necesario para fortalecer las políticas de seguridad existentes y prevenir posibles daño o pérdida de información tributaria; evitando el déficit en el recaudo, escasez en la inversión, factores que intervienen directamente en el crecimiento económico que se traduce en mayores ingresos para el municipio encargado.

Con el presente proyecto se pretende diseñar un plan estratégico para la seguridad de la información tributaria, fortaleciendo las políticas de seguridad existentes en las bases de datos y la creación de una cultura de seguridad informática entre los funcionarios para el cumplimiento de las metas propuestas y el buen servicio a los contribuyentes en las próximas vigencias.

1.2 ENUNCIADO DEL PROBLEMA

¿Cuáles serían las consecuencias al no diseñar un plan estratégico para fortalecer las políticas de seguridad que se aplican a las bases de datos en una entidad pública?

1.3 SUBPREGUNTAS

¿Cuáles son las políticas de seguridad que actualmente tiene la entidad pública?
¿Cuáles son las vulnerabilidades que se están presentando en la actualidad?
¿Qué tipo de políticas son viables para aplicarlas en la entidad?

2. JUSTIFICACIÓN

Hoy en día al beneficiarse de las innovaciones tecnológicas para mejorar el rendimiento, atención y servicio, las entidades públicas administradoras de los recursos del estado se ven obligadas a diseñar nuevas políticas de seguridad que les faciliten identificar mediante el análisis de vulnerabilidades los riesgos a que se exponen y así evitar pérdidas sensibles como es la información tributaria contenida en las bases de datos.

Realizar campañas de recuperación de cartera, incentivar con descuentos por pronto pago y ofrecer descuentos en intereses a contribuyentes morosos ha permitido que las entidades públicas crezcan en su recaudo disponible; por lo anterior crece la necesidad fortalecer los procesos, procedimientos y la seguridad en la información y a la vez integrar a todo el personal que interviene en los procesos de consulta y actualización de las bases de datos.

Para evaluar la integridad, confidencialidad y disponibilidad en las bases de datos, así como el control de acceso, consulta y modificación; se analiza el manejo de la información por parte de los funcionarios, se realizan entrevistas al ingenieros de apoyo y a los directores de áreas, emplean encuestas a una muestra representativa de funcionarios con el fin de medir el cumplimiento de las políticas y se identifican qué acciones inseguras exponen y comprometen la información

De acuerdo al estado real de la seguridad en la entidad, al análisis de los resultados obtenidos y a la experiencia durante el desarrollo del presente proyecto, se propone diseñar un plan estratégico para la seguridad de la información tributaria, fortaleciendo las políticas de seguridad en las bases de datos, la recuperación de la misma ante posibles fallas en los procesos y la responsabilidad en el manejo de los procedimientos en el interior de la entidad, minimizando las potenciales amenazas que pueden ser introducidas accidentalmente o deliberadamente.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Plan estratégico para proteger la información tributaria de accesos no autorizados y amenazas en una entidad pública.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar las áreas vulnerables ataques informáticos en la entidad pública.
- ✓ Determinar el estado actual de la seguridad en las bases de datos en la entidad, con el fin de aplicar las medidas necesarias.
- ✓ Proteger los recursos que administran la información tributaria, la cual es utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información.
- ✓ Establecer un Diseño de seguridad en las bases de datos aplicables a las necesidades requeridas.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES

Con el objetivo de contar con una guía para la protección de información, se elaboran las políticas y estándares de seguridad en las bases de datos tomando en cuenta el estándar de seguridad de información ISO/IEC 27001, Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad en las bases de datos. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones[1].

En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en AENOR. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC27001), Chile (NCh-ISO27001) Uruguay (UNIT-ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

4.2 MARCO CONCEPTUAL

Sistema de Seguridad Informática: es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados[2].

La seguridad informática, es la aceptación clara de cada uno de los usuarios del sistema informático de la compañía, en conocer las PSI, herramienta que

[1] FASK's El portal de ISO 27001 en Español. http://www.iso27000.es/iso27000.html

[2] Elvira Mifsud. Monográfico: Introducción a la Seguridad Informática, Observatorio Tecnológico, Marzo 2012 http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

permite adoptar una cultura de seguridad informática, orientado a proteger el activo informático y estratégico de la compañía, los cuales deben estar alineados con los objetivos del negocio y los criterios de seguridad informática considerados por *El Information Technology Evaluation Criteria* (ITSEC)" mencionados por: (Romero 2003 p.35). Que para la seguridad informática se debe tener en cuenta como:

- ✓ La integridad: Consiste en garantizar que los datos sean los reales y que el activo no ha sido alterado de manera no autorizada.

- ✓ Confidencialidad: Garantizar que la información sea accedida solo por personal debidamente autorizado y tengan acceso a los recursos que se intercambian.

- ✓ Disponibilidad: Garantizar que la información siempre esté disponible para el usuario que lo requiere o final.

- ✓ Privacidad: Los componentes del sistema son accesibles solo para el personal debidamente autorizado.

- ✓ No repudio: Garantizar de que no puedan negar una operación realizada o no pueda alegar desconocer el hecho.
- ✓ Autenticación: asegurar que el acceso a los recursos del sistema informático, solo se realice por personal autorizado y asegura el origen y destino en las bases de datos.

- ✓ Control: asegurar su conformidad con la estructura de seguridad informática y procedimientos establecidos por la compañía en cuanto el acceso a la información y el monitoreo de los usuarios autorizados.

- ✓ Auditoria: determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema comprobando la idoneidad de los controles.

- ✓ La seguridad informática, es la aceptación clara de cada uno de los usuarios del sistema informático de la compañía, en conocer las PSI, herramienta que permite adoptar una cultura de seguridad informática, orientado a proteger el activo informático y estratégico de la compañía[3], los cuales deben estar alineados con los objetivos del negocio y los criterios.

- ✓ Política de Seguridad: Es una declaración de intenciones de alto nivel que cubren la seguridad de los sistemas informáticos y que proporciona las

[3] Bella Romero (6 SlideShares) , mananger at PROTSEIN, Políticas de seguridad: http://es.slideshare.net/bellaroagui/politicas-deseguridad-13610538

bases para definir y delimitar las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

- ✓ Plan de seguridad: Es el conjunto de decisiones que definen cursos de acción futuros, así como medios que se van a utilizar para conseguirlos.

- ✓ Procedimiento de Seguridad: Es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de Seguridad permiten aplicar e implantar Políticas de Seguridad que han sido aprobadas por la organización.

- ✓ Seguridad informática en bases de datos: La seguridad informática en una base de datos es crítica, debido a que se podría considerar como la caja fuerte de una compañía, en donde la mayoría en las bases de datos es sensible y de mucha importancia por guardarse las transacciones financieras de la compañía. Una base de datos se puede definir como una recopilación de información sobre diversos aspectos tales como: personas, productos, pedidos, contabilidad, transacciones, etc. Por lo cual se debe contemplar un buen plan de seguridad informática para que sea efectiva, para ello necesita contar con elementos indispensables de apoyo: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.

Ante la necesidad de manejar grandes volúmenes de información y compartir con un conjunto de clientes a través de una interfaz única y bien definida de una manera segura, surgen los servidores de base de datos, quienes tienen el control sobre los datos a través de un programa que provee servicios de base de datos a otros programas de aplicación de gestión de base de datos u otras computadoras (servidores), dedicadas a ejecutar programas que prestan el servicio, definido por el modelo o arquitectura cliente-servidor.

- ✓ Amenazas: Eventos, hechos o tendencias en el entorno de una Organización que inhiben, limitan o dificultan su desarrollo operativo.

- ✓ Debilidades: Actividades o atributos internos de una Organización que inhiben o dificultan el éxito de la Entidad.

- ✓ Fortalezas: Actividades y atributos internos de una Organización que contribuyen y apoyan el logro de los objetivos de la Entidad[4].

- ✓ Estrategias: es un conjunto de acciones que se llevan a cabo para lograr un determinado fin. La palabra estrategia significa literalmente "guía de los ejércitos". "Estrategia es la determinación de los objetivos a largo plazo y la elección de las acciones y la asignación de los recursos necesarios para conseguirlos" A. Chandler.

4.2.1 Planeación Estratégica

Es el arte y ciencia de formular, implantar y evaluar decisiones interfuncionales que permitan a la organización llevar a cabo sus objetivos.

4.2.1.1 Etapas de la Planeación estratégica:

- ✓ Formulación de las Estrategias: incluye el desarrollo de la misión del negocio, la identificación de las oportunidades y amenazas externas a la organización, la determinación de las fuerzas y debilidades internas, el establecimiento de objetivos a largo plazo, la generación de estrategias alternativas, y la selección de estrategias específicas a llevarse a cabo.

- ✓ Implantación de Estrategias: requiere que la Entidad establezca objetivos anuales, proyecte políticas, motive empleados, y asigne recursos de manera que las estrategias formuladas se puedan llevar a cabo; incluye el desarrollo de una cultura que soporte las estrategias, la creación de una estructura organizacional efectiva, mercadotecnia, presupuestos, sistemas de información y motivación a la acción.

- ✓ Evaluación de Estrategias: (a) revisar los factores internos y externos que fundamentan las estrategias actuales; (b) medir el desempeño, y (c) tomar acciones correctivas. Todas las estrategias están sujetas a cambio.

[4] Diseño e implementación de un plan estratégico para la empresa Disempack Ltda, Andrés Felipe cano del castillo diana Alejandra Cifuentes Salazar
http://repository.lasalle.edu.co/bitstream/handle/10185/2984/T11.11%20C165d.pdf?sequence=2
Gestión estratégica organizacional, edited by Jorge Eliécer prieto herrera.

- ✓ ISO/IEC 27000. Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización[5].

- ✓ Plan de Contingencia: El plan de contingencia es un procedimiento alternativo para el desarrollo normal de las actividades de la compañía, aunque algunas de sus funciones se hubiesen dañado por accidentes internos o externos; tener un plan de contingencia no significa que reconozca la ineficiencia de la compañía, por el contrario es estar preparados, para superar cualquier eventualidad que pueda acarrear pérdidas materiales, de información y personales, con el fin de hacer frente a futuros acontecimientos para lo cual se debe estar preparados con el único fin de dar continuidad a las actividades de la compañía.

Para la elaboración de un buen Plan de Contingencia se debe dividir en cuatro etapas, las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro:

- ✓ Evaluación. Los responsables de la Planificación, deben evaluar constantemente los planes creados, del mismo modo deberán pensar en otras situaciones que se pudiesen producir.

- ✓ Planificación. Teniendo en cuenta la probabilidad y el impacto de los riesgos existentes en la compañía, los cuales pueden causar un siniestro, sirviendo este como punto de partida para planificar las respuestas en caso de emergencia, se debe trabajar con hipótesis y desarrollar los posibles escenarios de solucionar la emergencia.

- ✓ Pruebas de viabilidad. Se trata de demostrar cada uno de los procedimientos que se están utilizando estén completos y de acuerdo a lo establecido, los recursos materiales están disponibles, para cuando estos se vayan a utilizar; las copias sean actualizadas y estén disponibles, y cada uno de los empleados participantes del grupo se encuentren preparados. Además, se debe documentar cada una de las pruebas que se realice y se tenga planeado, determinar el procedimiento de cada prueba, ejecutar cada una de las pruebas documentadas en base a los resultados obtenidos, actualizar el plan de contingencia de acuerdo a los procedimientos y calendarios de mantenimiento establecidos.

- ✓ Ejecución. Cuando un siniestro se materializa, el grupo de contingencia, debe regirse al plan de contingencia diseñado y los procesos planeados y validados, dando respuesta inmediata para dar continuidad a los servicios informáticos.

[5] FASK's El portal de ISO 27001 en Español. http://www.iso27000.es/iso27000.html

Entre los programas de implementación de la seguridad informática se debe tener diseñado un buen plan de contingencia que a la compañía le permita salvaguardar sus activos de información con las siguientes características[6]:

- ✓ Aprobación: el plan debe ser aprobado por la dirección y aceptado por los usuarios y la auditoria.

- ✓ Flexibilidad: no debe presentar situaciones individuales de desastre, debe estar especificado mediante guías.

- ✓ Mantenimiento: debe ser fácilmente actualizable y evitar especificar al mínimo detalle.

- ✓ Costo-efectividad: la proporción de inversión entre las medidas a aplicar y las ventajas que se conseguirán deben ser justas y razonables.

- ✓ Repuesta organizada: la respuesta a un plan de emergencia inmediata debe proporcionar una lista de acciones y servicios ante el desastre, para ello se debe incluir listas de teléfonos y direcciones de individuos involucrados en el plan, para poder contactar con ellos.

- ✓ Responsabilidad: las responsabilidades asignadas a cada individuo determinada en las funciones como respuesta al plan.

4.3 MARCO CONTEXTUAL

Para el desarrollo del presente proyecto y optar el título de especialista en seguridad informática, se utiliza una Entidad Pública encargada de la gestión financiera, económica, fiscal y presupuestal a través del recaudo optimo y preciso, y que por efectos de seguridad en las bases de datos se manejara de forma prudente.

La entidad pública se encuentra dividida en 5 grupos de trabajo como son: Tesorería, Rentas, Presupuesto, Contabilidad y Grupo Informático y Telecomunicaciones. Actualmente la entidad cuenta con tres Ingenieros de sistemas que brindan soporte de manera general, los cuales dependen directamente del Grupo Informático, compuesto por el Director, Ingenieros desarrolladores, Auxiliares de mantenimiento y dos Ingenieros supervisores de los procesos y proyectos.

[6] Privacy Rights Clearinghouse, Empowering Consumers. Protecting Privacy. Cómo Proteger su Computadora y su Privacidad. https://www.privacyrights.org/pi36

Los usuarios que tienen acceso a las bases de datos y a los sistemas de información acceden a este por medio de computadores asignada por la misma entidad, quien cuenta con alrededor de 210 funcionarios activos, de los cuales alrededor de 30 son considerados usuarios principales debido a que participan en los procesos de actualización y liquidación de los diferentes impuestos.

Se utilizan medios de comunicación como: fibra óptica, cable UTP, Router, red telefónica entre otros, ubicadas en las diferentes dependencias. El estudio se realiza únicamente en el manejo en las bases de datos de los diferentes impuesto.

4.4 MARCO LEGAL

Con el objetivo de contar con una guía para la protección de las bases de datos en una entidad de pública, se elaborarán nuevas políticas y estándares de teniendo en cuenta el manual del INTECO sobre un Sistema de Gestión de Seguridad en las bases de datos según norma UNE-ISO27000 disponible en la web del INTECO bajo licencia CC, el esquema del SGSI según ISO27001 engloba un marco legal completo, compuesto por las siguientes leyes:

4.4.1. Ley Orgánica 15/99 de Protección de Datos de Carácter Personal

Esta ley se complementa con el reglamento estipulado en el Real Decreto RD 1720/2007.

El objetivo de esta Ley es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

Los derechos recogidos en la LOPD son:

Las personas de las que se almacena datos de carácter personal, tienen una serie de derechos amparados por esta ley:

- ✓ Derecho de información: Cuando alguien proporciona sus datos debe ser informado de que van a ser almacenados.

- ✓ Derecho de acceso, cancelación, rectificación y oposición: La persona puede ver la información que se dispone de él, puede cambiar esos datos para que sean correctos y exactos, cancelar la información que se almacene de él y oponerse a que se almacene.

4.4.2. Ley 34/2002 de servicios de la sociedad en las bases de datos y de comercio electrónico (LSSI)

Esta Ley se encarga de regular las obligaciones de los prestadores de servicios y los servicios que prestan. Entre las obligaciones que estipula la Ley están:

- ✓ Los prestadores de servicios deben facilitar sus datos de contacto.
- ✓ Deben colaborar con las autoridades, reteniendo los datos de conexión y tráfico durante 12 meses.
- ✓ Los que albergan datos proporcionados por un cliente, no serán responsables por la información almacenada a petición del destinatario, siempre que:

  No tengan conocimiento efectivo de que la actividad o la información almacenada son ilícitas o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Cuando transmitan información de terceros, los proveedores de servicio no tendrán responsabilidad al respecto si:

- ✓ No modifican la información.
- ✓ Permiten el acceso a ella sólo a los destinatarios autorizados.
- ✓ Actualizan correctamente la información.
- ✓ No utilizan su posición con el fin de obtener datos sobre la utilización en las bases de datos.
- ✓ Se retire la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto sepan que ha sido retirada del lugar de la red en que se encontraba, o que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

4.4.3 Ley 32/2003, general de telecomunicaciones

El objeto de esta ley es la regulación de las telecomunicaciones. Entre los objetivos de esta Ley están:

- ✓ Fomentar la competencia.
- ✓ Garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas.
- ✓ Promover el desarrollo del sector de las telecomunicaciones.
- ✓ Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones.
- ✓ Defender los intereses de los usuarios.
- ✓ Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
- ✓ Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
- ✓ Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

4.4.4 Ley 59/2003 de firma electrónica

Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel, por lo que tanto su generación como su utilización deben ser cuidadosamente controladas para evitar problemas.

4.4.5. R.D.L, 1/1996 Ley de Propiedad Intelectual

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor y le da la plena disposición y el derecho exclusivo a la explotación de la obra. Las obras pueden estar expresadas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro como:

- ✓ Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, etc.
- ✓ Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.
- ✓ Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.
- ✓ Las obras fotográficas.
- ✓ Los programas de ordenador.

Al amparo de esta Ley, las organizaciones protegen su conocimiento y las obliga a respetar el de las demás. El otro punto relevante en el ámbito de la seguridad en las bases de datos es la obligación de contar únicamente con software original (propietario o libre), ya que la utilización de software sin licencia sería una infracción de la Ley.

4.4.6 Ley 17/2001 de Propiedad Industrial

Es la que regula los derechos sobre:

- ✓ Las marcas.
- ✓ Los nombres comerciales.

El organismo que se encarga de mantener el registro de marcas es la Oficina de Patentes y Marcas. Para tener derechos de propiedad sobre una marca hay que registrarla en dicha Oficina.

4.4.7 Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos

Los puntos más destacables de la Ley son:

- ✓ Los ciudadanos verán reconocidos nuevos derechos en sus relaciones con las administraciones públicas.
- ✓ Se creará la figura del Defensor del Usuario.
- ✓ Los trámites y gestiones podrán hacerse desde cualquier lugar, en cualquier momento.

- ✓ La administración será más fácil, más ágil y más eficaz.

- ✓ Los ciudadanos pasan a tomar la iniciativa en sus relaciones con la administración.

Contará con un Esquema Nacional de Seguridad y otro de Interoperabilidad, para que los servicios ofrecidos cuenten con un mínimo nivel de seguridad y las distintas administraciones puedan comunicarse con fluidez[7].

4.5 Estándares normativos.

Los estándares normativos más destacados para la implementación de la seguridad informática están:

- ✓ **ISO 27001-2005.** Estándar Internacional proporciona un modelo para: establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad en las bases de datos (SGSI) en una compañía. Permite evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad en las bases de datos.

- ✓ **ISO 27002** Recopilación de buenas prácticas para un SGSI en la compañía la cual contiene recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una compañía y describe los aspectos a analizar para garantizar la seguridad en las bases de datos y especifica los controles y medidas recomendables a implementar[8].

- ✓ **ISO 27005-2008**. Establece las directrices para la gestión del riesgo en la seguridad en las bases de datos. para lo cual previamente se debe tener conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad en las bases de datos.

4.6 Leyes y Decretos Colombianos.

Las leyes, resoluciones y circulares creadas en Colombia en pro de la protección de los medios informáticos, la información y el comercio electrónico, se destacan los siguientes:

---

[7] Seguridad Información -Blog de seguridad de la información: Marco legal de la ISO 27001
Posted on September 21, 2011 by Emaza http://www.seguridadinformacion.net/marco-legal-de-la-iso-27001/
[8] An Introduction to ISO 27001, ISO 27002....ISO 27008: http://www.27000.org/

- ✓ Ley 527 de 1999. COMERCIO ELECTRÓNICO Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"[9].

