DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ CUNDINAMARCA BAJO LA NORMA ISO 27001:2013

LUZ DARY ACOSTA CONTRERAS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2017

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ CUNDINAMARCA BAJO LA NORMA ISO 27001:2013

LUZ DARY ACOSTA CONTRERAS

Trabajo de grado realizado para optar por título de especialista en seguridad de la Información

Asesor
Álvaro escobar
Director Especialización en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2017

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C. 1 de febrero de 2017

Primeramente a Dios, a mis padres, hermanos y sobrinos quienes son el motor para enfrentar retos y a las demás personas que aportaron una parte de su tiempo y apoyo incondicional durante este proceso.

A mi hermano que desde el cielo me protege y es la inspiración para luchar por mis sueños.

A las instituciones educativas, compañeros y docentes que aportaron a mi formación profesional y formación como una persona con principios, honestidad y responsabilidad.

Luz Dary Acosta

CONTENIDO

Página

LISTA DE FIGURAS

Página

LISTA DE CUADROS

Página

GLOSARIO

ACEPTACIÓN DEL RIESGO: “decisión a asumir el riesgo”[1].

ACTIVO: “cualquier cosa que tiene valor para la organización”[2].

CONFIDENCIALIDAD: “propiedad que determina que la información no esté disponible, ni sea revelada a individuos, entidades o procesos no autorizados”[3].

DISPONIBILIDAD: “propiedad de que la información se accesible u utilizable por solicitud de una entidad autorizada”[4].

EVALUACIÓN DEL RIESGO: “proceso de comprar el riesgo estimado contra criterios de riesgos dados, para determinar la importancia del riesgo”[5].

INTEGRIDAD: “propiedad de salvaguardar la exactitud y estado completo de los activos”[6].

SEGURIDAD DE LA INFORMACIÓN: “preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad”[7].

TRATAMIENTO DEL RIESGO: “proceso de selección e implementación de medidas para modificar el riesgo”[8].

VALORACIÓN DEL RIESGO: “proceso global de análisis y evaluación del riesgo"[9].

---

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma Técnica ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de seguridad de la información. Requisitos. Primera edición, Bogotá, D.C. 2013, p.2, [en línea]. Disponible en: http://tienda.icontec.org.
[2] Ibíd. p. 2.
[3] Ibíd. p. 2.
[4] Ibíd. p. 2.
[5] Ibíd. p. 3.
[6] Ibíd. p. 3.
[7] Ibíd. p.3.
[8] Ibíd. p. 4.
[9] Ibíd. p. 4

RESUMEN

Con la realización del presente proyecto se tiene como finalidad identificar las amenazas y riesgos a los que puede estar expuesta la alcaldía municipal de Cucunubá en el área de la Secretaría de Hacienda donde se manejan los recursos y presupuesto del municipio, razón por la cual se deben implementar las medidas para salvaguardar la información y de esta forma evitar que personas mal intencionadas puedan acceder a ella con fines fraudulentos o intereses de terceros, ocasionando inconvenientes para el buen funcionamiento de la entidad, el objetivo es hacer la implementación de controles regidos bajo la Norma ISO 27001 de 2013 y establecer así las políticas de seguridad de la información para mitigar los posibles riesgos que se identifiquen.

Palabras clave: Diseño – SGSI - Norma Técnica – Sistema de gestión.

SUMMARY

With the realization of this project, the purpose is to identify the threats and risks that can be exposed the municipal mayor of Cucunubá in the area of the Ministry of Finance where the resources and budget of the municipality are handled, which is why Implement the measures to safeguard the information and thus prevent malicious persons from accessing it for fraudulent purposes or interests of third parties, causing inconvenience to the proper functioning of the entity, the objective is to implement the controls governed by the Standard ISO 27001 of 2013 and thus establish the information security policies to mitigate the possible risks that are identified**.**

Key words: Design - ISMS - Technical Standard - Management system.

INTRODUCCIÓN

En la actualidad la seguridad de la información se ha convertido en uno de los activos más importantes para las organizaciones, lo cual hace que ellas trabajen todos los días en busca de estrategias para asegurar la integridad, confidencialidad y disponibilidad de la misma. Las entidades públicas deben empezar a pensar en implementar políticas de seguridad para evitar que intrusos o personas malintencionadas exploten posibles vulnerabilidades, por medio de las cuales puedan llegar a ocasionar daños o pérdidas económicas y/o materiales a los activos de información físicos y lógicos de la entidad.

En esta propuesta se realizará el diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013, construyendo, inicialmente el inventario de la información que se maneja en la Secretaría de Hacienda (dependencia en la cual se va a desarrollar la propuesta) de la alcaldía de Cucunubá, para identificar vulnerabilidades y aplicar los controles para evitar que estas se materialicen.

1. DESCRIPCIÓN DEL PROYECTO

Con este proyecto se pretende realizar un diagnóstico de los riesgos y vulnerabilidades que puede tener el activo más valioso para el municipio de Cucunubá, *la información*, e identificar posibles formas en que puede estar expuesta su disponibilidad, confidencialidad e integridad, implementando controles que permitan tratar y mitigar estos riesgos para poder garantizar la continuidad de esta administración, así mismo proponer políticas de seguridad de la información basados en la Norma ISO 27001 2013.

1.1 ANTECEDENTES

La Alcaldía municipal de Cucunubá no tiene creadas ni implementadas políticas de seguridad de la información. Lo que hace que los funcionarios no tengan la cultura de proteger la información y ser cuidadosos con datos, archivos, y documentación que se maneja, por ejemplo, dejan escritas las contraseñas en las pantallas de los computadores, en agendas sobre los escritorios, hasta el punto en que dejan las oficinas solas, y son tan confiados que se ha detectado que dejan sesiones abiertas, permiten que otras personas utilicen sus estaciones de trabajo, o revelan claves a las personas encargadas del área de, mantenimiento e informática. Sumado a esto tampoco se tiene implementado la realización de copias de seguridad periódicamente lo cual ha llevado a esta dependencia a perder información en pasadas ocasiones.

Los funcionarios de la Alcaldía aún no tienen la cultura de afrontar posibles riesgos y hacer las acciones correctas para evitarlo o contenerlo cuando se les presente en el desarrollo de sus actividades diarias; por ejemplo sucede el caso que llegan correos sospechosos a las cuentas institucionales de la Alcaldía siendo remitente los mismos correos institucionales, sin embargo no se tiene la cautela de detenerse a mirar si ese correo es correcto y la primera acción es abrirlo infectándose de esta manera de virus y reenviarlo a las demás dependencias sin percibir el hecho realizado .

También se evidencia que varios usuarios pueden acceder al mismo computador y a la base de datos con el mismo usuario y contraseña porque no se tienen definidos roles, ni permisos de cada uno.

2. ALCANCE

Diseñar el sistema de Gestión de Seguridad de la Información SGSI bajo la norma ISO 27001 2013 en la Secretaría de Hacienda del municipio de Cucunubá, identificando vulnerabilidades, amenazas y riesgos.

3. PLANTEAMIENTO DEL PROBLEMA

La Alcaldía Municipal de Cucunubá por ser una entidad pública debe cumplir con los requerimientos exigidos por la normatividad vigente, Ley 734 DE 2002 y Ley 1474 de 2011 las cuales tratan del "…cumplimiento de adoptar una política de la seguridad de la información para garantizar la custodia y uso adecuado de los recursos informáticos…"[10] cumpliendo con los objetivos del plan anticorrupción de la entidad, sin embargo esta no cuenta con un sistema de gestión de seguridad de la información, definido para garantizar la confidencialidad e integridad de los activos informáticos que se maneja al interior de la misma, y al ser desconocido por los funcionarios se expone la Entidad a eventualidades que quebranten la seguridad de la información, partiendo de que no se cuenta con planes ni políticas que les enseñe y concientice de cómo actuar ante posibles amenazas o vulnerabilidades que se puedan presentar en el desarrollo de las actividades laborales.

Una gran problemática identificada en la Secretaría de Hacienda es que los equipos de cómputo permanecen encendidos y conectados a la red; sin tener en cuenta que en éste municipio son constantes las fallas en el fluido eléctrico, tampoco se realizan copias de seguridad ni se tiene implementado mantenimiento preventivo y correctivo de los equipos. Y el no tener tampoco UPS puede llevar a materializar daños irreparables que lleven a la pérdida de la información de la entidad generando requerimientos jurídicos, disciplinarios y económicos a la Alcaldía, ya que afectaría directamente la ejecución del presupuesto municipal y el cumplimiento de las metas fijadas en el Plan de Desarrollo Municipal.

3.1 FORMULACIÓN DEL PROBLEMA

¿Qué controles se pueden dar a los riesgos a los que están expuestos los activos de la información en la Secretaría de Hacienda del municipio de Cucunubá Cundinamarca y que políticas se pueden proponer para mitigar estos riesgos?

[10] CONGRESO DE COLOMBIA. Ley 734 de 2002 (febrero 5). Código Disciplinario Único, [en línea] [citado julio 10 de 2015] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4589

4. JUSTIFICACIÓN

Para el ejercicio de las funciones de la Secretaría de Hacienda, se maneja el software contable SQL de módulos de presupuesto, recaudo, contabilidad, almacén, nómina e industria y comercio, los cuales se encuentran distribuidos en tres oficinas con un total de 6 usuarios, por lo que se hace necesario tener definidos los roles de cada uno y así mismo asignado los permisos correspondientes a cada rol, teniendo en cuenta que allí se administran los recursos del municipio de Cucunubá y no se tiene establecidas medidas para garantizar la seguridad de la información y el buen manejo de la misma, partiendo de que no existe la cultura de ser desconfiados con los documentos, archivos, y dispositivos de almacenamiento que se manipula diariamente en la oficina, además este sistema es monitoreado por acceso remoto para dar soporte por parte del SQL.

Teniendo en cuenta lo anterior se hace necesario la implementación de controles y estrategias de seguridad para crear concientización en los funcionarios y así poder detectar a tiempo los riesgos a los que están expuestos en las actividades de trabajo de cada uno, permitiendo que sepan identificar eventos irregulares y puedan actuar de la mejor manera ante alguna de estas situaciones. Ya que de esta oficina depende el buen funcionamiento, buen nombre y correcto manejo los recursos que tiene el municipio colocando a consideración el desempeño fiscal y administrativo en el ámbito regional, departamental y nacional.

La Secretaría de Hacienda es el motor para el desarrollo del municipio de Cucunubá, del cual depende aproximadamente 7200 habitantes, ya que es la dependencia responsable del manejo y distribución de los recursos económicos del municipio y de realizar todo lo relacionado con programaciones y ejecuciones presupuestales, también es en centro donde se manejan pagos en línea, transacciones, portales bancarios, gobierno en línea, lo que hace necesario que los equipos estén en red.

Si se realiza la concienciación e implementación de políticas en la Entidad acerca de la seguridad de la información se va a mitigar riesgos, vulnerabilidades y amenazas preparando así a los trabajadores ante posibles eventos malintencionados que se pueden encontrar en el desarrollo de su trabajo.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Diseñar el sistema de Gestión de seguridad de la Información (SGSI) para la Secretaría de Hacienda de la alcaldía municipal de Cucunubá – Cundinamarca alineado a la norma ISO 27001:2013

5.2 OBJETIVOS ESPECÍFICOS

1. Realizar el inventario de activos de la información de la Secretaría de Hacienda de la Alcaldía municipal de Cucunubá bajo la norma ISO 27001:2013.

2. Priorizar la información que se maneja en la Secretaría de Hacienda de la Alcaldía municipal de Cucunubá.

3. Realizar el análisis de riesgo de la información de la Secretaría de Hacienda de la Alcaldía municipal de Cucunubá bajo la norma ISO 27001:2013

4. Establecer controles de seguridad de la información entorno a la norma ISO 27001:2013 en la Secretaría de Hacienda del Alcaldía municipal de Cucunubá.

6. MARCO LEGAL

Hoy en día las organizaciones deben funcionar en línea con la normatividad existente y estar a su vez, a la vanguardia con las actualizaciones de las mismas, por consiguiente es importante nombrar en este trabajo alguna normatividad que se debe tener en cuenta al momento del diseño de un Sistema de Gestión de la información.

ISO 27001-2013: Esta Norma

> "Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. Incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza"[11].

MANUAL ESTRATEGIA DE GOBIERNO EN LÍNEA: esta estrategia comprende cuatro propósitos (TIC para gobierno abierto, TIC para servicio, TIC para gestión, seguridad y privacidad de la información), para que los servicios que brindan las entidades territoriales sea de mayor calidad y más óptimos, para lo cual se incorporaron tres herramientas transversales en busca de la confianza de los ciudadanos del servicio en línea que ofrecen las entidades.

DECRETO 2573 DEL 12 DE DICIEMBRE DE 2012: por medio de la cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea. "…Que así mismo, la anotada Ley determinó que es función del Estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector."[12]

DECRETO 103 DE 2015: Define el Registro de Activos de Información como "el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal"[13].

---

[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma Técnica ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de seguridad de la información. Requisitos. Primera edición, Bogotá, D.C. 2013, 27p, [en línea]. Disponible en: http://tienda.icontec.org.

[12] MINISTERIO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES. Marco de referencia, [en línea] [citado 26 de junio de 2015] disponible en <http://www.mintic.gov.co/marcodereferencia/624/articles-7663_recurso_1.pdf, manual de Gobierno en línea>

[13] ALCALDÍA DE BOGOTÁ. Normas. Decreto 103 de 2015. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556, Decreto 103 de 2015.

ACUERDO Nº 002 DE 2016: Por medio del cual se adopta el Plan de Desarrollo Municipal “Cucunubá productiva y social”. En el eje institucional, dentro del sector de fortalecimiento institucional en su componente estratégico tiene la siguiente meta de producto: “Implementar anualmente la Estrategia Municipal Gobierno en línea durante el periodo de gobierno. ODS 16

7. MARCO TEÓRICO

7.1 HISTÓRICO

7.1.1 Generalidades. El municipio de Cucunubá se encuentra ubicado en Colombia, Departamento de Cundinamarca, provincia de Ubaté a 2950 m.s.n.m. como se muestra en la figura 1. Con temperatura promedio de 14°, es un municipio de sexta categoría con 7.300 habitantes según base de datos del Sisbén Año 2014 y maneja un presupuesto anual aproximado a $5.496’491.234

Figura 1.Ubicación municipio de Cucunubá en el Departamento

Fuente: Secretaria de Planeación Departamento de Cundinamarca, 2016.

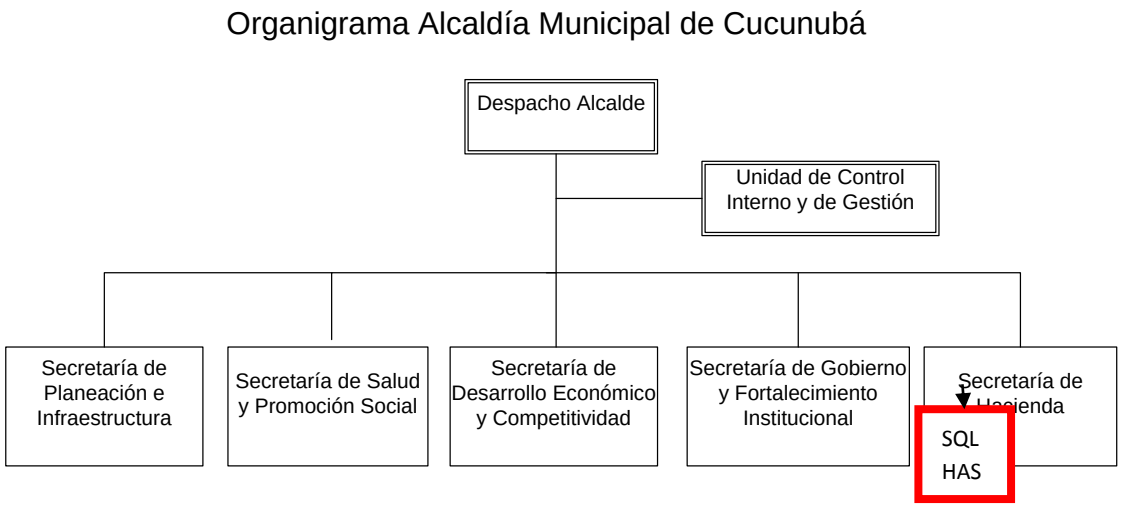
La administración municipal de Cucunubá está organizada por cinco dependencias y su distribución jerárquica es como se puede ver en la figura 2.

Figura 2. Distribución jerárquica de la Administración Municipal de Cucunubá

Fuente: Alcaldía Municipal de Cucunubá, 2016.

