	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Documento F-AC-DBL-007	Código 10-04-2012	Fecha A
DIVISIÓN DE BIBLIOTECA	Dependencia	Aprobado SUBDIRECTOR ACADEMICO	Pág. 1(162)	

RESUMEN – TRABAJO DE GRADO

AUTORES	JHON ALEXANDER ALVAREZ BAYONA
FACULTAD	FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS	PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
DIRECTOR	Ing. MAGRETH ROSSIO SANGUINO REYES
TÍTULO DE LA TESIS	EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE SANTANDER

RESUMEN

(70 palabras aproximadamente)

EN LA ACTUALIDAD LAS EMPRESAS HAN EXPERIMENTADO TRANSFORMACIÓN EN ALGUNOS ASPECTOS DE SEGURIDAD; LA SITUACIÓN ACTUAL NOS DA A CONOCER QUE TANTO LOS SISTEMAS DE INFORMACIÓN, COMO TAMBIÉN LA MISMA INFORMACIÓN SON EL ACTIVO MÁS VALIOSO Y AL MISMO TIEMPO EL MÁS VULNERABLE. LA SEGURIDAD INFORMÁTICA HA ADQUIRIDO GRAN AUJE, DADA LAS CAMBIANTES CONDICIONES Y NUEVAS PLATAFORMAS DE COMPUTACIÓN DISPONIBLES, SITUACIÓN QUE CONVERGE EN LA APARICIÓN DE NUEVAS AMENAZAS EN LOS SISTEMAS INFORMÁTICOS.

CARACTERÍSTICAS

PÁGINAS: 162	PLANOS:	ILUSTRACIONES:	CD-ROM: 1
---------------------	----------------	-----------------------	------------------



VÍA ACOLSURE, SEDE EL ALGODONAL, OCAÑA N. DE S.
 Línea Gratuita Nacional 018000 121022 / PBX: 097-5690088
www.ufpso.edu.co



**EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE
SANTANDER**

JHON ALEXANDER ALVAREZ BAYONA

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014**

**EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE
SANTANDER**

JHON ALEXANDER ALVAREZ BAYONA

Proyecto presentado como requisito para optar el título de Ingeniero de Sistemas

Director
Ing. MAGRETH ROSSIO SANGUINO REYES
Especialista en Informática Educativa

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014

CONTENIDO

	Pág.
<u>INTRODUCCIÓN</u>	12
<u>1. EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE SANTANDER</u>	13
<u>1.1 PLANTEAMIENTO DEL PROBLEMA</u>	13
<u>1.2 FORMULACIÓN DEL PROBLEMA</u>	13
<u>1.3 OBJETIVOS</u>	13
1.3.1 Objetivo General	14
1.3.2 Objetivos Específicos	14
<u>1.4 JUSTIFICACIÓN</u>	14
<u>1.5 DELIMITACIONES</u>	15
1.5.1 Geográfica	15
1.5.2 Conceptual	15
1.5.3 Operativa	15
1.5.4 Conceptual	15
<u>2. MARCO REFERENCIAL</u>	16
<u>2.1 MARCO HISTÓRICO</u>	16
2.1.1 Historia de la auditoría	16
2.1.2 Historia de la auditoría de los sistemas de información	18
2.1.3 Historia de la información	19
<u>2.2 MARCO CONCEPTUAL</u>	21
2.2.1 Auditoría	21
2.2.2 Auditoría de Sistemas	21
2.2.3 Sistemas de información	21
2.2.4 Seguridad física	22
2.2.5 Seguridad lógica	23
2.2.6 Seguridad de la información	23
2.2.7 Controles	23
2.2.7.1 Clasificación de los controles	23
2.2.7.1.1 Controles preventivos	23
2.2.7.1.2 Controles detectivos	24
2.2.7.1.3 Controles correctivos	24
2.2.7.1.4 Controles físicos	24
2.2.7.1.5 Controles lógicos	24
2.2.8. Norma ISO/IEC 27001:2005	24
<u>2.3 MARCO TEÓRICO</u>	25
<u>2.4 MARCO LEGAL</u>	27
2.4.1 Congreso de la República (Ley 1273 DE 2009)	27

2.4.1.1 Artículo 269A: Acceso abusivo a un sistema informático	27
2.4.1.2. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación	28
2.4.1.3 Artículo 269C: Interceptación de datos informáticos	28
2.4.1.4 Artículo 269D: Daño Informático	28
2.4.1.5. Artículo 269F: Violación de datos personales	28
2.4.2 Ley organica de proteccion de datos	28
2.4.2.1 Artículo 4. Calidad de los datos	28
2.4.2.2 Artículo 5. Derecho de información en la recogida de datos	29
2.4.2.3 Artículo 6. Consentimiento del afectado	30
2.4.2.4 Artículo 7. Datos especialmente protegidos	31
2.4.2.5 Artículo 8. Datos relativos a la salud	32
2.4.2.6 Artículo 9. Seguridad de los datos	32
2.4.2.7 Artículo 10. Deber de secreto	32
2.4.2.8 Artículo 11. Comunicación de datos	33
2.4.2.9 Artículo 12. Acceso a los datos por cuenta de terceros	34
<u>3. DISEÑO METODOLÓGICO</u>	35
<u>3.1 TIPO DE INVESTIGACIÓN.</u>	35
<u>3.2 POBLACIÓN Y MUESTRA</u>	35
3.2.1 POBLACIÓN	35
3.2.2 MUESTRA	35
<u>3.3 TÉCNICA E INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN</u>	35
<u>4. PRESENTACIÓN DE RESULTADOS</u>	36
<u>4.1. GENERALIDADES</u>	36
<u>4.2. ASPECTOS GENERALES DE LA EMPRESA AUDITADA</u>	36
<u>4.3. ALCANCES DE LA AUDITORÍA.</u>	42
<u>4.4. RESTRICCIONES DE LA EVALUACIÓN</u>	44
<u>4.5. RESULTADOS DE LA AUDITORÍA</u>	45
4.5.1. Conclusiones	45
4.5.2. Recomendaciones	45
<u>4.6. INFORME FINAL DE AUDITORÍA</u>	46
4.6.1. Objetivos	46
4.6.2. Alcances	46
4.6.3. Tiempo	46
4.6.4. Recursos	46
4.6.5. Actividades de la auditoría	47
4.6.5.1. Recolección de información primaria	47
4.6.5.2. Diseño de papeles de trabajo	47
4.6.5.3. Análisis de resultados obtenidos	48
4.6.5.4. Análisis de riesgos	50
<u>4.7. DIAGNÓSTICO</u>	58

<u>CONCLUSIONES</u>	71
<u>RECOMENDACIONES</u>	72
<u>BIBLIOGRAFÍA</u>	73
<u>REFERENCIAS DOCUMENTALES ELECTRÓNICAS</u>	74
<u>ANEXOS</u>	75

LISTA DE CUADROS

	Pág.
Cuadro 1. Mapa cronológico donde se reseñe la historia y evolución de la auditoría.	16
Cuadro 2. Responsables en la entrega de información de la Alcaldía Municipal de Ábrego.	47
Cuadro 3. Elementos de información.	50
Cuadro 4. Categorización para valorar la magnitud del daño.	51
Cuadro 5. Valoración de la magnitud del daño de los activos de información.	51
Cuadro 6. Rango de valoración para la probabilidad de amenaza.	52
Cuadro 7. Grupos de Amenazas o Ataques.	52
Cuadro 8. Categorización para valorar la magnitud del daño.	53
Cuadro 9. Elementos de información.	54
Cuadro 10. Nivel de Riesgo.	55
Cuadro No.11. Equipo No. 1: Oficina De Planeación Y Obras Civiles	64
Cuadro No.12. Equipo No.2: Oficina De Planeación Y Obras Civiles.	65
Cuadro No.13: Equipo Oficina Sisben.	66
Cuadro No.14. Equipo No.1: Oficina Secretaria De Gobierno.	66
Cuadro No.15. Equipo No.2: Oficina Secretaria De Gobierno.	67
Cuadro No.16. Equipo oficina unidad de servicios públicos.	67
Cuadro No.17. Equipo oficina almacén.	68
Cuadro No.18. Equipo No.1: Oficina Tesorería.	69
Cuadro No.19. Equipo No.2: Oficina Tesorería.	69
Cuadro No.20. Especificaciones equipos de cómputo	69

LISTAS DE ANEXOS

Anexo 1. Entrevista Alcalde o Secretaria de Gobierno (ENT01).	76
Anexo 2. Solicitud documentación institucional (SDI01).	45
Anexo 3. Plan de auditoría (PLA01).	79
Anexo 4. Programa de Auditoría (PRA01).	82
Anexo 5. Guías de auditoría (GUA01-GUA02-GUA03-GUA04-GUA05).	84
Anexo 6. Evaluación a la seguridad física en las áreas seguras (ESF01).	91
Anexo 7. Checklist binaria para la evaluación a la seguridad física en las áreas seguras (CHL01).	92
Anexo 8. Archivo fotográfico N° 1. (AF001).	94
Anexo 9. Entrevista para verificar la existencia de controles de protección de los equipos fuera de las instalaciones (ESE06).	95
Anexo 10. Evaluación a la seguridad física en los controles de protección contra amenazas externas e internas (ESF02).	97
Anexo 11. CheckList binario para la evaluación a la seguridad física a los controles de protección contra amenazas externas e internas (CHL02).	99
Anexo 12. Archivo fotográfico N° 8. (AF008).	101
Anexo 13. Archivo fotográfico N° 6 (AF006).	102
Anexo 14. Archivo Fotográfico N° 4 (AF004).	103
Anexo 15. Archivo Fotográfico N° 2 (AF002).	104
Anexo 16. Formato de verificación seguridad física respecto a los controles para la protección de los equipos contra amenazas externas e internas (FVE02).	105
Anexo 17. Archivo fotográfico N° 3 (AF003).	113
Anexo 18. Archivo fotográfico N° 10 (AF010).	114
Anexo 19. Archivo fotográfico N° 11 (AF011).	115
Anexo 20. Evaluación a la seguridad lógica (ESL03).	116
Anexo 21. CheckList binario para la evaluación a la seguridad lógica (CHL03).	118
Anexo 22. Archivo fotográfico N° 7 (AF007).	120
Anexo 23. Archivo de imágenes N° 3 (AIM03).	121
Anexo 24. Archivo de imágenes N° 5 (AIM05).	122
Anexo 25. Archivo de imágenes No 5 (AIM05).	123
Anexo 26. Formato de verificación seguridad lógica (FVE03).	124
Anexo 27. Evaluación al servicio de mantenimiento de equipos (EME04).	128
Anexo 28. CheckList al servicio de mantenimiento de equipos (CHL04).	130
Anexo 29. Evaluación a la red de datos (ERD05).	132
Anexo 30. CheckList para evaluar la red de datos (CHL05).	134
Anexo 31. Encuesta para verificar la protección de los equipos fuera de las instalaciones (ENC01).	137
Anexo 32. Archivo de imágenes N° 4. (AIM04).	139
Anexo 33. Archivo de imágenes No. 2 (AIM02).	140
Anexo 34. Hallazgos seguridad física (HAZ01).	141
Anexo 35. Hallazgos seguridad lógica (HAZ02).	144
Anexo 36. Hallazgos red de datos (HZA03).	147
Anexo 37. Prueba sustantiva N° 1 (PSU01).	150

Anexo 38. Prueba sustantiva N° 2 (PSU02).	152
Anexo 39. Prueba sustantiva N° 3. (PSU03).	154
Anexo 40. Prueba sustantiva N° 4 (PSU04).	156
Anexo 41. Prueba sustantiva N° 5 (PSU05).	158
Anexo 42. Prueba sustantiva No. 6 (PSU06).	161

INTRODUCCIÓN

En la actualidad, el auge en los avances de la tecnología ha hecho que los procesos en las organizaciones sean considerablemente más fáciles que hace un siglo, pero a medida que la tecnología nos facilita nuestras labores diarias, aumenta la tendencia de ataques informáticos que afectan a diversos sectores como a personas particulares o a organizaciones públicas o privadas causando quebrantos en sus sistemas. Por tal motivo, las empresas han optado por implementar mecanismos de seguridad para salvaguardar sus sistemas de información con el objetivo de que no estén en el blanco de ataques informáticos que diariamente se estén presentando en las organizaciones, cuyo único objetivo es causar daño o alterar de manera significativa la información presente en dichas organizaciones.

Las organizaciones tienen presente que los sistemas de información constantemente sufren ataques informáticos y esto conlleva a que estén en constante riesgo ya que la información al ser el activo más importante en las organizaciones pueda ser seriamente afectado. Por todo esto es indiscutible concientizar a las organizaciones de la protección que se debe hacer a la información, con el objetivo de poder minimizar en gran parte los riesgos y asegurar la continuidad de las organizaciones.

1. EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE SANTANDER

1.1. PLANTEAMIENTO DEL PROBLEMA

El desarrollo tecnológico ha provocado que los sistemas e incluso la misma información sean complejos a medida en la que la tecnología evolucione con el pasar del tiempo; por este motivo, las organizaciones necesitan alguna herramienta capaz de administrar y mitigar los riesgos que puedan presentar sus negocios. En estos casos las organizaciones desean mejorar, proteger y controlar sus sistemas con el propósito de asegurar la confiabilidad, integridad de los datos y la disponibilidad de la información.

La Alcaldía Municipal de Ábrego como toda institución que maneja gran cantidad de información y en su mayoría de gran confidencialidad, necesita saber el estado actual de sus sistemas informáticos y de sus instalaciones al momento de manejar grandes flujos de información que son vitales para el óptimo funcionamiento de la Alcaldía.

Actualmente, la Alcaldía Municipal de Ábrego maneja un gran volumen de transacciones de información por día. En algunas oportunidades, la Alcaldía Municipal no ha tenido certeza de la confidencialidad de la información que se maneja en sus sistemas informáticos, lo que puede generar mala imagen institucional y pérdida de activos y de clientes que utilizan sus servicios.

Es evidente además que la empresa en mención, pese a que no se ha presentado ningún inconveniente de tipo técnico o humano que pudiera poner en riesgo la seguridad de la información, no cuenta con planes de contingencia, ni informes de auditoría que evidencien la realización de evaluaciones periódicas a los recursos informáticos con los que cuenta.

1.2 FORMULACIÓN DEL PROBLEMA

En la actualidad las empresas han experimentado transformación en algunos aspectos de seguridad; la situación actual nos da a conocer que tanto los sistemas de información, como también la misma información son el activo más valioso y al mismo tiempo el más vulnerable.

La seguridad informática ha adquirido gran auge, dada las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que converge en la aparición de nuevas amenazas en los sistemas informáticos.

¿Una evaluación a la seguridad física y lógica de la Alcaldía del municipio de Ábrego determinará el estado en que se encuentran los sistemas de información?

1.3 OBJETIVOS

1.3.1 Objetivo General

Evaluar la seguridad física y lógica de los sistemas de información de la Alcaldía del municipio de Ábrego, Norte de Santander.

1.3.2 Objetivos Específicos

- Utilizar la norma ISO/IEC 27001:2005 para evaluar la seguridad física y lógica de los sistemas de información de la Alcaldía del municipio de Ábrego, Norte de Santander.
- Elaborar un informe con los posibles hallazgos sobre la seguridad física y lógica a partir de los resultados obtenidos.
- Proponer un plan de recomendaciones para la Alcaldía del municipio de Ábrego con base en el análisis de riesgos previamente elaborado.

1.4 JUSTIFICACIÓN

Actualmente las empresas prestan mayor importancia a la seguridad de la información, ya que esta es uno de los activos más importantes que las empresas puedan poseer y toma más importancia en el sentido de que la información se mueve con mayor facilidad entre las organizaciones, siendo susceptibles a un número cada vez mayor y una variedad de amenazas y vulnerabilidades.

La presente auditoría, se realiza con el objetivo de identificar irregularidades, errores y defectos en los recursos informáticos, así como de evaluar los servicios soportados por dichos recursos, que ofrece la Alcaldía del municipio de Ábrego. Así mismo, pretende verificar el cumplimiento de las normas, políticas, procedimientos y otras actividades, tendientes al logro de los objetivos institucionales.

De igual forma, la evaluación a la seguridad física y lógica de los sistemas informáticos de la Alcaldía de Ábrego, servirá de orientación para la adopción de las mejores alternativas que permitan mitigar el impacto de las amenazas a las que pueden estar sometidos los servicios informáticos, y por consecuencia, ofrecer productos y servicios de calidad.