- ✓ Ley 962 de 2005[10]. Con esta Ley invita a los organismos, que ejercen funciones públicas a utilizar medios tecnológicos integrados con el apoyo del ministerio de comunicaciones, para disminuir tiempos y costos en la realización de gestiones administrativas, aplicando los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa y deberá garantizar los principios de autenticidad, disponibilidad e integridad. Para el efecto, podrán implementar las condiciones y requisitos de seguridad informática que para cada caso sea procedentes, sin perjuicio de las competencias que esta materia tengan algunas entidades especializadas. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos (GALLO 2005).

- ✓ Ley 1273 de 2009[11]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección en las bases de datos y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías en las bases de datos y las comunicaciones, entre otras disposiciones, como penas de prisión de 120 meses y multa de hasta 1500 salarios mínimos legales mensuales vigentes. La ley castiga los atentados contra la confidencialidad, la integridad y la confidencialidad de los datos y de los sistemas informáticos, entre otras infracciones como hurto por medios informáticos y semejantes, transferencia no consentida de activos y circunstancias de mayor unidad (ANDRADE 2009).

- ✓ Ley 1341 de 2009[12]. La presente ley, determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías en las bases de datos y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente

[9] Sara Flórez. La ley 527 1999, sobre Comercio Electrónico y Firmas Electrónicas, marzo de 2011 http://es.slideshare.net/saracflorez/ley-527-de-1999

[10] Ley 962 de 2005 (julio 8) Diario Oficial No. 46.023 de 6 de septiembre de 2005 http://www.mintic.gov.co/portal/604/articles-3725_documento.pdf

[11] Ministerio de las TIC, Ley 1273 de 2009 http://www.mintic.gov.co/portal/604/w3-article-3705.html

[12] Carlos Chavarría, docente at unipanamericana - aulas digitales ley 1341 de 2009 ppt http://es.slideshare.net/chavarria2010/ley-1341-de-2009-ppt

de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad en las bases de datos (GUERRA 2009).

También se referencian guías, procedimientos y estándares internacionales sobre auditoría de sistemas, sistemas de seguridad informática, evaluación y seguimiento recomendados por las organizaciones más reconocidas en el ámbito internacional, como la Asociación para la Auditoría y Control de Sistemas de Información, ISACA[13] (Information Systems Audit and Control Association) y su IT Governance Institute, ITGI[14], que desarrollaron los Objetivos de Control para la Información y Tecnologías relacionadas, CObIT (Control Objectives for Information and related Technology) y varias de las certificaciones internacionales más difundidas. De la misma manera, se estudiaron las bases jurídicas para el tratamiento de los delitos informáticos en Colombia[15], como la Ley 599 del 24 de julio de 2000 y la Ley 1273 del 5 de enero de 2009. Con base en los referentes jurídicos y los estándares internacionales, se analizaron las condiciones de seguridad informática de una muestra de entidades financieras.

[13] Isaca, Trust in, and value from, information systems https://www.isaca.org/Pages/default.aspx

[14] http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx

[15] Colombia ley n° 599 de 2000 (24 de julio) - por la cual se expide el código penal http://www.wipo.int/wipolex/es/details.jsp?id=7305

5. DELIMITACIÓN

5.1 Delimitación Conceptual

Este proyecto abarca la investigación del diseño de un plan estratégico para fortalecer las políticas de seguridad existentes para el manejo de la información tributaria en una entidad pública. De ahí que se identifican los siguientes límites y alcances.

5.2 Delimitación Espacial

Esta investigación es para ser aplicada exclusivamente en la entidad pública seleccionada. El diseño de la estrategia para para fortalecer las políticas de seguridad existentes en las bases de datos se realizó en base al análisis de riesgo detectado.

5.3 Delimitación Metodológica

Los principales métodos a utilizar en esta investigación son los estadísticos como encuestas de diferentes tipos, entrevistas, organización en las bases de datos e interpretación de los resultados para llegar a conclusiones útiles donde se reflejan las vulnerabilidades encontradas.

5.4 Delimitación Financiera

El costo del proyecto es gastos en horas de tabulación e interpretación en las bases de datos, los diferentes recursos ofimáticos a utilizar como papel, impresoras, medios ópticos y magnéticos de almacenamiento y otros recursos que pueden ser facilitados por los realizadores del proyecto como son los sistemas de cómputo, conexiones a internet, etc.

5.5 Delimitación Cronológica

El proyecto de investigación tendrá un tiempo estimado de seis meses dividido en etapas según las necesidades.

6. METODOLOGÍA

6.1 Método de la Investigación

La metodología que se utiliza fue Mixta, cualitativa y cuantitativa, donde se pudo evidenciar que se realizó la recolección de la información, se analizó el manejo de las bases de datos, el cumplimiento de las políticas existentes y finalmente la tabulación de los resultados.

6.1.1 Investigación mixta: En las investigaciones de métodos mixtos, la recolección y análisis de información se realizan mediante datos cuantitativos y cualitativos para llegar a meta inferencias más allá de las estadísticas y más allá de las categorías cuantitativas; Este enfoque requiere trabajo en equipo, triangulación de datos, teorías, disciplinas, diseños, métodos y, sobre todo, debe estar presente la triangulación epistemológica[16].

6.1.2 Investigación cualitativa: La investigación es importante la creatividad, administración, la interpretación de los datos, está da el acceso preciso a la información y tiene formas para realizar la exploración rigorosa de los temas y permite descubrir patrones y someterlos a pruebas[17].

También este tipo de investigación es utilizado en muchas ciencias como, las sociales, saludo, investigaciones y la evaluación de programas.

6.2 TIPO DE INVESTIGACIÓN

La investigación que se llevó a cabo fue mixta, lo que permite realizar un análisis en las bases de datos utilizando los dos métodos, donde se manejan las características y se logra realizar la descripción de la situación actual de la seguridad en las bases de datos en la entidad pública.

Los instrumentos son las herramientas que ayudan a obtener la información necesaria como las que se utilizan en esta investigación, puede ser la observación y más concretamente las entrevistas, en este caso se basó en entrevistas realizadas al Director del Grupo de Informática de la Entidad investigada, al Administrador de la base de datos, asesores de mantenimientos y 15 encuestas

[16] Dulce Hernández, Quinta edición Metodología de la investigación 5ta Edición Sampieri http://www.academia.edu/6399195/Metodologia_de_la_investigacion_5ta_Edicion_Sampieri

[17] Dr. Lamberto Vera Vélez, UIPR, Ponce, P.R. la Investigación Cualitativa.http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html

cerradas realizadas a una muestra de 15 usuarios que acceden, consultan y actualizan las bases de datos; las entrevistas se crearon con base en los objetivos descritos esto para conocer los diferentes puntos de vista de cada una de las partes en lo que refiere al trabajo de la seguridad en la información y específicamente a la seguridad en las bases de datos .

6.2.1 DISEÑO DE LA INVESTIGACIÓN

En esta sección se describe los pasos que se siguieron en el transcurso del estudio y aplicación de la metodología utilizada, en los procedimientos de selección de la muestra, recolección de datos.

La encuesta se realiza a 15 usuarios que acceden de manera frecuente a las bases de datos y hacen parte del proceso de alimentación de la misma, el diseño de la encuesta es cerrada eligiendo preguntas que respondan a los objetivos generales y particulares teniendo en cuenta las hipótesis.

Las preguntas son una manera general de informar y alimentar la investigación para justificar la continuación del trabajo de investigación y la aceptación por parte de la entidad pública, ya que son una manera abierta de aportar a la investigación en el caso de la entrevista y una manera complementaria para informar y evaluar que tanto están los usuarios comprometidos con la seguridad de las bases de datos.

6.3 POBLACIÓN Y MUESTRA

6.3.1 Población

Este tipo de muestra fue aplicado al Director del Grupo de informática a usuarios activos que acceden al sistema de información y a las bases de datos y al personal de apoyo del área de sistemas de la entidad investigada.

6.3.2 Muestra

De acuerdo al objetivo de la investigación se realiza la encuesta de forma informativa a 15 usuarios de que acceden al sistema de información y a las bases de datos, colaboradores del área de sistemas; de los cuales se utilizaron seudónimos en sus nombres ya que se trata de información privada y no quieren verse cuestionados por el manejo de la información que tienen bajo su responsabilidad. Entrevistas realizadas al Director del Grupo de Informática, y al Administrador de la base de datos de la Entidad investigada, el cual accedió a

contestar ciertas preguntas que arrojó resultados finales para darle una dirección al proyecto de investigación.

6.4 FUENTES EN LAS BASES DE DATOS

Las fuentes de información que se tienen en cuenta para el desarrollo del proyecto son: información primaria y secundaria.

Información primaria. Las fuentes primarias la componen información recogida mediante las encuestas y las entrevistas realizadas, observación directa a funcionarios y manejo de los activos de la entidad.

Información Secundaria: información obtenida de un historial de intentos de ataque que ha enfrentado la entidad junto con información documental que orienta al análisis y evaluación de la seguridad en bases de datos, que se encuentra consignada en documentos como: normas: NTC- ISO-IEC-27001, NTC- ISO-IEC-27002 [18] y Metodología MAGERIT[21], modelos de seguridad informática COBIT[19].

6.5 TECNICAS E INSTRUMENTOS DE RECOLECIÓN DE DATOS

6.5.1 ENCUESTA

Para obtener la información y los pormenores para realizar la investigación se aplicó el instrumento de la encuesta donde se puede encontrar las áreas a fortalecer en la entidad.

6.5.2 ENTREVISTA

Realizada al Director del Área de Informática y el Administrador de la base de datos de la entidad investigada, quienes acceden contestar preguntas con el fin de dar su opinión personal de cómo está estructurada la seguridad en las bases de datos en dicha entidad y analizar los resultados obtenidos de las encuestas.

[18] Norma técnica NTC-iso-iec colombiana 27001 2013-12-11 Tecnologías de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos http://tienda.icontec.org/brief/NTC-ISO-IEC27001.pdf

[19] Camilo Gutiérrez Amaya. May 2013. magerit: metodología práctica para gestionar riesgos Http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

6.5.3 OBSERVACIÓN

La observación fue de mucha utilidad debido a que por este medio se pudo observar el manejo de los procedimientos y el uso en las bases de datos en la entidad investigada.

6.5.4 HERRAMIENTAS

En las herramientas de utilizo el programa office, Servidor de base de datos [SBD_RH], Medios de Impresión [IMP_RH], Computadoras de escritorio [PC_RH], Router [ROUT_RH], Software que se maneja Windows server 2003computador e impresora.

6.6 INFORMACIÓN DE ACTIVOS QUE MANEJA LA ENTIDAD PUBLICA

La Entidad Pública encargada de la gestión financiera, económica, fiscal y presupuestal cuenta con los siguientes activos, para el éxito en el desarrollo de las actividades para la cual fue creada:

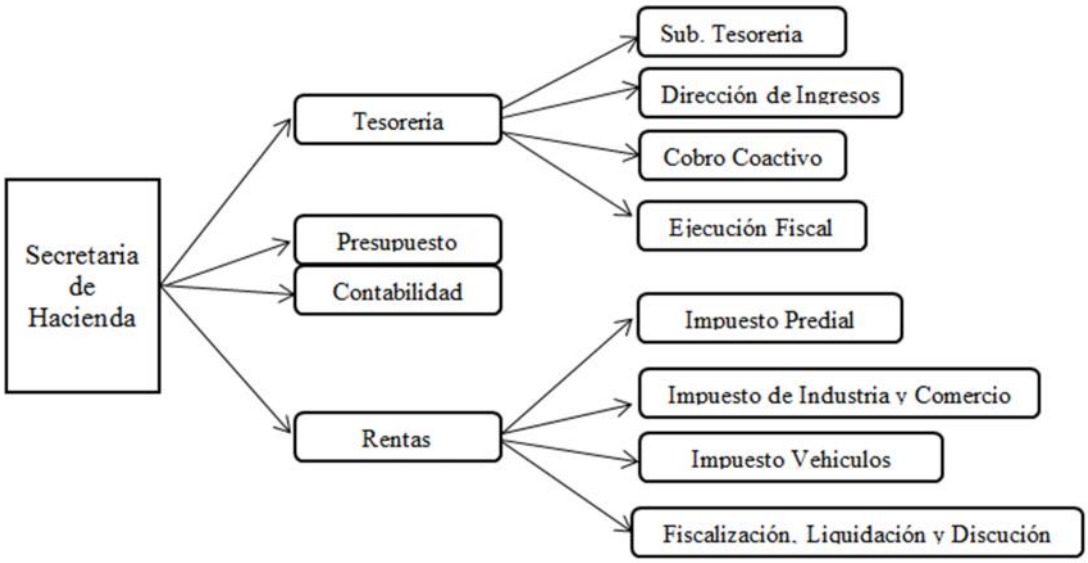
Tipo de Archivo	Nombre de la Información	Descripción	Proceso de Custodia	Proceso Prioritario	Clasificación
Activos de Información	Oficios, resoluciones de devolución, compensación	Solicitudes de devolución por doble pago, cobro por ajuste en sus avalúos o solicitud de aclaración por los cobros facturados.	Oficina Impuesto Predial	Rentas	Publica
Activos de Información	Base de Datos de los predios activos en el Municipio	Relación de los predios activos en el Municipio investigado, propietarios, avalúos, morosos y tarifas.	Oficina Impuesto Predial	Rentas	Privada
Activos de Información	Base de datos de información Tributaria de Comerciantes	Montos declarados por empresa, saldos y datos personales de las entidades.	Oficina Industria y Comercio	Rentas	Privada
Activos de Información	Base de datos de Comerciantes Omisos	Comerciantes a los cuales se les realiza emplazamientos por los incumplimientos de sus obligaciones.	Oficia Fiscalización	Rentas	Privada
Activos de Información	Citación, Notificación y Mandamiento de Pago	Procesos que se les realiza a los Predios que se encuentran en mora.	Oficia de Cobro Coactivo	Tesorería	Publica
Activos de Información	Boletines de Ingreso Mensual	Reporte generados por una Fiduciaria del valor de los ingresos generado por los impuestos mensuales.	Tesorería	Tesorería	Privada

Activos de Software	Sistema de liquidación Impuesto Predial	Programa que factura el impuesto predial, una vez es actualizado con la información enviada por el IGAC.	Oficina Impuesto Predial	Rentas	Privada
Activos de Software	Sistema de liquidación del Impuesto de Industria y Comercio	Programa que permite generar las declaraciones de cada contribuyente y facturar los pagos que son por cuotas.	Oficina Industria y Comercio	Rentas	Privada
Activos de Software	Sistema de Georreferenciación de Predios y Comerciantes	Sistema para la fácil localización de predios y establecimientos comerciales y apoyo en los procesos de trabajos.	Rentas - Tesorería	Rentas - Tesorería	Privada
Activos de Hardware	Impresoras	Apoyo en Comunicaciones.	Rentas - Tesorería	Rentas - Tesorería	Privada
Activos de Hardware	Estaciones de Trabajo	Equipo de cómputos para el desarrollo de las actividades.	Rentas - Tesorería	Rentas - Tesorería	Privada
Activos de Software	Windows 2003 server, Linux	Sistema Operativo para los Servidor.	Informática	Informática	Privada
Activos de Software	Servidor de base de datos [SBD_RH].	Administración de la información tributaria	Informática	Informática	Privada
Activos de Hardware	Procesador Intel® Xeon® E5-2430L 2.00GHz, 15MB Caché.	Servidor	Informática	Informática	Privada
Activos de Software	Sistema Operativo Windows 7	Sistemas Operativos de unos equipos.	Informática	Informática	Privada
Activos de Software	Sistema Operativo Windows 8	Sistemas Operativos de unos equipos.	Informática	Informática	Privada
Activos de Hardware	Fibra óptica	Apoyo en las conexiones de red e Internet.	Informática	Informática	Privada
Activos de Hardware	Cable UTP	Apoyo en las conexiones de red e Internet.	Informática	Informática	Privada
Activos de Hardware	Router	Apoyo en las conexiones de red e Internet.	Informática	Informática	Privada
Activos de Hardware	Red Telefónica	Apoyo para las comunicaciones telefónicas.	Informática	Informática	Privada

Tabla No. 1: Activos que maneja la Entidad Pública

Para identificar los activos se utilizó la observación y la encuesta, se solicitó el permiso para revisar documentos institucionales como inventarios de software y hardware, planes para la continuidad del negocio, investigación, manuales de usuario, material de formación e información encontrada en la página web[20].

[20] Funciones de la Entidad http://www.entidad deibague.gov.co/website/index.php/funciones-hacienda



Fuente: Investigadores. Imagen No. 1: Organigrama

6.6.1Grupo de Tesorería.

La tesorería es una de las áreas más complejas ya que de ella dependen varias direcciones como son:

De las cuales se desprenden varias funciones y actividades que realizan cada una de ellas para que se lleve a cabo los fines administrativos y legales que le son asignados, estas actividades se pueden clasificar de la siguiente manera:

1. Recaudación de ingresos por impuestos, derechos, productos, aprovechamiento y servicios: Cobro de tenencia estatal, cobro a contribuyentes por servicios en otras dependencias, cobro por expedición de certificados, recaudación del impuesto predial ejidal y sus servicios, recaudación del impuesto predial, industria y comercio y otros, y la recepción y control del rastro, convenios de cuentas por cobrar.

2. Control administrativo de ingresos y de egresos, que son: Elaboración del informe de ingresos, control interno, control de ingresos reportes mensuales, control financiero de programas de inversión, administración y control de recursos mediante una Fiduciaria.

3. Registro contable de ingresos y egresos de recursos financieros del ayuntamiento: Elaboración y registro de pólizas de egresos, informe diario sobre movimientos bancarios, obtención de estados financieros, captura de presupuesto de egresos, conciliaciones bancarias, recibo y archivo de pólizas, registro de proveedores, registro de póliza de diario, llenado de retenciones del ISR.

4. Servicios: Atención al público en general, generación de paz y salvos municipales, administración de archivo de cobro coactivo, entrega de cheques por servicios, solicitud audiencias con tesorero municipal, servicios pagados al ayuntamiento con porcentaje a terceros.

5. Administrativo: Procedimientos administrativos de ejecución fiscal, control y nómina de ejecutores fiscales.

6.6.2 Grupo de Rentas

EL Código de Rentas contiene las reglas generales sobre administración, percepción y cobro de las rentas y la determinación de sus recursos, impuestos, contribuciones tasas y honorarios, así como también la tarificación de los mismos[21].

6.6.2.1Garantías de los Bienes y Rentas del Municipio:

Los bienes y rentas son de su exclusiva propiedad y gozan de las garantías consagradas en el artículo 183 de la Constitución Nacional.

Son rentas del Municipio:

El producto de los bienes municipales que le pertenezcan en ejercicio de atribuciones de dominio público o privado.

El producto de impuestos, derechos, tasas, precios y contribuciones especiales.

Las Participaciones, aportes, auxilios y cesión de rentas de los tesoros Nacional y Departamental.

Los aportes y contribuciones de establecimientos descentralizados y las contribuciones que deban hacer otras Dependencias en favor de Fondos comunes, y Los ingresos o recursos de carácter extraordinario o eventual.

[21] Funciones de la Entidad http://www.entidad deibague.gov.co/website/index.php/funciones-hacienda

Grávense los bienes inmuebles situados en jurisdicción correspondiente, de acuerdo con las tarifas y formalidades que se establecen en el presente acuerdo.

6.6.2.2 Gravámenes a la Propiedad Inmueble

EL impuesto Predial se liquidará y cobrará de acuerdo con las siguientes tarifas:

Para inmuebles no edificados situados en el perímetro urbano a razón de seis por mil (6x1000), sobre el avalúo catastral respectivo y de dos por (2x100) adicional sobre el mismo avalúo.

Para inmuebles no edificados situados en el perímetro urbano a razón de doce por mil (12x1000) sobre el avalúo catastral respectivo.