La presente propuesta se va a ejecutar en la Secretaría de Hacienda partiendo de que es una de las cinco dependencias que conforman la Administración Municipal como se puede ver en la figura 3; quién es la encargada de manejar y administrar los recursos y presupuesto del municipio, por consiguiente, está más expuesta a ataques por personas inescrupulosas si no se detectan las vulnerabilidades y son controladas justo a tiempo:

Figura 3. Ubicación de la Secretaría de Hacienda en la administración municipal



Fuente: El autor, 2016.

7.2 DESCRIPCIÓN DEL HARDWARE EN LA ENTIDAD TERRITORIAL

La red de la Alcaldía municipal de Cucunubá es inalámbrica salvo los equipos de la Secretaría de hacienda los cuales se encuentran conectados alámbricamente; el inventario de los activos de hardware se compone como se muestra en el Cuadro 1.

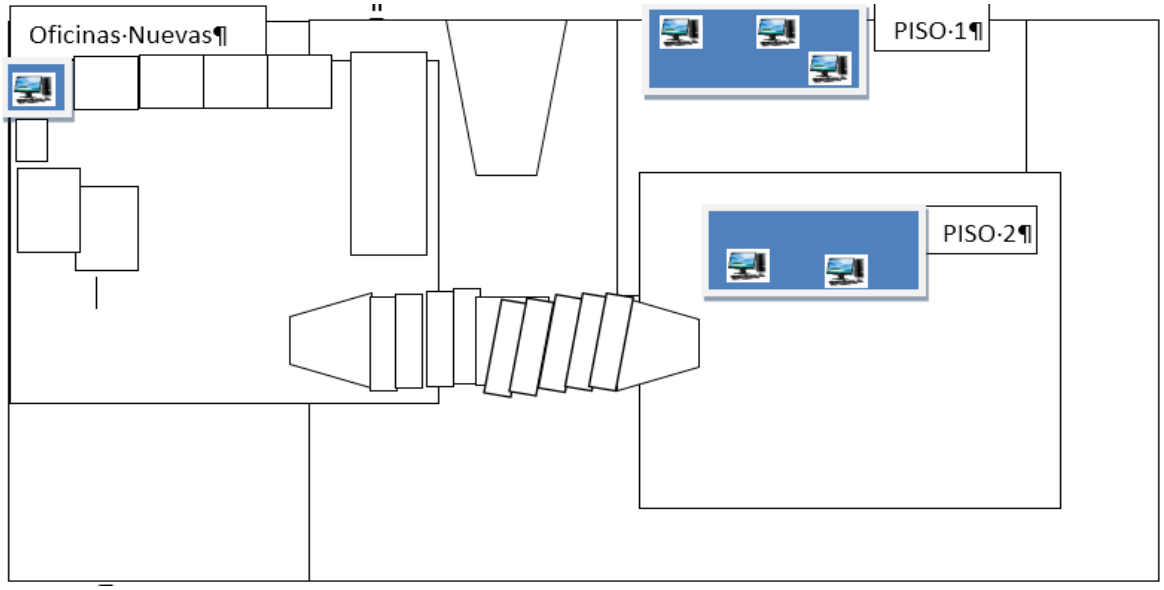
Cuadro 1. Hardware de la Alcaldía Municipal

Ítem	Nombre	Cantidad
1	Computador portátil	11
2	Computador de escritorio	26
3	Router	3
4	Swich	1
5	Servidor	1
6	Impresoras	23
7	Teléfonos móvil instituciones	7
8	Teléfono fijo	10
9	Ups	4
10	Disco duro	3
11	Cámara fotográfica	1

Fuente: El autor, 2016.

La distribución física de las estaciones de trabajo de la Administración Municipal pertenecientes a la Secretaría de Hacienda se muestran en la **figura 4**, y la conexión que se tiene es: en la oficina de almacén alámbrica (1 computador de escritorio y 1 impresora), oficina de recaudo inalámbrica (2 computadores de escritorio y 2 impresoras), Secretaría de hacienda alámbrica (2 computadores de escritorio, 1 servidor, 1 computador portátil y 3 impresoras).

Figura 4. Distribución física de las estaciones de trabajo dentro de la administración central



Fuente: El autor, 2016

Como se muestra en la figura 4, las instalaciones de la Alcaldía Municipal están organizadas en tres secciones: primer piso, segundo piso y una parte anexa a la Alcaldía.

7.3 DESCRIPCIÓN DEL SOFTWARE – SECRETARÍA DE HACIENDA

Cuadro 2. Software secretaría de hacienda

Ítem	Descripción	Módulo
1	SQL HAS	Contabilidad
2	SQL HAS	Industria y comercio
3	SQL HAS	Almacén
4	SQL HAS	Nomina
5	SQL HAS	Presupuesto
6	SQL HAS	Impuesto predial

Fuente: El autor, 2016.

En el cuadro 2 se muestra los módulos contables que tiene implementados la Secretaría de Hacienda de Cucunubá.

7.4 ¿QUÉ ES SQL HAS?

"El día 15 de octubre de 2000, se fundó la compañía con el nombre de HAS 2001 LTDA. Luego del desarrollo y comercialización de los módulos de Contabilidad, Presupuesto y Almacén, la creación de otros módulos como Industria y Comercio, Impuesto Predial y Servicios Públicos en plataforma Access, se realizó el nuevo desarrollo de todos los programas en plataforma SQL. Estos programas se registraron en la Dirección Nacional de Derechos de Autor el día 4 de marzo de 2004. Cabe anotar que todos los programas se han enfocado en la solución de necesidades para clientes del Sector Público colombiano y basan su desarrollo en la legislación que para cada caso emiten las autoridades correspondientes."[14]

En la actualidad, HAS SQL LTDA., cuenta con 34 empleados, ha desarrollado 15 módulos en plataforma SQL y se encuentra en proceso de diseño y desarrollo de los módulos en la plataforma .NET"[15].

7.5 NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

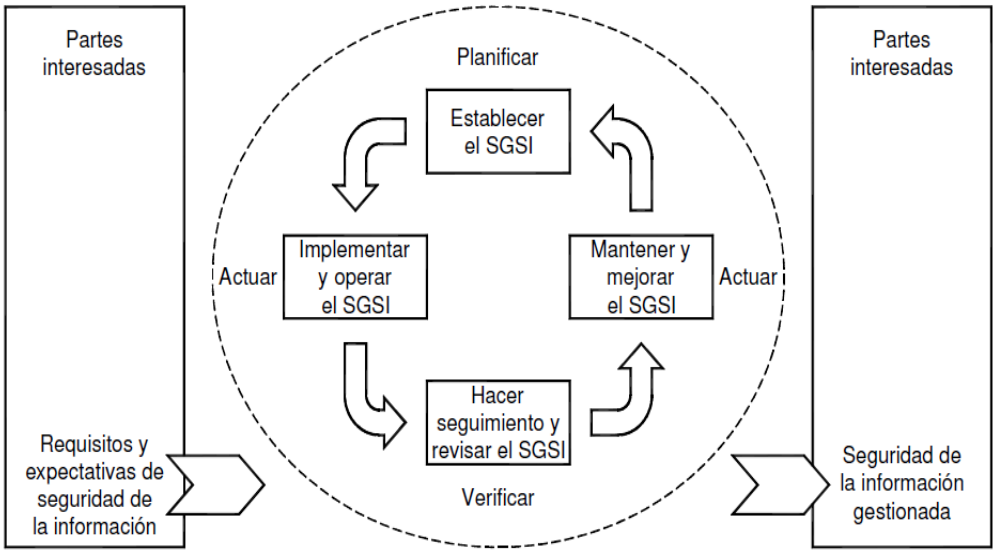
NTC-ISO/IEC 27001 es una norma internacional las cual establece controles que permiten "brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), este diseño está influenciado por las necesidades, objetivos, requisitos de seguridad, procesos empleados, tamaño y estructura de la Organización"[16].

7.6 MODELO PHVA, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013

Este modelo se aplica para estructurar los procesos del Sistema de Gestión de Seguridad de la Información como se ilustra en la figura 5 y por medio de la cual se pretende cumplir con los requisitos de seguridad de la Información.

[14] HASSQL LTDA. Concepto HASSQL. Bogotá, 2015, p.1, [en línea], Bogotá. Disponible en : http://www.hassql.com.co/
[15] Ibíd. p.2.
[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS –ICONTEC. NTC-ISO/IEC 27001:2013.

Figura 5. Modelo PHVA.



Fuente**:** Icontec. NTC-ISO-IEC 27001:2013.

7.6.1 Planificar. En esta parte se establecen los objetivos a los que se quiere llegar con el diseño del SGSI, a su vez identificar el inventario de los activos de la información implicados para su alcance, aplicando controles a cada uno de los riesgos encontrados durante la formulación del SGSI.

7.6.2 Hacer. Para la mitigación de los riesgos identificados se deben implementar los controles de acuerdo a la Norma ISO-IEC- 27001:2013

7.6.3 Verificar. Monitoreo de los controles implementados y análisis de sus resultados.

7.6.4 Actuar. De acuerdo a los resultados obtenidos en la verificación se toman las respectivas medidas para mejorar o retroalimentar la implementación de los controles, además se debe dejar todo hallazgo documentado.

8. ESTADO ACTUAL DE LA SECRETARÍA DE HACIENDA FRENTE A LA NORMA ISO-IEC-27001:2013

8.1 ¿CÓMO FUNCIONA SQL HAS EN LA SECRETARÍA DE HACIENDA?

La Secretaría de Hacienda del municipio de Cucunubá, para el ejercicio de su buen funcionamiento y desempeño adquirió la licencia del software del sistema administrativo y financiero desarrollado por SQL HAS, para administrar los recursos del municipio, comprando los módulos de: presupuesto, contabilidad, almacén, nómina, industria y comercio e impuesto predial, con sus requerimientos generales y específicos de los Entes de Control y de la Entidad. Cuenta con seis estaciones de trabajo ubicadas en tres oficinas en las instalaciones del palacio municipal, por consiguiente cuenta con seis usuarios que no tienen definidos ni establecidos los permisos y tampoco la concientización de la importancia y responsabilidad que cada uno asume al momento de manipular alguno de estos equipos, prestándose esto para evadir posibles responsabilidades, de esta forma, tampoco se tiene las medidas necesarias dentro de las oficinas para proteger la información que se maneja ya sea en medio magnético, físico o desde el hecho de crear contraseñas, no se hace con los respectivos niveles de seguridad.

8.1.1 Interfaz de usuarios. Durante el ejercicio de la identificación y verificación del computador de cada uno se encontró lo siguiente:

En el equipo que hace las veces de servidor trabaja la contadora y están instalados todos los módulos como se muestra en la figura 6.

Figura 6. Módulos en el equipo que hace las veces de servidor

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En las figuras 7, 8, 9 y 10 se muestra la interfaz que tiene cada usuario al momento de ingresar al sistema.

Figura 7. Interfaz de usuario presupuesto.

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En la figura 7 se muestra el ingreso al módulo presupuestal del HAS.

Figura 8. Interfaz de usuario Sistema Financiero

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En la figura 8 se muestra la interfaz de ingreso al módulo financiero.

Figura 9. Interfaz de usuario módulo de nómina

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En la figura 9 se muestra la interfaz de ingreso al módulo de nómina del HAS

Figura 10. Interfaz de usuario de Impuesto predial

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En la figura 10 se muestra la interfaz de ingreso al módulo de impuesto predial del HAS.

Figura 11. Interfaz de usuario módulo Almacén

Fuente: SQL HAS Secretaría de Hacienda, municipio de Cucunubá, 2016.

En la figura 11 se muestra la interfaz de ingreso al módulo de almacén.

8.2 SECRETARÍA DE HACIENDA FRENTE A LA NORMA ISO 27001:2013

Para tener un punto de partida de cómo se encuentra la secretaría de Hacienda del municipio de Cucunubá frente a la Norma ISO 27001:2013 se implementa el autodiagnóstico SGSI (ver Cuadro 3) que consiste en una herramienta tomada de internet “autodiagnóstico SGSI v2”. La cual permite comparar el estado de cumplimiento de esta Norma:

Cuadro 3. Autodiagnóstico SGSI v2.

ANEXO			ESTADO
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes			
A5.1.1	Políticas para la seguridad de la información	Control: se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	No cumple
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A6.1	Organización interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple parcialmente
ANEXO			**ESTADO**
A6.1.2	Separación de deberes	Control: los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Cumple parcialmente
A6.1.3	Contacto con las autoridades	Control: se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple parcialmente
A6.1.4	Contacto con grupos de interés especial	Control: se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: la seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple
A6.2	Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles			

Cuadro 3. (Continuación)

ANEXO			ESTADO
A6.2.1	Política para dispositivos móviles	Control: se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Cumple parcialmente
A6.2.2	Teletrabajo	Control: se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No cumple
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A7.1	Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			
A7.1.1	Selección	Control: las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Cumple parcialmente
A7.1.2	Términos y condiciones del empleo	Control: los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Cumple parcialmente
A7.2	Durante la ejecución del empleo		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A7.2.1	Responsabilidades de la dirección	Control: la dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Cumple parcialmente
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	Cumple parcialmente

Cuadro 3. (Continuación)

ANEXO			ESTADO
A7.2.3	Proceso disciplinario	Control: se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No cumple
A7.3	Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo			
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple parcialmente
A8	**GESTIÓN DE ACTIVOS**		
A8.1	Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.			
A8.1.1	Inventario de activos	Control: se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Cumple parcialmente
A8.1.2	Propiedad de los activos	Control: los activos mantenidos en el inventario deben tener un propietario.	No cumple
A8.1.3	Uso aceptable de los activos	Control: se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No cumple
A8.1.4	Devolución de activos	Control: todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple satisfactoriamente
A8.2	Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A8.2.1	Clasificación de la información	Control: la información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Cumple parcialmente

Cuadro 3. (Continuación)

ANEXO			ESTADO
A8.2.2	Etiquetado de la información	Control: se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple
A8.2.3	Manejo de activos	Control: se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple
A8.3	Manejo de medios		
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios			
A8.3.1	Gestión de medio removibles	Control: se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple parcialmente
A8.3.2	Disposición de los medios	Control: se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Cumple parcialmente
A8.3.3	Transferencia de medios físicos	Control: los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No cumple
A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
A9.1.1	Política de control de acceso	Control: se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	No cumple
A9.1.2	Acceso a redes y a servicios en red	Control: solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple satisfactoriamente
A9.2	Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A9.2.1	Registro y cancelación del registro de usuarios	Control: se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Cumple parcialmente
A9.2.2	Suministro de acceso de usuarios	Control: se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Cumple parcialmente

Cuadro 3. (Continuación)

ANEXO			ESTADO
A9.2.3	Gestión de derechos de acceso privilegiado	Control: se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	No cumple
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: la asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No cumple
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple parcialmente
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple satisfactoriamente
A9.3	Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
A9.3.1	Uso de información de autenticación secreta	Control: se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No cumple
A9.4	Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			
A9.4.1	Restricción de acceso a la información	Control: el acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple parcialmente
A9.4.2	Procedimiento de ingreso seguro	Control: cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cumple parcialmente
A9.4.3	Sistema de gestión de contraseñas	Control: los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple parcialmente
A9.4.4	Uso de programas utilitarios privilegiados	Control: se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No cumple
A9.4.5	Control de acceso a códigos fuente de programas	Control: se debe restringir el acceso a los códigos fuente de los programas.	No aplica

Cuadro 3. (Continuación)

ANEXO			ESTADO
A10	**CRIPTOGRAFÍA**		
A10.1	Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información			
A10.1.1	Política sobre el uso de controles criptográficos	Control: se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No cumple
A10.1.2	Gestión de llaves	Control: se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No cumple
A11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A11.1	Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A11.1.1	Perímetro de seguridad física	Control: se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	Cumple parcialmente
A11.1.2	Controles de acceso físicos	Control: las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	No cumple
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Cumple parcialmente
A11.1.4	Protección contra amenazas externas y ambientales.	Control: se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Cumple parcialmente
A11.1.5	Trabajo en áreas seguras.	Control: se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No cumple
A11.1.6	Áreas de carga, despacho y acceso público	Control: se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Cumple parcialmente
A11.2	Equipos		
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			

Cuadro 3. (Continuación)