El resultado de dicha evaluación, será un informe que recopile todos los procesos que fueron evaluados, un diagnóstico producto de la aplicación de pruebas e instrumentos de recolección de información, y un análisis de dichos datos. El dictamen final, será un elemento importante a tener en cuenta en la toma de decisiones por parte del nivel ejecutivo, de tal manera, que redunden en beneficio para los usuarios que utilizan los servicios ofrecidos por la Alcaldía del municipio de Ábrego.

1.5 DELIMITACIONES

1.5.1 Geográfica. Para la realización de este trabajo de grado se realizará en el municipio de Ábrego, Norte de Santander, más específico en la Alcaldía Municipal del mismo municipio.

1.5.2 Conceptual. Para el desarrollo de este trabajo se tendrán en cuenta los siguientes términos: información, auditoría, auditoría de sistemas, seguridad física, sistema de información, controles, seguridad lógica, seguridad de la información.

1.5.3 Operativa. Este proyecto se realizará en el área de auditoría de sistemas de información, basándose en normas internacionales y legislación colombiana para auditoría informática, así como con la asesoría de la directora del proyecto de grado.

1.5.4 Temporal. El proyecto en cuestión tendrá una duración de 6 meses, a partir de la fecha de aprobación del anteproyecto y teniendo en cuenta las actividades que se deben realizar para dicha evaluación.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

2.1.1 Historia de la Auditoría

Cuadro 1. Mapa cronológico donde se reseña la historia y evolución de la auditoría según Carlos Muños Razo.

RESEÑA HISTÓRICA Y EVOLUCIÓN DE LA AUDITORIA	
FECHA	ANTECEDENTES HISTÓRICOS
1284	Sancho VI “EL BRAVO” Control de los caudales públicos Origen del tribunal de cuentas de España
1492	Descubrimiento de América Revisión de las cuentas y resultados de las colonias descubiertas
	En México, revisión de los tesoros, recaudos, gastos, y la forma en que sus encargados gobernaban en la Nueva España
Siglo XV	Registro de las primeras operaciones mercantiles por escribas
	Nacimiento de los servicios revisores de cuentas
	Registro y evaluación de los primeros negocios
Siglo XVI	Teneduría del libro
Siglo XVIII	
1800	Revolución industrial Aumento de las actividades mercantiles y fabriles
1894	Audidores de la marina y guerra
Siglo XIX	Ley de empresas del reino unido de Inglaterra Se impone la obligación de ejecutar auditorias(resultados financieros, balance general, registros contables, actividades financieras, otros)
	Audidores eclesiásticos de la rota romana
Siglo xx	Profesionalización de la contabilidad financiera
ANTECEDENTES DE LA AUDITORIA(SIGLO XX)	
1912	Instituto de contadores públicos de España Surge en forma colegiada la actividad del auditor
1917	Colegio de censores de Bilbao
1932	T.G. Rose Con su tesis “[...] independientemente de la utilidad de la Auditoría financiera también es útil la auditoría administrativa...”
	James Mckinsey Concluye que la empresa tiene que hacer periódicamente auditorias
1936	Colegio de contadores jurados de Madrid
1945	Instituto de auditores internos, estados unidos
	Primeros escritos sobre la auditoria de operaciones

1946	Institutos de censores jurados de cuentas de España
1948	Arthur h. Kent Realiza importantes aportaciones sobre la auditoría de operaciones
1950	Jackson Martindell Desarrollo los primeros programas de auditoría administrativa, procedimientos de control y sistema de evaluación
1955	Larke A.G Plantea la necesidad de llevar una auditoría en pequeñas empresas, con el fin de evaluar su forma de actuar
1962	William P. Leonard Estudio completo sobre la auditoría administrativa
1964	Cadmus y Bradford En su publicación “operational auditing handbook, N.Y” expone la necesidad de una auditoría denominada auditoría operativa
1968	John C. Burton The journal of accountancy. N.Y Rigg F.J Enfoque de la auditoría administrativa en su obra “themanagementaudit, theinternal auditor ”
1969	Langenderfer H.Q y Robertson J.C Propusieron una teoría para entender la función de la auditoría en las empresas
1970	Kelth D y Bloomstrom R. Exposición sobre la auditoría administrativa
1977	Clark C. abr. Presenta una perspectiva sobre la medición de la conducta social de las empresas(auditoría social)
1980	Whitmore G.M Expone que la auditoría administrativa se utiliza para apoyar a los funcionarios públicos y gerentes de empresas privadas. Sobre las técnicas en el ámbito gubernamental, las estrategias y pasos para una auditoría administrativa.
1983	Spencer Hayden Expone la necesidad de evaluar procedimientos administrativos y el enfoque de la auditoría en el camino organizacional.
1984	Robert J. Thierauf Hablas sobre la auditoría administrativa como una técnica para evaluar las áreas operacionales de una organización

2.1.2 Historia de la auditoría de sistemas de información. La Auditoría de los Sistemas de Información ha surgido cuando las empresas e instituciones han tomado conciencia de que la información que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de progreso.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información, agregándolos en uno solo denominado sistema de información. En consecuencia, por su naturaleza crítica, el enfoque de auditoría debe adoptar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoría tradicional, o sea mediante la creación de unos nuevos. Pero al principio esto no era así. La introducción de las máquinas de proceso de datos en las empresas se produjo en los años 50's, principalmente dedicadas a sustituir a los empleados en las tareas repetitivas en el cálculo de nóminas y facturas de clientes.¹

Dada su utilización como supercalculadoras, con un volumen considerable de datos de entrada, y un volumen similar de datos de salida en función de los anteriores, el auditor se limitaba a verificar la corrección de los datos de salida frente a los datos de entrada, ignorando la lógica y funcionamiento interno de las máquinas de proceso de datos. Este tipo de auditoría se suele denominar auditoría alrededor del ordenador.

Prácticamente era una auditoría convencional con un elemento exótico que producía información de distinta manera que los empleados de la empresa. Esta situación se prolongó hasta mediados de la década de los 60's, cuando las organizaciones de auditoría propugnaron un cambio en el enfoque, en base a los resultados de baja calidad obtenidos en las auditorías de áreas que comportaban proceso de datos a través de ordenadores. Este cambio consistía fundamentalmente en la adaptación de los criterios para la evaluación del control interno, en los sistemas organizativos, financieros y contables, al centro de proceso de datos y, concretamente, a la sala del ordenador.

Esta etapa se suele denominar auditoría del ordenador. Con la introducción de nuevas tecnologías, como las comunicaciones entre ordenadores en tiempo real, pronto se detectaron las limitaciones del enfoque, ya que se producían pérdidas progresivas de las pistas de auditoría y el auditor era incapaz de controlar determinadas actividades. Así, a finales de los años 70's, se llega a una tercera etapa: la auditoría a través del ordenador. En este enfoque se estudia también el tratamiento lógico de la información a través de los programas y las aplicaciones que los integran.

Posteriormente, a principios de los años 80's, se empieza a aplicar técnicas de tratamiento de la información por medio de ordenadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución

¹Introducción a la auditoría de sistemas de información. Breve historia de la auditoría de sistemas de información [en línea] Disponible en Internet : <http://www.escet.urjc.es/~ai/T2Apuntes.pdf>

de pruebas y obtención de evidencia. Surge de este modo la denominada auditoría con el ordenador. En la misma década se empieza a aplicar los principios básicos de la auditoría operativa a la auditoría de los sistemas de información, dando lugar a la auditoría operativa de proceso de datos, que se centra principalmente en la eficacia y eficiencia del tratamiento automático de los datos.

2.1.3 Historia de la Información. La historia de la información está asociada a su producción, tratamiento y transmisión. Una cronología de esa historia detallada puede ser:

- Siglos V a X - Alta Edad Media. El almacenamiento, acceso y uso limitado de la información se realiza en las bibliotecas de los monasterios de forma amanuense o manual.
- Siglo XII. Los Incas (Perú) usan un sistema de cuerdas para el registro de información numérica llamada Quipu, usado principalmente para contar ganado.
- Siglo XV - Edad Moderna. Con el nacimiento de la imprenta (Gutenberg), los libros comienzan a fabricarse en serie. Surgen los primeros periódicos.
- Siglo XX. 1926. Se inicia la primera retransmisión de televisión que afectará al manejo y tratamiento de la información con gran impacto en los métodos de comunicación social durante todo el siglo.
- Siglo XX. 1940. Jeremy Campbell, definió el término información desde una perspectiva científica, en el contexto de la era de la comunicación electrónica.
- Siglo XX. 1943. El austro-húngaro Nikola Tesla inventa la radio, aunque inicialmente dicho invento se atribuye a Guglielmo Marconi y la patente no se reconoce a su autor hasta los años 1960.
- Siglo XX. 1947. En diciembre John Bardeen, Walter Houser Brattain y William Bradford Shockley, inventan el transistor. Serán galardonados por ello con el Premio Nobel de Física en 1956. Acaban de sentar sin saberlo la primera de las dos bases para una nueva revolución tecnológica y económica, actuando como detonante de un aumento exponencial de la capacidad de integración microelectrónica, de la popularización y la potencia de cálculo del ordenador.²
- Siglo XX. 1948. Claude E. Shannon, elabora las bases matemáticas de la Teoría de la Información.³ Acaba de dar la segunda base de la revolución de las tecnologías de la información y la comunicación: la aplicación del Álgebra de Boole será el fundamento

²Manso Coronado, Francisco Javier (2003). *Diccionario enciclopédico de estrategia empresarial*. ISBN 8479785659. «"Nos hallamos inmersos en una revolución... la tecnología de silicio se inventó en 1945, el transistor en 1947, el primer ordenador en 1948..." pag257»

³Shannon, Claude E (1948). «A Mathematical Theory of Communication». *Bell System Technical Journal* **27** (b-1598). ISSN, 379-423.

matemático para industrializar el procesamiento de la información. Nace así la Ciencia de la Computación o Ingeniería informática. La nueva revolución económica está servida. La humanidad entra en la Era Digital usando el transistor y la numeración binaria para simbolizar, transmitir y compartir la información.^{4 5}

- Siglo XX. 1948. Norbert Wiener, elabora la idea de cibernética en su famosa obra *Cibernética o el control y comunicación en animales y máquinas (Cybernetics or Control and Communication in the Animal and the Machine)* (1948) donde se encargó de "mantener el orden" en cualquier sistema natural o artificial de información.
- Siglo XX. 1951-1953. James Watson y Francis Crick descubren los principios de los códigos de ADN, que forman un sistema de información a partir de la doble espiral de ADN y la forma en que trabajan los genes.
- Siglo XX. 1969. En el contexto de la guerra fría, el movimiento contracultural de los años 60', nace la embrionaria Internet cuando se establece la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos, con el objetivo inicial de facilitar una red de comunicaciones militares *a prueba de bomba*. Su expansión y popularización, y la democratización del conocimiento que facilita, transformará radicalmente las relaciones económicas, sociales y culturales en un mundo más y más interdependiente.⁶
- Actualmente, ya en el siglo XXI, en un corto período de tiempo, el mundo desarrollado se ha propuesto lograr la globalización del acceso a los enormes volúmenes de información existentes en medios cada vez más complejos, con capacidades exponencialmente crecientes de almacenamiento⁷ y en soportes cada vez más reducidos. A pesar de ello todavía existen muchas fuentes de información en formato no digital o inaccesible digitalmente por diversas causas.⁸

En este marco la proliferación de redes de transmisión de datos e información, de bases de datos con acceso en línea, ubicadas en cualquier lugar, localizables mediante Internet, permiten el hallazgo de otras redes y centros de información de diferentes tipos en cualquier momento desde cualquier lugar. Es el resultado de datos gestionados a través de aplicaciones informáticas donde los datos son procesados y transformados en información

⁴ Leer, Anne (2001). *La visión de los líderes en la era digital (2001)*. México: Prentice-Hall. ISBN 968-444-440-0.

⁵ Tubella i Casadevall, Immna (2005). «2.2. La economía de las TIC y la revolución digital». En UOC. *Sociedad Del conocimiento*.

⁶«An Internet Pioneer Ponders the Next Revolution». *An Internet Pioneer Ponders the Next Revolution*. Consultado el 25 de noviembre de 2005. <http://partners.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-bobb.html>

⁷«The size Of.The World Wide Web». Consultado el 21 de Febrero de 2010. <http://www.worldwidewebsite.com/>

⁸«El saber perdido en la era digital. Lucha por preservar la memoria colectiva en el ciberespacio». EL PAÍS (22/2007). Consultado el 21 de Febrero de 2010. http://tecnologia.elpais.com/tecnologia/2007/03/22/actualidad/1174555678_850215.html

que posteriormente es manejada como signo integrador y característico de progreso económico del siglo XXI.⁹

2.2 MARCO CONCEPTUAL

2.2.1 Auditoría. La auditoría es un proceso sistemático que se realiza para obtener y evaluar de manera objetiva las evidencias relacionadas con informes presentados sobre acciones que tienen que ver directamente con las actividades que se desarrollan en un área o una organización, sea pública o privada.

La auditoría es un proceso sistemático. Esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que se deben cumplir para la recopilación de la información con el fin de emitir una opinión final.

2.2.2 Auditoria De Sistemas. Definiciones de algunos expertos acerca del tema:

Ron Weber: Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

Mr. William: auditoría en informática es la verificación de los controles en las siguientes tres áreas de la organización (informática):

- Aplicaciones(programas de producción)
- Desarrollo de sistemas
- Instalación del centro de proceso

Por lo tanto podemos decir que la auditoría de sistemas es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.¹⁰

2.2.3 Sistema De Información. Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware), sin embargo en la práctica se utiliza como sinónimo de sistema de información computarizado.

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las

⁹ Federación de Cajas de Ahorros Vasco-Navarras-. «La revolución digital: Nueva economía e Integración Social». EKONOMI GERIZAN **VOLUMEN** (9).

¹⁰Auditoría en informática- José Antonio Echenique García editorial McGraw-Hill segunda edición pág. 17-18

telecomunicaciones y los procedimientos de políticas y reglas de operación. Un Sistema de Información realiza cuatro actividades básicas:

Entrada de información: Proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.

Almacenamiento de información: Es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sesión o proceso anterior.

Procesamiento de la información: Esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

Salida de información: Es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, cintas magnéticas, diskettes, la voz, etc.¹¹

2.2.4 Seguridad Física. Para intentar definir el ámbito de seguridad física, diremos que comprende todas aquellas medidas de seguridad aplicables a un sistema de información o a un programa específico, que traten de proteger a este y a su entorno tanto de las amenazas de carácter físico procedentes de la naturaleza, de los propios medios técnicos y de las personas como de las amenazas de carácter lógico, cuyas medidas de protección son de carácter físico.¹²

Cuando nos referimos a los aspectos físicos de la seguridad, nos referimos a todos aquellos dispositivos y mecanismos destinados a proteger físicamente cualquier recurso, considerando desde un simple medio de respaldo y almacenamiento (disco, cinta, CD, DVD, etc.) hasta un notebook.¹³

2.2.5 Seguridad lógica. Hace referencia a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

¹¹ VEGA BRICEÑO, Edgar Armando. Los sistemas de información y su importancia para las organizaciones y empresas. [en línea] Investigación de mercados [citado en junio de 2005] Disponible en Internet: <<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>>

¹² PIATTINI VELTHUIS. Mario. Auditoría de las tecnologías de sistemas de información. Editorial Alfa omega. Edición Ra-Ma 2008. Depósito legal: M-3989-2008. p. 287.

¹³SCHULZ, Héctor. Seguridad física y seguridad lógica. Tesis de grado Auditor de sistemas. Santiago de Chile: Universidad de los Lagos. Facultad de Ingeniería. Departamento de Sistemas, 2010. 4 p.

Habiendo cubierto los aspectos más relevantes de seguridad física, se prosigue a continuación las técnicas, mecanismos y barreras que buscan mantener la integridad y consistencia de los datos que residen en la base de datos.¹⁴

2.2.6 Seguridad de la Información. Para entender qué es seguridad de la información, en primer lugar, debemos conocer que la información en esta área es referida a los activos de información (es decir, los datos por supuesto, pero también los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, transmitir y distribuir la información), que tienen un valor para la organización. En las complejas organizaciones de hoy en día, se recogen, gestionan y transmiten multitud de datos a través de diferentes medios, a mucha gente, y todas las acciones relacionadas con ello pueden necesitar protección.