Para inmuebles situados dentro del área rural, a razón de seis por mil (6x1000) sobre avalúo catastral respectivo y dos por mil (2x1000) adicional sobre el mismo avalúo.
PARARRAYO: Entiéndase por tarifa mínima para efectos del artículo 17 de la 14 de 19983 y artículos 49 y 50 del Decreto 3496 de 1993 Reglamentario de la misma ley, la del seis por mil (6x1000).

6.6.2.3 Facturación Y Pago Del Impuesto

El pago del Impuesto Predial y sus complementarios será por trimestres anticipados y corresponde a quien en la fecha de la exigibilidad sea el dueño o poseedor del inmueble objeto de la imposición[22].

Dicho pago podrá efectuarse en la Caja de la Tesorería o en los Bancos con los cuales haya celebrado contrato sobre el particular. El pago deberá hacerse dentro de los plazos fijados en las cuentas de cobro y la mora causará los recargos de ley, que serán liquidados en cuenta siguiente y podrán ser cobrados por jurisdicción coactiva.

Si dentro del plazo previsto para el pago de la cuenta ocurrieren en su mayor valor para la liquidación pero sólo en cuanto se refiere a la persona que debe atender al pago de los siguientes períodos.

6.6.2.4 Impuesto de Industria y Comercio y de Avisos y Tableros

El hecho generador de los Impuestos de Industria y Comercio y de avisos y Tableros está constituido por el ejercicio o realización directa o indirecta de cualquier actividad industrial, comercial o de servicios, en la jurisdicción correspondiente, sea que dicha actividad se cumpla en forma permanente u ocasional, en inmueble determinado, con establecimiento o sin él.

6.6.2.5 Sujeto Activo

Es sujeto activo de los Impuestos de Industria, Comercio y de Avisos y Tableros ente administrativo a favor del cual se establece este Impuesto y en el que radican las potestades tributarias de liquidación, administración, control, investigación y recaudo.

---

[22] Acuerdo 060 del 29 de Julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda

6.6.2.6 Sujeto Pasivo

Es sujeto pasivo de estos Impuestos la persona natural, jurídica o la sociedad de hecho que realice el hecho generador de la obligación tributaria.

6.6.2.7Actividades No Sujetas

No están sujetas a los Impuestos de Industria, comercio y de avisos y Tableros las siguientes actividades[23]:

La producción primaria agrícola, ganadera y avícola, sin que se incluyan la fabricación de productos alimenticios o toda industria donde haya un proceso de transformación por elemental que ésta sea.
La producción Nacional de artículos destinados a las exportaciones.

La explotación de canteras y minas diferentes de sal, esmeraldas y metales preciosos cuando las regalías o participaciones sean iguales o superiores a lo que corresponderá pagar por concepto de los Impuestos de Industria, Comercio y Avisos y Tableros.

La educación pública, las Entidades de Beneficencia, las culturales y deportivas, los sindicatos las asociaciones de profesionales y gremiales sin ánimo de lucro, los partidos políticos y los hospitales adscritos o vinculados al sistema nacional de salud.

Las actividades de tránsito de los artículos de cualquier género que atraviesen por el territorio del municipio de Ibagué encaminados a un lugar diferente consagrados en la ley 26 de 1904[24].

6.6.2.8 Obligación Tributaria

Es aquella que surge a cargo del sujeto pasivo y en favor del sujeto activo como consecuencia de la realización del hecho generador.

Los adquirentes o beneficiarios de un establecimiento de comercio donde se desarrollen actividades gravables serán solidariamente responsables, con los contribuyentes anteriores, de las obligaciones tributarias, sanciones e intereses insolutos causados con anterioridad a la adquisición del establecimiento de comercio.
Obligaciones:

[23] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda
[24] https://www.redjurista.com/documents/l0026_04.aspx

Los sujetos pasivos de los impuestos de Industria, Comercio y de avisos y tableros, deberán cumplir con las siguientes obligaciones:

- ✓ Registrarse en la división de rentas, dentro de los treinta (30) días calendarios siguientes a la fecha de iniciación de la actividad gravable, para lo cual presentarán el respectivo certificado de uso.

- ✓ Presentar anualmente, dentro de los plazos que determine la administración, la declaración de industria, comercio y de avisos y tableros, junto con la liquidación privada del gravamen incluyendo el valor de la sanción pro extemporaneidad, si fuere el caso.

- ✓ Atender los requerimientos que le haga la Dirección de Rentas.
- ✓ Recibir a los visitadores de la División de Rentas y presentar los documentos que conforme a la ley se les solicite.

- ✓ Comunicar oportunamente a la División de Rentas dentro de los términos previstos en el presente Acuerdo, cualquier novedad que pueda afectar los registros de dicha dependencia, de conformidad con las instrucciones divulgadas y los formatos diseñados para tal efecto.

Efectuar los pagos relativos a la obligación tributaria de conformidad con las disposiciones vigentes.

Llevar un registro contable que se ajuste a lo previsto en Código de Comercio y las demás disposiciones vigentes.

6.6.2.9 Vallas De Propaganda

Las vallas dedicadas a propagandas, situadas en vía pública o lugar adyacente, pagarán un impuesto de sesenta pesos ($60,00) mensuales por cada metro cuadrado. Para la fijación de las vallas se requiere el permiso previo del Departamento del Planeación y el pago del impuesto correspondiente. Cuando una valla fuere colocada sin el correspondiente. El impuesto se liquidará con un recargo del quinientos por ciento (500%) del gravamen mensual, sin perjuicio de legalización posteriormente[25].

[25] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda

6.6.3.0 Registro y Declaración

Las personas naturales, jurídicas o sociedades de hecho que realicen actividades gravables están obligadas a registrarse en la división de renta dentro de los treinta (30) días calendario siguiente a la iniciación de sus actividades, en los formularios que para tal efecto diseñe la División de rentas. El Impuesto se cobrará desde el día de iniciación de actividades.

6.6.3.1 Paz y Salvo

El pago efectuado dará derecho a que se expida la correspondiente paz y salvo por el período cubierto[26].

Mientras los recursos interpuestos por la vía gubernativa se encuentren pendientes del fallo, los contribuyentes tendrán derecho a la expedición del paz y salvo, previa consignación de las sumas que admitan deber (ART. 83 numeral 2o. De este Código).

6.6. 3.2 Espectáculos Públicos

Para los efectos de este impuesto entiéndase por espectáculos públicos, entre otros, los siguientes: exhibiciones cinematográficas, actuaciones de compañías teatrales, ferias exposiciones, riñas de gallos, ciudades de hierro y atracciones mecánicas, carreras y concursos de autos, exhibiciones deportivas y las que tengan lugar en circos, estadios y coliseos, corralejas y demás sitios en donde se presenten eventos deportivos, artísticos y de recreación.

El impuesto de Espectáculos públicos se cobrará a razón del diez por ciento (10%) sobre el producto bruto de los espectáculos definidos en el artículo anterior.

6.6.3.3 Circulación y Transito

Los vehículos automotores de uso particular que circulen habitualmente, serán gravados por concepto del Impuesto de Circulación y Tránsito de que trata la Ley 48 de 1968, con una tarifa anual equivalente al dos por mil (2 x mil) de su valor comercial.

[26] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda

Para la determinación del valor comercial de los vehículos automotores, el Instituto Nacional del Transporte INTRA establecerá anualmente una Tabla con los valores correspondientes. Para vehículos no contemplados en esta Tabla, el propietario deberá solicitar el valor comercial al INTRA.

Cuando el vehículo entre en circulación por primera vez, conforme a las regulaciones vigentes, pagará por el impuesto de que trata el Artículo 156 del presente Acuerdo, una suma proporcional al número de meses o fracción que reste del año.

El Impuesto de Circulación y Tránsito sobre vehículos tendrá un límite mínimo anual de doscientos pesos ($200, oo). A partir de 1988, esta suma se reajustará anualmente en el porcentaje señalado por el Gobierno Nacional en el año inmediatamente anterior para el Impuesto sobre la renta y complementarios[27].

6.6.3.4 Hilos, Niveles y Licencias de Construcción

Para construir, reconstruir, reparar o adicionar cualquier clase de edificaciones, será preciso proveerse de la correspondiente licencia expedida por la oficina de Planeación y no podrá otorgarse sino mediante la exhibición del recibo que acredita el pago del impuesto contemplado en el artículo siguiente.

Cuando se trate de exenciones se acompañará la nota del Departamento Administrativo de Planeación que así lo exprese.

Prohíbase la expedición de licencia o permiso provisionales para construir, reparar o adicionar cualquier clase de edificaciones, sin el pago previo del impuesto de que trata en este Capítulo.

6.6.3.5 Ocupación de Vías, Plazas y Lugares de uso Público

El establecimiento de vehículos en vías públicas o la ocupación de éstas con materiales de construcción, escombros o casetas, requerirán permiso de la Administración actual y causará a favor del Municipio, las tasas y multas que se establecen en este Capítulo.

[27] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda

6.6.3.6 Tarifas por Estacionamiento de Vehículos

Por el derecho de estacionar vehículos en puestos determinados, cuya ubicación será señalada por la autoridad competente previa solicitud del interesado, se cobrará la siguiente tarifa mensual:

Vehículos particulares con exclusividad	$ 500
Vehículos de servicio público con exclusividad para la Entidad.	$ 200

6.6.4 Grupo de Presupuesto

El Presupuesto ordena en forma eficiente los recursos con que se cuente, así como los gastos en que incurre, en función de las directrices principales que lo definen. Como herramienta de administración financiera, el presupuesto constituye la base para planificar de acuerdo al origen de los recursos y el destino que se les dará para concretar las actividades que se propone la organización en un periodo determinado[28].
Es un sistema dinámico, porque a través del control de ingresos y gastos permite efectuar modificaciones adecuadas a las necesidades e implementación de proyectos[29].

A la vez constituye una importante fuente de información pues el presupuesto manifiesta las políticas municipales de desarrollo comunal en lo social y económico, así como las acciones y actividades que realiza el municipio para el logro de los objetivos.

De su análisis financiero se extraen conclusiones, tales como la evolución de los recursos y su asignación, participación de los ingresos y de los gastos en el total.

En consecuencia, el presupuesto se transforma en una herramienta básica que es determinante en el éxito futuro de la gestión de los recursos.

Sin embargo, el presupuesto en muchos casos es visto como un ejercicio formal de ordenamiento de ingresos y gastos, sujeto a un formato específico. Si bien dicho formato permite controlar la regularidad y transparencia de los ingresos y gastos municipales, no parece ser suficientemente comprendido por los encargados, observándose falencias, errores y omisiones en su elaboración.

Algunos elementos a considerar en este punto son:

---

[28] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda.
[29] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda.

La planificación presupuestaria no es una práctica generalizada al interior de las municipalidades. Esta actividad se limita, en muchos casos, a la elaboración del presupuesto anual en función del año anterior, con escasa participación de las unidades de la institución. La proyección presupuestaria que se realiza es, por lo general, una corrección inflacionaria. El presupuesto se concibe, de esta forma, como un objetivo aislado más que como una herramienta de gestión.

Esta inercia en las prácticas presupuestarias municipales ha hecho muy poco eficiente el manejo de los recursos a nivel local. La inexistencia de presupuestos por unidades o por programas, la carencia de sistemas de control de costos y otros factores atentan en forma permanente contra la gestión.

Estas limitaciones han significado que un buen número de municipios presenten las siguientes características:

- ✓ Improvisación con respecto a la ejecución presupuestaria producto de la falta de coordinación y sistematización en el proceso de elaboración del presupuesto[30].
- ✓ La asignación presupuestaria no responde a un sistema de prioridades, lo que genera un destino arbitrario y tradicional de recursos a distintos ítems del presupuesto.
- ✓ El presupuesto no se elabora en función de proyectos determinados, lo cual dificultad el proceso de control presupuestario y limita el horizonte de planificación.

Ciclo de la elaboración del Presupuesto. El proceso de elaboración de un presupuesto comienza antes del mes de octubre del año anterior al de ejecución. Este es confeccionado por las Unidades de Planificación y Finanzas de la municipalidad, de acuerdo a los lineamientos básicos definidos por el alcalde.

La primera semana de octubre el alcalde someterá a consideración del Concejo las orientaciones globales del municipio, el presupuesto municipal y el programa anual, con sus metas y líneas de acción. El Concejo deberá pronunciarse antes del 15 de diciembre.

El Concejo no podrá aumentar las partidas de gastos, sino solamente disminuir o realizar cambios de ítems. Además, es obligación del Concejo aprobar solamente presupuestos debidamente financiados, al igual que velar de que no ocurra déficit, aprobando durante el ejercicio- modificaciones correctivas a proposición del alcalde. Esto es muy importante, ya que la ley indica que si "no introdujere las

[30] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda.

rectificaciones pertinentes, el alcalde que no propusiere las modificaciones correspondientes o los concejales que las rechacen serán solidariamente responsables de la parte deficitaria que arroje la ejecución presupuestaria anual al 31 de diciembre del año respectivo. Habrá acción pública para reclamar el cumplimiento de esta actividad". En el caso que "los pronunciamientos realizados por el Concejo, no se produjeren dentro de los términos legales señalados, se regirá lo propuesto por el Alcalde".

6.6.5 Grupo de Contabilidad

La Contabilidad Pública ha estado muy ligada a la vida institucional de las Contralorías en Colombia, no sólo por constituir probablemente la principal herramienta para el ejercicio del control fiscal, sino que desde su institucionalización le quedaron asignadas competencias en materia de prescripción contable al máximo órgano de control fiscal. Pero también se colige de lo que históricamente nos ha legado el proceso evolutivo de las organizaciones instauradas por el Estado para velar por el buen uso de los recursos públicos.

Se considera que la información contable pública sirve entre otros aspectos para:

- ✓ Evaluar la aplicación y destinación eficiente de los recursos en los diferentes sectores de la acción social del Estado.

- ✓ Realizar el seguimiento a la gestión y los resultados de las entidades del sector público, así como verificar el cumplimiento y legalidad de sus operaciones, pretendiendo con ello que los recursos públicos sean utilizados bajo conceptos de eficiencia, eficacia, transparencia y equidad.

- ✓ Evaluar la ejecución de planes, programas y proyectos de los diferentes niveles y órdenes estatales, en función de los objetivos, metas y prioridades para la política económica, social y ambiental.

La información contable aporta substancialmente instrumentos para el ejercicio del control en sus diferentes manifestaciones: en materia de control interno, para que cada administración pueda mantener un permanente seguimiento de las transacciones, variaciones, proyecciones y evaluaciones del comportamiento financiero-patrimonial del ente público, aprovechando la cronología de los registros y las cifras en términos individuales y consolidados. En lo que respecta al control ciudadano, puede generar resultados que la comunidad está en capacidad de analizar y poder tener un conocimiento general de la manera como se están administrando sus recursos; para facilitar estos deberes institucionales, hoy día se exige por parte de la Contaduría General de la Nación, la publicación de los resultados financieros en lugares visibles de los órganos y entidades públicas. No

hay duda que para el ejercicio del control fiscal externo que ejercen las Contralorías, es fundamental disponer de información útil, confiable, oportuna, verificable, entre otras características, con fines de evaluación histórica de la gestión.

La contabilidad precisamente permite, a diferencia de otros instrumentos como el presupuestal, poder mostrar resultados de cada vigencia fiscal, con los cuales se inicia la siguiente, permitiendo conocer la evolución institucional con el fin de establecer los efectos de las diferentes transacciones a través de la vida institucional o de gestión continuada, evidenciadas mediante el control y evaluación financieros. Sabemos también, que la contabilidad es el principal insumo en que se fundamenta la práctica de la auditoría financiera, regida por importantes elementos técnicos y acogida a principios de general aceptación, para establecer la razonabilidad de los estados financieros, sobre las cuales los órganos de control fiscal y revisorías fiscales profieren un dictamen u opinión, pronunciamiento que va a depender de la disposición de información contable, pues ya que es factible inclusive abstenerse de tal opinión, situación que aún es posible experimentar en algunas instituciones públicas de nuestro país. 30 Dentro de los controles a los cuales sirve la información contable pública encontramos el relacionado con el control político: Las instituciones estatales, cualquiera que sea el orden o nivel al que pertenezca, deben presentar a los organismos de control fiscal el resultado de sus finanzas, para que esta de manera individual y consolidada presenten ante las corporaciones de elección popular, las evaluaciones o análisis correspondientes, las glosas u observaciones que le ha formulado tanto a la información contable como a los Estados Financieros presentados, como también los planes de mejoramiento que han sido suscritos con el fin de poder sanear o depurar los saldos contables institucionales. El control disciplinario también se surte del sistema de información contable, del cual deriva evidencias para establecer el cumplimiento de las funciones de los responsables de su generación y análisis, con el fin de establecer e imponer las sanciones que sean del caso.

De qué sirve a las entidades contables públicas un sistema de información que no les permite en un momento determinado conocer en tiempo real cuál es su disponibilidad de saldos bancarios, la cartera morosa, las disponibilidades de caja, los excedentes de caja con fines de inversión, las existencias físicas de equipos de computación y de trasportes, el comportamiento de los ingresos y gastos causados, recaudos y erogaciones durante cada vigencia fiscal, como también los faltantes y procesos fiscales, penales, civiles, seguidos a favor y en contra de la entidad.

6.6.6 Activos de Hardware y Software.

Sistemas operativos: Los sistemas operativos que utilizan los servidores son: *Linux* y *Windows server*; los computadores de escritorio utilizan una variedad de sistemas operativos en versiones de *Windows*, como *Windows 7* y *Windows 8*[31].

Software para la liquidación de los Impuestos: La Entidad cuenta con dos sistemas para la liquidación de los impuestos, manejo del sistema financiero y sistematización en las bases de datos, cuenta además con un sistema de inteligencia visual de contribuyentes (Georreferenciación), como apoyo al fortalecimiento de las actividades tributarias que se desarrollan.

Los Aplicativos utilizados para la liquidación de los impuestos manejan varios módulos que involucran diferentes áreas de la entidad, como es la Facturación, Gestión Documental, Cartera, Cobro Coactivo, recaudo, fiscalización, Paz y Salvo. Administrado por funcionarios de planta que hacen parte del grupo de sistemas.
Diseño Web: Se cuenta con el diseño de un sitio Web que se ajuste al diseño Web de las entidades Gubernamentales.

El diseño gráfico fue implementado usando tecnologías estándar de la web, según lo especificado por el World Wide Web Consortium, el organismo encargado de establecer las políticas y especificaciones técnicas que regulan Internet (world wide web).

Concretamente, el diseño gráfico se ha creado con Hojas de Estilo, o CSS por sus siglas en inglés. Las hojas de estilo son un conjunto de instrucciones escritas en lenguaje HTML, (HTML es el lenguaje que se usa para publicar contenidos en internet) que definen las apariencias de una página web con el objetivo de que sus estilos se parezcan. Además de brindar una apariencia uniforme, las hojas de estilo presentan otras ventajas como[32]:

6.6.6.1 Accesibilidad para todas las personas

Las características técnicas de este sitio web permiten a las personas con discapacidades físicas navegar y obtener información con mayor facilidad. Muchos sitios presentes en la red no cuentan con estas especificaciones, lo que imposibilita el acceso a las personas con limitaciones físicas.

Para cumplir con los requisitos de accesibilidad, este sitio se ha diseñado siguiendo las pautas descritas en las Directivas de Accesibilidad para el Contenido

[31] http://definicion.de/sistema-operativo/
[32] http://www.w3c.es/

del Consorcio Web WAI. Además, estas pautas cumplen las Políticas y Estándares para publicación de información estatal en Internet de la Directiva Presidencial 02 de Gobierno en Línea.

El propósito del sitio es mantener informado a los usuarios de las noticias que suceden dentro de la entidad. También tienen la posibilidad de consultar los servicios que brindan Mediante los link de acceso como son: Informe de edictos, liquidación virtual de impuestos, calendario Tributario, PQRDS, intranet entre otros.

6.6.6.2 Servicios subcontratados.

Como servicios subcontratados está el internet, los mantenimientos de los equipos de cómputos.