ANEXO			ESTADO
A11.2.1	Ubicación y protección de los equipos	Control: los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple parcialmente
A11.2.2	Servicios de suministro	Control: los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple parcialmente
A11.2.3	Seguridad en el cableado.	Control: el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple satisfactoriamente
A11.2.4	Mantenimiento de los equipos.	Control: los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple parcialmente
A11.2.5	Retiro de activos	Control: los equipos, información o software no se deben retirar de su sitio sin autorización previa	Cumple satisfactoriamente
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Cumple parcialmente
A11.2.7	Disposición segura o reutilización de equipos	Control: se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.	Cumple parcialmente
A11.2.8	Equipos de usuario desatendido	Control: los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	No cumple
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	No cumple
A12	**SEGURIDAD DE LAS OPERACIONES**		
A12.1	Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			
A12.1.1	Procedimientos de operación documentados	Control: los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A12.1.2	Gestión de cambios	Control: se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Cumple parcialmente
A12.1.3	Gestión de capacidad	Control: se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No cumple
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No aplica
A12.2	Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			
A12.2.1	Controles contra códigos maliciosos	Control: se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	No cumple
A12.3	Copias de respaldo		
Objetivo: Proteger contra la perdida de datos			
A12.3.1	Respaldo de la información	Control: se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple parcialmente
A12.4	Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia			
A12.4.1	Registro de eventos	Control: se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No cumple
A12.4.2	Protección de la información de registro	Control: las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No cumple
A12.4.3	Registros del administrador y del operador	Control: las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A12.4.4	Sincronización de relojes	Control: los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple parcialmente
A12.5	Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales			
A12.5.1	Instalación de software en sistemas operativos	Control: se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	No cumple
A12.6	Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	No cumple
A12.6.2	Restricciones sobre la instalación de software	Control: se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	No cumple
A12.7	Consideraciones sobre auditorias de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos			
A12.7.1	Controles de auditorías de sistemas de información	Control: los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No cumple
A13	**SEGURIDAD DE LAS COMUNICACIONES**		
A13.1	Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A13.1.1	Controles de redes	Control: las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple parcialmente
A13.1.2	Seguridad de los servicios de red	Control: se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	No cumple
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A13.2	Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
A13.2.1	Políticas y procedimientos de transferencia de información	Control: se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	No cumple
A13.2.2	Acuerdos sobre transferencia de información	Control: los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	No cumple
A13.2.3	Mensajería Electrónica	Control: se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente
A13.2.4	Acuerdo de confidencialidad o de no divulgación	Control: se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	No cumple
A14	**Adquisición, desarrollo y mantenimiento de sistemas**		
A14.1	Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	No cumple
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No cumple
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: la información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	Control: se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplica
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplica
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No cumple
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No cumple
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No cumple
A.14.2.6	Ambiente de desarrollo seguro	Control: las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No cumple
A.14.2.7	Desarrollo contratado externamente	Control: la organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	No aplica
A.14.2.8	Pruebas de seguridad de sistemas	Control: durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	No aplica
A.14.2.9	Prueba de aceptación de sistemas	Control: para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	No aplica
A14.3	Datos de prueba		

Cuadro 3. (Continuación)

ANEXO			ESTADO
Objetivo: Asegurar la protección de los datos usados para pruebas.			
A.14.3.1	Protección de datos de prueba	Control: los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	No aplica
A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	Seguridad de la información en las relaciones con los proveedores.		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	No cumple
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	No cumple
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	No cumple
A15.2	Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.	No cumple
A16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			

Cuadro 3. (Continuación)

ANEXO			ESTADO
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	No cumple
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	No cumple
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	No cumple
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	No cumple
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No cumple
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No cumple
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No cumple
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**		
A17.1	Continuidad de Seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	No cumple
A17.2	Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Cumple parcialmente
A18	**CUMPLIMIENTO**		
A18.1	Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Cumple parcialmente
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	No aplica
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Cumple parcialmente
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Cumple parcialmente
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No cumple

Cuadro 3. (Continuación)

ANEXO			ESTADO
A18.2	Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	No cumple
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	No cumple
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No cumple

Fuente: Icontec. NTC-ISO-IEC 27001:2013.

El análisis GAP es un paso muy importante en la implementación de la Norma ISO 27001 ya que por medio de él se pueden identificar las amenazas que exponen la confidencialidad, integridad y disponibilidad de la información, por consiguiente se evalúan los controles que se están implementando en la empresa y se diagnostica su estado actual frente a la seguridad como se muestra en la figura 12:

Figura 12. Análisis matriz GAP

Fuente: Icontec. NTC-ISO-IEC 27001:2013

Es decir que de acuerdo al diagnóstico que muestra la figura 12; el porcentaje de cumplimiento de los controles implementados en la entidad se evidencia en el Cuadro. 4

Cuadro 4. Cumplimiento de controles en la entidad

Nombre dominios de control	Controles que aplican	Peso controles implementados y parcialmente implementados	Implementados	Parcialmente	No cumple	No aplica
Dominio 5 - políticas de seguridad de la información	2	0	0	0	2	0
Dominio 6 - organización de la seguridad de la información	7	2	0	4	3	0
Dominio 7 - seguridad de los recursos humanos	6	2,5	0	5	1	0
Dominio 8 - gestión de activos	10	3	1	4	5	0
Dominio 9 - control de acceso	13	5	2	6	5	1
Dominio 10 - criptografía	2	0	0	0	2	0
Dominio 11 - seguridad física y del entorno	15	6,5	2	9	4	0
Dominio 12 - seguridad de las operaciones	13	1,5	0	3	10	1
Dominio 13 - seguridad de las comunicaciones	7	1	0	2	5	0
Dominio 14 - adquisición, desarrollo y mantenimiento de sistemas	7	0	0	0	7	6
Dominio 15 - relación con los proveedores	5	0	0	0	5	0
Dominio 16 - gestión de incidentes de seguridad de la información	7	0	0	0	7	0
Dominio 17 - aspectos de seguridad de la información de la gestión de continuidad de negocio	4	0,5	0	1	3	0
Dominio 18 - seguridad de las comunicaciones	7	1,5	0	3	4	1
	105					

Fuente: Icontec. NTC-ISO-IEC 27001:2013

En lo cual se puede determinar que de los 114 controles que propone la Norma ISO 27001:2013, para la Entidad solo aplican 105, implementados 5, implementados parcialmente 37, no se cumplen 63 y no aplican 9.

9. METODOLOGÍA

El instrumento que se utilizó para determinar el conocimiento de los funcionarios frente a la seguridad de la información de la secretaría de hacienda del municipio de Cucunubá, fue una encuesta cerrada de 17 preguntas aplicada a 4 funcionarios de cinco que laboran en la dependencia de hacienda obteniendo los siguientes resultados (las encuestas están en los anexos de este documento):

1. ¿conoce usted qué es seguridad de la información?
a. Si
b. No
c. No tiene idea

2. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?
a. Si
b. No
c. Es compartida

3. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?
a. 1
b. 2 o 3
c. 3 o 5

4. ¿Cambia periódicamente la contraseña de sus cuentas?
a. Si
b. No
c. Rara vez
5. ¿Su equipo cuenta con antivirus licenciado?
a. Si
b. No

6. ¿usted tiene restringida algún tipo de página en su computador?
a. Si
b. No

7. ¿sabe que es un virus informático?
a. Si
b. No

8. ¿Sabe cómo actuar en caso de encontrarse con un virus?
a. Si
b. No

9. ¿Usted hace copias de seguridad de su información?
a. Si
b. No
c. Rara vez

10. ¿A su equipo le realizan mantenimiento preventivo?
a. Si
b. No
c. Casi nunca

11. ¿su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?
a. Si
b. No
12. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?
a. Si
b. No
c. No conozco restricciones para hacerlo

13. ¿Conoce que son los activos de la información?
a. Si
b. No

14. ¿usted guarda información personal (fotos, música, archivos) en los equipos institucionales?
a. Si
b. No
c. Rara vez

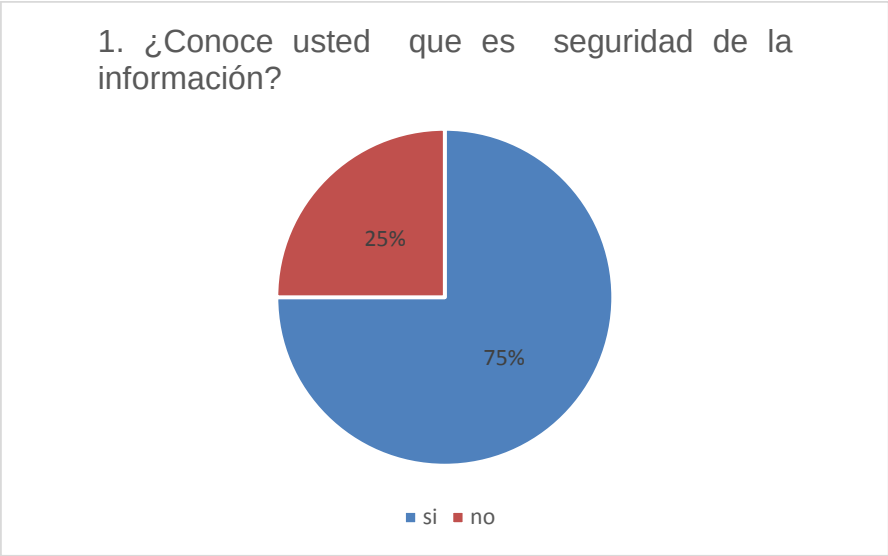
15. ¿Sabe que es un delito informático?
a. Si
b. No

16. ¿conoce alguna norma que proteja la seguridad de la información?
a. SI
b. NO
c. CUAL_____

17. ¿usted sabe que si en la Entidad existen políticas de seguridad de la información?
a. Si
b. No
c. No tiene idea

Los resultados de la anterior encuesta se representan mediante las siguientes gráficas.

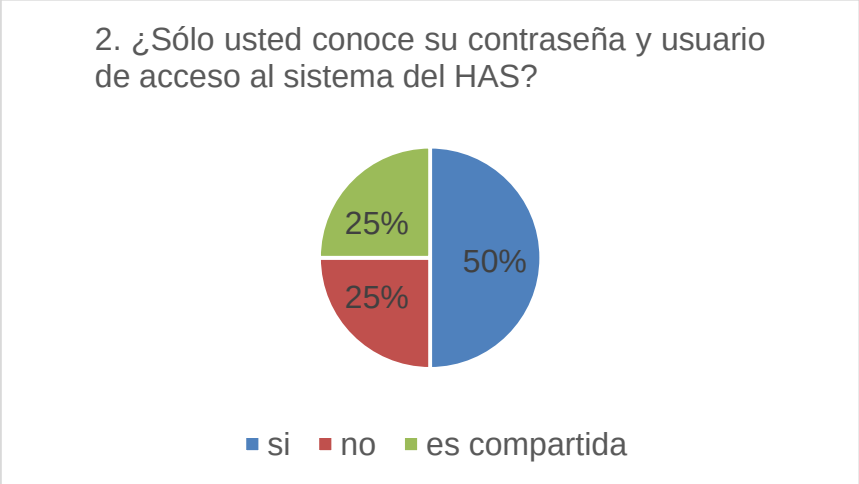
Figura 13. **¿Conoce usted que es seguridad de la información?**



Fuente: El autor, 2016.

En la figura 13 se evidencia que de las encuestas realizadas el 25% no sabe que es la seguridad de la información.

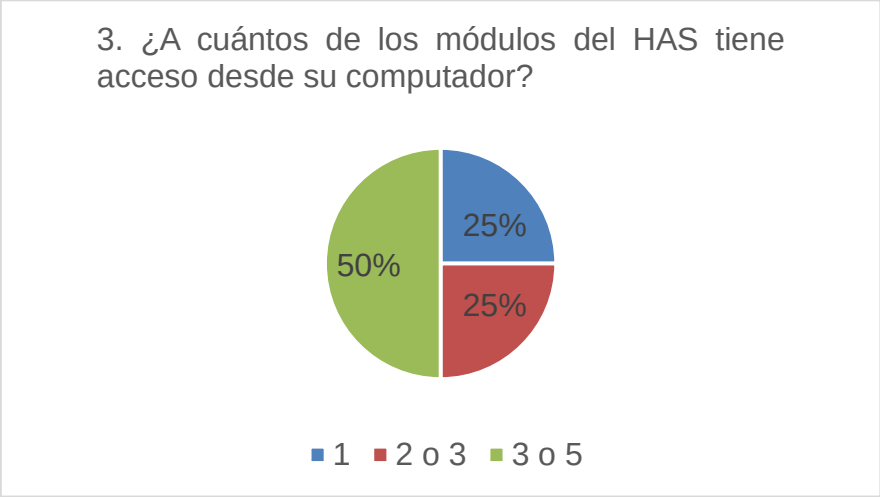
Figura 14. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?



Fuente: El autor, 2016.

La figura 14 muestra que la entidad no tiene definidos los roles que deben asumir los funcionarios frente a las contraseñas, puesto que esta debe ser única y solo la debe conocer su dueño.

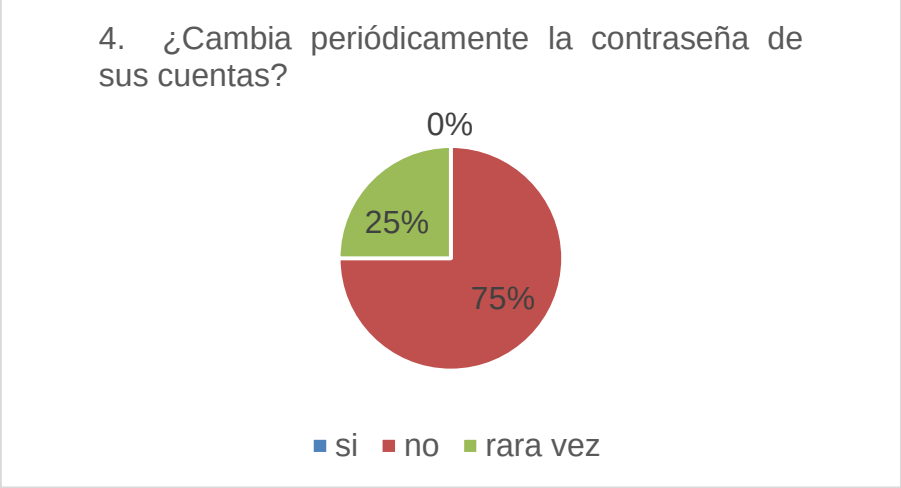
Figura 15. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?



Fuente: El autor, 2016.

En la figura 15 se evidencia que los diferentes módulos del programa HAS se encuentran instalados en diferentes computadores y además se puede ingresar por cualquiera de esos equipos al programa.

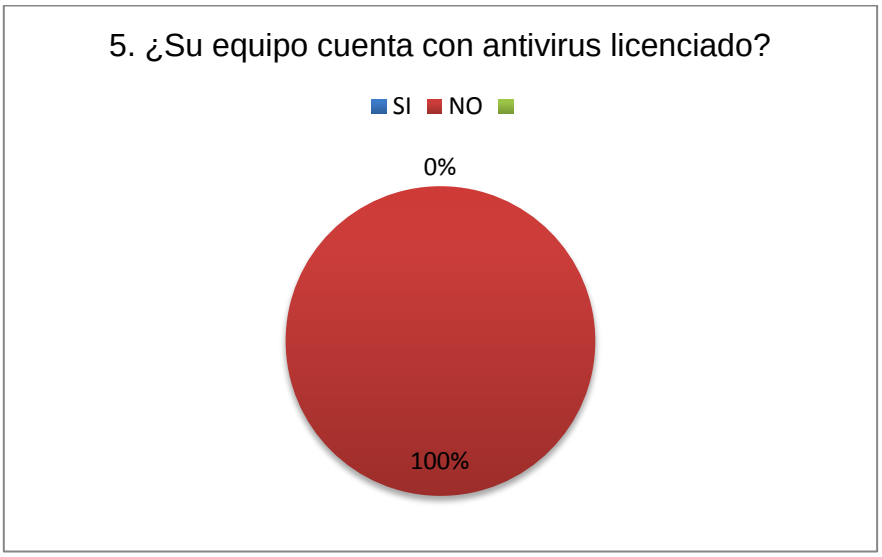
Figura 16. ¿Cambia periódicamente la contraseña de sus cuentas?



Fuente: El autor, 2016.

En la figura 16 se muestra que el 75% de los funcionarios de esta dependencia no cambia las contraseñas para ingresar a las diferentes cuentas mientras que el 25% si lo hacen.