No se debe confundir seguridad de la información con seguridad informática, ya que la seguridad de la información abarca muchas áreas mientras que la seguridad informática se encarga de la protección de las infraestructuras TIC que soportan el negocio. Por lo tanto seguridad de la información abarca la seguridad informática. La seguridad de la información, por lo tanto se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos del negocio de la organización. Estos tres parámetros básicos de la seguridad y se definen como:

-Confidencialidad: A la información sólo puede acceder las personas autorizadas para ello.

-Integridad: La información ha de estar completa y correcta en todo momento.

-Disponibilidad: La información estará lista para acceder a ella o utilizarse cuando se necesita.¹⁵

2.2.7 Controles. Es el mecanismo que se utiliza para comprobar que las cosas se realizan como fueron previstas, de acuerdo con las políticas, objetivos y metas fijadas previamente para garantizar el cumplimiento de la misión institucional.¹⁶

2.2.7.1 Clasificación general de los controles

2.2.7.1.1 Controles Preventivos. Son aquellos que reducen la frecuencia con que ocurren las causas de riesgo o evitan que ocurran errores.

¹⁴ SCHULZ, Héctor. Seguridad física y seguridad lógica. Tesis de grado Auditor de sistemas. Santiago de Chile: Universidad de los Lagos. Facultad de Ingeniería. Departamento de Sistemas, 2010. 10 p.

¹⁵ Instituto Nacional de Tecnologías de la Comunicación. Cursos de sistemas de gestión de seguridad de la información según la Norma ISO/IEC 17799. Bogotá: INTECO, 2010. p. 6-7.

¹⁶Auditoría Informática: controles de la auditoría informática [diapositiva].2009. 20 diapositivas, color Disponible en Internet: <[PPT] <https://www.u-cursos.cl/ieb/2009/1/0718/255001/material.../18815>>

2.2.7.1.2 Controles Detectivos. Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

2.2.7.1.3 Controles Correctivos. Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores, y es lo más caro para la organización.

2.2.7.1.4 Controles Físicos. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

2.2.7.1.5 Controles Lógicos. Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

2.2.8. Norma ISO/IEC 27001:2005. Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad

de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.¹⁷



2.3 MARCO TEÓRICO

Con la aparición de la Internet y su presencia en la vida de las personas y de las empresas, aparecen asociados nuevos riesgos que es necesario evitar o al menos, minimizar. Surge así el asunto de la Seguridad Informática, que no existe en términos absolutos, se debe tener bien claro que sólo es posible reducir las oportunidades de que un sistema sea comprometido o disminuir la duración y daños provocados a raíz de un ataque. Cuando se produce un ataque entran en juego tres elementos clave: la confidencialidad, la integridad y la disponibilidad de los datos, junto al impacto en los equipos físicos. En muchas oportunidades no cuentan las instituciones o empresas con una política escrita, formal, de Seguridad Informática. Es un tema que al no ser tan cotidiano, no es de factor vital para los usuarios y por lo tanto no están suficientemente concientizados en este asunto.

La seguridad de información es mucho más que establecer firewalls, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar en la bóveda los backups, es determinar qué hay que proteger y por qué, de qué se debe proteger y cómo protegerlo, la seguridad informática es una necesidad para una organización.¹⁸

¹⁷(Estándar Internacional ISO 27001. Tecnología de la información – Tecnicas de seguridad –Sistemas de gestión de seguridad de la información- Requerimiento)

¹⁸12DÍAZ PIRAQUIVE, Flor Nancy. “Principales estándares para la seguridad de la información IT, Alcances y consideraciones esenciales de los estándares”, Revista Eos No.2, Enero-abril de 2008, Argentina.

La seguridad de la información se considera como la herramienta fundamental para implantar nuevas mejoras en las empresas, razón por la cual éstas deben realizar un esfuerzo cada día mayor para optimizar su nivel de seguridad en este aspecto. La organización debe mejorar continuamente la eficacia del Sistema de Gestión del Sistema de Información (SGSI), mediante el establecimiento de políticas y objetivos de seguridad de la información, tomando en cuenta los resultados de las auditorías, análisis de eventos, y acciones correctivas y preventivas de los mismos. De igual manera, deben establecer procedimientos argumentados para identificar documentos que ya no se requieran porque se actualizaron o porque se remplazaron por otros.¹⁹

"Un sistema es una entidad autónoma dotada de una cierta permanencia, y constituida por elementos interrelacionados, que forman subsistemas estructurales y funcionales. Se transforma, dentro de ciertos límites de estabilidad, gracias a regulaciones internas que le permiten adaptarse a las variaciones de su entorno específico".

Brian Wilson sostiene que el vocablo sistema "tiene varias interpretaciones, dependiendo del contexto en el que es usado". Por otra parte, Stafford Beer refiere que "hablar de un sistema es hablar de la cohesión de un cierto número de entidades llamadas partes de un sistema. Un sistema no es algo dado por la naturaleza sino definido por la inteligencia".

Por lo tanto, se define a un Sistema como un conjunto de elementos interrelacionados que responden a un propósito determinado que como un todo tiene característica que sus partes separadamente no tienen. Está conectado, interactúa y es influenciado por su entorno.²⁰

Un Sistema de Información (SI) es un conjunto de componentes interrelacionados para recolectar, manipular y diseminar datos e información y para disponer de un mecanismo de retroalimentación útil en el cumplimiento de un objetivo.

"Todos interactuamos en forma cotidiana con sistemas de información, para fines tanto personales como profesionales; utilizamos cajeros automáticos, los empleados de las tiendas registran nuestras compras sirviéndose de códigos de barras y escáner u obtenemos información en módulos equipados con pantallas sensibles al tacto, las muy famosas touchscreen. Las principales compañías gastan en la actualidad más de 1 000 millones de dólares al año en tecnología de información y el futuro dependeremos aún más de los sistemas de información".²¹

"Un **sistema de información** se puede definir técnicamente como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.

¹⁹DÍAZ PIRAQUIVE, Floor Nancy, OP. cit., p.78.

²⁰ Villanueva sanchezgrover "sistema de gestión Estratégica aplicando el Enfoque Sistémico y las Tecnologías de la Información para lograr Ventajas Competitivas en el Instituto Nacional de Cultura de La Libertad" Ref. Tés [2].

²¹Ralph M. Stair, "Principios de SISTEMAS DE INFORMACION– Enfoque Administrativo". Ref. Lib [02]

Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores a analizar problemas, visualizar asuntos complejos y crear productos nuevos”.²²

Los sistemas de información contienen información acerca de gente, lugares y cosas importantes dentro de la organización o en el entorno que se desenvuelven. Por información se entiende los datos que se han modelado en una forma significativa y útil para los seres humanos. En contraste, los datos son consecuencia de los hechos en bruto y representan eventos que ocurren en las organizaciones o en el entorno físico antes de ser organizados y ordenados en una forma que las personas puedan entender y utilizar.

2.4 MARCO LEGAL

2.4.1 Congreso de la República (Ley 1273 DE 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.²³

EL CONGRESO DE COLOMBIA

Decreta:

Artículo 1°. Adiciónese el Código Penal con un Título VII BIS denominado “De la Protección de la información y de los datos.

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

2.4.1.1. Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

2.4.1.2. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales

²²Kenneth Laudon. & Jane Laudon“Sistemas De Información Gerencial”. Ref. Lib [03]

²³ Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en internet: http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm

mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

2.4.1.3. Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

2.4.1.4. Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

2.4.1.5. Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.4.2 Ley organiza de protección de datos. En su conjunto de artículos, se resaltan los siguientes:²⁴

TÍTULO II Principios de la protección de datos

2.4.2.1. Artículo 4. Calidad de los datos.

- Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
- Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad la situación actual del afectado.

²⁴Ley organiza de protección de datos http://www.ua.es/es/normativa/datospersonales/pdfs/Ley15_99.pdf

- Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

- Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

- Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

- Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2.4.2.2. Artículo 5. Derecho de información en la recogida de datos.

- Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

- Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

- No será necesaria la información a que se refieran las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
- Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
- No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
- Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

2.4.2.3. Artículo 6. Consentimiento del afectado.

- El tratamiento de los datos de carácter persona requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
- No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sean necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
- El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

- En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no dispóngalo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

2.4.2.4. Artículo 7. Datos especialmente protegidos.

- De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho no prestarlo.
- Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
- Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
- Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
- Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
- No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
- También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

2.4.2.5. Artículo 8. Datos relativos a la salud.

- Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

2.4.2.6. Artículo 9. Seguridad de los datos.

- El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
- Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

2.4.2.7. Artículo 10. Deber de secreto.

- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

2.4.2.8. Artículo 11. Comunicación de datos.

- Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
- El consentimiento exigido en el apartado anterior no será preciso:
 - a) Cuando la cesión está autorizada en una ley.
 - b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

d) En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

e) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

f) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

g) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizarlos estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

- Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

- El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

- Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

- Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

2.4.2.9. Artículo 12. Acceso a los datos por cuenta de terceros.

- No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

- La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento,

que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

- En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
- Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

En este proyecto se aplicara el método de recolección de datos de tipo descriptivo, cuyo objetivo principal es diagnosticar el estado actual de la seguridad física y lógica de los sistemas de información en la Alcaldía del municipio de Ábrego, Norte de Santander.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población. Para la realización de este proyecto, la población que será objeto de estudio está conformado por las personas que laboran en las dependencias, las cuales posean los sistemas de información, que actualmente son 9 personas quienes interactúan con algún programa o sistema de información en la Alcaldía Municipal de Ábrego, Norte de Santander.

3.2.2 Muestra. Debido a que el tamaño de la población es pequeña, la muestra que se tomara es la misma población.

3.3 TECNICAS Y HERRAMIENTAS DE RECOLECCION DE INFORMACION

Fuentes primarias

- Entrevista al alcalde del municipio de Ábrego y encuestas aplicadas a los empleados que interactúan con algún sistema de información o software.
- Visita de observación a cada una de las dependencias de la Alcaldía, ubicada en el municipio de Ábrego, Norte de Santander.
- Documentación institucional de la Alcaldía Municipal de Ábrego, Norte de Santander.

Fuentes secundarias

- Encuestas para determinar la seguridad física y lógica de los sistemas de información.
- Listas de chequeo para la seguridad física y lógica, teniendo en cuenta los parámetros dados por la norma ISO/IEC 27001: 2005.
- Formatos de verificación en donde se corrobora la información recolectada por las encuestas y las listas de chequeo.

4. PRESENTACIÓN DE RESULTADOS

4.1. GENERALIDADES

El proyecto en mención se realizó en la Alcaldía Municipal de Ábrego, Norte de Santander con el objetivo de evaluar aspectos como La Seguridad Física y Lógica de los Sistemas de Información bajo el estándar ISO/IEC 27001:2005.

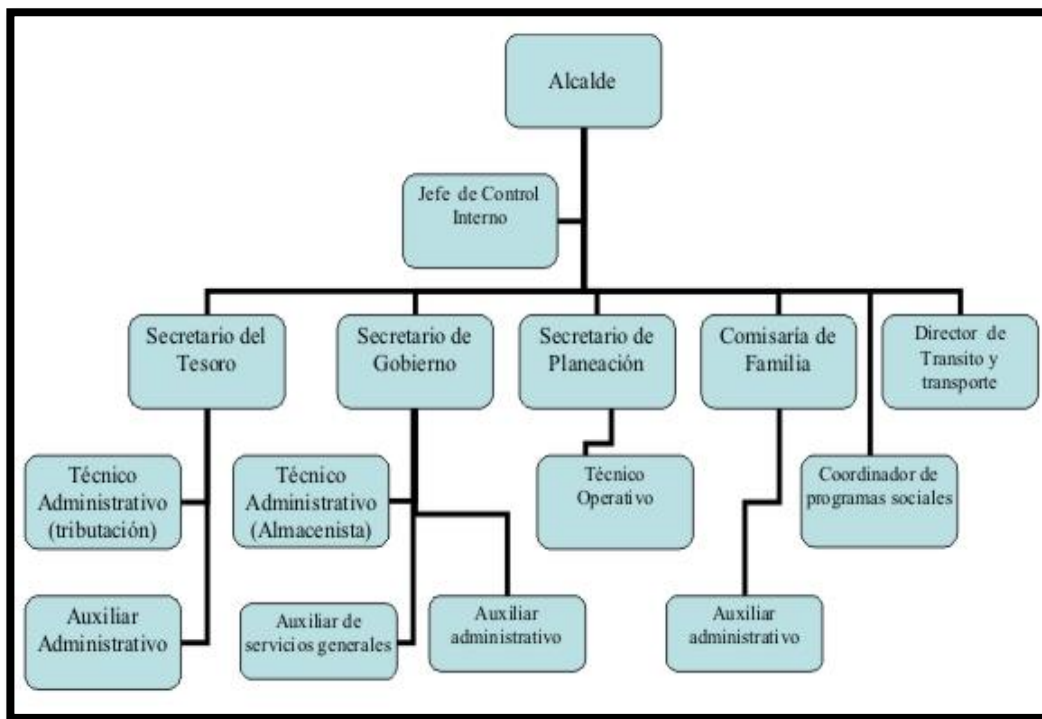
4.2 ASPECTOS GENERALES DE LA EMPRESA AUDITADA

La Alcaldía Municipal de Ábrego, Norte de Santander es una organización pública, en la cual dentro de sus funciones están:

- Administrar los asuntos municipales y prestar los servicios públicos que determine la Ley
- Ordenar el desarrollo de su territorio y construir las obras que demande el progreso municipal
- Promover la participación comunitaria y el mejoramiento social y cultural de sus habitantes.
- Planificar el desarrollo económico, social y ambiental de su territorio, de conformidad con la Ley y en coordinación con otras entidades.
- Solucionar las necesidades insatisfechas de salud, educación, saneamiento ambiental, agua potable, servicios públicos domiciliarios vivienda, recreación y deporte, con especial énfasis en la niñez, la mujer, la tercera edad y los sectores discapacitados, directamente y en concurrencia, complementariedad y coordinación con las demás entidades territoriales y la Nación, en los términos que defina la Ley.
- Velar por el adecuado manejo de los recursos naturales y del medio ambiente. Promover el mejoramiento económico y social de los habitantes del respectivo municipio.
- Hacer cuanto pueda adelantar por sí mismo, en subsidio de otras entidades territoriales, mientras éstas proveen lo necesario.

Actualmente la Alcaldía cuenta con el siguiente organigrama, organizado de forma jerárquica, en la que se observan las distintas dependencias que ayudan a cumplir las funciones de esta organización para la población del municipio de Ábrego, norte de Santander, la estructura organiza en mención se muestra a continuación:

ORGANIGRAMA ALCALDÍA MUNICIPAL DE ÁBREGO, NORTE DE SANTANDER



Fuente: Estructura orgánica Alcaldía Municipal de Ábrego, Norte de Santander.

Para llevar a cabo sus funciones, la Alcaldía Municipal de Ábrego, cuenta con los siguientes sistemas de información que dan soporte a los servicios ofrecidos por la misma, a la comunidad en general, en la cual están instalados en las siguientes oficinas a mencionar:

OFICINA DE PLANEACIÓN Y OBRAS CIVILES: La oficina de planeación y obras civiles se encarga de crear proyectos para el desarrollo del municipio, además de implementar el POBT (Plan de Ordenamiento Territorial), de otorgar las respectivas licencias de urbanismo y de construcción y de expedir a los establecimientos del municipio los respectivos usos del suelo y licencias de funcionamiento.²⁵ Por otra parte, la oficina de planeación y obras civiles cuenta con el siguiente sistema de información:

SISTEMA DE INFORMACIÓN MGA4: Es un sistema de información diseñado por el Departamento Nacional de Planeación que tiene por objetivo guiar y orientar al usuario en la realización de estudios de evaluación ex ante para la toma de decisiones de inversión. Esta metodología se encuentra reglamentada a través de la Resolución No. 0806 de 2005,

²⁵ (Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones) <http://www.abrego-nortedesantander.gov.co/>

por la cual se organizan criterios y procedimientos que permitan integrar los sistemas de planeación y la red nacional de Bancos de Programas Proyectos y que establece su aplicación a nivel nacional, distrital, departamental y municipal para la identificación, preparación y evaluación de proyectos de inversión pública. El responsable a cargo de dicho sistema actualmente es el secretario de planeación, quien se encuentra a cargo de la dependencia de planeación y obras civiles.²⁶

OFICINA DEL SISBEN: En la oficina del sisben se encarga de realizar las encuestas que sirve para identificar y clasificar a las personas de escasos recursos económicos, que por obvias razones no pueden cubrir sus necesidades básicas. Con el fin de que el Estado pueda subsidiarles parte de los derechos fundamentales, correspondientes a salud, a través del Régimen Subsidiado de Salud, vivienda y educación, entre otros. ²⁷Dicha oficina cuenta con el siguiente sistema de información que es manipulado por el director de la oficina de sisben:

SISTEMA DE INFORMACIÓN SISBENNET: El funcionario encargado de esta dependencia tiene la función de administrar la información socioeconómica confiable y actualizada de los grupos específicos del municipio, en donde se realizan consultas de puntaje, registro de nuevos usuarios, así como de registrar las solicitudes y se realiza el manejo de rutas y visitas. La dependencia sisben maneja el siguiente sistema llamado SISBENNET cuenta con los siguientes componentes: El primer sistema es SISBENNET local, que se debe instalar en los municipios, el segundo es SisbenNet Web, que se debe instalar en un servidor central dispuesto por el DNP. El tercero es el Web Service, que al igual que el anterior se instala en el servidor central y es consumido desde el SisbenNet local.