6.6.7 Personal.

Todo el personal que interviene en los diferentes procedimientos de la entidad debe conocer las políticas para el manejo adecuado de los activos existentes, implementando los controles establecidos por la entidad.

La liquidación y actualización en los módulos de los impuestos son responsabilidad de los grupos de Rentas y Tesorería, de los cuales 210 usuarios activos acceden a los sistemas de información por medio de computadores asignada por la misma entidad, de los cuales alrededor de 30 son considerados usuarios activos debido a que participan en los procesos de actualización y liquidación de los diferentes impuestos.

6.6.8 Grupo Sistemas y Telecomunicaciones

El grupo de sistemas y telecomunicaciones establece los objetivos de mantener en funcionamiento los sistemas informáticos de la entidad, proponer la implementación de nuevas tecnologías y sistemas informáticos. Dentro de las funciones del grupo de sistemas se encuentran:

- ✓ Implementación de Sistemas Informáticos.
- ✓ Servicios de Mantenimiento Preventivo.
- ✓ Capacitación de Personal.
- ✓ identificar vulnerabilidades y brechas de seguridad informática.

- ✓ realizar un Análisis de Riegos relacionado con la Seguridad de la Información.

- ✓ Crear estímulos e incentivos en los grupos de trabajo que por sus logros se destaquen.

- ✓ Realizar la inducción, capacitación y formación de los servidores públicos.

- ✓ Elaborar los estudios técnicos para la modificación de la planta de personal.

- ✓ Diseñar un plan que permita el mejoramiento continuo y el desarrollo integral del individuo para crear una cultura del servicio al usuario.

- ✓ Llevar el registro y control de las hojas de vida de los servidores públicos de la administración central municipal activo o inactivo.

- ✓ Instruir las causas disciplinarias que se generen como consecuencia de las acciones u omisiones de los servidores públicos de la Administración central y proyectar de las decisiones de primera instancia para la firma del Secretario Administrativo[33].

El grupo de informática cuenta con tres ingenieros de apoyo, los cuales se encargan de la auditoria de las bases de datos, funcionamiento del sistema de liquidación, soportes en la red y mantenimiento de los equipos de cómputos.

[33] Acuerdo 060 29 de julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda.

7. FASE 1: DISEÑO DE UN PLAN ESTRATEGICO PARA FORTALECER LAS POLITICAS DE SEGURIDAD EXISTENTES EN LAS BASES DE DATOS:

El plan estratégico consta de 3 fases:

Fase 1	Objetivos	Actividades a Analizar
Evaluación de Políticas existentes	Revisar y evaluar los controles en las bases de datos, su acceso, utilización, eficiencia y seguridad; frente a amenazas, internas o externas, deliberadas o accidentales, que puedan colocar en riesgo la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad en las bases de datos.	✓ Consulta de Manuales y Documentaciones. ✓ Recopilación en las bases de datos organizacional: Estructura orgánica, recursos humanos. ✓ Aplicación de la Encuesta a los funcionarios. ✓ Entrevistas a directores y usuarios activos de cada dependencia. ✓ Verificar el desempeño, condiciones de trabajo, recursos en materiales y financieros mobiliarios y equipos. ✓ Evaluación del Proceso de Datos y de los Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.

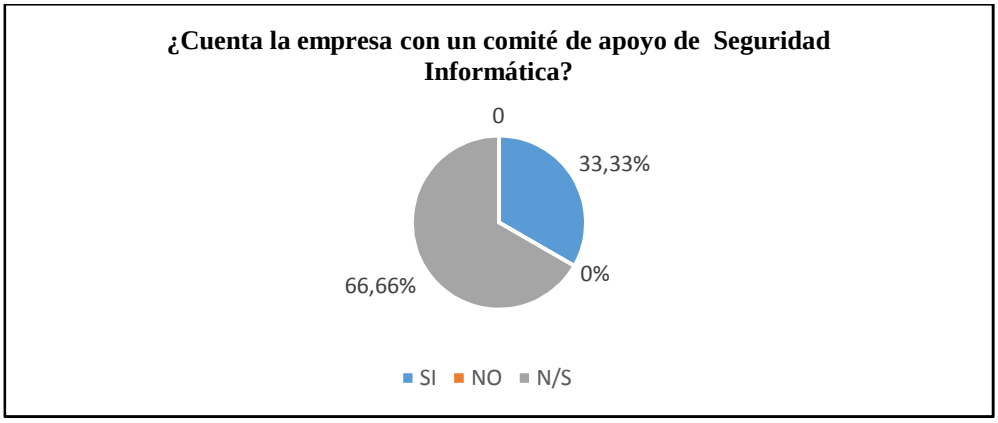
Tabla No.2 Evaluación de Políticas existentes

A partir en las bases de datos obtenida de las encuestas, entrevistas realizadas y de la observación directa se detectaron áreas con deficiencias de seguridad a continuación se mencionan los resultados obtenidos:

7.1. ANALISIS DE LAS DEBILIDADES DETECTADAS Y LAS AREAS A FORTALECER

Las debilidades existentes en los sistemas de información, son una de las principales amenazas, que pueden ser aprovechadas por atacantes; a partir de los datos obtenidos de las encuestas, entrevistas realizadas y a través de la observación directa se detectaron áreas donde no se están cumpliendo con las políticas de seguridad establecidas y se presentan deficiencias en las mismas, a continuación se mencionan los procedimientos a fortalecer:

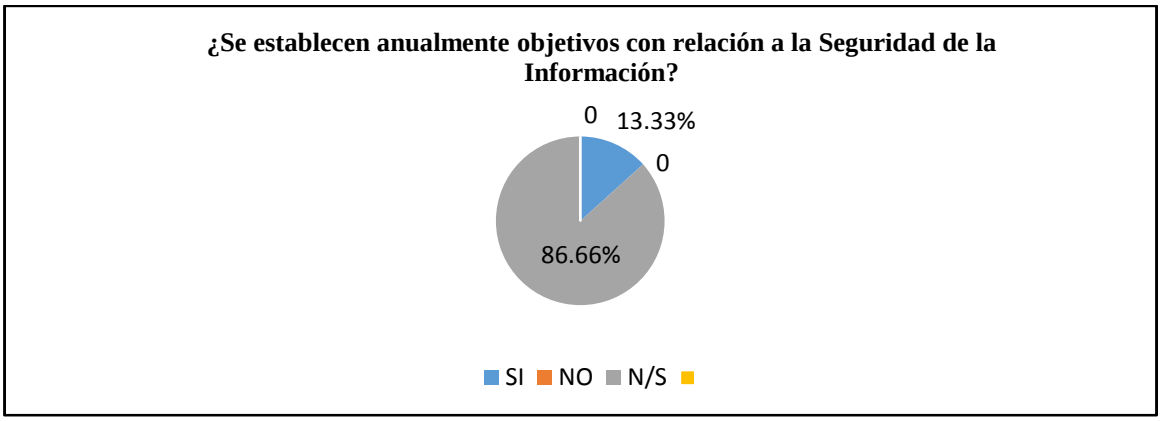
7.1.1Organización de la Seguridad



Gráfica No. 2 Fuente: Investigadores

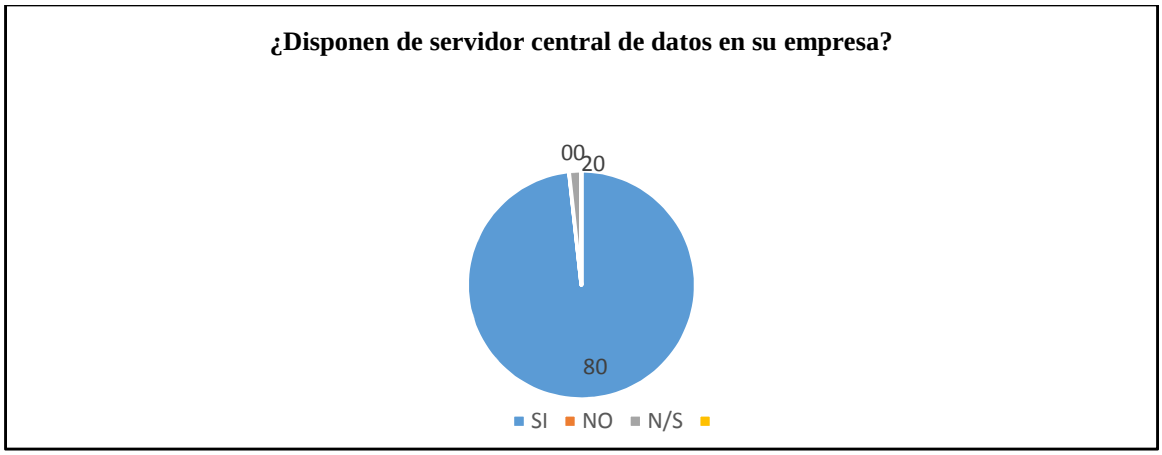
Actualmente la entidad cuenta con el apoyo del Grupo de Informática para el diseño de estrategias para fortalecer los niveles de seguridad, quien a su vez delega el tratamiento de las políticas de seguridad a dos ingenieros de planta.

Teniendo en cuenta el resultado el 66,6% de funcionarios desconocen el personal a cargo de la seguridad informática en la Entidad por tanto ante cualquier posible falla en la seguridad desconocen el protocolo que deben seguir y esto aumenta la vulnerabilidad de la información en las bases de datos, por eso es de vital importancia que todos los funcionarios el 100% conozcan cuales son los protocolos a seguir, que funcionarios están a cargo o son responsables de velar por la seguridad.



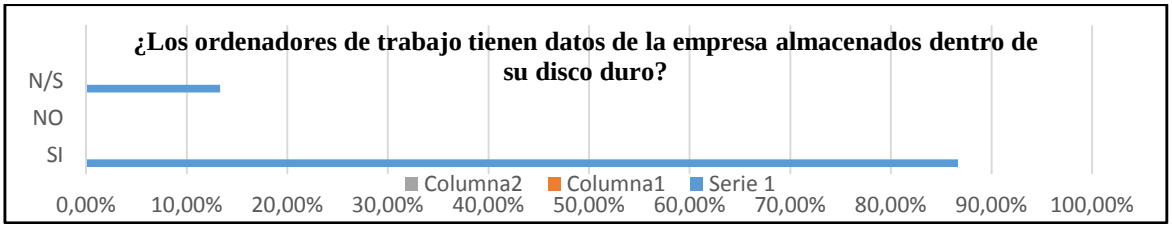
Gráfica No.3 Fuente: Investigadores

Teniendo en cuenta el resultado el 86.66% de funcionarios desconocen los ataques más comunes a bases de datos y los objetivos que traza el comité de seguridad Informática, este resultado permite ver que hay un alto grado de vulnerabilidad ya que si los funcionarios no saben cuál es el objetivo de las políticas que se plantean, es importante realizar una capacitación donde se dé a conocer los objetivos.



Gráfica No.4 Fuente: Investigadores

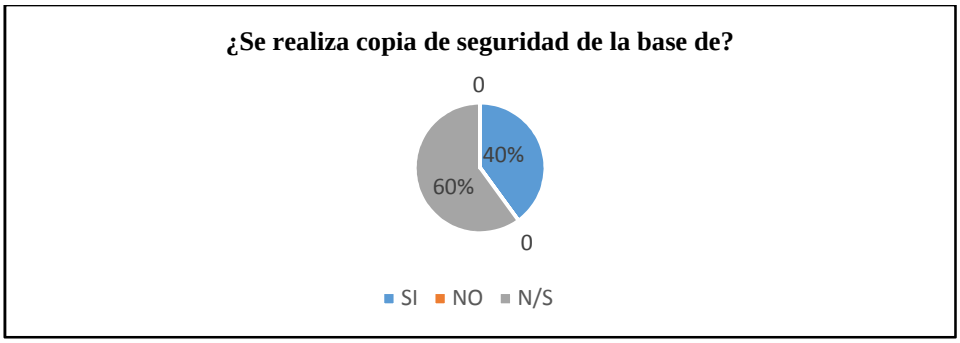
Teniendo en cuenta el resultado el 80% la gran mayoría de los funcionarios conoce la función de los servidores y para que están diseñados. Se debe tener en cuenta que los funcionarios tienen claro donde se almacenan y administran la información principal de la entidad, por ende la prudencia al no ingresar a los centros de datos.



Gráfica No. 5 Fuente: Investigadores

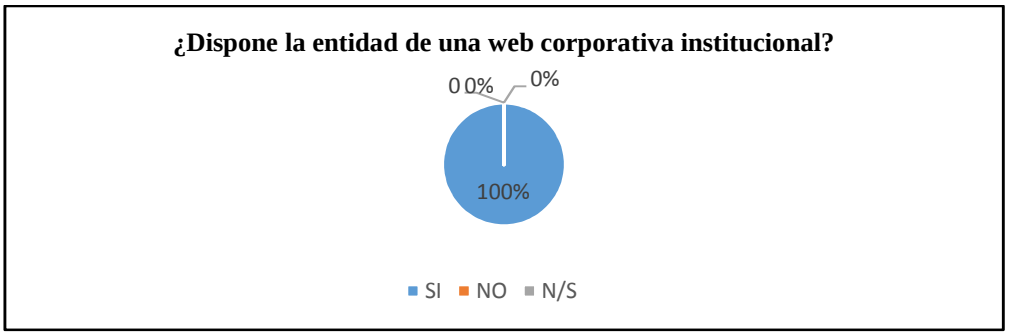
Teniendo en cuenta el resultado el 86.66% confirman que conservan información laboral en los equipos de cómputos; información vulnerable a robo, alteración, confidencialidad en las bases de datos, la transparencia de los datos, hay que

tener en cuenta que entre más información se guarde es más lo que debe proteger.



Gráfica No. 6 Fuente: Investigadores

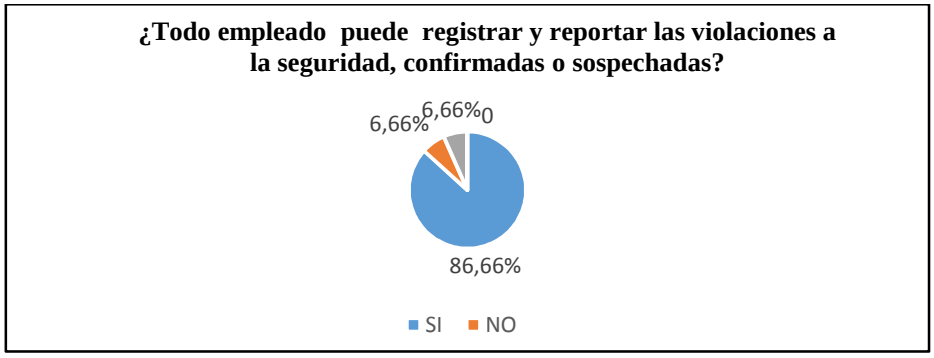
En este ítem, 9 personas no saben no responden constituyendo el 60% del 100%, se puede concluir que en la entidad la mayoría de los usuarios no tienen el conocimiento sobre el manejo que se le debe dar a la información, por lo que se convierte en una amenaza para la perdida de la misma.



Gráfica No. 7 Fuente: Investigadores

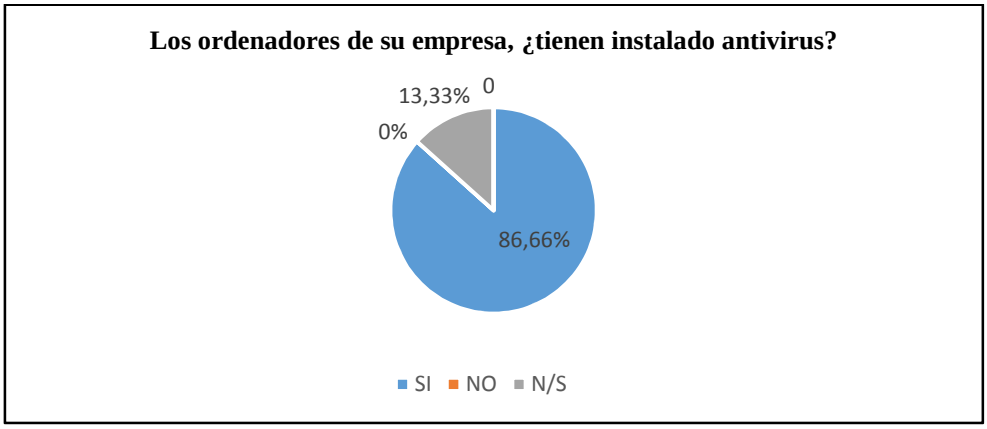
En este ítem, el 15% del 100% contesto de forma afirmativa. La entidad cuenta con una página web y los funcionarios están familiarizados con la misma; Se recomienda hacer auditorías a los procesos de liquidación y tener en cuenta que cuanto más valiosa sea la información en su base de datos, mayores serán las probabilidades de que la información sea blanco de ataques como el de Injection, el cual corresponde a inyección de código “inyecciones SQL”, el cual es uno de los ataque más comunes; Otro ataque que se puede presentar es el de Unvalidated Redirects and Forwards, con este la página corporativa, esta puede ser atacada por los atacantes utilizando las direcciones que utilizan los funcionarios desde la página corporativa a otros sitios, mediante la modalidad de untrusted, dirigiéndolos a otros sitios de phishing o que pueden contener Malware.

7.1.2 Responsabilidad y Control de los Activos



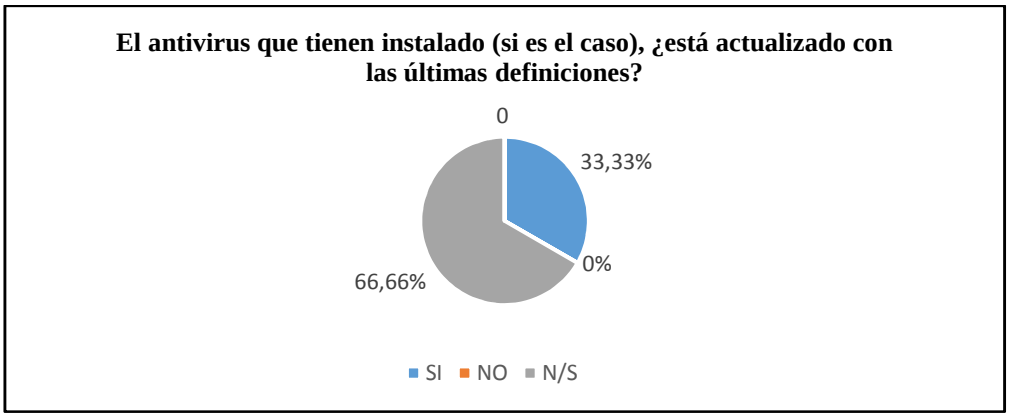
Gráfica No.8 Fuente: Investigadores

En este apartado 13 funcionarios contestaron de forma afirmativa lo cual es el 86,66 %, de 100% tienen la libertad y autoridad de reportar cualquier riesgo que pueda exponer la seguridad en las bases de datos, según en este resultado se evidencia que se presenta desconocimiento al protocolo a seguir; es importante que en todas las dependencia exista un representante del comité de seguridad el cual será el encargado de recibir los registros de violaciones de cualquier índole y a la vez realizar el registro ante el comité.



Gráfica No. 9 Fuente: Investigadores

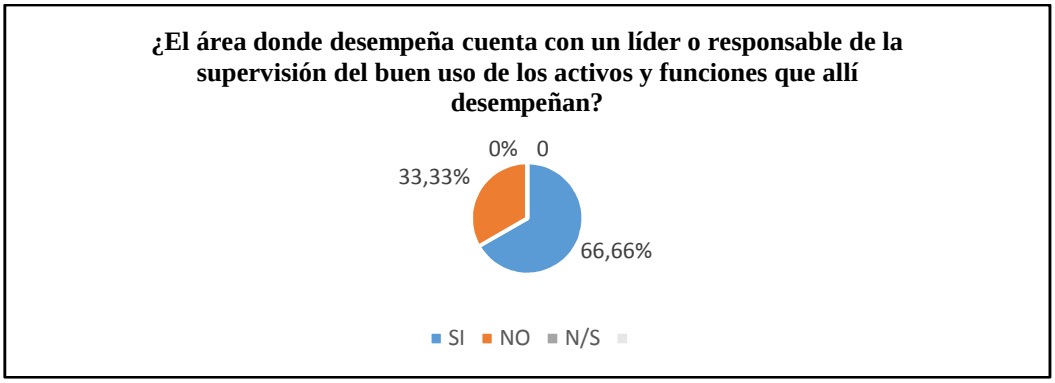
El análisis arroja que los equipos de cómputos cuentan con antivirus, en la actualidad, es prácticamente imposible navegar la web sin estar debidamente protegidos ante las amenazas. Los engaños son muchos, y las probabilidades de ser víctimas de un ataque de Virus o Malwares también. Es por ello que una de las mejores tácticas para prevenir ser infectados es la utilización de un buen antivirus y su constante actualización.