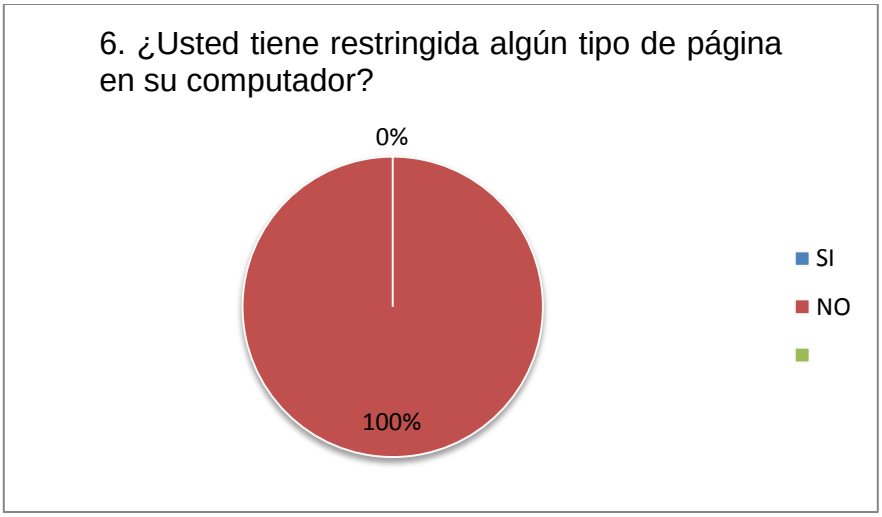
Figura 17. ¿Su equipo cuenta con antivirus licenciado?



Fuente: El autor, 2016.

En la gráfica de la figura 17 se evidencia que la Secretaría de hacienda del municipio de Cucunubá no cuenta con antivirus licenciados, lo que genera hacer la recomendación para adquirirlo en el menor tiempo.

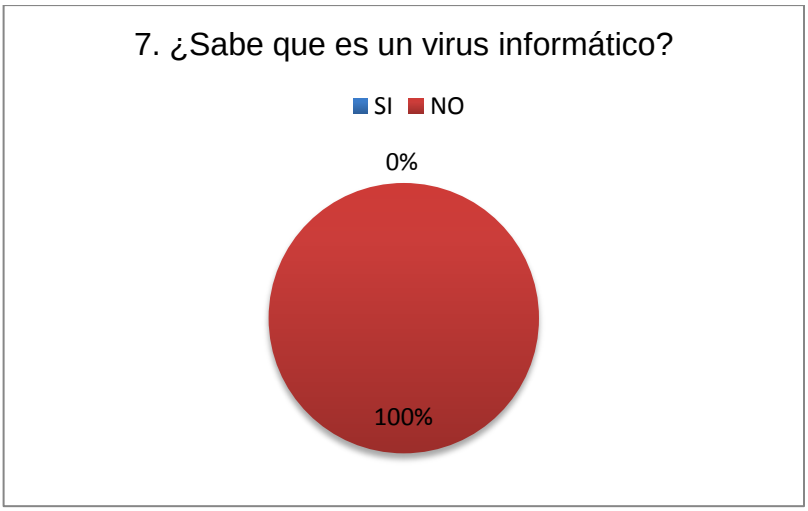
Figura 18. ¿Usted tiene restringida algún tipo de página en su computador?



Fuente: El autor, 2016.

En la figura 18 se puede determinar que la Entidad no tiene ningún tipo de restricción en la navegación de internet, se recomienda hacerlo para proteger la integridad, confiabilidad y disponibilidad de la información que se maneja en la Secretaría de Hacienda del Municipio de Cucunubá.

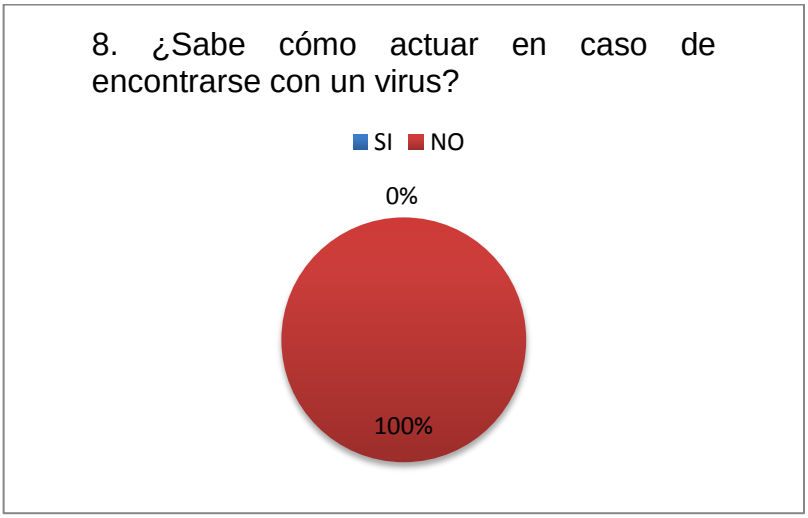
Figura 19. ¿Sabe que es un virus informático?



Fuente: El autor, 2016.

En la figura 19 muestra que el 100% de los funcionarios no saben en qué consiste un virus informático.

Figura 20. ¿Sabe cómo actuar en caso de encontrarse con un virus?



Fuente: El autor, 2016.

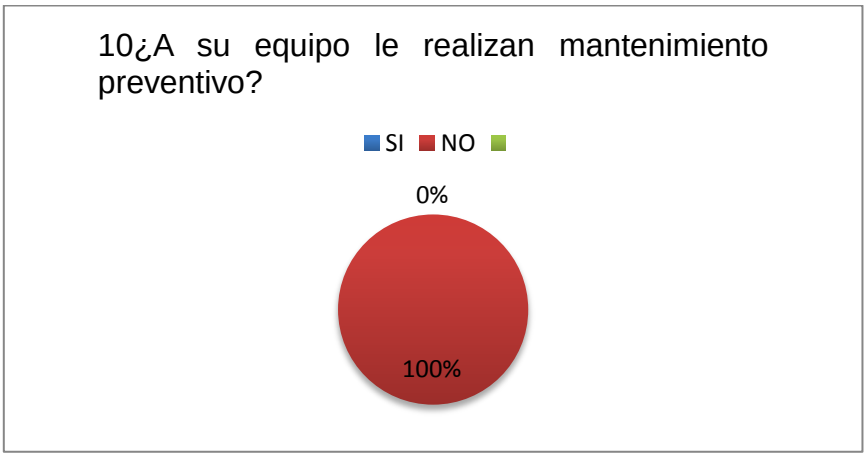
En la figura 20 el 100% de los funcionarios han respondido que no saben qué hacer en caso de encontrarse con un virus informático en medio de sus tareas diarias.

Figura 21. ¿Usted hace copias de seguridad de su información?

Fuente: El autor, 2016.

En la figura 21 se puede ver que los funcionarios no tienen la cultura de hacer copias de respaldo periódicamente para garantizar la disponibilidad de la información que se maneja en la Secretaría de Hacienda del municipio.

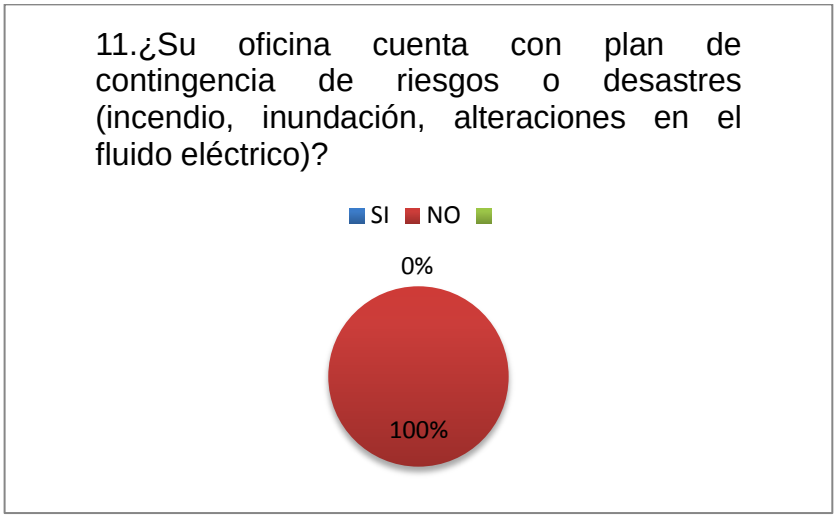
Figura 22. ¿A su equipo le realizan mantenimiento preventivo?



Fuente: El autor, 2016.

En la pregunta de la figura 22 los funcionarios manifestaron que a sus equipos no les realizan mantenimiento preventivo, por lo que se recomienda realizarlo periódicamente para evitar tener problemas de funcionamiento de los equipos.

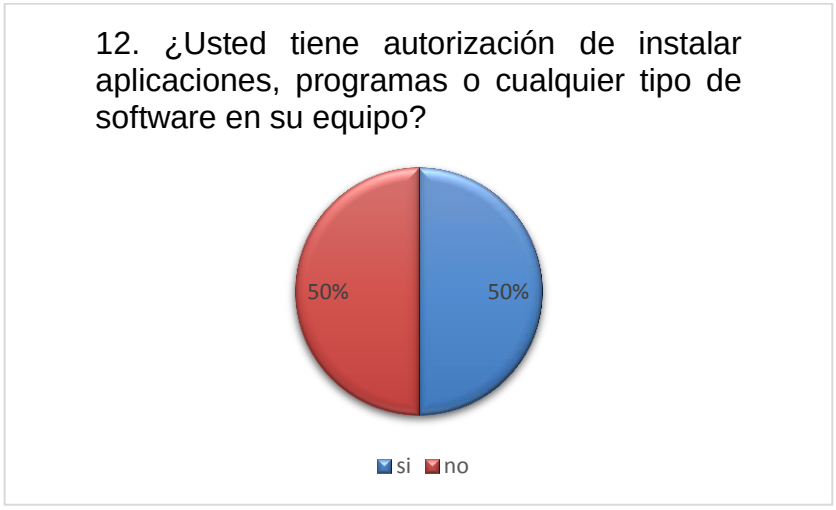
Figura 23. ¿Su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?



Fuente: El autor, 2016.

En la figura 23 se detecta que la entidad no tiene preparados planes de contingencia para enfrentar cualquier eventualidad que se presente.

Figura 24. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?



Fuente: El autor, 2016.

Se evidencia en la figura 24 que dos de los funcionarios respondieron que no tienen libertad de navegación y dos respondieron que si pueden hacer descargas e instalación de aplicaciones, lo cual se llega a deducir que ellos no tienen la certeza si están habilitados sus equipos para realizar instalaciones de aplicativos o no.

Figura 25. ¿Conoce que son los activos de la información?

Fuente: El autor, 2016.

En figura 25 representa que los funcionarios manifestaron no conocer que son los activos de la información.

Figura 26. ¿Usted guarda información personal (fotos, música, archivos) en los equipos institucionales?

Fuente: El autor, 2016.

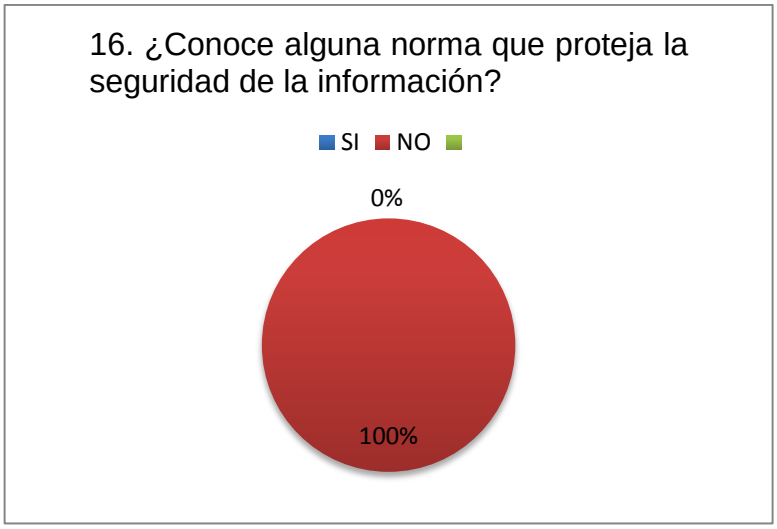
En la figura 26 se evidencia que los funcionarios están teniendo una buena práctica con los equipos institucionales, ya que no guardan información personal en los computadores de la Entidad.

Figura 27. ¿Sabe que es un delito informático?

Fuente: El autor, 2016.

En la figura 27 se refleja que los funcionarios de la Secretaría de Hacienda no tienen conocimiento en lo que consiste un delito informático.

Figura 28. ¿Conoce alguna norma que proteja la seguridad de la información?



Fuente: El autor, 2016.

En la figura 28 nos damos cuenta que los funcionarios de la Secretaría de Hacienda desconocen las normas que existen en torno a la seguridad de la información.

Figura 29. ¿Usted sabe que si en la Entidad existen políticas de seguridad de la información?

Fuente: El autor, 2016.

En la pregunta que representa la figura 29, se evidencia que los funcionarios no saben si en la Entidad existen políticas de seguridad de la información.

10. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

10.1 REQUISITOS GENERALES

La secretaría de Hacienda del municipio de Cucunubá debe hacer un seguimiento al sistema de Gestión de Seguridad de la Información diseñado para esta dependencia estableciendo formatos y estándares para hacer la debida documentación de todo el proceso.

10.2. ALCANCE

El sistema de Gestión de Seguridad de la Información se desarrollará en la Secretaría de Hacienda del Municipio de Cucunubá – Cundinamarca, entidad pública.

10.2.1 Marco de referencia. En la Alcaldía municipal de Cucunubá no se han implementado políticas de seguridad de la información y tampoco se tiene la cultura informática de proteger siempre la información que se maneja ya que los funcionarios desconocen la importancia de saber protegerla y exponerla.

10.2.2 inventario de activos de la información de la secretaría de hacienda del municipio de Cucunubá. Basados en el contexto de activo según la ISO 27001. Activo: cualquier cosa que tiene valor para la organización"[17] se definió el siguiente inventario de activos para la Secretaría de Hacienda del municipio de Cucunubá

10.2.2.1 Activos intangibles

Sistemas de información: SQL HAS módulo de contabilidad, nomina, impuesto predial, almacén, presupuesto.
Bases de datos: funcionarios alcaldía, DISFON transporte escolar.
Software: licencias
Documentos electrónicos: correos electrónicos, página institucional, cuentas bancarias, aplicativos gubernamentales.
Conocimiento: experiencia, conocimiento técnico, imagen corporativa.

10.2.2.2 activos físicos

Caja fuerte: chequeras, token, documentos reservados.
Llaves de la oficina: definir el responsable de las mismas
Hardware: servidor, estaciones de trabajo, impresoras, discos duros, usb, cd´s.
Información impresa: carpetas de documentación foliadas.
Teléfono, teléfono móvil.

[17] Icontec. NTC-ISO/IEC 27001. Op.cit.

10.2.2.3 Activos humanos

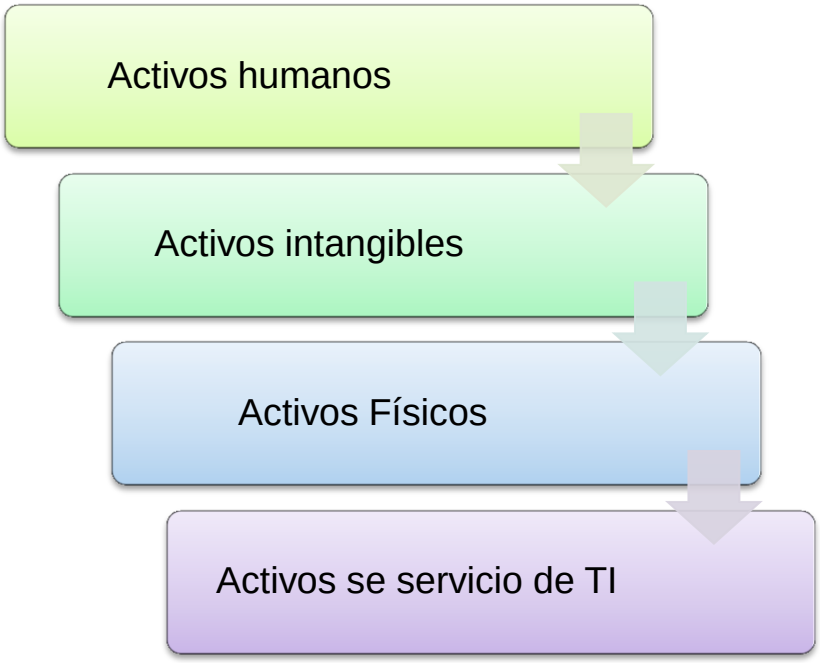
Funcionarios: Secretario de Hacienda, contadora, almacenista, 1 auxiliar.
Funcionarios contratistas. 1 auxiliar

10.2.2.4 activos de servicios de TI

Servicio de red: inalámbrico
Asistencia remota.
Mantenimiento de software por acceso remoto.

10.2.2.5 Priorización de la información. Para priorizar la información de la Secretaría de Hacienda del municipio de Cucunubá, se parte de los parámetros principales de la seguridad de la información (integridad, confidencialidad y disponibilidad), se propone la clasificados de los activos al dueño de la información (en este caso la secretaria de Hacienda), quien prioriza la información como muestra la figura 30.