El sistema de información SISBENNET web cuenta con tres subsistemas: el primero es datos básicos, desde donde se administra la información básica de entidades, responsables y usuarios del sistema, creados inicialmente desde el DNP para permitir la descarga de los aplicativos desde el ambiente web. El segundo subsistema es control de envíos, desde donde los usuarios municipales pueden realizar los envíos de información al DNP y hacer seguimiento de ellos. El tercer subsistema es instalador, en donde los usuarios municipales pueden descargar los aplicativos, las bases de datos y consultar los archivos de resultados de sus envíos.

El sistema de información SISBENNET local cuenta con varios subsistemas. el primer subsistema es administración del sistema, mediante el cual se administran , usuarios y perfiles, y se realiza la creación de Backus; el segundo subsistema es operación del sistema, en donde se especifica cómo se administran los de datos de las fichas, procesos del sistema, consultas y reportes, interoperabilidad y control de calidad; el tercer subsistema es atención

²⁶ (Sistema General de Regalias) [http:// www.sgr.gov.co/Inicio.aspx](http://www.sgr.gov.co/Inicio.aspx)

²⁷ (Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones) <http://www.abrego-nortedesantander.gov.co/>

al usuario, en donde se registran las solicitudes y se realiza el manejo de rutas y visitas; por último se describe de forma detallada el proceso de sincronización, a nivel local y central.²⁸

OFICINA DE UNIDAD DE SERVICIOS PÚBLICOS: Dentro de los objetivos que presenta esa oficina están el de Buscar métodos para concienciar a la población referente al ahorro del agua, Lograr que el suministro de agua llegue a todos los barrios, el de mantener en buen estado el carro compactador del aseo, lograr total eficiencia en el recaudo, actualizar información referente al SUI, actualizar el registro de la Unidad de Servicios Públicos ante la superintendencia de servicios público, bajar índice de contaminación de la laguna de oxidación al río algodonal y de rendir información a la Contraloría departamental.²⁹

SISTEMA DE INFORMACIÓN USPA: La aplicación USPA es utilizado para el registro de los servicios de acueducto, alcantarillado y aseo de la alcaldía municipal, además de generar las facturas correspondientes para el pago de recibos del agua, acueducto y alcantarillado.

OFICINA DE REGIMEN SUBSIDIADO: En esta oficina cumple unas actividades como Disminuir el porcentaje de las necesidades básicas insatisfechas, Cubrir la totalidad de los sisbenizados en los niveles 1 y 2 y de mejorar la calidad de vida de los habitantes del municipio.³⁰ Esta oficina cuenta con el siguiente sistema de información que le sirve de apoyo para realizar estos procesos anteriormente mencionados:

SISTEMA DE INFORMACIÓN FOSYGA: La dependencia de régimen subsidiado cuenta con el siguiente sistema de información llamado FOSYGA que es Fondo de Solidaridad y Garantía. Este fondo fue creado con la Ley 100 de 1993, con el fin de garantizar la compensación entre las personas de diferentes ingresos, la solidaridad del sistema general de seguridad social y salud para cubrir los riesgos catastróficos y accidentes de tránsito. Es una cuenta adscrita al Ministerio de Salud y Protección Social manejada por encargo fiduciario, sin personería jurídica ni planta de personal propia, cuyos recursos se destinan a la inversión en salud. Además Esta ley estableció la estructura del Fosyga en subcuentas independientes. Estas subcuentas son las siguientes: De Compensación Interna del Régimen Contributivo • De solidaridad del régimen de subsidios en salud • De promoción de la salud • Del Seguro de Riesgos Catastróficos y Accidentes de Tránsito, ECAT.

Esta plataforma web fue creada empleando el entorno de desarrollo Visual Studio 2008 (C#, HTML, JavaScript) y Gestor de base de datos Microsoft SQL 2005 (T-SQL).³¹

²⁸ (Scribd- Manual de Usuario SISBENNET version 7.0.0.0 demanda)
<https://es.scribd.com/doc/153938902/MANUAL-USUARIO-SisbenNet-Web-Local-V7-0-0-0-Demanda>

²⁹ (Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones)
<http://www.abrego-nortedesantander.gov.co/>

³⁰ (Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones)
<http://www.abrego-nortedesantander.gov.co/>

³¹ (FOSYGA) <http://www.fosyga.gov.co/>

OFICINA DE SECRETARIA DEL TESORO: En esta dependencia se realizan una serie de procesos como son: Organizar y dirigir el recaudo de las rentas, tasas, multas y contribuciones a favor del municipio, el de asesorar al Alcalde en la formulación de políticas financieras, fiscales y económicas y encargarse del recaudo de los ingresos y pagos de las obligaciones a cargo del municipio, recibir los fondos de las entidades oficiales, consignados y responder por su custodia, así como de valores o dineros encomendados a la dependencia de la Tesorería, formular políticas que en materia fiscal y financiera se consideran más convenientes para el Municipio dentro del marco que las normas y disposiciones legales le permiten. Preparar el proyecto anual del presupuesto de Ingresos y Gastos, en colaboración con las demás Secretarías y la coordinación de la oficina de Planeación y Obras públicas.

Velar por el oportuno recaudo de los impuestos, aportes, participaciones y demás ingresos municipales.³² Esta dependencia cuenta para el apoyo de sus actividades con los siguientes sistemas de información:

SISTEMA DE INFORMACIÓN VISUAL TNS: la dependencia de tesorería maneja el siguiente sistema de información que se llama VISUAL TNS el cual está diseñado para llevar la información contable, adaptada al manejo de normas internacionales de información financiera, con la generación de todos los comprobantes desde los módulos operativos hacia contabilidad, facturación, inventario, cartera, tesorería y activos fijos.

Libros exigidos por ley, estados financieros medios magnéticos XML, IVA, ICA, CREE, ICO y certificados de retención , presenta seguridad por usuario, operación en línea mediante escritorio remoto utiliza visual reporte para generar reportes en Excel para elaborar informes gerenciales y gráficos para la toma de decisiones. Sistema de gestión de la calidad certificado por Incontec, norma ISO 9001; 2008 código 2978-1. Certificación de Colciencias como producto de una investigación tecnológica con alto contenido nacional según resolución No. 00028 de 2007.

El servidor en sistemas operativos Windows y los clientes en sistemas Windows u otros que manejen escritorio remoto además de servidor ISS para ambiente web y su motor de base de datos es Firebird, además de ser desarrollado en Delphi y asp.net cuya licencia puede ser monousuario o multiusuario.³³

SISTEMA DE INFORMACIÓN PREDIAL: En es donde se tiene el registro de los bienes que posee el municipio de Abrego, así como el de la generación de los formatos para el pago de los impuestos prediales de los bienes para cada año, así mismo, la persona que este a paz y salvo con lo del predial, el sistema tiene la opción de sacarlo del sistema.

³² (Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones) <http://www.abrego-nortedesantander.gov.co/>

³³ (Catalogo de software- Visual TNS) <http://www.catalogodesoftware.com/producto-visual-tns-592>

SISTEMA DE INFORMACIÓN SACE: Es un sistema de información en donde se almacena las estampillas que genera la Alcaldía municipal en cuto al concepto de estampilla para el hospital universitario Erasmo Meoz.

OFICINA FAMILIAS EN ACCION: En esta dependencia se realizan las siguientes actividades: Contribuir a la reducción de la pobreza y la desigualdad del ingreso, incentivar la asistencia y permanencia escolar de los menores de 18 años, impulsar la atención de salud, particular la asistencia a controles de crecimiento y desarrollo de los niños menores de siete años, incentivar las prácticas de cuidado de los niños, mujeres, adolescentes y jóvenes, en aspectos tales como la salud, lactancia materna, desarrollo infantil temprano y nutrición y de contribuir, a partir del conocimiento de la población beneficiaria del programa y del análisis de su comportamiento en cuanto al cumplimiento de compromisos, a la cualificación de la oferta en salud y educación.³⁴

SISTEMA DE INFORMACIÓN SIFA: En este sistema se registra la información de los hogares beneficiarios del Programa. La consulta en el Sistema, para verificar si un hogar fue inscrito, puede realizarse en la oficina del Enlace Municipal. Además, el sistema de información de familias en acción realiza las siguientes funciones:

Inscripción de familias

Este módulo permite la captura de la información relevante de la familia que pretende inscribirse al programa.

Registro de novedades

Este módulo permite hacer actualización a la información de la familia una vez inscrita.

Verificación de compromisos

Este módulo permite generar los listados para realizar la verificación de cumplimientos en salud o educación y los listados para actualización escolar.

Liquidación, pagos y conciliación

Este módulo permite calcular el valor de los subsidios que serán pagados a las familias que cumplan con los requisitos, adicionalmente genera el material para realizar el pago y la conciliación. Es aquí donde dependiendo de los casos el sistema realiza automáticamente novedades de recálculo negativo o positivo. Los valores se calculan tomando como base la parametrización de los subsidios, que son las reglas con las que el sistema determina quién es apto o no para recibir el subsidio y que valores debe tomar para liquidarlo.

³⁴ (Familias en acción) http://www.dps.gov.co/Ingreso_Social/FamiliasenAccion.aspx

Quejas y Reclamos

Este módulo permite registrar las quejas y los reclamos de las familias beneficiarias del programa, la persona encargada del programa, contesta el reclamo y de acuerdo con el caso genera una novedad.

Seguimiento

Este módulo permite generar informes consolidados de la información de las familias, para la toma de decisiones e informes gerenciales.

Administración

Este módulo permite la creación, bloqueo / desbloqueo de usuarios, cambios de claves, asignaciones de perfiles, roles y permisos sobre las opciones del aplicativo.

Parametrización

Este módulo permite crear la información base para que el aplicativo funcione correctamente tales como:

- Crear entidades educativas.
- Crear IPS.
- Modificar los valores de los subsidios.
- Crear nuevos subsidios.
- Asignar fuente de financiación.
- Asignar sucursal bancaria.

No obstante, el sistema de información SIFA presenta motor de base de datos es Oracle 10G y la arquitectura del sistema de información es mixta, una parte Web que comprende los procesos de inscripción, novedades, seguimiento, quejas y reclamos, la otra que comprende servicios Web con un cliente Windows Form para el proceso de liquidación, pagos y conciliaciones.

4.3 ALCANCES DE LA AUDITORÍA

Teniendo en cuenta el estándar internacional ISO/IEC 27001:2005, la evaluación de la seguridad física y lógica de los sistemas de información de la Alcaldía del municipio de Ábrego, Norte de Santander, se realizó teniendo en cuenta los siguientes dominios:

A. Seguridad Física y Ambiental

i. Áreas seguras

- Perímetro de seguridad física
- Controles de ingreso físico
- Asegurar las oficinas, habitaciones y medios
- Protección contra amenazas externas e internas
- Trabajo en áreas aseguradas
- Áreas de acceso público, entrega y carga

ii. Equipo de seguridad

- Ubicación y protección del equipo
- Servicios públicos de soporte
- Seguridad del cableado
- Mantenimiento de equipos
- Seguridad del equipo fuera del local
- Seguridad de la eliminación o re-uso del equipo
- Retiro de propiedad

B. Control del Acceso

i. Requerimiento del negocio para el control del acceso

- Política de control del acceso

ii. Gestión de acceso del usuario

- Registro del usuario
- Gestión de privilegios
- Gestión de las claves secretas de los usuarios
- Revisión de los derechos de acceso del usuario

iii. Responsabilidades del usuario

- Uso de claves secretas
- Equipo del usuario desatendido
- Política de escritorio y pantallas limpias

iiii. Control de acceso a la red

- Política sobre el uso de los servicios de la red
- Autenticación del usuario para las conexiones externas
- Identificación del equipo en las redes
- Protección del puerto de diagnóstico y configuración remota
- Segregación de redes
- Control de conexión a la red
- Control de routing de la red

iiii. Control de acceso al sistema operativo

- Procedimientos para un registro seguro
- Identificación y autenticación del usuario
- Sistema de gestión de claves secretas
- Uso de las utilidades del sistema
- Cierre de una sesión por inactividad
- Limitación del tiempo de conexión

iiiii. Control de acceso a la aplicación y la información

- Restricción del acceso a la información
- Aislar el sistema confidencial

iiiii. Computación y tele-trabajo

- Computación y comunicaciones móviles
- Tele-trabajo

4.4 RESTRICCIONES DE LA EVALUACIÓN

A pesar de que se evaluará los sistemas de información de la Alcaldía Municipal de Ábrego, solo se podrá evaluar los sistemas que son propios de la Alcaldía.

Los demás sistemas de información son plataformas de los cuales no se tiene administración de la información puesto que son sistemas centralizados y alimentados a través de una plataforma web.

Restricción del subdominio de Control del Acceso: Computación y tele-trabajo móvil. También hay restricciones a los subdominios de control de acceso y seguridad física y ambiental como los siguientes:

- Retiro de propiedad
- Seguridad de la eliminación o re-uso del equipo
- Política de control de acceso
- Equipo del usuario desatendido
- Protección del puerto de diagnóstico y configuración remota
- Uso de las utilidades del sistema
- Cierre de sesión por inactividad

4.5 RESULTADOS DE LA AUDITORÍA

Después de haber aplicado los instrumentos de recolección de información y hecho el respectivo análisis de los datos obtenidos, se pudo llegar a las siguientes conclusiones, a partir de las cuales, se formularon las recomendaciones que se describen a continuación:

4.5.1 Conclusiones. La Alcaldía Municipal de Ábrego carece de procedimientos, políticas y programas que garanticen la protección tanto de las instalaciones como de los equipos que manejan información sensible y que es útil para el cumplimiento de los objetivos institucionales. Así mismo, la falta de controles posibilita la pérdida parcial o total de los activos informáticos de la Alcaldía y la insatisfacción de los usuarios en la prestación de sus servicios.

Además de que los administradores de la Alcaldía Municipal no están al tanto de la importancia que presenta la utilización de la auditoría de sistemas para poder evaluar aspectos relacionados con la infraestructura tecnológica que posea actualmente.

4.5.2 Recomendaciones. Se sugiere implementar para la Alcaldía de Ábrego políticas adecuadas para la protección de la seguridad física de sus activos informáticos como perímetros de seguridad, sistemas de vigilancia, sistemas de refrigeración para sus equipos, así mismo de la revisión de su infraestructura de comunicaciones para que se maneje protocolos actuales para mejorar servicios en sus redes.

Así mismo, crear el servicio de mantenimiento (preventivo y correctivo) para los equipos de cómputo o de red con un tiempo o cronograma estipulado y el manejo de un formato de registros de acuerdo a las pautas que se dan en la norma técnica ISO/IEC 27001:2005, con el fin de llevar un adecuado registro de las falles que se presentan en los equipos de cómputos.

La norma técnica ISO/IEC 27001:2005 proporciona los parámetros para elaborar e implementar un plan de contingencias, en las que se detallaran todas las actividades que le permitan a la Alcaldía mantener la continuidad de sus operaciones en un nivel mínimo, frente a eventos críticos como desastres naturales o cualquier incidente que ponga en riesgo su funcionamiento y la seguridad de su información. Así mismo, realizar simulacros y capacitar al personal interno en la implementación del Plan.

Se sugiere además, diseñar, implantar e implementar un modelo de Gestión de Seguridad de la Información, como herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información; todo esto en pro de la reducción de costos operativos y financieros para la Alcaldía y la creación de una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y de las actividades institucionales.