Gráfica No. 10 Fuente: Investigadores

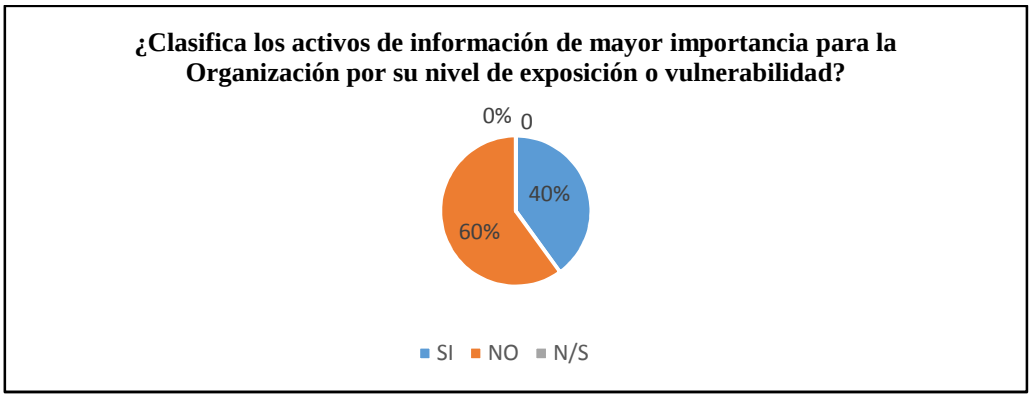
En este ítem, el 66.66% no saben no responden. Cada día se crean virus con fines malintencionados y si no se actualiza el antivirus, la base de datos donde están los códigos de detección estará obsoleta, colocando en peligro el sistema operativo y los archivos existentes en el equipo de cómputo.

Los funcionarios deben estar comprometidos con la entidad y velar por la seguridad en las bases de datos e informar cuando estos se encuentren caducados.



Gráfica No. 11 Fuente: Investigadores

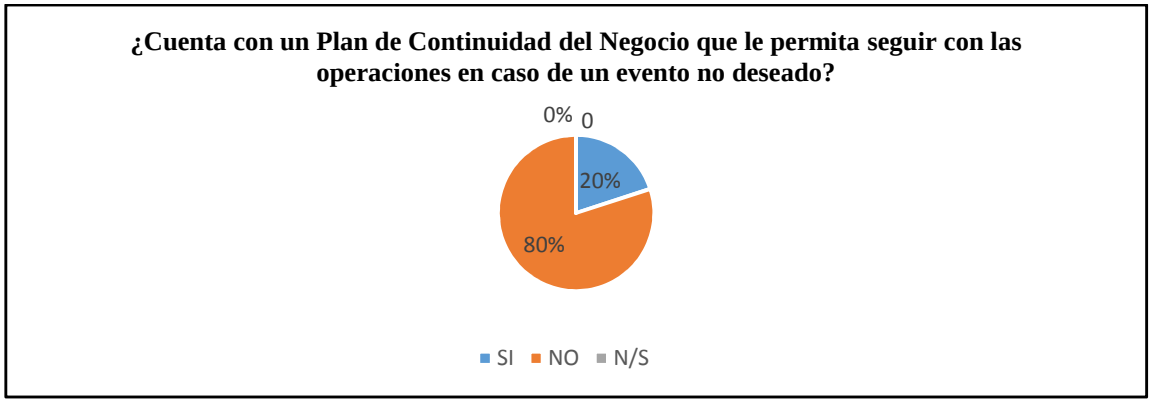
Existen amenazas relacionadas con falla humanas, con ataques malintencionados, por eso la importancia que exista un Asesor para poyar cada una de las actividades y velar por el buen uso en las bases de datos y de los recursos físicos.



Gráfica No. 12 Fuente: Investigadores

El análisis reporta que el 60% del 100% los funcionarios no clasifica la información de mayor importancia según el nivel de vulnerabilidad, lo que indica que falta un poco conocimiento de las políticas de seguridad existentes, lo cual pone en riesgo información confidencial.

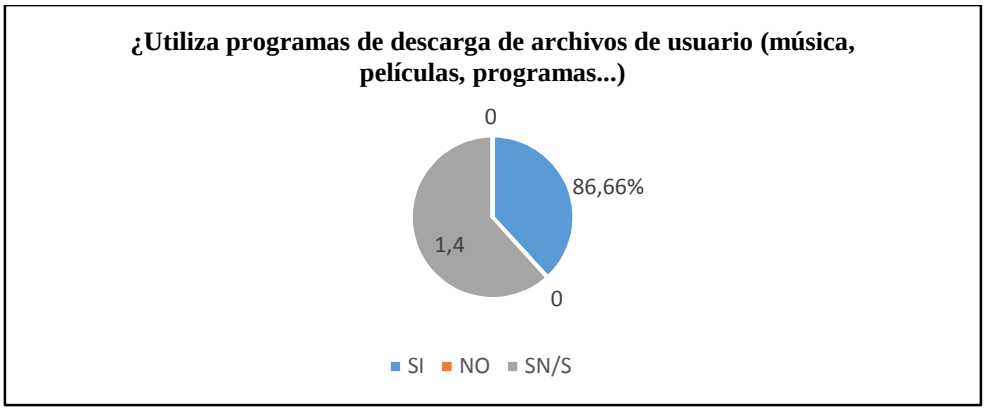
Frente a los resultados, es importante que se realice la gestión de activos donde se incluye la clasificación de estos, tales como servidores, estaciones de trabajo, computadores de escritorio, portátiles; teniendo en cuanta que estos permiten el acceso a las bases de datos y a información confidencial tributaria.



Gráfica No. 13 Fuente: Investigadores

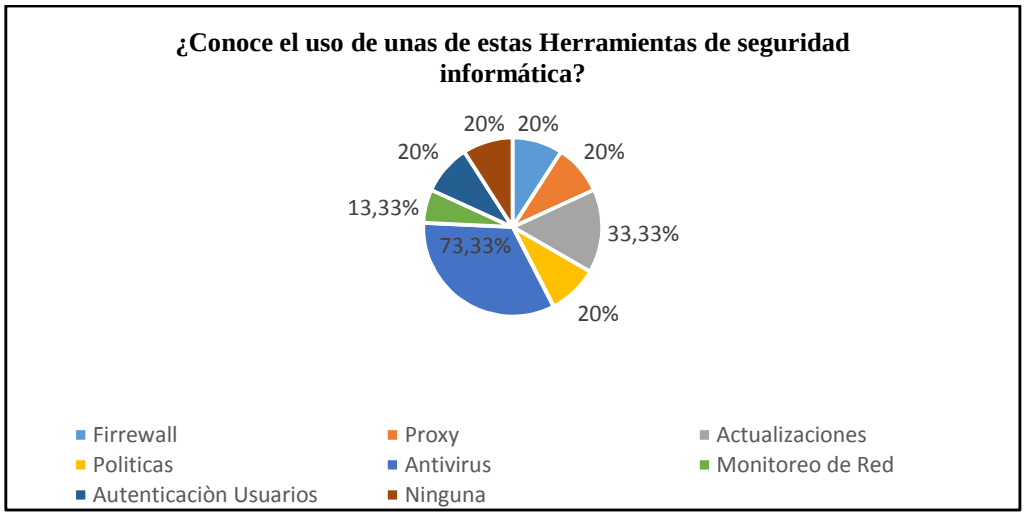
El plan de continuidad de negocio tiene como objetivo principal proteger los procesos críticos y operativos del negocio contra desastres naturales o fallas mayores por la interrupción de las operaciones de una entidad, disminuyendo el impacto financiero, pérdida de información crítica, credibilidad y productividad, por lo anterior se debe incluir dentro de las políticas de seguridad implementar un plan de continuidad en cada uno de los procedimientos que se realizan y así garantizar la integridad y disponibilidad en las Bases de Datos.

7.1.3 Seguridad Personal, Física y Ambiental



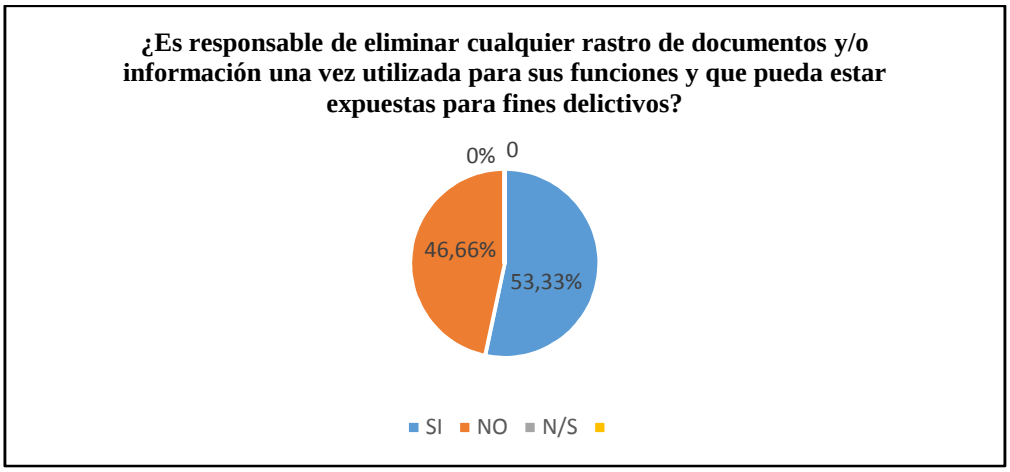
Gráfica No. 14 Fuente: Investigadores

El 86.66% contestaron que si realizaban descargas y sólo el 1.4% contestaron de forma negativa, lo cual se convierte en una vulnerabilidad, debido a que comúnmente no se verifica si la fuente que se consulta es legítima y de confianza; y se tiene el riesgo de descargar virus o permitir el fácil acceso al equipo de cómputo.



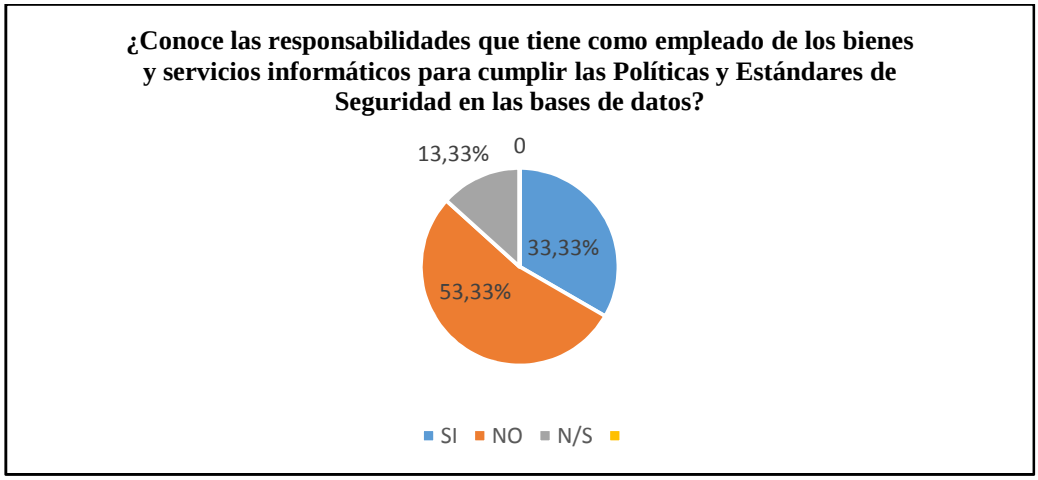
Gráfica No. 15 Fuente: Investigadores

En el presente Ítem podemos observar que hay un conocimiento general de las herramientas de Seguridad en los cuales se pueden apoyar para proteger la información y los equipos de la Entidad.



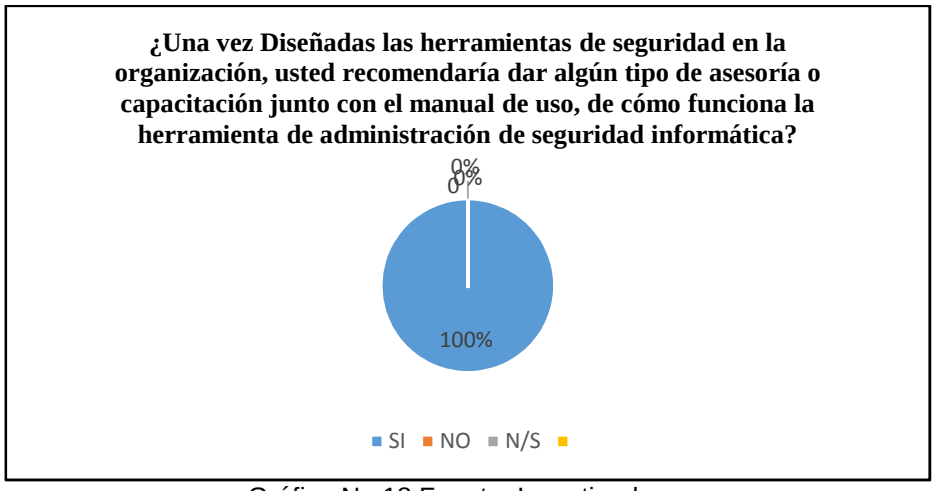
Gráfica No. 16 Fuente: Investigadores

En este Ítem el 46.66% respondió que no. Dejar a la vista información confidencial crea puntos débiles y vulnerables en la seguridad de las bases de datos. Comúnmente se toma nota de los usuarios y contraseñas que se asignan para acceder el sistema sin tener la precaución de eliminar o resguardar dicha información; este tipo de vulnerabilidad pone en riesgo el acceso a los sistemas de información y a las bases de datos.



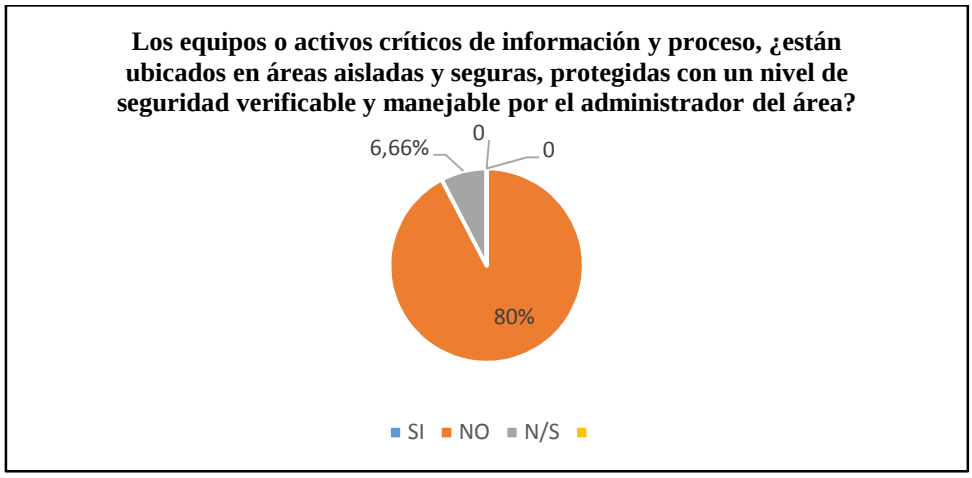
Gráfica No. 17 Fuente: Investigadores

El 53,33% desconoce las responsabilidades que tiene en cuanto las políticas de seguridad, el desconocimiento del riesgo que puede causar como operador activo en las bases de datos expone a posibles ataques los sistemas de información y las bases de datos.



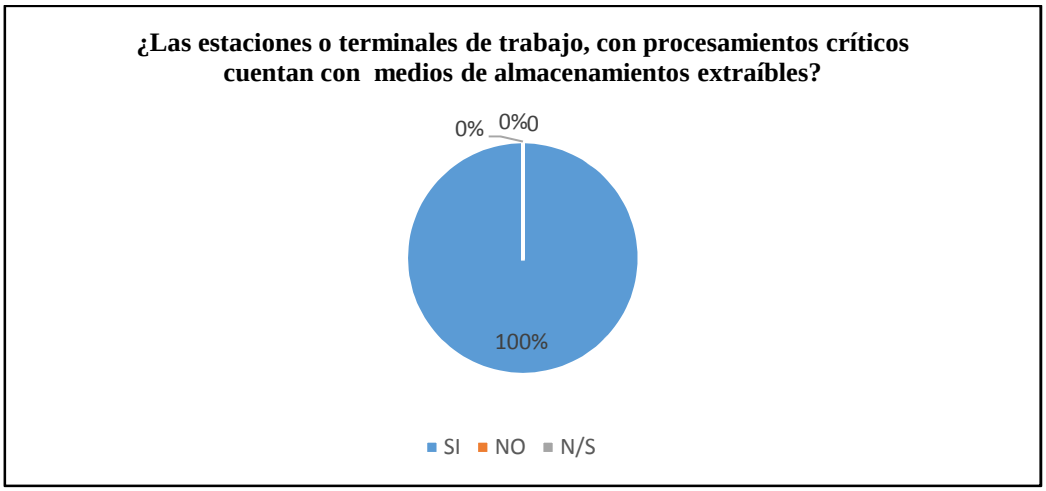
Gráfica No.18 Fuente: Investigadores

En este ítem puede ver que los encuestados están de acuerdo con la realización capacitaciones sobre las políticas de seguridad ya que con esto se minimiza la exposición y pérdida de los activos para este caso información tributaria.



Gráfica No. 19 Fuente: Investigadores

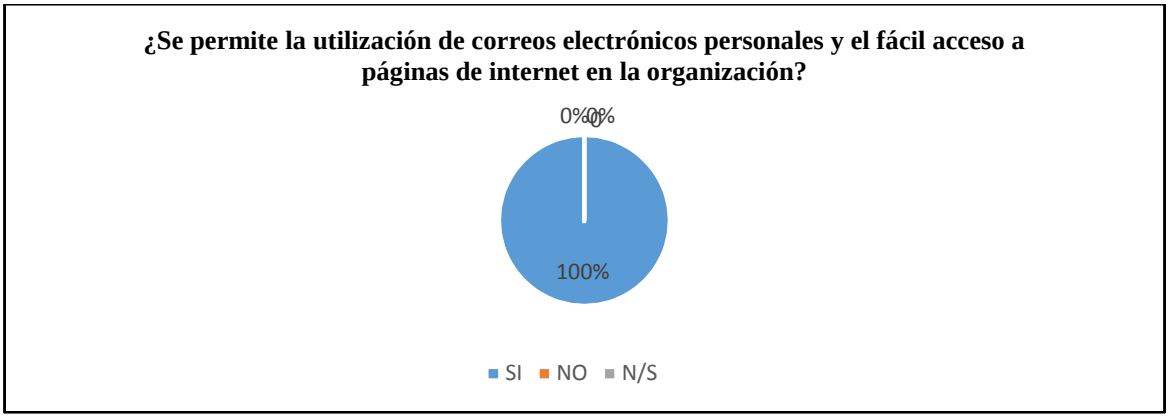
El 80% contestaron de forma negativa lo que lo convierte en una vulnerabilidad ya que actualmente cualquier funcionario puede hacer uso de ellos.