Figura 30. Priorización de la información



Fuente: El autor, 2016.

11. IMPLEMENTACIÓN DE PROCESOS DE ACUERDO A LA ISO 27001

En el diseño del SGSI para la Secretaría de Hacienda del municipio de Cucunubá se alinea con el ciclo: Planificar, Hacer, verificar y Actuar de acuerdo como lo indica la Norma ISO 27001 2013:

11.1 PLANEAR

- Para la inicialización del diseño del SGSI se definieron los objetivos para determinar lo que se quiere lograr y hacia donde apunta el diseño que se está creando.
- Se definieron e identificaron los activos de la seguridad de la información para saber lo que se quiere proteger y así mismo se identificó el nivel de riesgo de cada uno junto con sus vulnerabilidades y amenazas a los que están expuestos.
- En este diseño del SGSI se proponen unas políticas para implementarlas en pro de mitigar los riesgos a los que se enfrenta la seguridad de la información de la dependencia de Secretarías de Hacienda.

11.2 HACER

- Una vez identificados los riesgos se prevén los controles de acuerdo a la Norma ISO 27001 que se van a aplicar a cada uno de los riesgos identificados para mitigarlos, controlarlos, eliminarlos o transferirlo.
- Se proponen unas políticas para concientizar a los empleados y poder controlar las amenazas y vulnerabilidades.

11.3 ACTUAR

- Una vez identificados los riesgos se pueden controlar acciones correctivas o preventivas para controlarlos.
- El diseño del SGSI propone llevar un registro de todos los incidentes y el tratamiento que se da a cada uno y así mismo implementar mejoras preventivas y correctivas.

11.4 VERIFICAR

- El diseño del SGSI realizado para la Secretaría de Hacienda del municipio de Cucunubá propone en las políticas estipuladas hacer un seguimiento periódico para evaluar la forma como se está implementando el SGSI.

12. PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ – CUNDINAMARCA

12.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: definir lineamientos que lleven a mantener la protección de los activos de la información de la Secretaría de Hacienda del municipio de Cucunubá – Cundinamarca.

Resumen: Estas políticas se aplican al recurso humano de la Secretaría de Hacienda del Municipio de Cucunubá**.**

Se debe establecer la política de seguridad de la Información para la Secretaría de Hacienda del municipio de Cucunubá.

Se debe socializar la política diseñada con el funcionario directamente afectado en la protección de la información.

Capacitar a los funcionarios de la dependencia en cultura informática para que puedan saber qué hacer en caso de que se les presente una eventualidad en el transcurso de sus labores diarias.

Diseñar e implementar un programa de auditorías periódicas por parte de la oficina de control interno para verificar la información, programas o aplicativos que maneja cada usuario en su equipo.

Implementar un área responsable de informática y seguridad de la información quien sea el encargado de aprobar cualquier instalación de software o aplicaciones en los equipos de la dependencia.

Para mejorar la seguridad se debe implementar un firewall para la seguridad perimetral en la conexión a internet.

Las conexiones remotas realizadas al sistema deben llevar un registro mínimo con los siguientes datos que muestra la Cuadro 5.

Cuadro 5. Registro

Nº de incidente	Nombre de la persona responsable del esquipo	Nombre de la persona que atiende el caso	Fecha de inicio Fecha de terminación	Descripción del incidente	Acciones realizadas

Fuente: El autor, 2016.

El secretario de Hacienda debe velar porque se estén aplicando las políticas de seguridad de la información dentro de su dependencia.

La transferencia de archivos se debe realizar implementando protocolos seguros.

12.1.1 Acuerdos de confidencialidad

- Todos los contratos laborales realizados por parte de la Secretaría de Hacienda deben tener acuerdos de confidencialidad para proteger la información.
- Cuando se realiza contratos a prestadores de servicios deben tener una cláusula de confidencialidad.
- Todos los funcionarios que trabajen en la Secretaría de Hacienda deben firmar un acuerdo de confidencialidad antes de iniciar a tener acceso a ella.

12.1.2 Acceso a internet

- Bloquear todas las páginas de redes sociales.
- Bloquear programas no autorizados de descargas no autorizadas.
- Prohibir en ingreso a páginas que atenten contra la ética y la normatividad vigente.
- Restringir el acceso a la mensajería instantánea para evitar la transferencia de archivos maliciosos.
- No permitir la instalación de o descarga de archivos o programas no autorizados en los equipos.
- Realizar actividades de inspección de navegación de cada funcionario.

12.1.3 Uso adecuado de los activos de la información

- Tener clasificada la información para controlar el acceso a ella por parte de los usuarios y / o funcionarios.
- Implementar por parte de la oficina de Control interno auditorías internas para hacer seguimiento al cumplimiento de las políticas establecidas.

12.1.4 Correo electrónico

- Correo electrónico que se maneja en la Secretaría de Hacienda del municipio de Cucunubá es institucional y su uso debe ser exclusivo para las funciones relacionadas con esta dependencia.

- El correo institucional solo de debe utilizar para asuntos de la secretaría de hacienda y no para envío y recepción de información de carácter personal de algún funcionario.
- No acceder al correo electrónico institucional desde equipos y conexiones públicas que sean inseguras.
- No dejar sesión abierta en los computadores o teléfonos móviles.
- Prohibir el envío de mensajes que contengan código malicioso o con algún interés personal que atenten contra la integridad y el buen nombre de la Entidad.
- El correo electrónico institucional no se debe manejar de ninguna manera de forma personal.
- Se debe realizarle cambio periódico de contraseña.
- Se debe tener solo una persona responsable del correo electrónico.

12.1.5 Recursos tecnológicos

- Cualquier tipo de instalación que se necesite hacer, lo debe hacer solo la persona autorizada y en efecto supervisado por la persona encargada de la seguridad de la información.
- La configuración de los equipos solo la debe hacer el responsable del área de informática.
- El soporte al sistema de información sólo podrán realizarlos los ingenieros de soporte autorizados por el proveedor, el responsable de la seguridad de la Alcaldía debe llevar el control de todas las actividades realizadas durante los procesos de soporte.
- Se deben implementar antivirus y software licenciado y mantenerlos siempre actualizados.
- Sólo los equipos autorizados podrán ser registrados ante el proveedor de internet para poderse conectar a internet.
- Se debe desactivar los equipos de la red de internet de los funcionarios que dejen de trabajar en la dependencia de Hacienda.
- Solo las personas autorizadas podrán hacer conexiones remotas.

12.1.6 Control de acceso físico.

- Teniendo en cuenta que son oficinas a las que ingresan usuarios no se deben dejar solas en ningún momento o si es el caso cerrarla.

12.1.7 Gestión de contraseñas

- Se deben cambiar las contraseñas con periodicidad manteniendo un nivel alto de seguridad, es decir combinar números, mayúsculas y minúsculas.

- Las contraseñas deben ser combinaciones alfanuméricas y no utilizar nombres de familiares ni fechas de acontecimientos.
- No se deben dejar las contraseñas escritas en fechas visibles o revelarlas a otras personas.
- La contraseña de cada aplicativo o sistema de información él debe manejar y saber solo la persona responsable del mismo.

12.1.8 Protección de los equipos.

- Se debe mantener la infraestructura de las oficinas en óptimo estado, como puertas, ventanas, paredes y tejados.
- Se debe tener una oficina solo para atención a los usuarios por parte de la Secretaría de Hacienda para que no tengas ningún tipo de acceso o contacto con información privilegiada que se maneje en la oficina.
- Se beben implementar las normas y equipos de emergencia para estar preparados contra eventos externos, internos y ambientales, ya sean incendios, inundaciones, explosiones, manifestaciones sociales o cualquier otro desastre.
- Controlar el acceso de personal no autorizado a las oficinas y mantenerlos aislados de los servicios de procesamiento de información.
- Implementar UPS y estabilizadores en todos los equipos de cómputo teniendo en cuenta que el municipio se presenta continuas fallas en el suministro de energía.
- Se debe realizar el mantenimiento preventivo de hardware y software de los equipos para garantizar la integridad y buen funcionamiento de los mismos.
- Se debe contar con autorización para poder sacar un equipo de la entidad y llevarle una hoja de actividades, así mismo responsabilizarse de la información que allí se encuentre almacenada.
- No se puede realizar eliminación, cambio, modificación de software sin una autorización previa.

12.1.9 Copias de seguridad.

- Se deben implementar la cultura de hacer por lo menos dos copias de la información periódicamente y almacenarlas en dos medios diferentes y lugares diferentes.
- Los medios donde se guarde la información deben garantizar los controles de seguridad de la misma y ninguna persona diferente puede tener acceso a la misma.

12.1.10 Cultura de escritorios y pantallas limpias

- Todos los equipos deben tener contraseñas seguras.
- Los escritorios de los computadores deben estar libres de carpetas y documentos.
- No se debe dejar documentos o medios de almacenamiento sobre el escritorio.
- No dejar claves anotadas en lugares visibles.
- Mantener con seguro los cajones de escritorios.
- No permitir el acceso de otras personas a los sistemas de información.

12.1.11 Uso de dispositivos móviles

- Tener contraseña para el ingreso al teléfono móvil y a todas sus aplicaciones.
- No prestar el teléfono a personas externas a la dependencia.

12.1.12 Recursos humanos

- Socializar e implementar la política de seguridad de la información con todos los funcionarios de la dependencia.
- Tener el compromiso de la alta dirección para apoyar activamente el cumplimiento de las políticas de seguridad.
- Asignar responsabilidades para el cumplimiento de las políticas de seguridad de la información.
- Llevar un seguimiento a las cláusulas de confidencialidad de los contratos de los funcionarios de la dependencia.
- Deben asignarse el responsable de los activos de la información.
- Se debe realizar una revisión de antecedentes de los funcionarios de la dependencia y clasificar la información que se va a disponer como responsabilidad de cada uno.
- Deshabilitar permisos y roles cuando se terminen contratos laborales.
- Una vez se termine un contrato el funcionario debe hacer devolución de los equipos o información que se encontraba a su cargo.

12.2 POLÍTICAS DE SOFTWARE

Se deben implementar controles de prevención y detección de código malicioso.

12.2.1 Uso de token

- El token debe permanecer bajo llave y solo puede tener a él el jefe de dependencia.
- No dejar el toquen sobre el escritorio.

- En caso de portar el token fuera de la Secretaría garantizar su seguridad e integridad.
- El administrador del token debe ser el mismo responsable del portal o sitio a utilizar este dispositivo.

12.2.2 Equipos institucionales

- No se deben conectar dispositivos personales o de terceros en los equipos institucionales.
- Evitar guardar información personal en los computadores, toda vez que todo lo que allí se guarde será sujeto a revisión por parte de auditorías internas.
- La entidad no responde por información personal guardada en los equipos institucionales.
- Establecer lineamientos para no utilizar medios de almacenamiento persona

13. VALORACIÓN DE LOS RIESGOS

Se implementa la siguiente matriz, ver Cuadro 6 Para realizar un análisis y valoración de los riesgos identificados.

Cuadro 6. Valoración de riesgos

ANÁLISIS DE RIESGO			
MAYOR (3)	3	6	9
MODERADO (2)	2	4	6
MENOR (1)	1	2	3
	RARO (1	POSIBLE (2)	PROBABLE (3)

Fuente: El autor, 2016.

RIESGO = PROBABILIDAD X IMPACTO

Dónde:
La probabilidad puede ser: raro – posible - probable
El impacto puede ser: menor – moderado - mayor

13.1 IDENTIFICACIÓN DE LOS RIESGOS

Una vez identificados los activos de la información de la Secretaría de Hacienda de la Alcaldía municipal de Cucunubá, se identifican los riesgos, amenazas, vulnerabilidades e impactos de cada uno que puedan llegar a afectar su integridad confidencialidad y disponibilidad de la información a los cuales se les da un valoración de acuerdo a la matriz de riesgo expuesta anteriormente y la cual define que: riesgo=impacto x probabilidad

Cuadro 7. Valoración de riesgos

NOMBRE DEL ACTIVO	***IDENTIFICACIÓN DEL RIESGO***	***AMENAZA***	***VULNERABILIDADES***	***RIESGO***
SOFTWARE SQL HAS	**R1** Permiso de los usuarios de acceso al sistema no definidos	Uso indebido de los sistemas de información en delitos informáticos	Tener acceso a diferentes roles	4
	R2 Existen módulos instalados en equipos de usuarios que no corresponde ese rol	Acceder s módulos sin ser el usuario correspondiente y realizar alteraciones en la información	Tener instalados todos los módulos en diferentes computadores	6
	R3 Alteración de información	Conexión remota desde lugares externos a la administración municipal	Conexiones no seguras a través de internet	2
	R4 Filtración de usuarios y contraseñas	Terceros pueden llegar a deducirlas	Información enviada a través de telefonía móvil o de correos electrónicos	6
	R5 Un usuario puede iniciar múltiples sesiones en diferentes máquinas al mismo tiempo sin tener un control.	Múltiples usuarios manejan la misma contraseña para ingresar al sistema	Estar conectado la red y conectarse de forma remota	4
NOMBRE DEL ACTIVO	**IDENTIFICACIÓN DEL RIESGO**	AMENAZA	VULNERABILIDADES	RIESGO
BASES DE DATOS	**R6** No están definidos y documentados los roles de cada funcionario con el manejo de las BD que se manejan en la Secretaría de Hacienda del municipio de Cucunubá	Interacción de múltiples usuarios con las bases de datos almacenadas en los equipos.	No tener control y seguimiento a las funciones de cada rol del sistema	9
	R7 Conexión en red de los equipos de la Secretaría de Hacienda del municipio de Cucunubá	Estar los equipos de la secretará de Hacienda del municipio de Cucunubá con todos los de las demás dependencias de la alcaldía.	Estar todos los equipos de la Alcaldía conectados a la misma red	9

Cuadro 7. (Continuación)

NOMBRE DEL ACTIVO	***IDENTIFICACIÓN DEL RIESGO***	***AMENAZA***	***VULNERABILIDADES***	***RIESGO***
	R8 No tener contraseñas seguras en los equipos de la Secretaría de Hacienda del municipio de Cucunubá	Cualquier usuario puede ingresar en cualquiera de los equipos pertenecientes a la Secretaría de Hacienda	Baja o ausencia de contraseñas seguras en los computadores (contraseñas obvias)	4
CONTROL DE ACCESO	**R9** Acceso no autorizado	Alteración de la integridad de la información	No tener definías las funciones de cada rol	6
SOFTWARE	**R10** Programas sin licenciamiento	Puede llegar a materializarse en virus o malware	No tener las licencias de antivirus	9
	R11 Aplicaciones no autorizadas	Descarga e instalación de virus y software malicioso	Estar conectado a internet	4
NOMBRE DEL ACTIVO	**IDENTIFICACIÓN DEL RIESGO**	AMENAZA	VULNERABILIDADES	RIESGO
DOCUMENTOS ELECTRÓNICOS	**R12** Correo electrónico institucional	Alteración de envío y recepción de información no autorizada	Varios usuarios manejan el mismo correo y saben la contraseña	6
	R13 No hay políticas de navegabilidad en internet	Robo de información en la red		6
	R14 Funcionalidad irregular del servidor	Contaminar el equipo con virus y malware	No tener antivirus instalado	9
	R15 No actualizar credenciales de los dispositivos de red	Alteraciones de terceros malintencionadas	Conexión a la red	4
	R16 No proteger los archivos con contraseñas seguras	Que cualquier persona pueda acceder a los documentos	No hay cultura de colocar contraseñas seguras y dejar de utilizar las tradicionales	6
CONOCIMIENTO	**R17** No reconocer el trabajo de los funcionarios	Divulgación de información sensible	Funcionarios insatisfechos	1
CAJA FUERTE	**R18** Filtración de la contraseña por las personas que frecuentan la oficina	Interacción con usuarios y más funcionarios de la administración municipal	Tener la caja fuerte a la vista de los usuarios	3

Cuadro 7. (Continuación)

NOMBRE DEL ACTIVO	***IDENTIFICACIÓN DEL RIESGO***	***AMENAZA***	***VULNERABILIDADES***	***RIESGO***
LLAVES DE LA OFICINA	**R19** Varios de los funcionarios tienen llave de la oficina	Evadir responsabilidades	No tener control de acceso a la oficina	3
HARDWARE	**R20** Quema de equipos	Alteración en la energía eléctrica	Equipos sin estabilizadores de energía	6
NOMBRE DEL ACTIVO	**IDENTIFICACIÓN DEL RIESGO**	AMENAZA	VULNERABILIDADES	RIESGO
	R21 Pérdida de información	Alteraciones en el fluido eléctrico	En la Secretaría de hacienda no se cuenta con UPS para los equipos de cómputo	6
	R22 Daños en los equipos	Perder información	No hacer copias de seguridad con periodicidad	3
	R23 Daño de los equipos	Movimientos bruscos de los computadores estando encendidos	Susceptibilidad del disco duro	3
	R24 Fallas en los equipos	No mantenimiento preventivo y correctivo de los equipos de cómputo	Suciedad en el hardware y malware	2
INFORMACIÓN IMPRESA	**R25** Incendios	Alteraciones en la energía	Archivo guardado en la oficina	3
	R26 Humedad	Goteo en el tejado cerca de la oficina	Piso de oficina alfombrado	3
	R27 Deterioro de documentos	Manejo constante de documentos impresos	Desgaste del papel	1
	R28 No tener tablas de retención actualizadas	No tener cuantificada y relacionada la información impresa existente	No haber tablas de retención actualizadas constantemente	1
	R29 Préstamo de documentos o carpetas	Pérdida de documentos o alteración de información	Buena fe en las personas	6
TELÉFONO MÓVIL	**R30** Estar expuesto y disponible para todos los funcionarios	Extraer información del teléfono	Estar disponible para los funcionarios y a cargo de una sola persona.	3

Cuadro 7. (Continuación)

NOMBRE DEL ACTIVO	***IDENTIFICACIÓN DEL RIESGO***	***AMENAZA***	***VULNERABILIDADES***	***RIESGO***
NOMBRE DEL ACTIVO	**IDENTIFICACIÓN DEL RIESGO**	AMENAZA	VULNERABILIDADES	RIESGO
FUNCIONARIOS	**R31** Conocimiento adquirida de la Secretaría de Hacienda	Divulgación de información	Interacción de múltiples funcionarios con múltiples procesos de la secretaría de Hacienda.	4
ASISTENCIA REMOTA	**R32** Acceso de terceros al sistema de información de la Secretaría de Hacienda del municipio de Cucunubá	Realizar a través de la asistencia remota procedimientos no autorizados con intereses particulares	Conexión remota.	3
MANTENIMIENTO DEL SISTEMA SQL HAS POR ACCESO REMOTO	**R33** Terceros interactuando con el sistema de información y sin tener control de acceso	Realizar actividades con intereses particulares	Conexión remota	3

Fuente: El autor, 2016.