Dada la importancia de la seguridad de la información para el éxito de las actividades en una organización, se recomienda que la Alcaldía del municipio de Ábrego, contrate a una

persona con el perfil técnico necesario para llevar a cabo los procesos de administración y protección de sus datos y no que esta tarea se realice de forma descentralizada como se bien haciendo, buscando en el momento de crisis, quien solucione los problemas de información.

4.6 INFORME FINAL DE AUDITORÍA

4.6.1. Objetivos

- Evaluar los controles de acceso a las áreas seguras en la Alcaldía Municipal de Ábrego, Norte de Santander.
- Evaluar la eficacia de los controles para la protección física de los equipos de cómputo que administra la Alcaldía municipal de Abrego, Norte de Santander.
- Verificar los controles de acceso a la información que se maneja en la Alcaldía Municipal de Ábrego.
- Verificar la existencia y eficiencia de los controles de acceso a la red de datos que soporta los servicios de la Alcaldía Municipal.

4.6.2. Alcances. Se definió que la auditoría se realizará bajo los aspectos de seguridad física y ambiental y control de acceso, además no se pudo evaluar las bases de datos de las aplicaciones presentes en la Alcaldía, porque los sistemas de información que son propios de la Alcaldía no me entregaron los privilegios de acceso a sus base de datos, por otra parte, los demás sistemas de información son plataformas son centralizados y son otorgados por el gobierno.

4.6.3. Tiempo. El tiempo empleado para la realización de esta evaluación, se planteó en un lapso de 6 meses contados a partir del 02 de febrero hasta el 20 de agosto del presente año.

4.6.4. Recursos

Los recursos con los que se contó para realizar la evaluación física y lógica de los sistemas de información de la Alcaldía Municipal de Ábrego, fueron los siguientes:

- **Recursos de Hardware:** Computador, impresora, cámara fotográfica.
- **Recursos de Software:** Paquete Office 2013, Wireless Network Watcher.
- **Recursos Físicos:** Papel, tinta, entre otros.
- **Recursos Humanos:** El personal que apoyó el proceso de auditoría en el suministro de información se relaciona a continuación:

Cuadro 2: Responsables en la entrega de información de la Alcaldía Municipal de Ábrego.

NOMBRE	PROFESION	CARGO
Juan Pablo Álvarez	Ingeniero electrónico	Ingeniero a cargo del área de sistemas
Ingrid Mileidy Reyes	Abogada	Secretaria de gobierno
Tilcia Avendaño	Bachiller académico	Auxiliar administrativo

4.6.5. Actividades de la auditoría. Para llevar a cabo la evaluación de la Seguridad Física y Lógica de los sistemas de información de la Alcaldía Municipal de Ábrego, Norte de Santander, se llevaron a cabo las siguientes actividades:

4.6.5.1. Recolección de información primaria. En primera instancia se realizó una entrevista con la secretaria de gobierno de la Alcaldía Municipal, quien está autorizada por el Alcalde para dar los objetivos y alcances de la auditoría. Además de la entrevista se solicitó la documentación institucional, como visión, misión, organigrama, manuales de funciones y de procedimientos, con el fin de tener una idea general de las actividades que se desarrollan en la Alcaldía Municipal. También como actividad simultanea se solicitó documentación del área informática, a pesar que dentro de la estructura orgánica no existe un área informática, ni en la planta física de la Alcaldía tampoco existe un área informática, se solicitó documentación como planes de contingencia, políticas de seguridad de la información, manuales de usuario, inventario de hardware y software para hacer un estudio más profundo.

De toda esta información, solo recibí lo siguiente:

Misión y visión de la empresa
Organigrama de la empresa
Manual de funciones
Manual de procedimientos
Inventario de equipos

Como gran parte de la información que se solicitó no se pudo obtener, se procedió a diseñar los papeles de trabajo para realizar dicha evaluación.

4.6.5.2. Diseño de papeles de trabajo

Para cumplir con esta actividad se utilizaron diferentes instrumentos de recolección de información, entre los cuales están:

- Entrevista al Alcalde o secretaria de gobierno. (Ver Anexo 1)
- Solicitud de documentación institucional. (Ver Anexo 2)
- Plan de auditoría. (Ver Anexo 3)
- Programa de auditoría. (Ver Anexo 4)

- Guías de auditoría. (Ver Anexo 5)
- Encuesta para evaluar la seguridad física en las áreas seguras. (Ver Anexo 6)
- Lista de chequeo para la evaluación de la seguridad física en las áreas seguras. (Ver Anexo 7)
- Encuesta para verificar la existencia de controles de protección de los equipos fuera de las instalaciones. (Ver Anexo 9)
- Encuesta para evaluar la seguridad física en los controles de protección contra amenazas externas e internas. (Ver Anexo 10)
- Lista de chequeo para la evaluación de la seguridad física a los controles de protección contra amenazas externas e internas. (Ver Anexo 11)
- Formato de verificación de seguridad física respecto a los controles para la protección de los equipos contra amenazas externas e internas. (Ver Anexo 16)
- Encuesta para evaluar la seguridad lógica. (Ver Anexo 20)
- Lista de chequeo para la evaluación de la seguridad lógica. (Ver Anexo 21)
- Formato de verificación de seguridad lógica. (Ver Anexo 26)
- Encuesta para evaluar el servicio de mantenimiento de equipos. (Ver Anexo 27)
- Lista de chequeo para la evaluación al servicio de mantenimiento de equipos. (Ver Anexo 28)
- Encuesta para evaluar la red de datos. (Ver Anexo 29)
- Lista de chequeo para la evaluación de la red de datos. (Ver Anexo 30)
- Encuesta para verificar la protección de los equipos fuera de las instalaciones. (Ver Anexo 31)
- Formato de hallazgos para la seguridad física. (Ver Anexo 34)
- Formato de hallazgos para la seguridad lógica. (Ver Anexo 35)
- Formato de hallazgos para la red de datos. (Ver Anexo 36)
- Formato de pruebas sustantiva No.1. (Ver Anexo 37)
- Formato de pruebas sustantiva No.2. (Ver Anexo 38)
- Formato de pruebas sustantiva No.3. (Ver Anexo 39)
- Formato de pruebas sustantiva No.4. (Ver Anexo 40)
- Formato de pruebas sustantiva No.5. (Ver Anexo 41)
- Formato de pruebas sustantiva No.6. (Ver Anexo 42)

4.6.5.3. Análisis de resultados obtenidos. Después de aplicar los instrumentos respectivos para evaluar la situación actual de la Alcaldía Municipal de Abrego respecto a la seguridad física y lógica de sus sistemas de información, se realizó un proceso de organización, clasificación y análisis de la información recopilada, con el fin de obtener un diagnóstico que permitiera acercarse a la realidad de la Alcaldía Municipal en cuanto a la seguridad de sus sistemas de información.

El análisis de la información se realizó dependiendo del instrumento utilizado para recopilar la información necesaria:

Los CheckList Binarios, se evaluaron teniendo en cuenta que aquellos aspectos enmarcados dentro del **Si** o **Verdadero**, correspondiente al valor **1**, son considerados como **Fortalezas** de la Alcaldía dentro del aspecto evaluado. Por su parte, los aspectos cuya respuesta se encontraron en el **No** o **Falso**, correspondiente al valor **0**, son tomados como **Debilidades**, sobre las cuales deben enfocarse las Recomendaciones.

Los CheckList de Rango, se evaluaron de acuerdo con la escala predefinida para tal fin. Cada valor conceptual de la escala tiene asociado un valor numérico, que permite promediar los resultados de cada elemento que se está evaluando, así:

O	Óptimo	=	5
B	Bueno	=	4
R	Regular	=	3
M	Malo	=	2
D	Deficiente	=	1

Los CheckList de Rango que se encuentran en los Anexos, tienen su respectiva evaluación.

Con relación a los CheckList de seguridad física respecto a los controles de acceso a las áreas seguras y los controles de protección de los equipos contra amenazas externas e internas, se realizó un análisis cualitativo, teniendo en cuenta las respuestas entregadas por parte del ingeniero a cargo del área de sistemas, se pudo concluir que los controles que posee la Alcaldía Municipal sobre la seguridad física, son deficientes ya que carecen de mecanismos y procedimientos que permitan restringir el acceso no autorizado tanto a equipos como a información confidencial, además de que presentan deficiencias en los controles que posee la Alcaldía Municipal para proteger sus equipos de amenazas externas e internas y que es necesario mejorar dichos controles utilizando e implementando controles que ayuden a minimizar los riesgos a sus activos informáticos.

Con relación al CheckList respecto a la seguridad lógica de los sistemas de información, se realizó un análisis cualitativo teniendo en cuenta las respuestas entregadas por el ingeniero a cargo del área de sistemas, en los cuales se pudo concluir que los controles en cuanto a la seguridad lógica son aceptables, pero a su vez necesitan mejorar tanto los controles que posean actualmente como de implementar más controles que ayuden a mitigar fallas que se presenten con lo relacionado a la seguridad lógica.

Con respecto al CheckList sobre el servicio de mantenimiento de equipos, se analizaron las respuestas entregadas por parte del ingeniero a cargo del área de sistemas se puede concluir que la Alcaldía Municipal carece de formatos o procedimientos adecuados a la hora de presentar planes de mantenimiento preventivo a sus equipos de cómputo, además de no contar con personal en la Alcaldía Municipal en caso de que se presenta fallas a sus equipos

Después de aplicar el procedimiento de evaluación del Checklist para la seguridad de la red de datos, se obtuvo el siguiente resultado.

Cantidad de Ítem = 8

Ítem 1 = 4
 Ítem 2 = 4
 Ítem 3 = 2
 Ítem 4 = 3
 Ítem 5 = 4
 Subtotal = Σ Ítem 1 hasta Ítem 8
 Subtotal = 27
 Total = Subtotal / Cantidad de ítems
 Total = 27 / 8
 Total = 3.375 \approx 3.3

Por lo anteriormente descrito en la fórmula, se puede concluir que la seguridad de la red de datos de la Alcaldía Municipal de Ábrego, Norte de Santander, es Regular, puesto que la alcaldía municipal presenta fallas en los controles que les permita implementar protección a la red de datos y de soportar los servicios que son utilizados en la red.

4.6.5.4. Análisis de riesgos. El análisis de Riesgo es un mecanismo que se utiliza para determinar, analizar, valorar y clasificar los niveles de vulnerabilidad a los que están propensas las empresas, por esta razón se analizaron varios aspectos con el fin de determinar el grado de riesgo a la que está sometida la Alcaldía Municipal de Abrego, Norte de Santander. Tales aspectos fueron clasificados de la siguiente manera:

El Análisis de Riesgos, consta de varias etapas:

- **Identificación de Activos o Elementos de Información.**

Para efectos de la evaluación, se realizó la siguiente identificación y clasificación de activos de información:

Cuadro 3. Elementos de información.

ELEMENTOS FÍSICOS	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD
Documentos institucionales			
Directorio de contactos			
Computadores			
Líneas telefónicas			
Cableado de datos			
Cableado eléctrico			
Módem			
Router			
Disco Duro			
ELEMENTOS LÓGICOS	INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD
Base de datos Financiera			
Base de datos Predial			

Internet			
Correo electrónico			
Copias de respaldo			

Fuente: Autor del Proyecto.

- **Valoración de la magnitud del daño de los Elementos de Información.** Para valorar la dimensión del daño que sufre un elemento de información como consecuencia de un impacto causado por una amenaza o un ataque exitoso, se utilizó el siguiente cuadro:

Cuadro 4. Categorización para valorar la magnitud del daño.

VALOR CONCEPTUAL	VALOR NUMÉRICO	DESCRIPCIÓN
INSIGNIFICANTE	1	No causa ningún tipo de impacto o daño a la organización.
BAJO	2	Causa daño aislado, que no perjudica a ningún componente de la organización.
MEDIO	3	Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
ALTO	4	En el corto plazo desmoviliza o desarticula a la organización.

Fuente: Autor del Proyecto.

Cuadro 5. Valoración de la magnitud del daño de los activos de información

ELEMENTO DE INFORMACIÓN	MAGNITUD DE DAÑO			
	NINGUNA	BAJO	MEDIO	ALTO
ELEMENTOS FÍSICOS				
Documentos institucionales		X		
Directorio de contactos		X		
Computadores			X	
Líneas telefónicas			X	
Cableado de datos				X
Cableado eléctrico				X
Módem			X	
Router			X	
Disco Duro				X
ELEMENTOS LÓGICOS				
Base de datos Financiera				X
Base de datos Predial				X
Internet			X	
Correo electrónico				X
Copias de respaldo			X	

Fuente: Autor del Proyecto

- **Valoración de la probabilidad de amenaza.** Para valorar la probabilidad de amenaza que podría causar perjuicio de disponibilidad, confidencialidad, integridad y autenticidad de la información, se utilizó el siguiente rango:

Cuadro 6. Rango de valoración para la probabilidad de amenaza.

Valor conceptual	Valor numérico	Descripción
Insignificante	1	No existen condiciones que impliquen riesgo/ataque.
Bajo	2	Existen condiciones que hacen muy lejana la posibilidad del ataque.
Medio	3	Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
Alto	4	La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

Fuente: autor del proyecto.

Luego de establecer el rango de valores para la probabilidad de amenaza, se seleccionaron tres grupos de amenazas o ataques que pueden considerarse trascendentales para la seguridad de la información, los cuales pueden ser vistos en el siguiente cuadro:

Cuadro 7. Grupos de Amenazas o Ataques

Tipo de Amenaza o Ataque	Probabilidad de Amenaza			
	Ninguna	Bajo	Medio	Alto
Actos originados por criminalidad				
Vandalismo		X		
Sabotaje			X	
Fraude			X	
Robo/hurto de equipos e información electrónica				X
Virus			X	
Ejecuciones no autorizadas de programas			X	
Infiltración		X		
Violación a derechos de autor			X	

Extorsión			X	
Suceso de origen físico	Ninguna	Bajo	Medio	Alto
Incendio		X		
Inundación		X		
Daños provocados por el polvo			X	
Fallas del sistemas			X	
Fallas fluido eléctrico		X		
Sismo				X
Falta de ventilación para los equipos			X	
Sobrecarga eléctrica			X	
Electromagnetismo			X	
Sucesos generados por negligencia	Ninguna	Bajo	Medio	Alto
Mal manejo de sistemas			X	
Uso de software ilegal			X	
Perdida de información			X	
Ausencia de documentación para los sistemas de información.		X		
Ausencia de plan de contingencia				X
Mantenimiento preventivo de equipos		X		
Compartir contraseñas sin autorización			X	
Transmisión de contraseña por teléfono			X	
Falta de mantenimiento físico				X
Red cableada expuesta				X
Fallas en permisos de usuarios			X	
Dependencia a servicio técnico externo			X	

Cuadro 8. Categorización para valorar la magnitud del daño.

Valor conceptual	Valor numérico	Descripción
Insignificante	1	No causa ningún tipo de impacto o daño a la organización.
Bajo	2	Causa daño aislado, que no perjudica a ningún componente de la organización.
Medio	3	Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.

Alto	4	En el corto plazo desmoviliza o desarticula a la organización.
-------------	----------	--

Fuente: autor del proyecto

Los elementos de información para valorar la magnitud del daño, se clasificaron en dos; elementos físicos y elementos lógicos. Éstos pueden ser vistos en el siguiente cuadro:

Cuadro 9. Elementos de información.

Elemento de información	Magnitud de daño			
	Ninguna	Bajo	Medio	Alto
Elementos físicos				
Documentos institucionales		X		
Directorio de Contactos		X		
Computadoras			X	
Líneas telefónicas			X	
Cableado de datos				X
Cableado eléctrico				X
Modem			X	
Router			X	
Disco Duro				X
Elementos lógicos	Ninguna	Bajo	Medio	Alto
Base de datos Financiera				X
Base de datos Predial				X
Internet			X	
Correo electrónico				X
Copias de seguridad			X	

Fuente: autor del proyecto

- **Valoración de la matriz de riesgo.** El riesgo se define como el producto de la Probabilidad de Amenaza por la Magnitud de Daño.

$$R = PA \times MD$$

Donde:

R: Riesgo

PA: Probabilidad de Amenaza

MD: Magnitud del Daño

El nivel de riesgo está agrupado en tres rangos, y para su mejor visualización, se utilizaron las siguientes convenciones:

Cuadro 10. Nivel de Riesgo.