Gráfica No. 20 Fuente: Investigadores

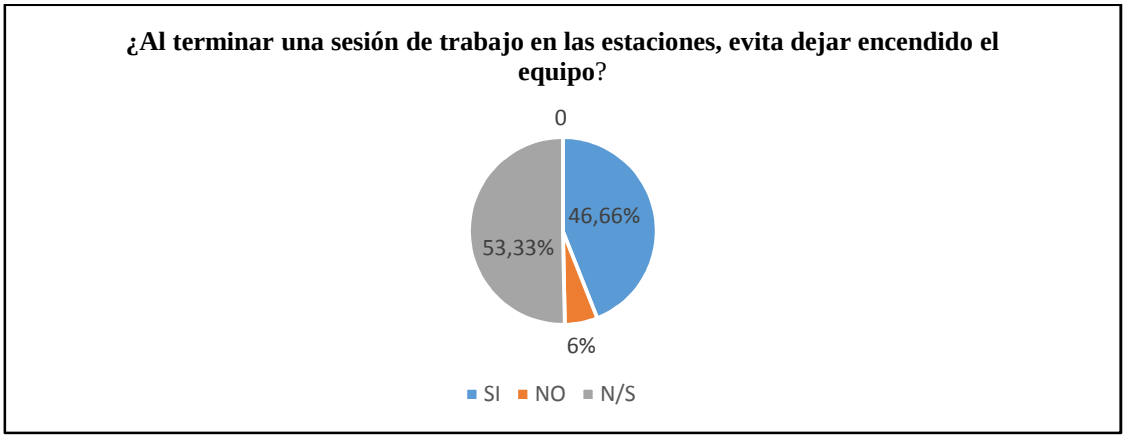
El 100% de los encuestados confirma que tienen acceso a medios de almacenamiento extraíble; ocasionado riesgos de hurto de información y/o contaminación de virus.

7.1.4 Control de Acceso



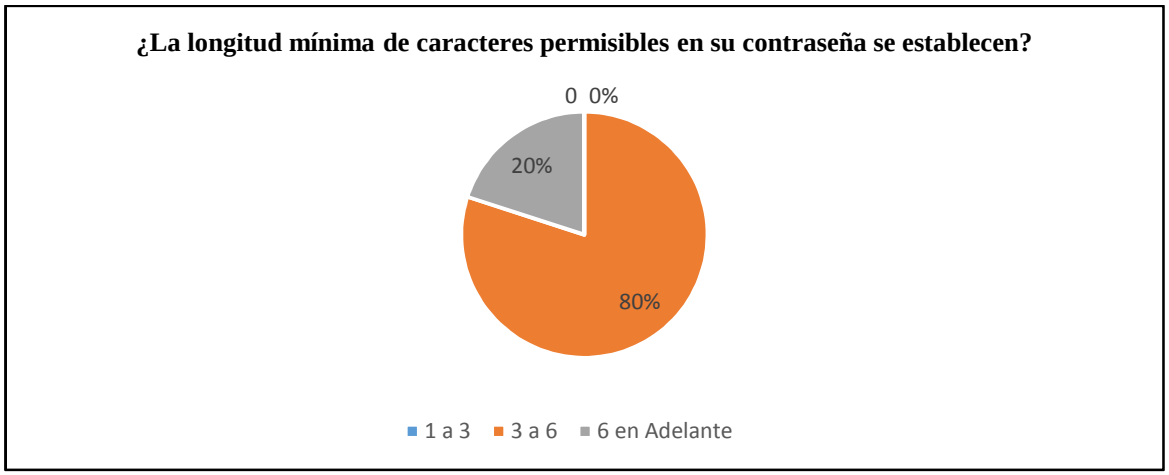
Gráfica No. 21 Fuente: Investigadores

En este ítem El 100% de los encuestados contestaron de forma afirmativa, se puede determinar que se presentan una vulnerabilidad por la falta de restricción a páginas y correos donde puede ingresar los hacker y tener acceso a la información o bases de datos.



Gráfica No. 22 Fuente: Investigadores

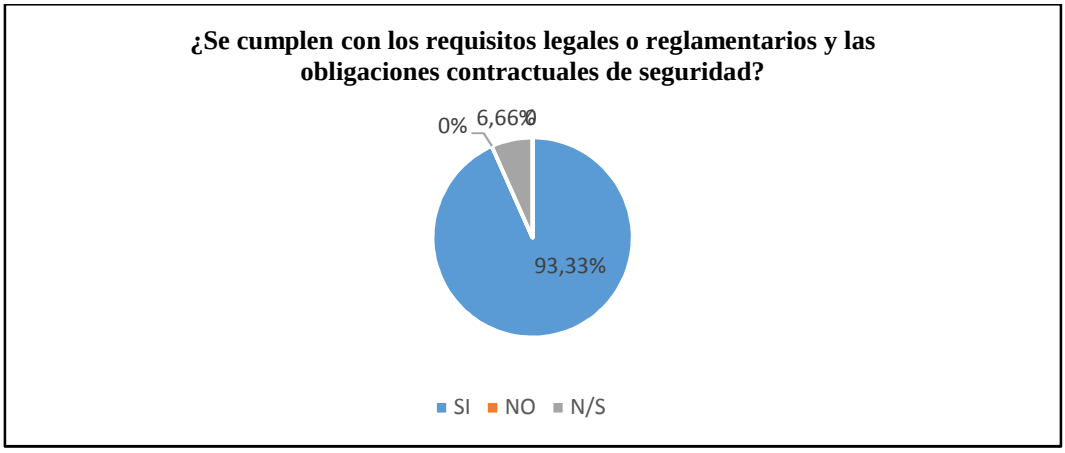
En este ítem más del 50% de las personas encuestadas contestaron que dejan encendidos los equipos de cómputos cuando están por fuera del área de trabajo, esta vulnerabilidad pone en riesgo la información y el acceso a las bases de datos.



Gráfica No. 23 Fuente: Investigadores

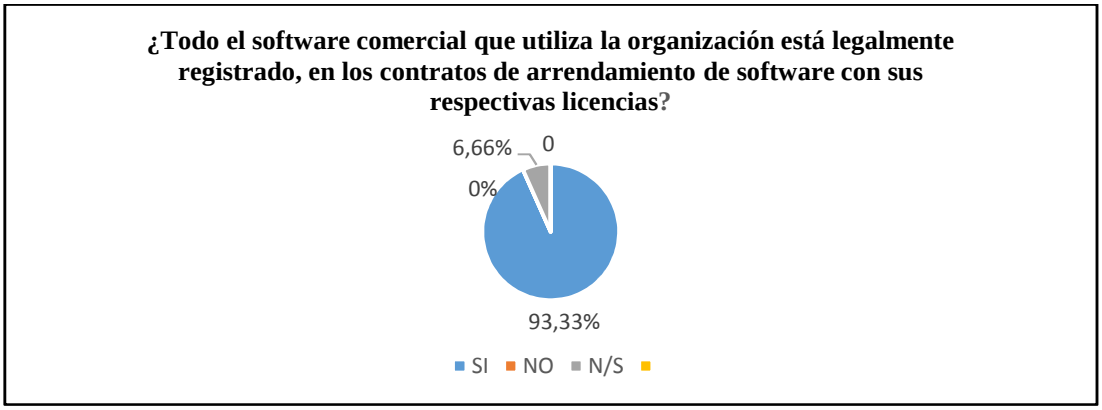
En necesario confeccionar contraseñas más seguras, de tipo alfanumérico y de 6 o más caracteres y así se evitara que cualquier "hacker" pueda romper las claves y acceder a las bases de datos.

7.1.5 Lineamientos Legales



Gráfica No. 24 Fuente: Investigadores

La respuesta de este Ítem fue de manera favorable ya que es indispensable que se cumplan con los lineamientos legales, lo que garantizara objetivos claros a la hora de implementar la seguridad en las bases de datos.



Gráfica No. 25 Fuente: Investigadores

La implementación de software legal con respaldo técnico es de mucha importancia para mantener un nivel aceptable de operación para el buen funcionamiento de los sistemas de información y protección de las bases de datos.

7.1.6 ANALISIS DE VULNERABILIDADES DE LA BASE DE DATOS PREDIALIBA

Para identificar las vulnerabilidades presentes en las Bases de Datos predialiba se utiliza una copia para evitar causar daños a la original.

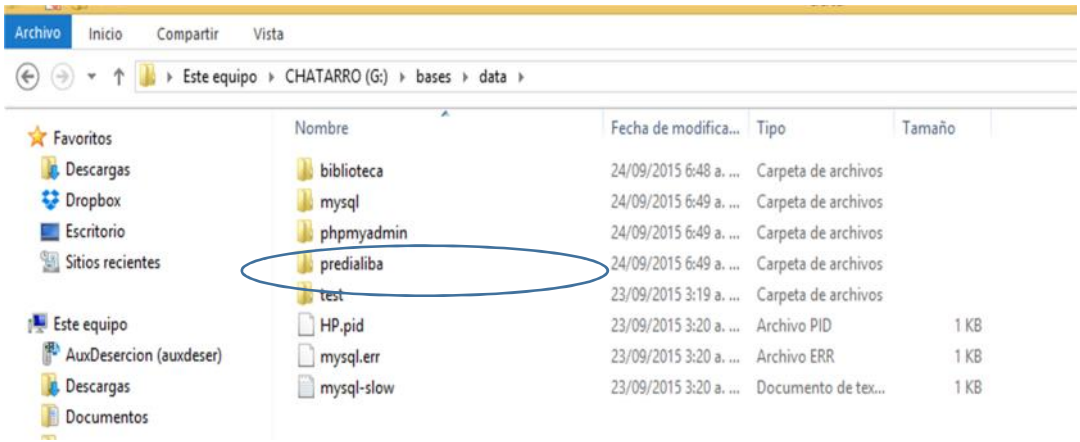


Imagen No.2 Identificación de la base de datos

Se maneja la herramienta sqlmap que permite detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web, además permite realizar ataques SQLi (SQL Injection), se encarga de realizar peticiones a los parámetros utilizados en una url que se le indique o también la ruta si es una base local para el caso trabajado.

Esta herramienta se utilizó en compañía del phyton

Se inicia sqlmap

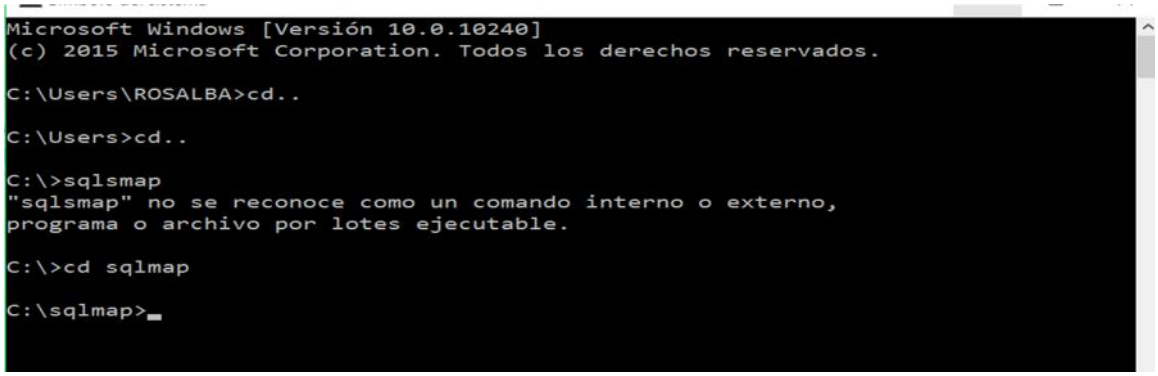


Imagen No.3 Se ejecuta herramienta sqlmap

7.1.6.1 Primer ataque de injection

Se realiza el primer ataque para saber cuáles bases de datos tiene con el siguiente código 1. sqlmap.py -u http://localhost/inyecciones.php?id=db c:\wamp\bin\mysql\mysql5.6.17\data –dbs

Como se puede ver se detecta la vulnerabilidad, se evidencia 5 bases de datos entre ellas **predialiba**

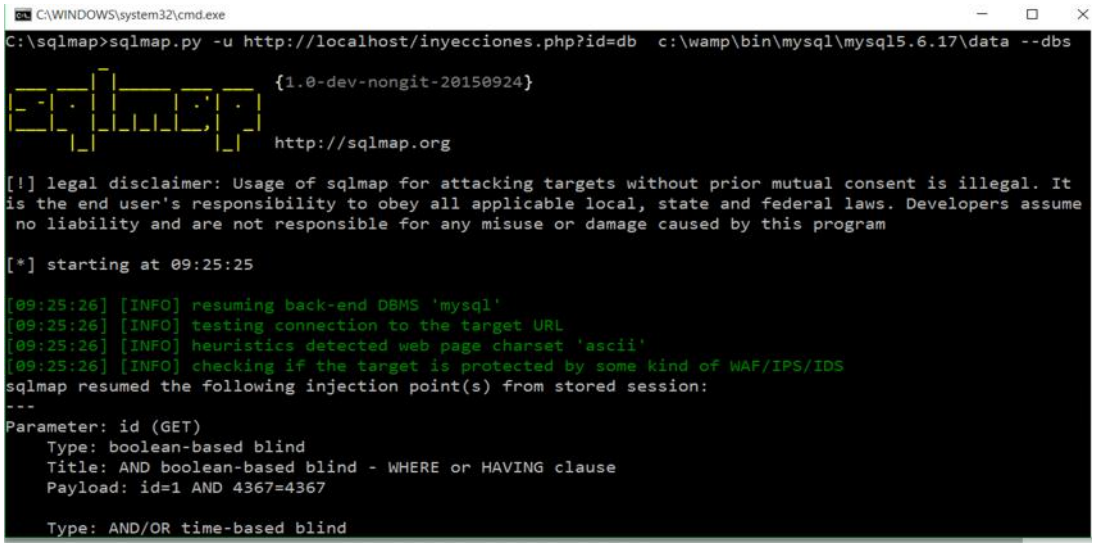


Imagen No.3 Ataque sqlmap.py -u http://localhost/inyecciones.php?id=db c:\wamp\bin\mysql\mysql5.6.17\data –dbs

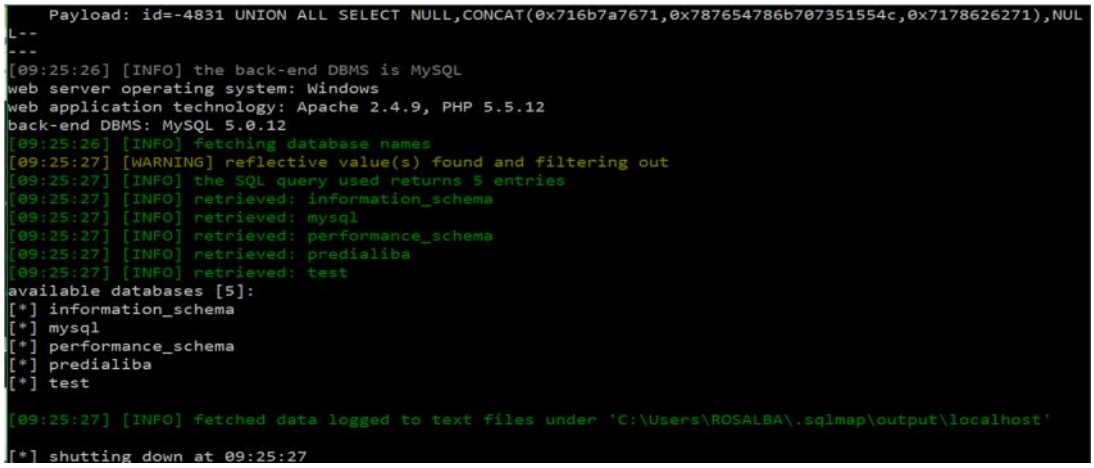


Imagen No. 4 Vulnerabilidades detectadas

7.1.6.2 Segundo ataque de injection

En este segundo ataque se busca poder ver las tablas que contiene la base de datos predialiba con el siguiente código

sqlmap.py -u http://localhost/inyecciones.php?id=predialiba
c:\wamp\bin\mysql\mysql5.6.17\data –tables

Imagen No. 5 Revelación de tablas

Se puede evidenciar la segunda vulnerabilidad se pueden visualizar las tablas, usarios_ login es para un hacker maligno la entrada con usuarios y realizar cambios, borrar o robar la información de la bases de datos.

7.1.6.2 Análisis Método Magerit

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Para el caso de este proyecto se seleccionó la metodología MAGERIT para la evaluación de riesgos en la entidad.

- ✓ Identificación de Riesgos

  Identificación de Activos

  Activo de Hardware

  Computadores de escritorios

  Activos de Software

  Linux

  Windows server 2003

  Windows 7 y Windows 8

- ✓ Dependencia entre Activos

Los activos dependen unos de otros por ejemplo un computador no funciona sin software

- ✓ Valoración de los Activos

La valoración que se realizó para los servicios depende de los siguientes items:

D: Disponibilidad, se indica el impacto que tendría en la entidad el hecho de que no estuviera la información cuando se requiera.

I: Integridad de los Datos, se indica el impacto que tendría la organización el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta.

C: Confidencialidad de los Datos, se indica el impacto que tendría la entidad el hecho de que la información que se maneja fuera accedida por personas no autorizadas.

A: Autenticidad de los Datos, se indica el impacto que tendría hecho de que no se pueda saber a ciencia cierta quién ha accedido a la información que se maneja para prestar el servicio.

T: Trazabilidad, se indica el impacto que tendría en la organización el hecho de que no se pudiera conocer quien hace cambios en la información.

- ✓ Identificación de Amenazas

Al ingresar a la bases de datos y poder ver el contenido de las mismas se pueden identificar las siguientes amenazas.

Robo de información

Borrar información

Cambio de información

- ✓ Identificación de Vulnerabilidades

De acuerdo a la identificación de amenazas de pueden ver las posibles amenazas a que están expuestas las bases de datos de la entidad, además de mostrar la frecuencia o posibilidad de las mismas (vulnerabilidad), que varían entre el nivel M (Medio) y A (alto).

Robo de información = A

Borrar información = A

Cambio de información = A

- ✓ Análisis y Evaluación De Riesgos

A partir de la información proporcionada por la práctica realizada, se procede a valorar el Impacto que puede producir la materialización de una amenaza sobre el activo.