13.2 MAPA DE RIESGOS IDENTIFICADOS SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ

Cuadro 8. Mapa de Riesgos

Análisis de riesgos			
Mayor (3)	**3 R22, R23, R25, R26, R30, R32, R33**	**6 R20, R21, R29**	**9 R6, R7, R10, R14**
Moderado (2)	**2 R24**	**4 R1, R5, R8, R11, R15, R31**	**6 R2, R4, R9, R12. R13, R16,**
Menor (1)	**1 R17, R27, R28**	**2 R3**	**3 R18, R19,**
	Raro (1)	Posible (2)	Probable (3)

Fuente: El autor, 2016, del diseño del SGSI.

En el Cuadro 8 se clasifican los riesgos según su impacto y probabilidad teniendo en cuenta que **riesgo=impacto*probabilidad,** este mapa de riesgos permite priorizarlos y de esta forma empezar a combatir los que generan un impacto más alto y de esta forma salvaguardar los activos de la información de la Secretaría de Hacienda del municipio de Cucunubá teniendo en cuenta la calificación del Cuadro 9.

Cuadro 9. Riesgo

Alto	9	
Medio	4 - 6	
Bajo	1-2-3	

Fuente: El autor, 2016.

13.3 ACEPTACIÓN DEL RIESGO

Una vez identificado el impacto de los riesgos se puede estimar el tratamiento de aceptación del riesgo (Aceptación, evitar, o transferir el riesgo)

14. APLICACIÓN DE CONTROLES A LOS RIESGOS IDENTIFICADOS

Partiendo de la Norma NTC-ISO/IEC 27001 en la cual especifica los requisitos para la implementación de controles de seguridad adaptados de acuerdo a las necesidades de la organización. En este caso a la Secretaría de Hacienda del municipio de Cucunubá; se diseña el Sistema de Gestión de Seguridad de la Información para que los controles implementados que se aplican en el Cuadro 10, 11, 12, 13 14 y 15 sean los necesarios para proteger los activos de la información de la Entidad.

Cuadro 10. Controles Gestión de Activos

DOMINIO A.7 GESTIÓN DE ACTIVOS				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R28	No tener Cuadros de retención actualizadas	**A.7.1.1**	Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	**Preventivo**
R29	Préstamo de documentos o carpetas	**A.7.1.2**	Toda la información y los activos asociados con los servicios de procesamiento de información deben ser parte designada de la organización.	**Correctivo**

Fuente: Icontec. NTC ISO 27001:2013.

Cuadro 11. Controles Seguridad de los recursos humanos

DOMINIO A.8 SEGURIDAD DE LOS RECURSOS HUMANOS				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R17	No reconocer el trabajo de los funcionarios	**A.8.2.3**	Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.	**Correctivo**
		A.8.3.2	Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	**Preventivo**
		A.8.3.3	Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	**Preventivo**

Cuadro 11. (Continuación)

DOMINIO A.8 SEGURIDAD DE LOS RECURSOS HUMANOS				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R31	Conocimiento adquirida de la Secretaría de Hacienda	**A.8.1.3**	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	**Correctivo**
		A.8.2.3	Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.	**Correctivo**

Fuente: Icontec. NTC ISO 27001:2013.

Cuadro 12. Controles seguridad física y del entorno

DOMINIO A.9 SEGURIDAD FÍSICA Y DEL ENTORNO				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R18	Filtración de la contraseña por las personas que frecuentan la oficina	**A.9.1.2**	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	**Preventivo**
R19	Varios de los funcionarios tienen llave de la oficina	**A.9.1.3**	Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	**Preventivo**
R20	Quema de equipos	**A.9.2.2**	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	**Preventivo**
R21	Pérdida de información			
R25	Incendios	**A.9.1.4**	Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	
R26	Humedad			**Preventivo**
R27	Deterioro de documentos	**A.9.1.5**	Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	**Preventivo**

Fuente: Icontec. NTC ISO 27001:2013.

Cuadro 13. Controles gestión de operaciones y comunicaciones

DOMINIO A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R6	No están definidos y documentados los roles de cada funcionario con el manejo de las BD que se manejan en la Secretaría de Hacienda del municipio de Cucunubá.	**A.10.1.3**	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso Inadecuado de los activos de la organización.	Preventivo
R9	Acceso no autorizado	**A.10.10.3**	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	Preventivo
R11	Aplicaciones no autorizadas	**A.10.9.3**	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no Autorizada.	Preventivo
R12	Correo electrónico institucional	**A.10.8.4**	Información contenida en la mensajería electrónica debe tener la protección adecuada.	**Preventivo**
R13	No hay políticas de navegabilidad en internet	**A.11.4.1**	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	**Preventivo**
R16	No proteger los archivos con contraseñas seguras	**A.10.7.3**	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	**Preventivo**
		A.10.7.4	La documentación del sistema debe estar protegida contra el acceso no autorizado.	**Preventivo**
R22	Daños en los equipos	A.10.5.1	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	Preventivo
R30	Estar expuesto y disponible para todos los funcionarios	A.10.8.3	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	Preventivo
R32	Acceso de terceros al sistema de información de la Secretaría de Hacienda del municipio de Cucunubá	A.10.10.4	Se deben registrar las actividades tanto del operador como del administrador del sistema.	Preventivo
		A.10.10.5	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	Preventivo

Fuente: Icontec. NTC ISO 27001:2013.

Cuadro 14. Control de acceso

DOMINIO A.11 CONTROL DE ACCESO				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R1	Permiso de los usuarios de acceso al sistema no definidos	**A.11.2.2**	Se debe restringir y controlar la asignación y uso de Privilegios.	Preventivo
		A.11.2.1	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de Información.	Preventivo
		A.11.2.4	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de Acceso de los usuarios.	Preventivo
R2	Existen módulos instalados en equipos de usuarios que no corresponde ese rol	**A.11.1.1.**	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	Preventivo
R3	Alteración de información	**A.11.6.1**	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	**Preventivo**
		A.11.7.1	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	Preventivo
R4	Filtración de usuarios y contraseñas	**A.11.4.2**	Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	Preventivo
R5	Un usuario puede iniciar múltiples sesiones en diferentes máquinas al mismo tiempo sin tener un control.	**A.11.5.2**	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	Preventivo

Cuadro 14. (Continuación)

Nº DE RIESGO	RIESGO	CÓD. CONTROL	CONTROL	TIPO DE CONTROL
R7	Conexión en red de los equipos de la Secretaría de Hacienda del municipio de Cucunubá	A.11.4.6	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio.	Preventivo
R8	No tener contraseñas seguras en los equipos de la Secretaría de Hacienda del municipio de Cucunubá	**A.11.3.1**	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	**Correctiva-Preventiva**
R10	Programas sin licenciamiento	**A.11.5.3**	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	**Correctivo**

Fuente: Icontec. NTC ISO 27001:2013.

Cuadro 15. Adquisición, desarrollo y mantenimiento de sistemas de información

DOMINIO A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN				
Nº DE RIESGO	**RIESGO**	**CÓD. CONTROL**	**CONTROL**	**TIPO DE CONTROL**
R14	Funcionalidad irregular del servidor	**A.12.5.3**	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	**Preventivo**
R23	Daño de los equipos	**A.12.6.1**	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	**Preventiva**
R24	Fallas en los equipos			

Fuente: Icontec. NTC ISO 27001:2013.

14.1 PLAN DE ACCIÓN IMPLEMENTADO A LOS CONTROLES

En el cuadro 16 se propone el plan de acción para seguir frente a los controles implementados y permitir tener una proyección en la línea del tiempo para salvaguardar los activos de la información de la Secretaría de Hacienda del municipio de Cucunubá.

Cuadro 16. Plan de acción

Control	Plazo	Acciones	Indicadores de medición
Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	Marzo de 2017	- Inducción y capacitación acerca de lo que es la seguridad de la información. - Cada uno de los funcionarios de la dependencia de Planeación deben realizar el inventario de activos relacionados al trabajo de cada uno.	Número de activos
Toda la información y los activos asociados con los servicios de procesamiento de información deben ser parte designada de la organización	Marzo de 2017	Los activos de la información deben ser asignados y distribuidos entre los diferentes funcionarios de acuerdo a su importancia.	Número de activos asignados a cada funcionario.
Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.	Mayo del 2017	Crear el reglamento para el buen uso y custodia de la información y activos relacionados.	Número de reglamentos implementados.
Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	Diciembre de 2017	En cada contrato se debe dejar esta cláusula, para que el contratista entregue todo lo relacionado con los activos de la información antes de la liquidación del contrato.	Febrero de 2017
Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	Diciembre de 2017	Al terminar el contrato de cualquier funcionario se debe realizar de inmediato el cambio de contraseñas	Número de contraseñas cambiadas o inhabilitadas
Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	Febrero de 2017	El empleado debe conocer y estar de acuerdo con las condiciones de su contrato laboral antes de firmarlo.	Número de contratos firmados.

Cuadro 16. (Continuación)

Control	Plazo	Acciones	Indicadores de medición
Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	Marzo de 2017	El reglamento del buen uso y custodia de la información debe especificar las sanciones impuestas a las faltas cometidas contra la seguridad de la información.	Número de sanciones impuestas
Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Marzo de 2017	Implementar barreras de seguridad en las oficinas garantizando que solo las personas autorizadas tengan el acceso a ellas y a la información guardada allí.	Seguridad de acceso implementada en las oficinas
Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	Junio de 2017	Activar planes de contingencia mediante el comité de gestión de riesgos para desastres naturales.	Número de planes de contingencia creados.
Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro	Julio de 2017	Dejar en el presupuesto municipal recursos para la compra de estabilizadores	Número de estabilizadores adquiridos.
Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	Abril de 2017	Asegurarse de que no haya anomalías físicas en las oficinas de la Secretaría de Hacienda del municipio.	Número de anomalías solucionadas.
Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso Inadecuado de los activos de la organización	Marzo de 2017	Se deben definir los roles y permisos de cada funcionario.	Permisos asignados a cada funcionario.
Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados	Julio de 2017	Los registros de la información debe estar debidamente custodiada y solo puede tener acceso a ella el personal autorizado.	Número de registros
La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no Autorizada.	Mayo de 2017	Toda la información de acceso público difundida por la organización debe estar en formato que no permita ser modificada ni manipulada por los ciudadanos.	Número de información publicada
información contenida en la mensajería electrónica debe tener la protección adecuada	Marzo de 2017	Sólo la persona autorizada puede tener acceso a los correos electrónicos. -Se debe establecer niveles de seguridad para las contraseñas.	Número de contraseñas

Cuadro 16. (Continuación)

Control	Plazo	Acciones	Indicadores de medición
Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	Mayo de 2017	Se deben restringir permisos a los usuarios	Número de permisos asignados a cada usuario.
Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado	Abril de 2017	Establecer lineamientos para el almacenamiento de la información.	Número de medios de almacenamiento implementados.
La documentación del sistema debe estar protegida contra el acceso no autorizado.	Febrero de 2017	Se debe tener restringido el acceso a la información mediante medidas de seguridad.	Número de controles de seguridad implementados.
Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas	Mayo de 2017	Se debe llevar el registro y seguimiento a las fallas presentadas	Número de seguimientos
Se debe restringir y controlar la asignación y uso de Privilegios.	Febrero de 2017	Definir los permisos de cada usuario	Número de permisos por usuario.
Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de Información	Diciembre de 2017	Deshabilitar acceso a los sistemas de información inmediatamente deje de trabajar en el funcionario en la Entidad.	Número de cuentas inhabilitadas
La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de Acceso de los usuarios	Agosto de 2017	Realizar auditorías internas al manejo de los sistemas de información.	Número de auditorías realizadas.
Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.	Diciembre de 2017	Realizar el SGSI y hacer implementaciones de inducción	Número de inducciones realizadas.
Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	Junio de 2017	Se debe llevar el seguimiento a las acciones realizadas por el personal de soporte	Número de soportes realizados.
Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	Abril de 2017	Se deben establecer buenas prácticas para el uso de dispositivos de almacenamiento de la información.	Número de acciones realizadas.

Cuadro 16. (Continuación)

Control	Plazo	Acciones	Indicadores de medición
Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	Febrero de 2017	Realizar por lo menos dos métodos de autenticación a los sistemas de información.	Número de métodos de autenticación implementados.
Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario	Febrero de 2017	Realizar por lo menos dos métodos de autenticación a los sistemas de información.	Número de métodos de autenticación implementados.
Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio.	Marzo de 2017	Restringir permisos de los usuarios a través de la red local.	Verificación de acceso y de permisos en la red local.
Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas	Febrero de 2017	Realizar inducción de buenas prácticas de la seguridad de la información.	Número de inducciones realizadas.
Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	Febrero de 2016	Restringir la descarga e instalación de programas no autorizados.	Numero de verificaciones realizadas a los computadores.
Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Abril de 2017	Sólo la persona autorizada puede hacer cambios o modificaciones en el sistema.	Número de cambios realizados o negados.
Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	Mayo de 2016	Llevar el registro y seguimiento a las vulnerabilidades detectadas	Número de acciones implementadas.

Fuente: El autor, 2016.

15. CONCLUSIONES, RECOMENDACIONES E IMPLICACIONES

El análisis realizado a la Secretaría de Hacienda permitió tener un diagnostico frente a la implementación de la Norma ISO 27001:2013.

La implementación de controles en la Secretaría de hacienda del municipio de Cucunubá permite mitigar los riesgos a los que puede estar expuesta la información que allí se maneja.

De acuerdo a las encuestas realizadas se concluye que los funcionarios que trabajan inicialmente en esta dependencia no tienen el conocimiento si tienen limitaciones en la navegación, en el almacenamiento de información, o el manejo de los equipos tecnológicos.

La administración municipal de Cucunubá en el ánimo de proteger sus activos de la información inicialmente en la Secretaría de Hacienda se debe implementar políticas de seguridad para lograr mitigar riesgos y amenazas a los cuales se está expuesto cuando no se tienen implementado controles y tampoco se tienen la sensibilización de los funcionarios de la importancia de proteger todos los activos de la información, además que se hace necesario que conozcan y se familiaricen más con la cultura informática y estén en disposición de poder saber qué hacer ante cualquier evento informático que pueden encontrarse en el transcurso de su trabajo.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. Normas. Decreto 103 de 2015. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556, Decreto 103 de 2015.