NIVEL DE RIESGO	VALORES	COLOR
BAJO	1 - 6	
MEDIO	8 - 9	
ALTO	12 - 16	

Fuente: Autor del Proyecto

TERMINOS PARA LA MATRIZ DE RIESGOS

Actos originados por criminalidad común

1. Vandalismo
2. Sabotaje
3. Fraude
4. Robo/hurto de equipos e información electrónica
5. Virus
6. Ejecuciones no autorizadas de programas
7. Infiltración

Suceso de origen físico

1. Incendio
2. Inundación
3. Daños provocados por el polvo
4. Fallas fluido eléctrico
5. Sismo
6. Falta de ventilación para los equipos
7. Sobrecarga eléctrica
8. Fallas del sistema
9. Electromagnetismo

Sucesos generados por negligencia

1. Mal manejo de sistemas
2. Uso de software ilegal
3. Pérdida de información
4. Ausencia de documentación para los sistemas de información
5. Ausencia de plan de contingencia
6. Mantenimiento preventivo de equipos
7. Compartir contraseñas sin autorización
8. Transmisión de contraseñas por teléfono
9. Falta de mantenimiento físico
10. Red cableada expuesta

- 11.** Fallas en permisos de usuario
- 12.** Dependencia a servicio técnico externo

MATRIZ DE RIESGO ALCALDÍA MUNICIPAL DE ÁBREGO, NORTE DE SANTANDER

ELEMENTOS FÍSICOS	MAGNITUD DE DAÑO 1= Ninguna 2= Bajo 3=Mediano 4= Alto	Actos originados por criminalidad común							Suceso de origen físico							Sucesos generados por negligencia											
		1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	12
		2	3	3	4	3	3	2	2	2	3	2	4	3	3	3	3	3	2	4	2	3	3	3	4	4	3
Computadoras	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Líneas telefónicas	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Cableado de datos	4	8	12	12	16	12	12	8	8	8	12	8	16	12	12	12	12	12	8	16	8	12	12	12	16	16	12
Cableado eléctrico	4	8	12	12	16	12	12	8	8	8	12	8	16	12	12	12	12	12	8	16	8	12	12	12	16	16	12
Documentos institucionales	2	4	6	6	8	6	6	4	4	4	6	4	8	6	6	6	6	6	4	8	4	6	6	6	8	8	6
Directorio contactos	2	4	6	6	8	6	6	4	4	4	6	4	8	6	6	6	6	6	4	8	4	6	6	6	8	8	6
Modem	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Router	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Disco duro	4	8	12	12	16	12	12	8	8	8	12	8	16	12	12	12	12	12	8	16	8	12	12	12	16	16	12
ELEMENTOS LÓGICOS																											
Base de datos Financiera	4	8	12	12	16	12	12	8	8	8	12	8	16	12	12	12	12	12	8	16	8	12	12	12	16	16	12
Internet	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Correo electrónico	4	8	12	12	16	12	12	8	8	8	12	8	16	12	12	12	12	12	8	16	8	12	12	12	16	16	12
Copias de seguridad	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9
Base datos Predial	3	6	9	9	12	9	9	6	6	6	9	6	12	9	9	9	9	9	6	12	6	9	9	9	12	12	9

Fuente: Autor del Proyecto

Después de analizar los resultados obtenidos mediante el análisis de riesgo para la Alcaldía Municipal de Ábrego, norte de Santander, se puede concluir que la Alcaldía Municipal presenta muchas falencias en diferentes aspectos que fueron evaluados para realizar dicho análisis. Los números que están de color amarillo y rojo, corresponden a nivel alto y medio de magnitud de daño y los de color verde su nivel de magnitud de daño es bajo, lo cual se puede ver que se necesita mejorar e implementar más controles que ayuden a mitigar riesgos a sus activos informáticos y también en mejorar los resultados obtenidos por el anterior análisis.

4.7. DIAGNOSTICO

A nivel de seguridad física y ambiental

Hallazgos

- No existen perímetros de seguridad para controlar el acceso de personal no autorizado a las dependencias de la Alcaldía. Las oficinas en algunos casos se dejan desatendidas posibilitando el acceso a información sensible o a cualquier otro activo de la institución.
- No existe un sistema de vigilancia a través de cámaras ni en las dependencias de la Alcaldía, ni en la parte externa de las instalaciones de la misma.
- La Alcaldía cuenta con un empleado que registra la hora de entrada y salida del personal interno a sus instalaciones.
- Existe una salida de emergencia señalizada pero es estrecha y permanece cerrada con candado. Esta situación imposibilita la evacuación de personal en casos de desastres o cualquier otra emergencia.
- Algunas de las dependencias de la Alcaldía, cuentan con un sistema de refrigeración (aire acondicionado) para los equipos, sin embargo, se pudo observar que la gran mayoría cuenta con ventiladores solo para uso del personal y no para los equipos de cómputo.
- Hay algunos extintores instalados en la Alcaldía, sin embargo, dependencias como el Centro de Convivencia Ciudadana, carece de ellos.
- En cuanto a equipos de fuente ininterrumpida de corriente (UPS), la Alcaldía utiliza unas UPS que están averiadas, como multitomas para conexiones de distintos dispositivos. De igual forma, no hay un sistema alterno de corriente. Este hecho pone en evidencia que no existe un mecanismo de contingencia para los casos en los que el servicio de energía se interrumpa temporal o de forma prolongada y que pueda evitar daños en los equipos y por ende, pérdida total o parcial de la información.
- No existen alarmas contra incendios, ni detectores de humo en las instalaciones de la Alcaldía Municipal.
- El cableado eléctrico está instalado de manera independiente a la conexión de datos, lo cual permite que no haya interferencia en las comunicaciones. Cabe aclarar que la red eléctrica del Centro de Convivencia está regulada, es decir, la instalación eléctrica para los equipos de cómputo es independiente de la instalación eléctrica del edificio.
- La Alcaldía cuenta con un inventario de sus equipos de cómputo.
- A pesar de que se realiza mantenimiento cada seis (6) meses a los equipos de cómputo, y que los equipos que presentan fallas son llevados a Almacén para que el Ingeniero los

revise, no existe un Plan de Mantenimiento Preventivo y Correctivo documentado, que indique los procedimientos formales de ejecución de dicho plan.

- En cuanto al cableado de la red de datos de la Alcaldía, se pudo evidenciar que cuenta con categoría 5 y 6, situación que puede poner en riesgo las comunicaciones, debido a los niveles de interferencia.
- Los equipos al conectarse a la red cableada tienen tres (3) opciones para configurar su red: como red pública, red privada o red doméstica; la Alcaldía no tiene definido una política a la hora de definir a qué grupo se deben conectar los empleados en la red.
- Se pudo evidenciar que existen equipos y otros dispositivos móviles que no pertenecen a la Alcaldía Municipal y que se encuentran conectados de forma permanente a la red inalámbrica de la misma, disminuyendo de esta manera el rendimiento de la red y por ende, poniendo en riesgo la confidencialidad y disponibilidad de la información.
- Tanto la Alcaldía Municipal como el Centro de Convivencia Ciudadana cuentan con un switch para cada instalación, pero dichos dispositivos no son administrables, por tal motivo no se puede acceder a ellos para configurarlos de manera óptima. Además estos equipos y otros dispositivos de red, se encuentran expuestos al público generando riesgos en la continuidad del servicio, debido a cortes intencionados o no del cableado, desconexiones, daño en los equipos, entre otros.
- No existen diseños de la red de datos cableada ni de la inalámbrica.
- Actualmente la Alcaldía Municipal no posee un Plan de Contingencias documentado, ni un Programa de Atención de Incidentes de Seguridad. Así mismo, no existen políticas de seguridad que indiquen cómo debe manejarse la información, ni quiénes son los responsables de ella.

CONCLUSIONES

- Posibilidad de que exista intrusiones no autorizadas de personas ajenas a la alcaldía lo cual ocasionaría pérdida parcial o total de información confidencial de cada dependencia, ya que no posee ni perímetros que dividan las oficinas y que algunas dependencias en algunas oportunidades están desatendidas.
- Al no presentar sistemas de vigilancia puede provocar de que se pueda perder tanto información, como activos informáticos en las instalaciones de la alcaldía municipal.
- Al no poseer un formato para registrar las fallas de los equipos de cómputo, genera que no se tenga certeza de las fallas que presentan los equipos y saber que procedimientos se llevaron a cabo para garantizar la continuidad de dichos equipos.
- Como la Alcaldía Municipal no implementa un tipo de cableado de red apto para garantizar sus servicios y sus telecomunicaciones, existe la posibilidad de fallas en las comunicaciones, ya que se debe adquirir una categoría de cableado que sea resistente a interferencias electromagnéticas y a cambios ambientales.
- Si no se define el tipo de ubicación con lo que los equipos en cada dependencia se vayan a conectar, posibilita la pérdida de información, ya que si varias dependencias poseen la misma ubicación de red, logran la visualización de documentos de distintas dependencias sin su debida autorización, aumentando considerablemente de que haya pérdida de información confidencial entre dependencias.
- Como no se cuenta con sistemas de alarmas contra incendios, ni detectores de humo, la Alcaldía Municipal puede presentar fallas en sus activos informáticos, ya que el fuego ocasiona daños considerables tanto en equipos como en la información con que trabaja dicha organización.
- Como la Alcaldía Municipal poseen ups averiadas, existe la posibilidad de que las fallas de suministro eléctrico provoquen averías a los equipos de cómputo que tengan instalados sistemas de información.
- Al no poseer un plan de contingencias para los incidentes de seguridad en la Alcaldía Municipal, puede provocar que los funcionarios no tengan certeza de cómo es el mejor manejo de la información y saber quiénes son los responsables de tener dicha información.
- Existe la posibilidad de que al estar expuestos los dispositivos de red de la Alcaldía Municipal, exista el riesgo de fallas en la continuidad del negocio, debido a cortes intencionados o no del cableado, desconexiones, daño en los equipos, entre otros.

RECOMENDACIONES

Implementar perímetros de seguridad para el acceso físico, como entradas con autenticación de usuarios, barreras que limiten el acceso de terceros a áreas críticas y a aquellas dependencias que manejan información privilegiada.

Implementar un sistema de vigilancia a través de cámaras en cada dependencia, así como en las áreas comunes de la Alcaldía Municipal, de tal manera que haya un control de entradas y salidas de personal a las instalaciones de la misma.

Diseñar un Plan de Contingencias en el que se detallen las actividades que le permitan a la Alcaldía mantener la continuidad de sus operaciones en un nivel mínimo, frente a eventos críticos como desastres naturales o cualquier incidente que ponga en riesgo su funcionamiento y la seguridad de su información. Así mismo, realizar simulacros y capacitar al personal interno en la implementación del Plan.

Adquirir e implementar un mecanismo alternativo de corriente para los casos de fallos prolongados en el flujo eléctrico.

Instalar sistemas de refrigeración en las dependencias de la Alcaldía Municipal, para mitigar los daños que puedan presentarse en los equipos por exposición a altas temperaturas.

Adquirir dispositivos de red que sean administrables para poder subnetear la red cableada y administrar mejor los servicios que se ofrezcan a través de este medio.

Cambiar el tipo de cableado de red utilizado actualmente en estas instalaciones, para pasar al cableado UTP Categoría 7 y a su vez el cambio de los conectores para dicho cable, ya que brinda mayor protección contra interferencias y mayores velocidades de transmisión.

Se recomienda cambiar la configuración de los routers a un protocolo estático y realizar el registro de los equipos que necesiten trabajar con las conexiones inalámbricas existentes.

Cambiar periódicamente las claves de acceso a las conexiones inalámbricas.

Se recomienda emplear políticas de autenticación a la hora de conectarse a la red, ya sea que se configure en una red pública o en una red privada dependiendo de la situación.

Se recomienda asignar a cada dependencia una ubicación de red específica para sus equipos, evitando que otras dependencias tengan la misma ubicación en la red provocando alguna falla en la seguridad.

A nivel de control del acceso

Hallazgos

- Las aplicaciones en funcionamiento en cada una de las áreas de la Alcaldía Municipal de Ábrego, cuentan con sistemas de login como mecanismo de protección frente a acceso por parte de usuarios no autorizados.
- Los programas antivirus de algunas equipos de cómputo son descargados por internet, lo cual significa que tiene un período de prueba de un mes para su uso, después de esto no se actualizan.
- Solamente los equipos que están instalados en el Centro de Convivencia Ciudadana, tienen licencias de sus sistemas operativos.
- Ningún equipo de cómputo de la Alcaldía Municipal tiene instalado algún software de detección de intrusos, solamente cuenta con la “protección” de los programas antivirus.
- Los funcionarios que tienen a cargo el manejo de algunas aplicaciones de software, generan diariamente copias de seguridad, incluso varias veces al día; sin embargo, dichos respaldos de información se guardan en el mismo equipo; no existe un lugar con las medidas de seguridad adecuadas para salvaguardar esta información.
- No se capacita periódicamente a los funcionarios en el buen uso de la información.
- En el momento de la contratación del personal, no se firma ningún acuerdo de confidencialidad que promueva la protección tanto de los activos como de la información que estará bajo su responsabilidad.
- La Alcaldía no posee un documento de Políticas de Seguridad que indique los procedimientos para la protección de la información y de los demás activos de la institución. Por tal motivo, existe un desconocimiento generalizado de la manera como deben administrarse los datos, poniendo en riesgo la confidencialidad, disponibilidad e integridad de la información que se maneja y se produce al interior de la Alcaldía, útil para una adecuada toma de decisiones.

Conclusiones

- Algunas dependencias al trabajar con programas antivirus que están en periodo de prueba, posibilita que los equipos al ser escaneados, las bases de datos de sus antivirus no realicen una detección minuciosa de las posibles intrusiones de código malicioso que pueda afectar notablemente la operabilidad de los equipos de cómputo.

- como en algunos equipos de cómputo no cuentan con sus respectivas licencias de sus sistemas operativos, provoca que dichos equipos no trabajen de forma óptima provocando lentitud en los procesos e insatisfacción de sus clientes.
- Como no se cuenta con aplicaciones que detecten intrusos, no se tiene certeza de la seguridad que posean los equipos de cómputo, ya que cuentan únicamente con la protección de los antivirus, pero algunos de estos equipos al poseer antivirus en periodo de prueba, posibilita que exista tanto daño de los equipos de cómputo y de información como intrusiones no autorizadas para apoderarse de información confidencial.
- Los funcionarios que manejan sistemas de información al realizar copias de seguridad no cuentan con un sitio adecuado para el almacenamiento de las copias de seguridad generadas y utilizan sus mismos equipos como medio de almacenaje de dichas copias, esto posibilita la pérdida de información ya que al ocurrir una falla en sus equipos, las copias de seguridad se perderían si dichos equipos no cuentan con discos duros particionados.
- Al no capacitar a los funcionarios que manipulan sistemas de información, provoca que los funcionarios no tengan certeza de nuevas modificaciones de sus sistemas y también tener guías en caso de que se presente fallas ya sean causadas por el software o por errores humanos.

Recomendaciones

Dada la importancia de la seguridad de la información para el éxito de las actividades en una organización, se recomienda que la Alcaldía del municipio de Ábrego, contrate a una persona con el perfil técnico necesario para llevar a cabo los procesos de administración y protección de sus datos y no que esta tarea se realice de forma descentralizada como se bien haciendo, buscando en el momento de crisis, quien solucione los problemas de información.

Se sugiere además, diseñar, implantar e implementar un modelo de Gestión de Seguridad de la Información, como herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información; todo esto en pro de la reducción de costos operativos y financieros para la Alcaldía y la creación de una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y de las actividades institucionales.

Instaurar un protocolo de realización de copias de respaldo de la información crítica de la Alcaldía Municipal de Ábrego. De igual forma, se sugiere contratar los servicios de un data center para la protección de dichas copias, asegurando la continuidad de las operaciones en casos de siniestros y mejorando los niveles de confidencialidad, integridad y disponibilidad de la información.

La Alcaldía Municipal debe adquirir las licencias de todas las aplicaciones de software que utilizan para el procesamiento de la información, de tal manera que se garantice el soporte a los mismos y se eviten problemas de actualizaciones. Así mismo, obviar inconvenientes legales.

La Alcaldía Municipal cuenta con el siguiente inventario de software, se cuenta con alrededor de 22 equipos incluyendo los equipos de cómputo con que cuenta el centro de convivencia con las siguientes especificaciones además del inventario de las aplicaciones, también se llevan registros de clientes y proveedores que acceden a los servicios que ofrece la Alcaldía Municipal, estos registros se hacen mediante archivos creados con las herramientas Word y Excel.