Muestra el impacto en la Disponibilidad = alto

Muestra el impacto en la Integridad = alto

Muestra el impacto en la Confidencialidad= critico

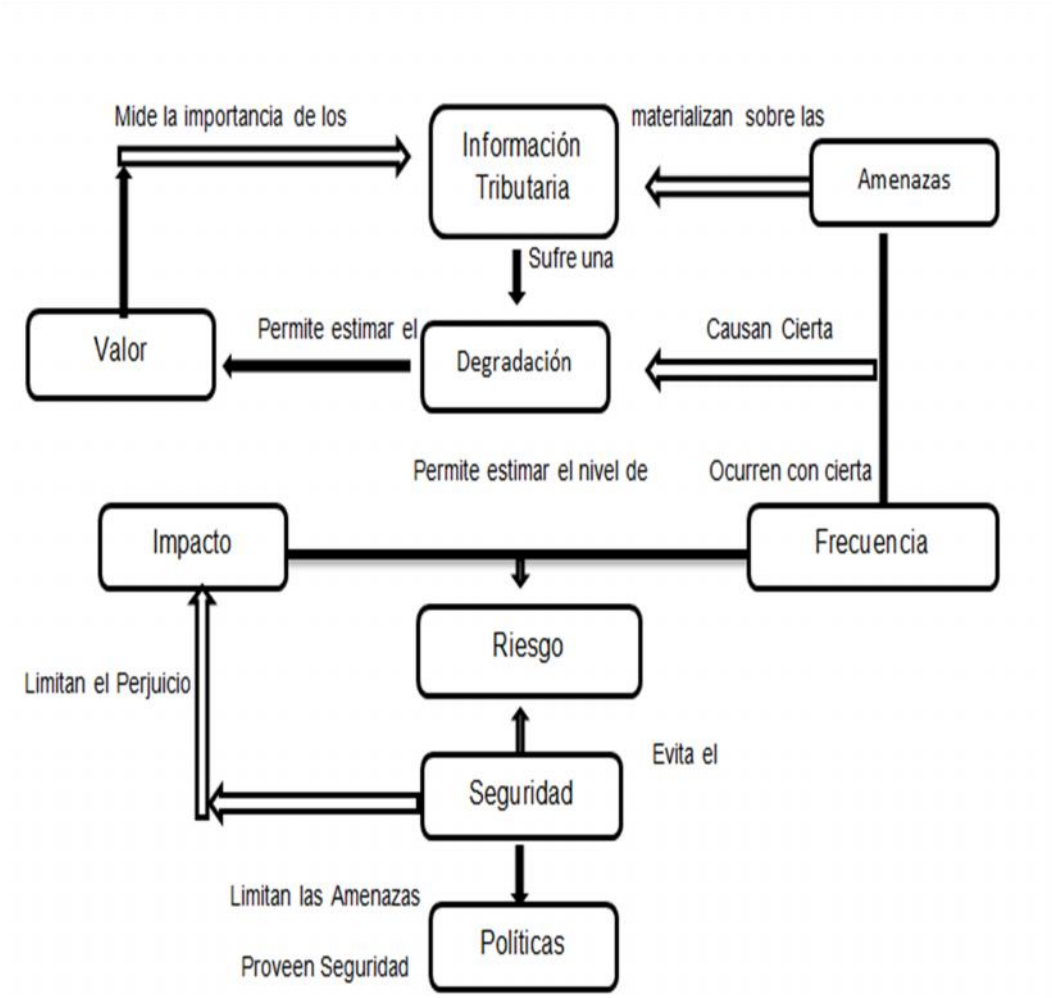


Imagen No. 6 Análisis Método Magerit

7.2 FASE 2: ANALISIS DE MATRIZ DOFA Y FORTALECIMIENTO DE LAS POLITICAS EXISTENTES

Fase 2	Objetivos	Actividades a Analizar
Análisis de Matriz DOFA y Fortalecimiento de las Políticas de Seguridad existentes	✓ Analizar las debilidades, oportunidades, fortalezas y amenazas que presentan las políticas de seguridad existentes. ✓ Proteger la información contra accesos no autorizados. ✓ Fortalecer las áreas donde se presentan deficiencias de seguridad.	✓ Realizar Análisis de Matriz DOFA. ✓ Creación de nuevas Políticas para fortalecer la seguridad en las bases de datos.

Tabla No. 3 Análisis de matriz Dofa y fortalecimiento de las políticas existentes

7.2.1 Matriz DOFA sobre la Seguridad en las bases de datos de una entidad pública.

DEBILIDADES	FORTALEZAS
Se presenta desconocimiento en los objetivos que se traza la entidad para la seguridad en las bases de datos.	Cuenta con comité de apoyo en Seguridad informática definido.
Se almacena información confidencial en los discos duros de los equipos de la entidad.	La entidad cuenta con servidores de bases de datos garantizan la seguridad y la integridad de los datos.
No todos los ordenadores cuentan con los antivirus actualizados.	Se realizan backup diarios para proteger la información ante cualquier eventualidad.
Los equipos no cuentan con restricción para descargar archivos o revisar páginas en línea.	Los Ordenadores de la entidad cuentan con antivirus.
Se presenta uso inadecuado en el manejo en las bases de datos y equipos de cómputos.	Se cuenta con un plan de continuidad.
Los activos críticos de información se encuentran expuestos.	Las contraseñas para ingresar al sistema de información y bases de datos son alfanuméricas y con capacidad de 6 caracteres en adelante.
Los equipos de cómputos se encuentran con puertos y unidades magnéticas extraíbles habilitadas.	La entidad cumple con los lineamientos legales de seguridad.
Se permite el acceso a correos personales.	La entidad cuenta con software legal con respaldo técnico
OPORTUNIDADES	**AMENAZAS**
Existencia de nuevas tecnologías informáticas.	Ausencia de voluntad para sumir la responsabilidad que tiene cada funcionario frente al manejo de seguridad en las bases de datos.
Apoyo al diseño de plan estratégico para fortalecer las políticas de seguridad en las bases de datos existentes propuestas en este trabajo de grado.	Insuficiente recurso humano para socializar las políticas y objetivos en seguridad informática que se traza cada año.
Contar con el presupuesto para comprar herramientas de apoyo y fortalecer la seguridad en las bases de datos.	Funcionarios que utilicen la información para fines no laborales.
	Pérdida de Información por infección de Virus.

Tabla No. 4: Matriz DOFA. Fuente: Gestión estratégica organizacional, edited by Jorge Eliécer Prieto

7.2.2 CREACION DE POLÍTICAS DE SEGURIDAD APLICABLES A LAS BASES DE DATOS

7.2.2.1 Responsabilidad

Es necesario de que los funcionarios de la Entidad, sin importar el nivel jerárquico se responsabilicen en aplicar las políticas de seguridad dentro del área que tienen a cargo.

7.2.2.2 Cumplimiento

El cumplimiento de las políticas de seguridad se debe hacer bajos las normas ley.

7.2.2.3 Sanciones por incumplimiento

El incumplimiento de las políticas de seguridad, llevara las sanciones de acuerdo a las normas penales de ley, y aplicación de las normas contractuales.

POLITICA	USO
Seguridad Institucional	Toda persona que firme cualquier tipo de contratación con la Entidad deberá firmar un documento de confidencialidad y buen uso en las bases de datos, que se encontrara anexo al contrato, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.
Capacitación en seguridad informática	Todo servidor o funcionario nuevo deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática y Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento. Esta capacitación se realizará de manera presencial y será requisito para iniciar labores.
Administración de Operaciones en los Centros de Cómputo	Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.

Publicación y Difusión de las Políticas de Seguridad	✓ Se debe decidir correctamente hacia qué grupos van dirigidas las políticas de seguridad, por qué medios se van a dar a conocer, si se desea que otros grupos puedan conocer su contenido. ✓ El objetivo principal de la publicación y difusión es que el grupo objetivo entienda en qué consisten las políticas y se cree conciencia sobre su importancia a través de pláticas y talleres para tal fin. ✓ Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
Realizar Backus de bases de datos	✓ Se diseña dentro de las Políticas de Seguridad Informática, la realización diaria de la copia de seguridad por parte de cada uno de los funcionarios, siendo su responsabilidad la información de la entidad que esté bajo su coordinación. Esta copia deberá ser coordinada con el Proceso de Gestión de Infraestructura con el fin de salvaguardar la información de la entidad, ante posibles riesgos ya sean por causas naturales, humanas o ataques de terceros. ✓ Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

Tabla No. 5: Políticas para la Organización de la Seguridad

POLITICA	USO
Protección en las bases de datos y de los bienes informáticos	✓ El usuario o funcionario deberá reportar de forma inmediata al Grupo de Informática cuando se detecte riesgo alguno real o potencial sobre la información contenida en las bases de datos y equipos de cómputo; la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes. ✓ Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo que tenga asignado. ✓ Se prohíbe el acceso a la red a cualquier equipo de cómputo que no pertenezca a la entidad, así como la instalación o almacenamiento de información en equipos de cómputo y medios extraíbles. ✓ Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información que pertenezcan a la entidad podrán ser retirados del lugar asignado únicamente con la autorización de salida del área de Inventarios, anexando el comunicado de autorización del equipo debidamente firmado por el Director del Grupo de Informática y/o Recursos Físicos. ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones fijadas al cargo, queda prohibido realizar cualquier otra actividad no autorizada. ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\. ✓ Los usuarios y funcionarios que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red. Dichas medidas la encuentran en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios. ✓ Los equipos de cómputo de la entidad solo contaran con la instalación del sistema de liquidación para su respetivo impuesto, páginas institucionales de Difusión, acceso a la intranet y el chat permitido para comunicaciones internas.

	✓ Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Grupo de Informática. ✓ Al momento de asignar un equipo de cómputo a los funcionarios será responsabilidad del soporte técnico del grupo de informática la desinstalación de unidades extraíbles e inhabilitar los puertos USB, para evitar perdida de información. ✓ Queda prohibido instalar software no autorizado o que no cuente con licencia, El Grupo de Informática deberá realizar las instalaciones de acuerdo con los estándares autorizados. ✓ El uso del enlace a Internet, para la navegación a páginas: con Internet Explorer, Mozilla FireFox o cualquier otro navegador desde los equipos de cómputo de la IUCMC, ✓ El servidor o funcionario deberán dar aviso inmediato al Grupo de Informática, de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.
Asignación y Uso de Contraseñas	✓ La solicitud de usuario y contraseña se realizara mediante un oficio autorizado por el Director del grupo asignado y debe registrar los datos básicos del funcionario como son: Actividad a realizar, Nombre completo, Identificación, Dirección, Email y Teléfono y esta se realizada de forma individual, la cual se le enviara al funcionario al Email que registro en su solicitud. ✓ Con tres (3) intentos fallidos para acceder al sistema, el sistema bloqueara a dicho usuario, el cual deberá acudir al Grupo de Informática para que se le restablezca dicho acceso. ✓ Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso o dejarlos visibles a personas no autorizadas puedan descubrirlos.

Tabla No. 6: Políticas para la seguridad personal, responsabilidad y control de los activos

POLITICA	USO
Seguridad en las bases de datos	✓ Los usuarios y servidores deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial. ✓ Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC´s) serán registradas y podrán ser objeto de auditoría.
Protección y ubicación de los equipos	✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Grupo de Informática, en caso de requerir este servicio deberá solicitarlo. ✓ El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos que se le asignen y de conservarlos en la ubicación autorizada por del Grupo de Informática. ✓ El Grupo de Informática velará para que los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups. ✓ Será responsabilidad del grupo de Informática, ubicar los servidores en un centro de Datos, al cual solo podrá acceder el administrador asignado para esa actividad. ✓ Únicamente el personal autorizado por el Grupo de Informática podrá llevar a cabo los servicios y reparaciones al equipo informático.

Tabla No. 7: Políticas para la seguridad Física y Ambiental

POLITICA	USO
Acceso Lógico	Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, de su "ID" login de usuario y contraseña necesarios para acceder a los sistemas de información y a la infraestructura tecnológica de la entidad, por tanto se deberá mantener de forma confidencial.
Cierre de sesión y bloqueo de acceso al equipo ante ausencias temporales	Cuando un usuario de cualquier Sistema de Información, se deba ausentar de su puesto de trabajo por periodos relativamente cortos, deberá dejar la pantalla de su equipo bloqueada con un password o clave que solo el funcionario conozca.
Acceso por parte de terceros	✓ El acceso a la información a terceros debe limitarse a lo mínimo indispensable para cumplir con el trabajo asignado. Las excepciones deben ser analizadas y aprobadas por el área de seguridad informática. ✓ Se asignara un supervisor a los contratos realizados con terceros de manera que sea el responsable en las bases de datos que se le suministra y la verificación del cumplimiento de la labor contratada.
Controles para Otorgar, Modificar y Retirar Accesos a Usuarios	✓ Cualquier nuevo rol creado por el grupo de Informática se deberá analizar y concertar con el Comité Técnico de Sistemas. ✓ El Grupo de Informática, en cabeza del Jefe de Sistemas o su delegado en caso de ausencia, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.
Uso del Correo electrónico	✓ Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Entidad, a menos que cuente con la autorización del Grupo de Informática. ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.

Tabla No. 8: Políticas para el Control de Acceso

POLITICA	USO
Lineamientos a seguir	✓ Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la entidad, que no esté autorizado por el Grupo de Informática. ✓ El Grupo de Informática, tiene a su cargo la tarea de informar periódicamente a la Directores y funcionarios, las Políticas y Estándares de Seguridad Informática en contra de la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Emails, Carteleras y Boletines. Debemos considerar también la publicación de las posibles sanciones o multas en los que se puede incurrir. ✓ El Grupo de Informatice tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Entidad.

Tabla No. 9: Políticas para Lineamientos Legales

POLITICA	USO
Derechos de Autor	Las bases de datos, o los distintos tipos de repositorios electrónicos, son creaciones intelectuales sujetas a la protección del Derecho de Autor. La Entidad es la titular de las bases de datos que utiliza, para lo cual se sujeta plenamente a las normas sobre protección de datos personales y Habeas Data. Por tanto es la única que tiene la facultad para autorizar el uso o disposición de la misma a terceros.
Administrador	La Entidad como titular de derechos sobre la base de datos, autoriza el uso y administración de la misma al Grupo de Informática de la Entidad de Ibagué; el cual designara como administrador de la base de datos a un funcionario de planta con capacidades idóneas para el cargo. El administrador contara con los privilegios requeridos para generar reportes, crear, modificar, actualizar y eliminar información de la bases de datos, documentando mediante observaciones las acciones que realice.
Usuario de Consultas	Se debe delimitar y definir a quien se le asignara el privilegio de realizar consultas a la base de datos por parte de la entidad, tomado así las medidas de seguridad pertinentes.
Manejador de Base de datos	Toda la información tributaria contenida en las bases de datos deberá ser operada a través de un mismo tipo de sistema manejador de la bases de datos, beneficiándose con esto de los mecanismos de integridad, seguridad y recuperación en las bases de datos en caso que se llegue a presentar una falla.
Responsabilidades de Uso	✓ Las bases de datos estarán alojadas en un centro de datos, bajo la supervisión y responsabilidad del grupo de informática. La Entidad debe disponer de recursos humanos y tecnológicos para proteger la confidencialidad, integridad y disponibilidad en las bases de datos y de sus bases de datos. Para cumplir con esta misión, El grupo de Informática cuenta con un firewall, un sistema de prevención de intrusos, una solución para gestión de vulnerabilidades técnicas, una solución para protección de código malicioso, planes de

	contingencia para los productos críticos y procedimientos para gestión de incidentes de seguridad. El Administrador reconoce que la administración de las bases de datos puede implicar un nivel de riesgo, el cual asume y acepta y, por consiguiente, la entidad no otorga ninguna garantía ni asume ninguna obligación o responsabilidad por pérdida o sustracción de información de su sistema informático. ✓ El Administrador designado se compromete a conservarla y mantenerla de manera estrictamente confidencial y no revelarla a terceros. Esta obligación cobija todas las informaciones personales, contables, técnicas, comerciales o de cualquier otro tipo suministradas en la ejecución y ejercicio de sus funciones.
Características en el diseño y Programación de las Bases de Datos	✓ El sistema debe diseñarse a prueba de intromisiones. No deben dejar pasar por alto los controles. ✓ El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las operaciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea. ✓ El Log de Auditoria debe registrar todas las entradas cada vez que un usuario entra, se debe chequear cuándo y desde dónde entró la vez anterior. ✓ Usar técnicas de cifrado para proteger datos en la base de datos. ✓ Administrar debe manejar la Tabla de usuarios con código y contraseña, controlar las operaciones efectuadas en cada sesión de trabajo por cada usuario, estas deberán ser anotadas en la bitácora, lo cual facilita la auditoría de la base de datos. ✓ Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permita tener contingencia y continuidad de negocio. ✓ Para la seguridad en bases de datos en entornos web se debe incluir tipos de seguridad como: los servidores proxy, cortafuegos,

	Algoritmo de Compendio de mensajes y firmas digitales, Secure Sockets Layer (SSL) y secure HTTP (S-HTTP). ✓ Realizar semanalmente los siguientes test de penetración al servidor de base de datos: adquisición fingerprinting/sondeo/descubrimiento, obtención de acceso, revisión de privilegios y compromiso total del host. ✓ El defecto debe ser: sin acceso. ✓ Chequear permanentemente. ✓ Los mecanismos de protección deben ser simples, uniformes y construidos en las capas más básicas del sistema. ✓ Servicio e autenticación, examinando la capacidad del login como único en la red para la autenticación y la seguridad. ✓ El Sistema de Archivos Encriptado proporcionando mayor seguridad. ✓ Proporcionar a los administradores elementos de defensa para la protección de la información en las bases de datos y redes implementando la seguridad IP, en el sistema operativo y la red. ✓ Establecer un SMBD con un subsistema de seguridad y autorización que se encargue de garantizar la seguridad en las bases de datos del acceso no autorizado. ✓ Autorización: usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día. ✓ Proteger todas las puertas que son las entradas en los formularios o cualquier elemento que utilice la etiqueta <input>. ✓ Utilizar como método en los formularios POST en vez de GET. En las entradas para introducir contraseñas, en ver de <input type="text"> se debe emplear: <input type="password"> .

	✓ Realizar pruebas semanales para detectar vulnerabilidades ante las inyecciones SQL usando la extensión de Firefox SQL Inject Me. Comprobando si un formulario de esta página es vulnerable a la inyección SQL con la extensión SQL Inject Me.

Tabla No. 10: Políticas para Fortalecer la Seguridad en la Base de Datos

7.3 FASE 3. DISEÑO DEL PLAN DE SENSIBILIZACION, CAPACITACION Y DIFUSION DE LA POLITICAS DE SEGURIDAD EN BASES DE DATOS.

Fase 3	Objetivos	Actividades a Analizar
DISEÑO DEL PLAN DE SENSIBILIZACION, CAPACITACION Y DIFUSION DE LA POLITICAS DE SEGURIDAD INFORMATICA	✓ Describir la forma en que la entidad proporcionará seguridad e integridad. ✓ Evaluar si las políticas han sido implementadas de manera efectiva. ✓ Evidenciar y/o documentar la corrección de cualquier falla en el cumplimiento de las normas establecidas.	✓ Definir los funcionarios a cargo de la evaluación. ✓ Realizar visitas periódicas a las dependencias que intervienen directamente con la información almacenadas en las bases de datos. ✓ Realizar capacitaciones trimestrales sobre los ataques informáticos realizados a bases de datos más frecuentes y de los cuales se puede ser víctima. ✓ Indagar con los funcionarios responsables de la administración de la información sobre dudas e inquietudes que se puedan presentar en el desarrollo de sus actividades. ✓ Realizar lecciones aprendidas de las fallas presentadas, socializarla y documentarla para el fortalecimiento de las políticas establecidas.

Tabla No. 11. Diseño del Plan de Sensibilización, Capacitación y Difusión de las Políticas

7.3.1 Plan de Seguimiento de las Actividades

ACTIVIDAD	OBJETIVO	ENCARGADO	RECURSO
Diseñar cronograma de capacitación.	Dar a conocer a los usuarios las políticas.	Director de informática Y Comité de Seguridad Informática.	Políticas de seguridad
Preparación del material.	Realizar el diseño del material con las políticas de seguridad.	Director de informática Y Comité de Seguridad Informática.	Económicos divulgación
Capacitación del personal la dependencia de la entidad.	Hacerle llegar a todo los funcionarios las políticas de seguridad establecidas.	Director de informática Y Comité de Seguridad Informática.	Carteleras Computador Proyectores Sala de juntas o auditorio
Evaluación de la puesta en marcha de las políticas.	Realizar la evaluación de los resultados al implantar políticas de seguridad establecidas.	Director de informática Y Comité de Seguridad Informática.	Encuestas

Tabla No. 12 Plan de Seguimiento de las Actividades

8. CONCLUSIONES

Se puede concluir la importancia la seguridad en las bases de datos en la entidad, con la cual se puede proteger los recursos informáticos desde el más simple riesgo has el más potente, siempre teniendo en cuenta el costo - beneficio de las consecuencias pueden acarrear la perdida de la información y los recursos informáticos y principalmente los factores que pueden llegar afectar negativamente esta entidad.

El cumplimiento de las políticas establecidas y el seguimiento de las mismas permitirán medir el nivel de riesgo a que está expuesta la información, por lo anterior se sugiere realizar comité de Seguridad donde se actualicen a los funcionarios de los ataques más frecuentes presentados y las lecciones aprendidas de ellas.

9. RECOMENDACIONES

- ✓ Se deben actualizar los manuales de funciones, adecuando las responsabilidades de los activos reconocidos en el estudio.