ALCALDÍA MUNICIPAL DE CUCUNUBÁ. 2016. [en línea], disponible en: http://www.cucunuba-cundinamarca.gov.co/dependencias.shtml

CONGRESO DE COLOMBIA. Ley 734 de 2002 (febrero 5). Código Disciplinario Único, [en línea] [citado julio 10 de 2015] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4589

HASSQL LTDA. Concepto HASSQL. Bogotá, 2015, p.1, [en línea], Bogotá. Disponible en: http://www.hassql.com.co/

HERNÁNDEZ MOLINA, Ignacio, Formulación de proyectos en ciencia e ingeniería, Bogotá D.C. 2012, primera edición.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma Técnica ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de seguridad de la información. Requisitos. Primera edición, Bogotá, D.C. 2013, 27p, [en línea]. Disponible en: http://tienda.icontec.org.

_____. Norma Técnica Colombiana NTC 1486 2008-07-23, Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación, sexta actualización.

INGERTEC, Gap análisis – auditoría inicial ISO 27001 [en línea] [citado mayo 25 de 2016] disponible en: http://ingertec.com/gap-analisis-auditoria-inicial-iso-27001/

MANUAL, estrategia de Gobierno en Línea [en línea] [citado] disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

MINISTERIO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES. Marco de referencia, [en línea] [citado 26 de junio de 2015] disponible en <http://www.mintic.gov.co/marcodereferencia/624/articles-7663_recurso_1.pdf, manual de Gobierno en línea>

MUNICIPIO DE CUCUNUBÁ, Plan de desarrollo Municipal “Cucunubá Compromiso de Todos 2012-2015” Acuerdo No 006 de 2012.

SECRETARIA DE PLANEACIÓN DEPARTAMENTO DE CUNDINAMARCA. Mapa de Cundinamarca. 2016. [en línea] disponible en: http://www.cundinamarca.gov.co

ANEXOS

ANEXO 1. ENCUESTAS REALIZADAS A LOS FUNCIONARIOS DE LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ

ENCUESTA

1. ¿Conoce usted qué es seguridad de la información?
X Si
b. No

2. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?
X Si
b. No
c. Es compartida

3. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?
a. 1
b. 2 o 3
X 3 o 5

4. ¿Cambia periódicamente la contraseña de sus cuentas?
a. Si
X No
c. Rara vez

5. ¿Su equipo cuenta con antivirus licenciado?
a. Si
X No

6. ¿usted tiene restringida algún tipo de página en su computador?
a. Si
X No

7. ¿sabe que es un virus informático?
X Si
b. No

8. ¿Sabe cómo actuar en caso de encontrarse con un antivirus?
9. Si
X No

9. ¿Usted hace copias de seguridad de su información?
X Si
b. No
c. Rara vez

37

10. ¿A su equipo le realizan mantenimiento preventivo?
a. Si
X No
c. Casi nunca

11. ¿su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?
a. Si
b. No
X NO

12. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?
a. Si
X No
c. No conozco restricciones para hacerlo

13. ¿Conoce que son los activos de la información?
X Si
b. No

14. ¿usted guarda información personal (fotos, música, archivos) en los equipos institucionales?
a. Si
X No
c. Rara vez

15. ¿Sabe qué es un delito informático?
X Si
b. No

16. ¿Conoce alguna norma que proteja la seguridad de la información?
a. Si
X No
c. Cual_____

17. ¿usted sabe si en la Entidad existen políticas de seguridad de la información?
a. Si
X No

SANDRA JACQUELINE ANGEL MURCIA
CONTADOR PUBLICO

Encuesta 2

ENCUESTA

1. ¿Conoce usted qué es seguridad de la información?
a. Si
X. No

2. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?
a. Si
b. No
X Es compartida

3. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?
X 1
b. 2 o 3
c. 3 o 5

4. ¿Cambia periódicamente la contraseña de sus cuentas?
a. Si
X No
c. Rara vez

5. ¿Su equipo cuenta con antivirus licenciado?
a. Si
X No

6. ¿usted tiene restringida algún tipo de página en su computador?
X Si
b. No

7. ¿sabe que es un virus informático?
X Si
b. No

8. ¿Sabe cómo actuar en caso de encontrarse con un antivirus?
X Si
10. No

9. ¿Usted hace copias de seguridad de su información?
a. Si
X No
c. Rara vez

37

10. ¿A su equipo le realizan mantenimiento preventivo?
a. Si
X No
c. Casi nunca

11. ¿su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?
a. Si
X No

12. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?
a. Si
X No
c. No conozco restricciones para hacerlo

13. ¿Conoce que son los activos de la información?
a. Si
X No

14. ¿usted guarda información personal (fotos, música, archivos) en los equipos institucionales?
a. Si
b. No
X Rara vez

15. ¿Sabe qué es un delito informático?
X Si
b. No

16. ¿Conoce alguna norma que proteja la seguridad de la información?
a. Si
X No
c. Cual_____

17. ¿usted sabe si en la Entidad existen políticas de seguridad de la información?
a. Si
X No

Encuesta 3

ENCUESTA

1. ¿Conoce usted qué es seguridad de la información?
a. Si
b. No

2. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?
a. Si
b. No
c. Es compartida

3. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?
a. 1
b. 2 o 3
c. 3 o 5

4. ¿Cambia periódicamente la contraseña de sus cuentas?
a. Si
b. No
c. Rara vez

5. ¿Su equipo cuenta con antivirus licenciado?
a. Si
b. No

6. ¿usted tiene restringida algún tipo de página en su computador?
a. Si
b. No

7. ¿sabe que es un virus informático?
a. Si
b. No

8. ¿Sabe cómo actuar en caso de encontrarse con un antivirus?
9. Si
10. No

9. ¿Usted hace copias de seguridad de su información?
a. Si
b. No
c. Rara vez

37

10. ¿A su equipo le realizan mantenimiento preventivo?
a. Si
b. No ✓
c. Casi nunca

11. ¿su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?
a. Si
b. No ✓

12. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?
a. Si
b. No ✓
c. No conozco restricciones para hacerlo

13. ¿Conoce que son los activos de la información?
a. Si
b. No ✓

14. ¿usted guarda información personal (fotos, música, archivos) en los equipos institucionales?
a. Si
b. No ✓
c. Rara vez

15. ¿Sabe qué es un delito informático?
a. Si ✓
b. No

16. ¿Conoce alguna norma que proteja la seguridad de la información?
a. Si
b. No ✓
c. Cual_____

17. ¿usted sabe si en la Entidad existen políticas de seguridad de la información?
a. Si
b. No ✓

Encuesta 4

ENCUESTA

1. ¿Conoce usted qué es seguridad de la información?
a. Si
b. No

2. ¿Sólo usted conoce su contraseña y usuario de acceso al sistema del HAS?
a. Si
b. No
c. Es compartida

3. ¿A cuántos de los módulos del HAS tiene acceso desde su computador?
a. 1
b. 2 o 3
c. 3 o 5

4. ¿Cambia periódicamente la contraseña de sus cuentas?
a. Si
b. No
c. Rara vez

5. ¿Su equipo cuenta con antivirus licenciado?
a. Si
b. No

6. ¿usted tiene restringida algún tipo de página en su computador?
a. Si
b. No

7. ¿sabe que es un virus informático?
a. Si
b. No

8. ¿Sabe cómo actuar en caso de encontrarse con un antivirus?
9. Si
10. No

9. ¿Usted hace copias de seguridad de su información?
a. Si
b. No
c. Rara vez

37

10. ¿A su equipo le realizan mantenimiento preventivo?
a. Si
b. No
c. Casi nunca

11. ¿su oficina cuenta con plan de contingencia de riesgos o desastres (incendio, inundación, alteraciones en el fluido eléctrico)?
a. Si
b. No

12. ¿Usted tiene autorización de instalar aplicaciones, programas o cualquier tipo de software en su equipo?
a. Si
b. No
c. No conozco restricciones para hacerlo

13. ¿Conoce que son los activos de la información?
a. Si
b. No

14. ¿usted guarda información personal (fotos, música, archivos) en los equipos institucionales?
a. Si
b. No
c. Rara vez

15. ¿Sabe qué es un delito informático?
a. Si
b. No

16. ¿Conoce alguna norma que proteja la seguridad de la información?
a. Si
b. No
c. Cual_____

17. ¿usted sabe si en la Entidad existen políticas de seguridad de la información?
a. Si
b. No

4

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ CUNDINAMARCA BAJO LA NORMA ISO 27001:2013

Luz Dary Acosta Contreras,
daryacost@yahoo.es
Universidad piloto de Colombia

RESUMEN: Con la realización del presente proyecto se tiene como finalidad identificar las amenazas y riesgos a los que puede estar expuesta la alcaldía municipal de Cucunubá en el área de la Secretaría de Hacienda donde se manejan los recursos y presupuesto del municipio, razón por la cual se deben implementar las medidas para salvaguardar la información y de esta forma evitar que personas mal intencionadas puedan acceder a ella con fines fraudulentos o intereses de terceros, ocasionando inconvenientes para el buen funcionamiento de la entidad, el objetivo es hacer la implementación de controles regidos bajo la Norma ISO 27001 de 2013 y establecer así las políticas de seguridad de la información para mitigar los posibles riesgos que se identifiquen.

Abstract— The purpose of this project is to identify the threats and risks to which the municipality of Cucunubá may be exposed in the area of the Ministry of Finance where the resources and budget of the municipality are handled. Implement the measures to safeguard the information and thus prevent malicious persons from accessing it for fraudulent purposes or interests of third parties, causing inconvenience to the proper functioning of the entity, the objective is to implement the controls governed by the Standard ISO 27001 of 2013 and thus establish the information security policies to mitigate the possible risks that are identified.

Index Terms— activo, amenaza, impacto, información, control, riesgo, seguridad, vulnerabilidad, probabilidad.

1. INTRODUCTION

En la actualidad la seguridad de la información se ha convertido en uno de los activos más importantes para las organizaciones, lo cual hace que ellas trabajen todos los días en busca de estrategias para asegurar la integridad, confidencialidad y disponibilidad de la misma. Las entidades públicas deben empezar a pensar en implementar políticas de seguridad para evitar que intrusos o personas malintencionadas exploten posibles vulnerabilidades, por medio de las cuales puedan llegar a ocasionar daños o pérdidas económicas y/o materiales a los activos de información físicos y lógicos de la entidad.

En esta propuesta se realizará el diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013, construyendo, inicialmente el

inventario de la información que se maneja en la Secretaría de Hacienda (dependencia en la cual se va a desarrollar la propuesta) de la alcaldía de Cucunubá, para identificar vulnerabilidades y aplicar los controles para evitar que estas se materialicen

2. MARCO LEGAL

Hoy en día las organizaciones deben funcionar en línea con la normatividad existente y estar a su vez, a la vanguardia con las actualizaciones de las mismas, por consiguiente es importante nombrar en este trabajo alguna normatividad que se debe tener en cuenta al momento del diseño de un Sistema de Gestión de la información.

ISO 27001-2013: "Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza" .

MANUAL ESTRATEGIA DE GOBIERNO EN LINEA: esta estrategia comprende cuatro propósitos (TIC para gobierno abierto, TIC para servicio, TIC para gestión, seguridad y privacidad de la información), para que los servicios que brindan las entidades territoriales sea de mayor calidad y mas óptimos, para lo cual se incorporaron tres herramientas transversales en busca de la confianza de los ciudadanos del servicio en línea que ofrecen las entidades

DECRETO 2573 DEL 12 DE DICIEMBRE DE 2012: por medio de la cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

"…Que así mismo, la anotada Ley determinó que es función del Estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector…"

DECRETO 103 DE 2015: Define el Registro de Activos de Información como "el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal".

ACUERDO Nº 002 DE 2016: Por medio del cual se adopta el Plan de Desarrollo Municipal "Cucunubá productiva y social". En el eje institucional, dentro del sector de fortalecimiento institucional en su componente estratégico tiene la siguiente meta de producto: "Implementar anualmente la Estrategia Municipal Gobierno en línea durante el periodo de gobierno. ODS 16

3. MARCO TEÓRICO

GENERALIDADES: El municipio de Cucunubá se encuentra ubicado en Colombia, Departamento de Cundinamarca, provincia de Ubaté a 2950 m.s.n.m. como se muestra en la figura 1. Con temperatura promedio de 14°, es un municipio de sexta categoría con 7.300 habitantes según base de datos del Sisbén Año 2014 y maneja un presupuesto anual aproximado a $5.496'491.234.

La presente propuesta se va a ejecutar en la Secretaría de Hacienda partiendo de que es una de las cinco dependencias que conforman la Administración Municipal como se puede ver en la figura 3; quién es la encargada de manejar y administrar los recursos y presupuesto del municipio, por consiguiente, está más expuesta a ataques por personas inescrupulosas si no se detectan las vulnerabilidades y son controladas justo a tiempo:

4. SOFTWARE SECRETARÍA DE HACIENDA

Cuadro 1. Software secretaría de hacienda

Ítem	Descripción	Módulo
1	SQL HAS	Contabilidad
2	SQL HAS	Industria y comercio
3	SQL HAS	Almacén
4	SQL HAS	Nomina
5	SQL HAS	Presupuesto
6	SQL HAS	Impuesto predial

Fuente: el autor, 2016

En el cuadro 1 se muestra los módulos contables que tiene implementados la Secretaría de Hacienda de Cucunubá.

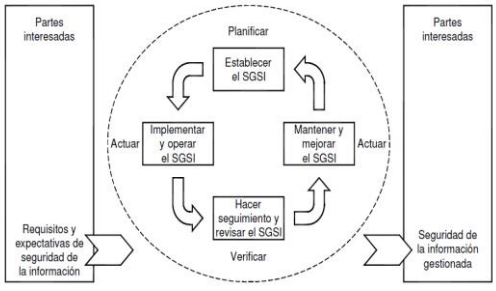
5. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC-27001

NTC-ISO/IEC 27001 es una norma internacional las cual establece controles que permiten "brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), este diseño está influenciado por las necesidades, objetivos, requisitos de seguridad, procesos empleados, tamaño y estructura de la Organización

6. MODELO PHVA, NORMA TÉCNICA-COLOMBIANA NTC-ISO/IEC 27001:2013

Este modelo se aplica para estructurar los procesos del Sistema de Gestión de Seguridad de la Información como se ilustra en la figura 1 y por medio de la cual se pretende cumplir con los requisitos de seguridad de la Información.

Figura 1. Modelo PHVA



Fuente: Tomada de la Norma NTC-ISO-IEC 27001:2013

A. Planificar. En esta parte se establecen los objetivos a los que se quiere llegar con el diseño del SGSI, a su vez identificar el inventario de los activos de la información implicados para su alcance, aplicando controles a cada uno de los riesgos encontrados durante la formulación del SGSI.

B. Hacer. Para la mitigación de los riesgos identificados se deben implementar los controles de acuerdo a la Norma ISO-IEC-27001:2013

C. Verificar. Monitoreo de los controles implementados y análisis de sus resultados.

D. Actuar. De acuerdo a los resultados obtenidos en la verificación se toman las respectivas medidas para mejorar o retroalimentar la implementación de los controles, además se debe dejar todo hallazgo documentado

7. ESTADO ACTUAL DE LA SECRETARÍA DE HACIENDA FRENTE A LA NORMA ISO-IEC-27001:2013

La Secretaría de Hacienda del municipio de Cucunubá, para el ejercicio de su buen funcionamiento y desempeño adquirió la licencia del software del sistema administrativo y financiero desarrollado por SQL HAS, para administrar los recursos del municipio, comprando los módulos de: presupuesto, contabilidad, almacén, nómina, industria y comercio e impuesto predial, con sus requerimientos generales y específicos de los Entes de Control y de la Entidad. Cuenta con seis estaciones de trabajo ubicadas en tres oficinas en las instalaciones del palacio municipal, por consiguiente cuenta con seis usuarios que no tienen definidos ni establecidos los permisos y tampoco la concientización de la importancia y responsabilidad que cada uno asume al momento de manipular alguno de estos equipos, prestándose esto para evadir posibles responsabilidades, de esta forma, tampoco se tiene las medidas necesarias dentro de las oficinas para proteger la información que se maneja ya sea en medio magnético, físico o desde el hecho de crear contraseñas, no se hace con los respectivos niveles de seguridad.

El análisis GAP es un paso muy importante en la implementación de la Norma ISO 27001 ya que por medio de él se pueden identificar las amenazas que exponen la confidencialidad, integridad y disponibilidad de la información, por consiguiente se evalúan los controles que se

están implementando en la empresa y se diagnostica su estado actual frente a la seguridad como se muestra en la figura 2.