Equipo No.1: Equipo No.1: OFICINA DE PLANEACIÓN Y OBRAS CIVILES

Sistema operativo: Microsoft Windows 7 ultimate versión 2009
 Memoria RAM: 4 GB
 Disco duro: 500 GB
 Tipo de sistema: sistema operativo de 64 bits
 Procesador: Intel(R) Celeron(R) CPU 540@1.86GHz

Cuadro No.11.Equipo No. 1: OFICINA DE PLANEACIÓN Y OBRAS CIVILES

PROGRAMAS	LICENCIA
Microsoft Windows 7 ultimate versión 2009	Pre instalada
Microsoft office 2010	Sin licencia
AutoCAD 2013 – Español	Sin licencia
Compresor WinRAR	Free
Escritor de VSS de Microsoft SQL Server Microsoft Corporation	Pre instalada
Nero	Licencia expirada
WinRAR	Free
Skype	Free
Navegadores (Explorer, Mozilla, Chrome)	Pre instalada
Microsoft SQL Server 2005	Pre instalada
Antivirus Avast	Pre instalada
Cleaner	Free

Fuente: autor del proyecto

Equipo No.2: Equipo No.2: OFICINA DE PLANEACIÓN Y OBRAS CIVILES.

Sistema operativo: Microsoft Windows 7 ultimate versión 2009 Service Pack 1
 Memoria RAM: 4 GB 1.86 GHz
 Disco duro: 500 GB
 Tipo de sistema: sistema operativo de 32 bits
 Procesador: Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz (4 CPUs), ~3.1GHz

Cuadro No.12. Equipo No.2: OFICINA DE PLANEACIÓN Y OBRAS CIVILES.

PROGRAMAS	LICENCIA
Microsoft Windows 7 ultimate versión 2009	Licencia expirada
Microsoft office 2007	Sin licencia
Compresor WinRAR	Free
Adobe Reader	Licencia pre instalada
AutoCAD 2008	Licencia expirada
Nero	Licencia expirada
WinRAR	Free
Skype	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
Canon MP280 series MP Drivers	Licenciado
Antivirus avast	Free
Ccleaner	Free

Fuente: autor del proyecto.

Equipo No.3: EQUIPO OFICINA SISBEN.

Sistema operativo: Microsoft Windows 7 ultimate versión 2009 Service Pack 1

Memoria RAM: 4 GB 1.86 GHz

Disco duro: 750 GB

Tipo de sistema: sistema operativo de 32 bits

Procesador: Intel Dual Core 1.8 GHz

Cuadro No.13: EQUIPO OFICINA SISBEN.

PROGRAMAS	LICENCIA
Microsoft Windows 7 ultimate versión 2009	Licencia expirada
Microsoft Office Professional Plus 2010	Sin licencia
Compresor WinRAR	Free
Adobe Reader X	Free
Sisben 8 Departamento Nacional de Planeación - DNP	Licenciado
SISBENNet Cliente + Server DNP	Licenciado
Nero	Free
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
Epson Event Manager SEIKO EPSON CORPORATION	Licenciado
Antivirus McAfee Agent	Licencia pre instalada
Winzip	Free

Fuente: autor del proyecto.

Equipo No.4: Equipo No.1: OFICINA SECRETARIA DE GOBIERNO.

Sistema operativo: Microsoft Windows 7 Profesional Versión 2009

Memoria RAM: 2GB

Disco duro: 450 GB

Tipo de sistema: sistema operativo de 32 bits

Procesador: INTEL DUAL CORE 2.8 GHZ

Cuadro No.14. Equipo No1: OFICINA SECRETARIA DE GOBIERNO.

PROGRAMAS	LICENCIA
Microsoft Windows 7 Profesional Versión 2009	Licencia pre instalada
Microsoft Office 2010 Professional	Licencia pre instalada
Compresor WinRAR	Free
Adobe Reader XI	Licencia pre instalada
Antivirus avast	Sin licencia
Ccleaner	Free
Nero	Free
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
TeamViewer 6	Free
Cyberlink power DVD	Licencia pre instalada
Winzip	Free

Fuente: autor del proyecto.

Equipo No.5: Equipo No.2: OFICINA SECRETARIA DE GOBIERNO.

Sistema operativo: Microsoft Windows 8 Pro

Memoria RAM: 4GB

Disco duro: 300 GB

Tipo de sistema: sistema operativo de 64 bits

Procesador: Intel core i3

Cuadro No.15. Equipo No.2: OFICINA SECRETARIA DE GOBIERNO.

PROGRAMAS	LICENCIA
Microsoft Windows 8 pro	Licencia expirada
Microsoft Office 2007	Licencia pre instalada
Compresor WinRAR	Free
Adobe Reader XI	Licencia pre instalada
Antivirus avast	Licencia pre instalada
Microsoft SQL Server 2005 Microsoft Corporation	Licencia preinstalada
Microsoft SQL Server Native Client	Licencia preinstalada
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada

TeamViewer 6	Sin licencia
Cyberlink power DVD	Licencia expirada
Winzip	Free

Fuente: autor del proyecto.

Equipo No.6: EQUIPO OFICINA UNIDAD DE SERVICIOS PÚBLICOS.

Sistema operativo: Microsoft Windows 7 ultimate versión 2009

Memoria RAM: 2.5 GB

Disco duro: 750 GB

Tipo de sistema: sistema operativo de 32 bits

Procesador: Intel Pentium 1.8 GHZ

Cuadro No.16. EQUIPO OFICINA UNIDAD DE SERVICIOS PÚBLICOS.

PROGRAMAS	LICENCIA
Microsoft Windows 7 ultimate versión 2009	Licencia pre instalada
Microsoft Office 2007 Enterprise	Licencia expirada
Compresor WinRAR	Licencia pre instalada
Adobe Reader X	Free
Norton antivirus	Free
Microsoft SQL Server 2005 Microsoft Corporation	Licencia preinstalada
Microsoft SQL Server Native Client	Licencia preinstalada
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
TeamViewer 6	Free
7-zip	Free
Winzip	Licencia pre instalada

Fuente: autor del proyecto.

Equipo No.7: EQUIPO OFICINA ALMACÉN.

Sistema operativo: Microsoft Windows 7 ultimate

Memoria RAM: 2 GB

Disco duro: 250 GB

Tipo de sistema: sistema operativo de 32 bits

Procesador: Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz (2 CPUs), ~2.0GHz

Cuadro No.17. EQUIPO OFICINA ALMACÉN.

PROGRAMAS	LICENCIA
Microsoft Windows 7 ultimate	Licencia expirada
Microsoft Office Professional Plus 2010	Licencia pre instalada
Compresor WinRAR	Free
Adobe Reader X	Free

Antivirus AVG PC Tuneup 2011	Licencia pre instalada
Nero 7 Ultra Edition	Free
Microsoft SQL Server Native Client	Licencia preinstalada
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
Ccleaner	Free
7-zip	Free
Winzip	Licencia pre instalada

Fuente: autor del proyecto.

Equipo No.8: Equipo No.1: OFICINA TESORERÍA.

Sistema operativo: Microsoft Windows 7 professional Versión 2009

Memoria RAM: 4 GB

Disco duro: 500 GB

Tipo de sistema: sistema operativo de 32 bits

Procesador: Intel Pentium 1.8 GHZ

Cuadro No.18. Equipo No.: OFICINA TESORERÍA.

PROGRAMAS	LICENCIA
Microsoft Windows 7 professional Versión 2009	Licencia expirada
Microsoft Office Professional Plus 2010	Licencia pre instalada
Compresor WinRAR	Free
Adobe Reader X	Free
Antivirus avast! Free Antivirus	Free
CorelDraw Graphics Suite 12	Licencia preinstalada
HP LaserJet P1000 series	Licenciado
Compresor WinRAR	Free
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
Ccleaner	Free
7-zip	Free
Winzip	Licencia pre instalada
Microsoft Office 97 Professional	Licencia pre instalada
Microsoft Office XP Professional con FrontPage	Licencia pre instalada
Microsoft Visual FoxPro 7.0 Professional	Licenciado
Visual TNS	Licenciado
Firebird 2.5.0.26074	Licenciado

Fuente: autor del proyecto.

Equipo No.9: Equipo No.2: OFICINA TESORERÍA.

Sistema operativo: Microsoft Windows XP profesional Versión 2002 Service Pack 3

Memoria RAM: 1 GB

Disco duro: 120 GB
 Tipo de sistema: sistema operativo de 32 bits
 Procesador: AMD AHTON II X3435 2.916Hz

Cuadro No.19. Equipo No.2: OFICINA TESORERÍA.

PROGRAMAS	LICENCIA
Microsoft Windows XP profesional Versión 2002 Service Pack 3	Licencia expirada
Microsoft Office Enterprise 2007	Licencia pre instalada
Compresor WinRAR	Free
Adobe Reader X	Free
Antivirus McAfee Security Scan Plus	Free
Pasivocol 4.0 Ministerio de Hacienda y Crédito Público	Licencia preinstalada
Xerox Phaser 3117	Licencia preinstalada
Microsoft .NET Framework 4 Client Profile	Free
Navegador Explorer	Licencia expirada
Ccleaner	Licencia expirada
7-zip	Free
Winzip	Free
Firebird 2.5.0.26074	Licenciado

Fuente: autor del proyecto.

Los equipos de cómputo tanto de las oficinas de Contabilidad, Control interno, Familias en Acción y las oficinas que comprende el Centro de Convivencia Ciudadana, presentan los mismos programas y las mismas características:

Sistema operativo: Windows 7 Professional Service Pack 1

Memoria RAM: 4 GB

Disco duro: 500 GB

Tipo de sistema: sistema operativo de 64 bits

Procesador: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz (4 CPUs), ~3.3GHz

Cuadro No.20. Especificaciones equipos de cómputo

PROGRAMAS	LICENCIA
Windows 7 Professional Service Pack 1	Licenciado
Microsoft Office Standard 2013	Licencia pre instalada
Compresor WinRAR	Licencia pre instalada
Adobe Reader X	Free
Microsoft security essentials	Sin licencia
PowerDVD	Sin licencia
Team Viewer 8	Licencia expirada
Oracle VM Virtual Box 4.2.18	Sin licencia
Navegadores(Explorer, mozilla, chrome)	Licencia pre instalada
Ccleaner	free

Microsoft Silverlight	Licencia pre instalada
Nero 8.3.2.1	Sin licencia
Windows 7 Professional Service Pack 1	Licenciado

Fuente: autor del proyecto.

CONCLUSIONES

En el desarrollo de este proyecto en el ambiente tecnológico de la Alcaldía Municipal de Ábrego, Norte de Santander, se pudo evidenciar que se presenta deficiencias tanto en la seguridad física y lógica de sus sistemas de información, teniendo como base los parámetros que rigen la norma ISO/IEC 27001:2005.

La alcaldía Municipal carece de procedimientos y de políticas de seguridad, en lo referente a activos informáticos, no existen políticas de seguridad, planes de contingencia, manuales o guías para mejorar los procesos y actividades que se desarrollan.

El proyecto, permitió hacer recomendaciones en el uso adecuado de políticas que se pueden aplicar a la alcaldía de Ábrego, con el objetivo de mitigar los riesgos en cuanto a la seguridad física y lógico de los sistemas de información, aplicando la norma ISO/IEC 27001:2005.

RECOMENDACIONES

El uso de las tecnologías que utiliza la agencia objeto de estudio, como herramienta base en la administración de sus activos, ha influido a que la empresa requiera intervención de profesionales en el área informática con el fin de evaluar, identificar y controlar amenazas que puedan llegar a convertirse en riesgos para sus actividades y transacciones.

Se sugiere que se establezca e implementen políticas de seguridad de la información, donde se evidencie el compromiso y valor de los activos de la empresa, así mismo de concientizar a los funcionarios sobre el mejor uso que se el debe hacer a los activos informáticos.

Se recomienda que este tipo de auditorías se realicen periódicamente en las instalaciones de la Alcaldía Municipal, con el fin de salvaguardar los distintos elementos tecnológicos que posea la Alcaldía Municipal de cualquier riesgo informático y mejorar sensiblemente la eficiencia en el funcionamiento de la organización.

BIBLIOGRAFÍA

Casadevall, I. T. (2005). Sociedad del conocimiento. la economia de las tic y la revolucion digital .

(2010). En i. n. comunicacion, sistemas de gestion de seguridad de la informacion segun norma iso/iec 17799 (págs. 6-7). Bogota.

Coronado, F. J. Diccionario enciclopedico de estrategia empresarial ISBN 8479785695.

En J. A. Garcia, Auditoria en informatica (págs. 17-18). mcgraw-hill.

Laudon, K. L. sistema de informacion gerencial.

Leer, A. (2001). La vision de los lideres en la era digital. mexico: Prentice-Hall.

Piraquive, N. F. (2008). principales estandares para la seguridad de la informacion IT, alcances y consideraciones esenciales de los estandares. revista Eos , 78.

Sanchez, G. V. sistema de gestion estrategica aplicando un enfoque sisitemico y las tecnologias de la informacion para lograr ventajas competitivas en el instituto nacional de cultura de la libertad.

Schulz, H. (2010). Seguridad fisica y logica . santiago de chile, chile: universidad de los lagos.

Shannon, C. E. (1948). A Mathematical Theory of Communication. Bell System TechnicalJournal27. En C. E. Shannon, A Mathematical Theory of Communication. (págs. 379-423).

Stair, R. M. Principios de sistemas de informacion- enfoque administrativo.

Vasco-Navarras, F. d. (s.f.). La revolucion digital. Nueva economia e integracion social. Ekonomi Geriza , volumen 9.

(2008). En M. P. Velthuis, auditoria de las tecnologias de sistemas de informacion (pág. 287). alfa omega edicion Ra-Ma.

Weber, R. (1988). Auditing conceptual foundations and practice. Mcgraw-Hill Series in Management Information Systems.

REFERENCIAS DOCUMENTALES ELECTRÓNICAS

An internet pioneer ponders the next revolution. (s.f.). Recuperado el 25 de noviembre de 2005, de <http://partners.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-bobb.html>

auditoria informatica: controles de la auditoria informatica. (2009). Obtenido de] <https://www.u-cursos.cl/ieb/2009/1/0718/255001/material.../18815>

Briceño, E. A. (s.f.). los sistemas de informacion y su importancia para las organizaciones y empresas. Recuperado el junio de 2005, de <<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>>
constitucion politica de colombia. de la proteccion de la informacion y de los datos, ley 1273 de 2009. (5 de enero de 2009). Obtenido de http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm

El saber perdido en la era digital. lucha por preservar la memoria colectiva en el ciberespacio. EL PAIS. (2007). Recuperado el 21 de febrero de 2010, de http://tecnologia.elpais.com/tecnologia/2007/03/22/actualidad/1174555678_850215.html

Fernandez, E. (s.f.). CFT soeduc concepto de auditoria disponible en internet. Obtenido de www.soeduc.cl/apuntes/concepto%20de%20auditoria.doc
introduccion a la auditoria de sistemas de informacion. Breve historia de la auditoria de sistemas de informacion. (s.f.). Obtenido de <http://www.escet.urjc.es/~ai/T2Apuntes.pdf>

Ley organica de proteccion de datos. (s.f.). Obtenido de http://www.ua.es/es/normativa/datospersonales/pdfs/Ley15_99.pd

Muñoz, C. R. (s.f.). auditoria en sistemas computacionales. Obtenido de auditoria en sistemas computacionales: http://books.google.co.ve/books?id=3hVDOuxTvxwC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true

the size of the world wide web. (s.f.). Recuperado el 21 de febrero de 2010, de <http://www.worldwidewebsize.com/>

ANEXOS

Anexo 1. Entrevista Alcalde o Secretaria de Gobierno (ENT01).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
INGENIERIA DE SISTEMAS



ENT01

EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DEL MUNICIPIO DE ÁBREGO, NORTE DE SANTANDER

¿Se ha realizado auditorias a los sistemas de información de la alcaldía?

No

Opcional:

Qué resultados se han obtenido de dicha auditoria

¿Porque cree que es importante que se evalué los sistemas de información?

Para tener una mejor comunicacion y saber que tipo de seguridad poseemos.

¿Actualmente la alcaldía cuenta con políticas de protección de la información?

No

¿Qué razones le motivaron para que se realice la auditoria?

La falta informacion, procedimientos para manejar informacion, el poco conocimiento que se tiene en los S.I

¿Se han presentado inconvenientes con la información que se procesa en los sistemas de cómputo en cada una de las dependencias de la alcaldía?