- ✓ Para proveer control efectivo y adecuado, la entidad debe ser capaz de apreciar los posibles beneficios y además manejar acertadamente los riesgos y límites de la tecnología de la informática; se deben apreciar precedentes conocidos como perdida y alteración en las bases de datos, que pueden ser ocasionadas por fraudes tecnológicos o por incidentes ocasionados por intrusos,

- ✓ Considerando estos riesgos la Entidad debe adoptar una política formal para la protección y seguridad en las bases de datos, para que sea aplicada a los productos o servicios que oferta, y mucho más conociendo que su operación depende en las bases de datos tributaria contenida en las bases de datos.

10. CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	RESPONSABLE	Febrero				Marzo				Abril					Mayo				Junio				Julio					Agosto				Septiembre				Octubre			
		1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4
Reunión para definir actividades a realizar	Rosalba Rozo Alexa Rodriguez																																						
Enviar documento al Director de Proyecto con los Avances realizados	Rosalba Rozo																																						
Reunión con el Director de Proyecto, para retroalimentar el Trabajo de Grado	Rosalba Rozo Alexa Rodriguez Ing Daniel Andres Guzman																																						
Realizar correcciones al Trabajo de Grado	Rosalba Rozo Alexa Rodriguez																																						
Aprobacion por parte del Director del Trabajo de Grado	Ing. Daniel Andres Guzman																																						
Ajustes finales al Trabajp de Grado	Rosalba Rozo Alexa Rodriguez																																						
Entrega final	Rosalba Rozo Alexa Rodriguez																																						
Reunión con Jurados Asignados por la Unad	Rosalba Rozo Alexa Rodriguez Ing. John Freddy Quintero Tamayo Ing. Salomon Gonzalez																																						
Sustentación de Proyecto de Grado																																							

11. REFERENCIAS BIBLIOGRÁFICAS

- [1]ISO 27000.es. FASK's El portal de ISO 27001 en Español. http://www.iso27000.es/iso27000.html

- [2]MIFSUD, Elvira. Monográfico: Introducción a la Seguridad Informática, Observatorio Tecnológico. Marzo de 2012. http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

- [3] ROMERO, Bella (6 SlideShares), mananger at PROTSEIN, Políticas de seguridad. 11 de julio de 2012. http://es.slideshare.net/bellaroagui/politicas-deseguridad-13610538

- [4] CANO DEL CASTILLO, Andrés Felipe. CIFUENTES SALAZAR, Diana Alejandra. Diseño e implementación de un plan estratégico para la Entidad Disempack Ltda. http://repository.lasalle.edu.co/bitstream/handle/10185/2984/T11.11%20C165d.pdf?sequence=2. Gestión estratégica organizacional, edited by Jorge Eliécer prieto herrera.

- [6]Privacy Rights Clearinghouse, Empowering Consumers. Protecting Privacy. Agosto de 2012. Cómo Proteger su Computadora y su Privacidad. https://www.privacyrights.org/pi36

- [7] BY EMAZA. Seguridad Información -Blog de seguridad en las bases de datos: Marco legal de la ISO 2700. Posted on September 21, 2011 by Emaza http://www.seguridadinformacion.net/marco-legal-de-la-iso-27001/

- [8] An Introduction to ISO 27001, ISO 27002....ISO 27008: http://www.27000.org/

- [9] FLÓREZ, Sara. La ley 527 1999, sobre Comercio Electrónico y Firmas Electrónicas, marzo de 2011. http://es.slideshare.net/saracflorez/ley-527-de-1999

- [10] Diario Oficial No. 46.023. Ley 962 de 2005 (julio 8) Diario Oficial No. 46.023. Disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Septiembre de 2005.

http://www.mintic.gov.co/portal/604/articles-3725_documento.pdf

- ✓ [11] MINISTERIO DE LAS TIC, Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección en las bases de datos y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías en las bases de datos y las comunicaciones, entre otras disposiciones". Septiembre de 2015. http://www.mintic.gov.co/portal/604/w3-article-3705.html

- ✓ [12] CHAVARRÍA, Carlos , docente at unipanamericana - aulas digitales ley 1341 de 2009 ppt. 25 de septiembre de 2010. http://es.slideshare.net/chavarria2010/ley-1341-de-2009-ppt

- ✓ [13] ISACA, Trust in, and value from, information systems https://www.isaca.org/Pages/default.aspx,

- ✓ 14 ISACA, IT Governance Institute http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx

- ✓ [15] OMPI, Colombia ley No. 599 de 2000 (24 de julio) - por la cual se expide el código penal http://www.wipo.int/wipolex/es/details.jsp?id=7305

- ✓ [16] HERNÁNDEZ, Dulce Quinta edición Metodología de la investigación 5ta Edición Sampieri. http://www.academia.edu/6399195/Metodologia_de_la_investigacion_5ta_Edicion_Sampieri

- ✓ [17] VERA VÉLEZ, Lamberto, UIPR, Ponce, P.R. la Investigación Cualitativa.http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html

- ✓ [18] Norma técnica NTC-iso-iec colombiana 27001 2013-12-11 Tecnologías en las bases de datos. Técnicas de seguridad. Sistemas de gestión de la seguridad en las bases de datos. Requisitos http://tienda.icontec.org/brief/NTC-ISO-IEC27001.pdf

- ✓ [19] GUTIÉRREZ AMAYA, Camilo. Magerit: metodología práctica para gestionar riesgos. Mayo 2013. Http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

- [20]ALCADIA DE IBAGUE. Funciones de la Entidad: http://gyhinvestments.com.co/wp-content/uploads/2014/09/IBAGUE-COMITE-ENAJENACION.pdf

- [21]ALCADIA DE IBAGUE. Funciones de la Entidad: http://gyhinvestments.com.co/wp-content/uploads/2014/09/IBAGUE-COMITE-ENAJENACION.pdf

- [22]–[30] Acuerdo 060 del 29 de Julio de 1987. http:/www.entidad deibague.gov.co/website/index.php/funciones-hacienda

APELLIDO (S), Nombre. Nombre del artículo. En: nombre del periódico. Ciudad: (fecha de publicación), Pagina.

- HERNÁNDEZ PINTO, María Gabriela, NARANJO SÁNCHEZ, Bertha Alice Artículo de revista no especializada: "Diseño de un plan estratégico de seguridad de información en una Entidad del sector comercial" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

- ALMANZA JUNCO, Andrés Ricardo. Documentos en Internet: A. (2012). Encuesta Seguridad Informática en Colombia. Tendencias 2011-2012. Sistemas (123). Recuperado de http://www.acis.org.co/fileadmin/Revista_123/Encuesta.pdf

- ALVAREZ - GAYOU, J.L, (1999), Investigación cualitativa, Archivos Hispanoamericanos de sexología, (5), (117-123).

- CRESWELL JW, (1998), Qualitative inquirí and reaserch design. Chossing among five traditions. Thousand Oaks, CA. Sage publications.

- DENZIN, Norman, K. & Lincoln, Yvonna (Eds) (1998), Strategiess of qualitative inquiry. Sage publications.

- VASILACHIS de Gialdino, I, (1992). Métodos cualitativos. Los problemas teórico-epistemológicos. Buenos Aires. Argentina, (pp. 23-25). Centro Editor de América Latina.

- CASTILLO SÁNCHEZ, Mauricio Guía para la formulación de proyectos de investigación. (2004). Recuperado de http://books.google.com.co/books?id=12QAoImkJxsC&pg=PA57&dq=como+elaborar+un

a+justificacion&hl=en&sa=X&ei=1R7uUJyFO4PA9QTCmICgBg&ved=0CDgQ6AEwAw #v=onepage&q&f=false

- ✓ ECHENIQUE GARCÍA, José Antonio, Auditoría en Informática (2da Edición, Mc. Graw Hill, 2001), pp. 194-241.

- ✓ Libro: ACEITUNO CANAL, Vicente. Seguridad en las bases de datos: expectativas, riesgos y técnicas de protección. 2004, 176 p. http://www.iberlibro.com/buscar-libro/autor/vicente-aceituno-canal/pagina-1/

- ✓ CARBALLAR, José Antonio. WI-FI instalación, seguridad y aplicaciones. 2007, 319 p. Recursos electrónicos: DHANJANI, Nitesh. La Nueva Generación Hacker. 2010, 320 p. FOROUZAN, Behrouz. Transmisión De Datos Y Redes De Comunicaciones. 2002, 462 p. http://repository.uniminuto.edu:8080/jspui/bitstream/10656/1787/1/TR_BermudezSanmiguelEdgar.pdf

- ✓ LUCAS, Henry, Plan de seguridad Informática para una Entidad Financiera, lima (2003) http://es.scribd.com/doc/24395296/PLAN-DE-SEGURIDAD-INFORMATICA-PARAUNA-ENTIDAD-FINANCIERA

- ✓ CORDOVA RODRÍGUEZ, Norma Edith. Tesis Digitales UNMSM Políticas de Seguridad en l Información.

- ✓ RAMIREZ, ElmasrI, NAVATHE, Shamkant B.; PÉREZ, ZABALLa Gloria. *Fundamentos de sistemas de bases de datos*. Addison-Wesley, 2002.

- ✓ ACOSTA, Ramón E.; ISAZAA, Gustavo A. Hacia un arquitectura de buenas prácticas de seguridad para sistemas ERP.

- ✓ LÓPEZ, Alexander Barinas; ALDANA, Andrea Catherine Alarcón; CUERVO, Mauro Callejas. Vulnerabilidad de Ambientes Virtuales de Aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus [Vulnerability in Virtual Learning Environments using SQLMap, RIPS, W3AF and Nessus]. *Ventana Informática*, 2014, no 30.

ANEXOS No.1: RESULTADO DE LA ENCUESTA

DISEÑO DE POLÍTICAS PARA FORTALECER LA SEGURIDAD EN LAS BASES DE DATOS

La siguiente encuesta permitirá evaluar riesgos que se presentan en el manejo en las bases de datos y el análisis de la misma se realizara en el desarrollo del proyecto: Diseño de un Plan Estratégico para la seguridad de la información tributaria en una entidad pública.

Nombre:	
Dependencia:	
Funciones:	

Tabla No.1 Organización de la Seguridad

1. ¿Cuenta la Entidad con un comité de apoyo de Seguridad Informática?	Cantidad	Valor %
a. Si	5	33.33 %
b. No	0	0 %
c. N/s	10	66.66 %
Total encuestados	15	100 %
2. ¿Se establecen anualmente objetivos con relación a la Seguridad en las bases de datos?	Cantidad	Valor %
a. Si	2	13.33 %
b. No	0	0 %
c. N/s	13	86.66 %
Total encuestados	15	100 %
3. ¿Disponen de servidor central de datos en su Entidad?	Cantidad	Valor %
a. Si	12	80 %
b. No	0	0 %
c. N/s	3	20 %
Total encuestados	15	100 %
4. ¿Los ordenadores de trabajo tienen datos de la Entidad almacenados dentro de su disco duro?	Cantidad	Valor %
a. Si	13	86.66 %
b. No	0	0 %
c. N/s	2	13.33 %
Total encuestados	15	100 %
5. ¿Se realiza copia de seguridad de los datos de la Entidad?	Cantidad	Valor %

a. Si	6	40 %
b. No	0	0 %
c. N/s	9	60 %
Total encuestados	15	100 %
6. ¿Dispone de una web corporativa (web de su Entidad)?	Cantidad	Valor %
a. Si	15	100 %
b. No	0	0 %
c. N/s	0	0 %
Total encuestados	15	100 %

Tabla No. 2 Responsabilidad y Control de los Activos

1. ¿Todo empleado puede registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas?	Cantidad	Valor %
a. Si	13	86.66 %
b. No	1	6.66 %
c. N/s	1	6.66 %
Total encuestados	15	100 %
2. Los ordenadores de su Entidad, ¿tienen instalado antivirus?	Cantidad	Valor %
a. Si	13	86.66 %
b. No	0	0 %
c. N/s	2	13.33 %
Total encuestados	15	100 %
3. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?	Cantidad	Valor %
a. Si	5	33.33 %
b. No	0	0 %
c. N/s	10	66.66 %
Total encuestados	15	100 %
4. ¿El área donde desempeña cuenta con un líder o responsable de la supervisión del buen uso de los activos y funciones que allí desempeñan?	Cantidad	Valor %
a. Si	10	66.66 %
b. No	5	33.33 %
c. N/s	0	0 %
Total encuestados	15	100 %
5. ¿Clasifica los activos de información de mayor importancia para la Organización por su nivel de exposición o vulnerabilidad?	Cantidad	Valor %
a. Si	6	40 %
b. No	9	60 %
c. N/s	0	0 %

Total encuestados	15	100 %
6. ¿Cuenta con un Plan de Continuidad del Negocio que le permita seguir con las operaciones en caso de un evento no deseado?	Cantidad	Valor %
a. Si	3	20%
b. No	12	80 %
c. N/s	0	0 %
Total encuestados	15	100 %

Tabla No. 3 Seguridad personal

1. ¿Utiliza programas de descarga de archivos de usuario (música, películas, programas...)?	Cantidad	Valor %
a. Si	13	86.66
b. No	2	13.33 %
c. N/s	0	0 %
Total encuestados	15	100 %
2. ¿Conoce el uso de unas de estas Herramientas de seguridad informática?	Cantidad	Valor %
a. Firewall	3	20%
b. Proxy	3	20%
c. Actualizaciones	5	33.33%
d. Políticas de seguridad	3	20%
e. Antivirus, Antispyware, Antimalware	11	73.33 %
f. Herramientas de monitoreo de red	2	13.33 %
g. Herramientas de autenticación de usuarios	3	20%
h. Ninguna de las anteriores	3	20%
Total encuestados	15	100 %
3. ¿Es responsable de eliminar cualquier rastro de documentos y/o información una vez utilizada para sus funciones y que pueda estar expuestas para fines delictivos?	Cantidad	Valor %
a. Si	8	53.33 %
b. No	7	46.66 %
c. N/s	0	0 %
Total encuestados	15	100 %
4. ¿Conoce las responsabilidades que tiene como empleado de los bienes y servicios informáticos para cumplir las Políticas y Estándares de Seguridad en las bases de datos?	Cantidad	Valor %
a. Si	5	33.33 %
b. No	8	53.33 %
c. N/s	2	13.33 %
Total encuestados	15	100 %

5. ¿Una vez Diseñadas las herramientas de seguridad en la organización, usted recomendaría dar algún tipo de asesoría o capacitación junto con el manual de uso, de cómo funciona la herramienta de administración de seguridad informática?	Cantidad	Valor %
a. Si se recomienda dar dicha capacitación	15	100 %
b. No es necesario recibir la capacitación	0	0 %
c. Con el manual de uso de la herramienta es suficiente	0	0 %
Total encuestados	15	100 %

Tabla No. 4 Seguridad física y Ambiental

1. Los equipos o activos críticos de información y proceso, ¿están ubicados en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el administrador del área?	Cantidad	Valor %
a. Si	2	13.33 %
b. No	12	80 %
c. N/s	1	6.66 %
Total encuestados	15	100 %
2. ¿Las estaciones o terminales de trabajo, con procesamientos críticos cuentan con medios de almacenamientos extraíbles?	Cantidad	Valor %
a. Si	15	100 %
b. No	0	0 %
c. N/s	0	0 %
Total encuestados	15	100 %

Tabla No. 5 Control de Acceso

1. ¿Se permite la utilización de correos electrónicos personales y el fácil acceso a páginas de internet en la organización?	Cantidad	Valor %
a. Si	15	100 %
b. No	0	0 %
c. N/s	0	0 %
Total encuestados	15	100 %
6. ¿Al terminar una sesión de trabajo en las estaciones, evita dejar encendido el equipo?	Cantidad	Valor %
a. Si	7	46.66 %
b. No	8	53.33 %
c. N/s	0	0 %
Total encuestados	15	100 %

3. ¿La longitud mínima de caracteres permisibles en su contraseña se establecen?	Cantidad	Valor %
a. 1 a 3 Caracteres con una combinación alfanumérica	0	0 %
b. 3 a 6 Caracteres con una combinación alfanumérica	12	80 %
c. 6 caracteres en adelante con una combinación alfanumérica	3	20 %
Total encuestados	15	100 %

Tabla No. 6 Lineamientos Legales

1. ¿Se cumplen con los requisitos legales o reglamentarios y las obligaciones contractuales de seguridad?	Cantidad	Valor %
a. Si	14	93.33 %
b. No	0	0 %
c. N/s	1	6.66 %
Total encuestados	15	100 %
5. Todo el software comercial que utiliza la organización está legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias?	Cantidad	Valor %
a. Si	14	93.33 %
b. No	0	0 %
c. N/s	1	6.66 %
Total encuestados	15	100 %
6. Si se presenta cualquier cambio en la política de utilización de software comercial o software libre, este es documentado en base a las disposiciones de la respectiva licencia?	Cantidad	Valor %
a. Si	13	86.66 %
b. No	0	0 %
c. N/s	2	13.33 %
Total encuestados	15	100 %

ANEXOS 2: MODELO DE ENTREVISTA PARA CONOCER LOS ASPECTOS ORGANIZATIVOS DE LA ENTIDAD Y ACEPTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Nombre:	
Dependencia:	
Funciones:	
Persona a cargo:	
Contacto:	

¿Se establecen anualmente objetivos con relación a la Seguridad en las bases de datos en la entidad?

¿Se desarrollan procesos de análisis del riesgo?

¿ Se establezcan los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de Análisis de riesgos manejado?.

¿Se cumplen con los requisitos legales o reglamentarios y las obligaciones contractuales de seguridad?

¿Está de acuerdo que se e establezcan los medidas de seguridad informática en las bases de datos?

¿Todo empleado puede registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas?

Como o en qué cree que puede tener utilidad para su entidad implantar un plan de seguridad de información? ¿A qué ayudaría?

¿Qué necesidades de nuevas tecnologías cree que tiene su asociación en la actualidad?

¿Qué necesidades de nuevas tecnologías cree que tendrá su asociación en el futuro (5-10 años)?

¿Qué uso cree que hace su asociación de las nuevas tecnologías?

- ✓ Alto
- ✓ Normal
- ✓ Regular
- ✓ Bajo

Por favor, explique el uso que en su opinión hace su dependencia de las siguientes herramientas tecnológicas frente a la seguridad de la información de acuerdo a los ítems señalados:

- ✓ Computador (nº de ordenadores, actualización etc.)
- ✓ Software
- ✓ Red
- ✓ Correo electrónico
- ✓ Internet
- ✓ Móviles
- ✓ Gestores de información y procesamiento de datos

En su opinión, ¿Necesita su entidad del uso de herramientas tecnológicas complejas como gestores contables, gestores de proyectos o de socios informatizados, pasarelas electrónicas, etc.? Por favor, razone su respuesta.

En su opinión, ¿qué aspectos tecnológicos necesitan mayor seguridad en su entidad?:

¿Aspectos de gestión?- Enumere cuáles y por qué ¿Aspectos de información?- Enumere cuáles y por qué.

- ✓ ¿Aspectos de comunicación?- Enumere cuáles y por qué.
- ✓ ¿Aspectos de seguimiento y evaluación?- Enumere cuáles y por qué.
- ✓ ¿Aspectos de coordinación interna?- Enumere cuáles y por qué.
- ✓ ¿Aspectos de coordinación externa?- Enumere cuáles y por qué.

¿Qué herramientas de seguridad tecnológicas ha contratado su entidad?

¿Cuenta su entidad con empleados que sepan gestionar estas herramientas de seguridad tecnológicas adecuadamente? Por favor, explique.

¿Cuenta su entidad con la infraestructura adecuada (aparatos) para gestionar esta tecnología?
¿Qué herramientas tecnológicas ha subcontratado su entidad?

¿Quién realiza tareas de soporte de seguridad informática para la entidad y qué perfil profesional tiene?

¿Quién realiza tareas de soporte web (webmaster y similar) y qué perfil profesional tiene?

¿Qué o perfiles relacionados con el ámbito tecnológico trabajan para su entidad? Por favor, de detalle de todos los perfiles existentes. Como contratistas.- Como Funcionarios de Planta.

¿Qué capacitación en nuevas tecnologías tiene su personal? ¿Qué formación en nuevas tecnologías se le exige a su personal?