Figura 2. Análisis matriz GAP

Fuente: NTC-ISO-IEC 27001:2013

La figura anterior lleva a tener el siguiente diagnostico en cuanto al cumplimiento de controles de seguridad de la información en la Secretaría de Hacienda del Municipio de Cucunubá:

Cuadro 2. Cumplimiento de controles en la entidad

Nombre dominios de control	**Controles que aplican**	**Implementados**	**Parcialmente**	**No cumple**	**No aplica**
Dominio 5 - políticas de seguridad de la información	2	0	0	2	0
Dominio 6 - organización de la seguridad de la información	7	0	4	3	0
Dominio 7 - seguridad de los recursos humanos	6	0	5	1	0
Dominio 8 - gestión de activos	10	1	4	5	0
Dominio 9 - control de acceso	13	2	6	5	1
Dominio 10 - criptografía	2	0	0	2	0
Dominio 11 - seguridad física y del entorno	15	2	9	4	0
Dominio 12 - seguridad de las operaciones	13	0	3	10	1
Dominio 13 - seguridad de las comunicaciones	7	0	2	5	0
Dominio 14 - adquisición, desarrollo y mantenimiento de sistemas	7	0	0	7	6
Dominio 15 - relación con los proveedores	5	0	0	5	0
Dominio 16 - gestión de incidentes de seguridad de la información	7	0	0	7	0
Dominio 17 - aspectos de seguridad de la información de la gestion de continuidad de negocio	4	0	1	3	0
Dominio 18 - seguridad de las comunicaciones	7	0	3	4	1
	105				

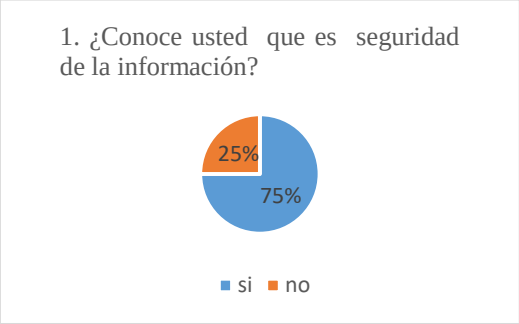
Fuente: NTC-ISO-IEC 27001:2013

En lo cual se puede determinar que de los 114 controles que propone la Norma ISO 27001:2013, para la Entidad solo aplican 105, implementados 5, implementados parcialmente 37, no se cumplen 63 y no aplican 9.

8. METODOLOGÍA

El instrumento que se utilizó para determinar el conocimiento de los funcionarios frente a la seguridad de la información de la secretaría de hacienda del municipio de Cucunubá, fue una encuesta cerrada de 17 preguntas aplicada a 4 funcionarios de cinco que laboran en la dependencia de hacienda, aplicando a cada una de las preguntas el análisis como muestra la figura 3.

Figura 3. ¿Conoce usted que es seguridad de la información?



Fuente: el autor

Una vez realizado este diagnóstico mediante la encuesta se llega a obtener los resultados de la figura 4.

Figura 4. Resultados de las encuestas.

Fuente: el autor, 2016

Este resultado lleva a concluir que de 1700 puntos posibles alcanzados en la encuesta, sólo 200 puntos son favorables para respuestas acerca del conocimiento que tienen sobre la seguridad de la información; mientras que las respuestas negativas alcanzan 1400 puntos; para otra respuesta se llegó 100 puntos.

9. VALORACION DE RIESGOS

En el siguiente cuadro se realiza un análisis y valoración de los riesgos., teniendo en cuenta que **riesgo = probabilidad * impacto; donde:**

La probabilidad puede ser: raro – posible - probable

El impacto puede ser: menor – moderado – mayor

Cuadro 3. Valoración de riesgos

ANALISIS DE RIESGOS			
MAYOR (3)	3	6	9
MODERADO (2)	2	4	6
MENOR (1)	1	2	3
	RARO (1)	POSIBLE (2)	PROBABLE (3)

Fuente: el autor

10. IDENTIFICACIÓN DE LOS RIESGOS

Una vez identificados los activos de la información de la Secretaría de Hacienda de la Alcaldía municipal de Cucunubá, se identifican los riesgos, amenazas, vulnerabilidades e impactos de cada uno que puedan llegar a afectar su integridad confidencialidad y disponibilidad de la información a los cuales se les da un valoración de acuerdo a la matriz de riesgo expuesta anteriormente y la cual define que: riesgo=impacto x probabilidad, se define el mapa de riesgos identificados en la Secretaría de Hacienda del municipio de Cucunubá

Cuadro 3. Mapa de riesgos

Análisis de riesgos			
Mayor (3)	3 **R22, R23, R25, R26, R30, R32, R33**	6 **R20, R21, R29**	9 **R6, R7, R10, R14**
Moderado (2)	2 **R24**	4 **R1, R5, R8, R11, R15, R31**	6 **R2, R4, R9, R12. R13, R16,**
Menor (1)	1 **R17, R27, R28**	2 **R3**	3 **R18, R19,**
	Raro (1)	Posible (2)	Probable (3)

Fuente: el autor

11. APLICACIÓN DE CONTROLES A LOS RIESGOS IDENTIFICADOS

Partiendo de la Norma NTC-ISO/IEC 27001 en la cual especifica los requisitos para la implementación de controles de seguridad adaptados de acuerdo a las necesidades de la organización. En este caso a la Secretaría de Hacienda del municipio de Cucunubá; se diseña el Sistema de Gestión de Seguridad de la Información para que los controles implementados que se aplican, sean los necesarios para proteger los activos de la información de la Entidad.

12. PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA SECRETARÍA DE HACIENDA DEL MUNICIPIO DE CUCUNUBÁ – CUNDINAMARCA

12.1 políticas de seguridad de la información

Objetivo: definir lineamientos que lleven a mantener la protección de los activos de la información de la Secretaría de Hacienda del municipio de Cucunubá – Cundinamarca.

Resumen: Estas políticas se aplican al recurso humano de la Secretaría de Hacienda del Municipio de Cucunubá.

Se debe establecer la política de seguridad de la Información para la Secretaría de Hacienda del municipio de Cucunubá.

Se debe socializar la política diseñada con el funcionario directamente afectado en la protección de la información.

Capacitar a los funcionarios de la dependencia en cultura informática para que puedan saber qué hacer en caso de que se les presente una eventualidad en el transcurso de sus labores diarias.

Diseñar e implementar un programa de auditorías periódicas por parte de la oficina de control interno para verificar la información, programas o aplicativos que maneja cada usuario en su equipo.

Implementar un área responsable de informática y seguridad de la información quien sea el encargado de aprobar cualquier instalación de software o aplicaciones en los equipos de la dependencia.

Para mejorar la seguridad se debe implementar un firewall para la seguridad perimetral en la conexión a internet.

Las conexiones remotas realizadas al sistema deben llevar un registro.

El secretario de Hacienda debe velar porque se estén aplicando las políticas de seguridad de la información dentro de su dependencia.

La transferencia de archivos se debe realizar implementando protocolos seguros.

12.2 Acuerdos de confidencialidad

•Todos los contratos laborales realizados por parte de la Secretaría de Hacienda deben tener acuerdos de confidencialidad para proteger la información.
•Cuando se realiza contratos a prestadores de servicios deben tener una cláusula de confidencialidad.
•Todos los funcionarios que trabajen en la Secretaría de Hacienda deben firmar un acuerdo de confidencialidad antes de iniciar a tener acceso a ella.

12.3 Acceso a internet

•Bloquear todas las páginas de redes sociales.
•Bloquear programas no autorizados de descargas no autorizadas.
•Prohibir en ingreso a páginas que atenten contra la ética y la normatividad vigente.
•Restringir el acceso a la mensajería instantánea para evitar la transferencia de archivos maliciosos.
•No permitir la instalación de o descarga de archivos o programas no autorizados en los equipos.
•Realizar actividades de inspección de navegación de cada funcionario.

12.4 Uso adecuado de los activos de la información

•Tener clasificada la información para controlar el acceso a ella por parte de los usuarios y / o funcionarios.
•Implementar por parte de la oficina de Control interno auditorías internas para hacer

seguimiento al cumplimiento de las políticas establecidas.

12.5 Correo electrónico

•Correo electrónico que se maneja en la Secretaría de Hacienda del municipio de Cucunubá es institucional y su uso debe ser exclusivo para las funciones relacionadas con esta dependencia.

•El correo institucional solo de debe utilizar para asuntos de la secretaría de hacienda y no para envío y recepción de información de carácter personal de algún funcionario.
•No acceder al correo electrónico institucional desde equipos y conexiones públicas que sean inseguras.
•No dejar sesión abierta en los computadores o teléfonos móviles.
•Prohibir el envío de mensajes que contengan código malicioso o con algún interés personal que atenten contra la integridad y el buen nombre de la Entidad.
•El correo electrónico institucional no se debe manejar de ninguna manera de forma personal.
•Se debe realizarle cambio periódico de contraseña.
•Se debe tener solo una persona responsable del correo electrónico.

12.6 Recursos tecnológicos

•Cualquier tipo de instalación que se necesite hacer, lo debe hacer solo la persona autorizada y en efecto supervisado por la persona encargada de la seguridad de la información.
•La configuración de los equipos solo la debe hacer el responsable del área de informática.
•El soporte al sistema de información sólo podrán realizarlos los ingenieros de soporte autorizados por el proveedor, el responsable de la seguridad de la Alcaldía debe llevar el control de todas las actividades realizadas durante los procesos de soporte.
•Se deben implementar antivirus y software licenciado y mantenerlos siempre actualizados.
•Sólo los equipos autorizados podrán ser registrados ante el proveedor de internet para poderse conectar a internet.
•Se debe desactivar los equipos de la red de internet de los funcionarios que dejen de trabajar en la dependencia de Hacienda.
•Solo las personas autorizadas podrán hacer conexiones remotas.

12.7 Control de acceso físico.

•Teniendo en cuenta que son oficinas a las que ingresan usuarios no se deben dejar solas en ningún momento o si es el caso cerrarla.

12.8 Gestión de contraseñas

•Se deben cambiar las contraseñas con periodicidad manteniendo un nivel alto de seguridad, es decir combinar números, mayúsculas y minúsculas.
•Las contraseñas deben ser combinaciones alfanuméricas y no utilizar nombres de familiares ni fechas de acontecimientos.
•No se deben dejar las contraseñas escritas en fechas visibles o revelarlas a otras personas.
•La contraseña de cada aplicativo o sistema de información él debe manejar y saber solo la persona responsable del mismo.

12.9 Protección de los equipos.

•Se debe mantener la infraestructura de las oficinas en óptimo estado, como puertas, ventanas, paredes y tejados.
•Se debe tener una oficina solo para atención a los usuarios por parte de la Secretaría de Hacienda para que no tengas ningún tipo de acceso o contacto con información privilegiada que se maneje en la oficina.
•Se beben implementar las normas y equipos de emergencia para estar preparados contra eventos externos, internos y ambientales, ya sean incendios, inundaciones, explosiones, manifestaciones sociales o cualquier otro desastre.
•Controlar el acceso de personal no autorizado a las oficinas y mantenerlos aislados de los servicios de procesamiento de información.
•Implementar UPS y estabilizadores en todos los equipos de cómputo teniendo en cuenta que el municipio se presenta continuas fallas en el suministro de energía.
•Se debe realizar el mantenimiento preventivo de hardware y software de los equipos para garantizar la integridad y buen funcionamiento de los mismos.
•Se debe contar con autorización para poder sacar un equipo de la entidad y llevarle una hoja de actividades, así mismo responsabilizarse de la información que allí se encuentre almacenada.
•No se puede realizar eliminación, cambio, modificación de software sin una autorización previa.

12.10 Copias de seguridad.

•Se deben implementar la cultura de hacer por lo menos dos copias de la información periódicamente y almacenarlas en dos medios diferentes y lugares diferentes.
•Los medios donde se guarde la información deben garantizar los controles de seguridad de la misma y ninguna persona diferente puede tener acceso a la misma.

12.11 Cultura de escritorios y pantallas limpias

•Todos los equipos deben tener contraseñas seguras.
•Los escritorios de los computadores deben estar libres de carpetas y documentos.
•No se debe dejar documentos o medios de almacenamiento sobre el escritorio.
•No dejar claves anotadas en lugares visibles.
•Mantener con seguro los cajones de escritorios.
•No permitir el acceso de otras personas a los sistemas de información.

12.12 Uso de dispositivos móviles

•Tener contraseña para el ingreso al teléfono móvil y a todas sus aplicaciones.
•No prestar el teléfono a personas externas a la dependencia.

12.13 Recursos humanos

•Socializar e implementar la política de seguridad de la información con todos los funcionarios de la dependencia.
•Tener el compromiso de la alta dirección para apoyar activamente el cumplimiento de las políticas de seguridad.
•Asignar responsabilidades para el cumplimiento de las políticas de seguridad de la información.
•Llevar un seguimiento a las cláusulas de confidencialidad de los contratos de los funcionarios de la dependencia.
•Deben asignarse el responsable de los activos de la información.
•Se debe realizar una revisión de antecedentes de los funcionarios de la dependencia y clasificar la información que se va a disponer como responsabilidad de cada uno.
•Deshabilitar permisos y roles cuando se terminen contratos laborales.
•Una vez se termine un contrato el funcionario debe hacer devolución de los equipos o información que se encontraba a su cargo.

12.14 políticas de software

Se deben implementar controles de prevención y detección de código malicioso.

12.15 Uso de token

•El token debe permanecer bajo llave y solo puede tener a él el jefe de dependencia.
•No dejar el toquen sobre el escritorio.
•En caso de portar el token fuera de la Secretaría garantizar su seguridad e integridad.
•El administrador del token debe ser el mismo responsable del portal o sitio a utilizar este dispositivo.

12.16 Equipos institucionales

•No se deben conectar dispositivos personales o de terceros en los equipos institucionales.
•Evitar guardar información personal en los computadores, toda vez que todo lo que allí se guarde será sujeto a revisión por parte de auditorías internas.
•La entidad no responde por información personal guardada en los equipos institucionales.
•Establecer lineamientos para no utilizar medios de almacenamiento persona.

CONCLUSIONES, RECOMENDACIONES E IMPLICACIONES

El análisis realizado a la Secretaría de Hacienda permitió tener un diagnostico frente a la implementación de la Norma ISO 27001:2013.

La implementación de controles en la Secretaría de hacienda del municipio de Cucunubá permite mitigar los riesgos a los que puede estar expuesta la información que allí se maneja.

De acuerdo a las encuestas realizadas se concluye que los funcionarios que trabajan inicialmente en esta dependencia no tienen el conocimiento si tienen limitaciones en la

navegación, en el almacenamiento de información, o el manejo de los equipos tecnológicos.

La administración municipal de Cucunubá en el ánimo de proteger sus activos de la información inicialmente en la Secretaría de Hacienda se debe implementar políticas de seguridad para lograr mitigar riesgos y amenazas a los cuales se está expuesto cuando no se tienen implementado controles y tampoco se tienen la sensibilización de los funcionarios de la importancia de proteger todos los activos de la información, además que se hace necesario que conozcan y se familiaricen más con la cultura informática y estén en disposición de poder saber qué hacer ante cualquier evento informático que pueden encontrarse en el transcurso de su trabajo.

REFERENCES

COLOMBIA. Ministerio de la tecnología de la información y las comunicaciones [en línea] [citado 26 de junio de 2015] disponible en <http://www.mintic.gov.co/marcodereferencia/624/articles-7663_recurso_1.pdf, manual de Gobierno en línea>

COLOMBIA. Congreso de Colombia. Ley 734 de 2002 [en línea] [citado julio 1º0 de 2015] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4589

HERNANDEZ MOLINA, Ignacio, Formulación de proyectos en ciencia e ingeniería, Bogotá D.C. 2012, primera edición.

Icontec internacional, NORMA TECNICA NTC-ISO-IEC-COLOMBIANA 27001 2013-12-11. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Primera edición Bogotá D.C. [en línea] disponible en: http://tienda.icontec.org/brief/NTC-ISO-IEC27001.pdf.

Icontec, NORMA TÉCNICA COLOMBIANA NTC 1486 2008-07-23, Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación, sexta actualización.

INGERTEC, Gap análisis – auditoría inicial ISO 27001 [en línea] [citado mayo 25 de 2016] disponible en: http://ingertec.com/gap-analisis-auditoria-inicial-iso-27001/

MANUAL, estrategia de Gobierno en Línea [en línea] [citado] disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

MUNICIPIO DE CUCUNUBÁ, Plan de desarrollo Municipal “Cucunubá Compromiso de Todos 2012-2015” Acuerdo No 006 de 2012.

Luz Dary Acosta Contreras (1989 - 2015) lugar de nacimiento Ubaté – Cundinamarca., vive actualmente en el municipio de Cucunubá – Cundinamarca, egresada de la universidad de Cundinamarca seccional Ubaté del programa de ingeniería de Sistemas en el año 2012, actualmente trabaja en la Alcaldía municipal de Cucunubá y adelanta estudios en la especialización de Seguridad informática en la universidad Piloto de Colombia.