Si, en el TNS, redes sociales, pagina institucional

¿Qué dependencias de la alcaldía manejan recursos de software?

programas sociales, tesoreria, servicios publicos, sisben, almacen, personeria, planeacion, familias en accion

¿La alcaldía cuenta con un área de sistemas que de soporte a los diferentes procesos que manejan la alcaldía a nivel tecnológico?

No


Firma entrevistador


Firma entrevistado

Anexo 2. Solicitud documentación institucional (SDI01).

Abrego, 17 de Diciembre de 2013

SDI01

Doctora
INGRID MILEIDY REYES BLANCO
Secretaria de Gobierno
Alcaldía Municipal
Abrego, Norte de Santander


Cordial saludo.

Con el ánimo de iniciar el proceso de evaluación de la Seguridad Física y Lógica de los Sistemas de Información de la Alcaldía Municipal de Abrego y en ejecución del estudio del entorno que se pretende auditar; me dirijo a Usted respetuosamente para solicitar los siguientes documentos:



- Misión y visión de la Alcaldía
- Estructura Orgánica
- Manual de Funciones
- Manual de Procedimientos
- Políticas de Seguridad de la Información
- Inventario de Equipos
- Planes de mantenimiento preventivo de equipos de cómputo
- Licencias de Software
- Inventario de equipos de la red de datos
- Planes de Contingencia de sistemas de información

Agradeciendo su valiosa colaboración.

Atentamente,


JHON ALEXANDER ALVAREZ BAYONA
Estudiante de Ingeniería de Sistemas
Universidad Francisco de Paula Santander



Anexo 3. Plan de auditoría (PLA01).

		UNIVERSIDAD FRANCISCO DE PAULA SANTANDER FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001				
PT No. <u>PLA01</u>						
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander			Fecha Inicio: <u>02/02/2014</u>			
Área o Proceso: Sistemas			Fecha Final: <u>30/06/2014</u>			
Directora proyecto: Magreth Rossio Sanguino Reyes – <u>M.R.S.R.</u>						
Auditor Junior: Jhon Alexander Álvarez Bayona – <u>J.A.A.B.</u>						
Objetivo General						
Evaluar la Seguridad Física y lógica de los sistemas de información de la Alcaldía municipal de Abrego.						
Objetivos Específicos						
<ol style="list-style-type: none"> 1. Evaluar los controles de acceso a las áreas seguras en la Alcaldía Municipal de Ábrego, Norte de Santander. 2. Evaluar la eficacia de los controles para la protección física de los equipos de cómputo que administra la Alcaldía municipal de Ábrego, Norte de Santander. 3. Verificar los controles de acceso de la información que se maneja en la Alcaldía Municipal de Ábrego. 4. Verificar la existencia y eficiencia de los controles de acceso a la red de datos que soporta los servicios de la Alcaldía Municipal. 						
Alcances						
La auditoría se llevará a cabo a la Seguridad Física y Ambiental en las instalaciones de la Alcaldía municipal de Abrego, norte de Santander, desde 02 de febrero hasta el 20 de agosto del presente año.						
Criterios de auditoría						
La auditoría se llevará a cabo bajo los lineamientos de implementación del estándar internacional ISO/IEC 17799 de 2005.						
No.	ACTIVIDAD	FECHA-HORA	LUGAR	AUDITADO	AUDITOR	
1	Entrevista con el alcalde del municipio de	02/02/2014	ALCALDÍA-	I.M.R.B	J.A.A.B.	

	Ábrego, Norte de Santander, para establecer los objetivos y límites de la auditoría.	09:00 a.m.	ABREGO		
2	Entrevista con el ingeniero a cargo del área de sistemas de la Alcaldía Municipal para socializar el trabajo que se realizará	17/02/2014 03:00 p.m.	ALCALDÍA- ABREGO	J.A.P	J.A.A.B.
2	Reunión con la directora del proyecto para definir responsabilidades y tareas.	23/02/2014 10:00 a.m.	OFICINA FIRMA AUDITORA		M.R.S.R. J.A.A.B.
3	Solicitud de Documentación de los procesos que se dan en las dependencias de la Alcaldía Municipal de Ábrego.	28/02/2014 08:00 a.m.	ALCALDÍA- ABREGO	J.A.P	J.A.A.B.
4	Reunión con la directora del proyecto para definir los métodos y procedimientos de auditoría.	12/03/2014 09:30 a.m.	OFICINA FIRMA AUDITORA		M.R.S.R. J.A.A.B.
5	Socialización del Programa de Auditoría	28/04/2014 09:30 a.m.	OFICINA FIRMA AUDITORA		M.R.S.R.
6	Reunión para discutir la pertinencia de los instrumentos de recolección de información	15/05/2014 9:00 a.m.	OFICINA FIRMA AUDITORA		M.R.S.R. J.A.A.B.
7	Elaboración del diagnóstico del área auditada	15/06/2014 09:00 a.m.	OFICINA FIRMA AUDITORA		M.A.A.S. M.R.S.R.
9	Entrega del Informe Final de Auditoría	10/07/2014 2:00 p.m.	ALCALDÍA- ABREGO	I.M.R.B	J.A.A.B.

APROBACIÓN	
JHON ALEXANDER ALVAREZ BAYONA	INGRID MILEIDY REYES BLANCO
Encargado Auditoria Auditor	Secretaria de gobierno Auditado

Anexo 4. Programa de Auditoría (PRA01).

 <p>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001</p> 		PT. No. PRA01		
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander Área o Proceso: Sistemas	Fecha Inicio: <u>02/02/2014</u> Fecha Final: <u>30/06/2014</u>			
Directora Proyecto: Magreth Rossio Sanguino Reyes – <u>M.R.S.R.</u> Auditor : Jhon Alexander Álvarez Bayona – <u>J.A.A.B.</u>				
Objetivo General Evaluar la Seguridad Física y lógica de los sistemas de información de la Alcaldía Municipal de Ábrego, Norte de Santander.				
Objetivos Específicos <ol style="list-style-type: none"> 5. Evaluar los controles de acceso a las áreas seguras en la Alcaldía Municipal de Ábrego, Norte de Santander. 6. Evaluar la eficacia de los controles para la protección física de los equipos de cómputo que administra la Alcaldía Municipal de Ábrego, Norte de Santander. 7. Verificar los controles de acceso de la información que se maneja en la Alcaldía Municipal de Ábrego. 8. Verificar la existencia y eficiencia de los controles de acceso a la red de datos que soporta los servicios de la Alcaldía Municipal. 				
Alcances La auditoría se llevará a cabo a la Seguridad Física y lógica en las instalaciones de la Alcaldía Municipal de Ábrego, Norte de Santander, desde el 02 de febrero al 20 de agosto de 2014.				
No.	ACTIVIDAD	AUDITADO	R/PT	OBSERVACIONES
1.1	Evaluar la existencia de controles de acceso físico a las instalaciones de las Alcaldía Municipal de Ábrego a través de lista de chequeo.	F.D.A	<u>CHL01</u>	

1.2	Verificar la existencia de controles para las actividades realizadas en las áreas seguras.	F.D.A	<u>FVE01</u>	
2.1	Evaluar la existencia y eficacia de los controles utilizados para la protección contra amenazas externas e internas, por medio de listas de chequeo.	F.D.A	<u>CHL02</u>	
2.2	Verificar la eficiencia de los controles implementados para la protección de los equipos.	F.D.A	<u>FVE02</u>	
2.3	Verificar la existencia de planes de mantenimiento preventivo y correctivo de equipos.	F.D.A	<u>CHL04</u>	
2.4	Verificar la existencia de controles para la seguridad de los equipos fuera de las instalaciones de la Alcaldía Municipal.	F.D.A	<u>ENC01</u>	
3.1	Evaluar la seguridad lógica y los controles para el acceso tanto a los equipos de cómputo como a los sistemas de información de la Alcaldía Municipal.	F.D.A	<u>CHL03</u>	
4.1	Verificar la existencia y eficiencia de controles a la seguridad de la red inalámbrica de la Alcaldía Municipal, a través de una prueba sustantiva.	F.D.A	<u>PSU02</u>	
4.2	Observar si los equipos que se conectan a la red son identificados de forma automática.	F.D.A	<u>PSU01</u>	
4.3	Realizar un análisis del entorno de red cableada que posee la Alcaldía municipal.	F.D.A	<u>PSU03</u>	

MARCAS O TILDES UTILIZADAS

PA01: Programa de Auditoría

F.D.A: Funcionarios Dependencias de la Alcaldía Municipal

CHL01: Lista de chequeo No. 1

CHL02: Lista de chequeo No. 2

CHL03: Lista de chequeo No. 3

FVE01: Formato de verificación No. 1

FVE02: Formato de verificación No. 2

ENT01: Entrevista No. 1

ENT02: Entrevista No. 2

Anexo 5. Guías de auditoría (GUA01-GUA02-GUA03-GUA04-GUA05).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001



EMPRESA: Alcaldía Municipal de Ábrego

PT. No.

GUA01

PROYECTO: Evaluación Física y Lógica de los Sistemas de Información

FASE: Iniciación

Elaboró: J.A.A.B.

Fecha: 20-02-2014

Revisó: M.R.S.R

Fecha: 25-02-2014

Objetivos

1. Identificar el entorno objeto de la auditoría.
2. Definir el objeto y alcances de la auditoría.
3. Realizar el estudio inicial de la empresa mediante la evaluación de la documentación institucional.

ITEM	DESCRIPCION DE LA ACTIVIDAD	R/PT	RESPONSABLE
1.1	Visita a las instalaciones de la Alcaldía Municipal de Ábrego.		
1.2	Reconocimiento de las dependencias de la Alcaldía para conocer su ubicación geográfica y servicios ofrecidos.		
2.1	Entrevista al alcalde o al encargado del despacho para conocer generalidades de la empresa y de los aspectos de la auditoría a realizarse.	EAE01	J.A.A.B
3.1	Solicitud formal de la documentación institucional de la Alcaldía Municipal de Ábrego.	SDI01	
3.2	Estudio de la documentación entregada por parte de la Alcaldía.		

MARCAS O TILDES

GUA01: Guía de auditoría No. 1

J.A.A.B: Jhon Alexander Álvarez Bayona- auditor

M.R.S.R: Magreth Rossio Sanguino Reyes-Director Proyecto

ENT01: Entrevista No.1 al Alcalde o encargado del despacho de la Alcaldía del municipio de Ábrego, Norte de Santander.

SDI01: Oficio No.1 de solicitud de información



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001



EMPRESA: Alcaldía Municipal de Ábrego	PT. No. <u>GUA02</u>
PROYECTO: Evaluación Física y Lógica de los Sistemas de Información	
FASE: Diseño de técnicas e instrumentos	
Elaboró: <u>J.A.A.B.</u> Revisó: <u>M.R.S.R</u>	Fecha: 27-02-2014 Fecha: 04-03-2014

Objetivos

1. Realizar los cuestionarios para la seguridad física.
2. Diseñar los cuestionarios para la seguridad lógica.
3. Elaboración de los formatos que nos permita verificar para la información recolectada.

ITEM	DESCRIPCION DE LA ACTIVIDAD	R/PT	RESPONSABLE
1.1	Diseñar los cuestionarios para la seguridad física a cada dependencia que utilice sistemas de información atendiendo a los requerimientos del estándar ISO/IEC 27001	<u>ESF01</u> <u>ESF02</u>	J.A.A.B
2.1	Elaboración de los cuestionarios para evaluar la seguridad lógica de los sistemas de información de las dependencias de la Alcaldía municipal de Ábrego.	<u>ESL03</u>	
3.1	Diseño y elaboración de los formatos de verificación de la información recolectada para la evaluación de la seguridad física.	<u>FVE01</u> <u>FVE02</u>	
3.2	Diseño y elaboración de los formatos de verificación de la información recolectada para la evaluación de la seguridad lógica.	<u>FVE03</u>	



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001



EMPRESA: Alcaldía Municipal de Ábrego		PT. No. GUA03	
PROYECTO: Evaluación Física y Lógica de los Sistemas de Información			
FASE: Evaluación y ejecución			
Elaboró: <u>J.A.A.B.</u> Revisó: <u>M.R.S.R</u>		Fecha: 10-03-2014 Fecha: 15-03-2014	
<p>Objetivos</p> <ol style="list-style-type: none"> 1. Identificar los activos de información que cuenta actualmente la Alcaldía Municipal de Ábrego. 2. Valorar como se encuentra las instalaciones de la Alcaldía con respecto a la seguridad física. 3. Comprobar y valorar las condiciones en que se da el mantenimiento de equipos de cómputo. 4. Revisar los servicios que soporta la red de datos de la Alcaldía de Ábrego. 5. Evaluar el software y las aplicaciones que dan soporte a los servicios ofrecidos por la Alcaldía Municipal. 6. Analizar las políticas de seguridad de la información. 7. Revisar y evaluar los procedimientos de realización de copias de respaldo de la información. 8. Analizar y evaluar los riesgos de los activos informáticos de la Alcaldía de acuerdo con el estándar ISO/IEC 27001. 			
ITEM	DESCRIPCION DE LA ACTIVIDAD	R/PT	RESPONSABLE
1.1	Clasificación de los activos informáticos de la Alcaldía Municipal de Ábrego.		J.A.A.B
1.2	Valoración de los activos de información.		
2.1	Evaluación de las condiciones de seguridad física en las que se encuentran las instalaciones de la Alcaldía.		
2.2	Revisión del estado del sistema de cableado y de las ubicaciones de los dispositivos de la red de datos de la Alcaldía.		
3.1	Verificación del estado actual en que se encuentran los equipos de cómputo de		

	la Alcaldía.		
3.2	Revisión de los planes de mantenimiento que se realizan a los equipos de cómputo de la Alcaldía.		
3.3	Verificación de la existencia de procedimientos formales para la realización de mantenimientos preventivos y correctivos de los equipos de cómputo de la Alcaldía Municipal de Ábrego.		
3.4	Verificación del cumplimiento de las actividades de mantenimiento que se le realiza a los sistemas de cómputo.		
4.1	Evaluación de los servicios de la red de datos de la Alcaldía Municipal.		
5.1	Verificación de los niveles de seguridad de los sistemas de información de la Alcaldía.		
5.2	Verificación de la existencia de aplicaciones que brindan seguridad a los sistemas de información.		
6.1	Verificación de la existencia de políticas de seguridad de la información		
6.2	Evaluación del cumplimiento de las políticas técnicas y de gestión de los sistemas de información de la Alcaldía.		
7.1	Evaluación de los procedimientos que emplean la Alcaldía para la realización de copias de seguridad a sus sistemas de información.		
8.1	Clasificación de las amenazas detectadas según su naturaleza para realizar su respectivo análisis de riesgo.		

MARCAS O TILDES

GUA03: Guía de auditoría No. 3

J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor

M.R.S.R: Magreth Rossio Sanguino Reyes-Director Proyecto



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA
MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001



EMPRESA: Alcaldía Municipal de Ábrego PT. No. **GUA04**

PROYECTO: Evaluación Física y Lógica de los Sistemas de Información

FASE: Organización de la información recolectada

Elaboró: J.A.A.B.

Revisó: M.R.S.R.

Fecha: 23-03-2014

Fecha: 02-04-2014

Objetivos

1. Organizar los papeles de trabajo.
2. Revisar los resultados producto de la aplicación de los instrumentos.
3. Evaluar y revisar de los resultados obtenidos.
4. Realizar el diagnóstico final de la auditoria.

ITEM	DESCRIPCION DE LA ACTIVIDAD	R/PT	RESPONSABLE
1.1	Ordenamiento de los documentos que se emplean a la hora de realizar la auditoria.		J.A.A.B
2.1	Análisis y tabulación de los resultados que se obtuvieron con la aplicación de los instrumentos.		
3.1	Evaluación de los resultados obtenidos.		
4.1	Elaboración del diagnóstico final.		

MARCAS O TILDES

GUA04: Guía de auditoría No. 5

J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor
M.R.S.R: Magreth Rossio Sanguino Reyes-Director Proyecto



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001



EMPRESA: Alcaldía Municipal de Ábrego PT.
 No. **GUA05**

PROYECTO: Evaluación Física y Lógica de los Sistemas de Información

FASE: Elaboración y presentación del informe de auditoría.

Elaboró: J.A.A.B. **Fecha:** 07-04-2014

Revisó: M.R.S.R **Fecha:** 14-04-2014

- Objetivos**
1. Realizar el informe de auditoría.
 2. Elaborar el plan de recomendaciones
 3. Exponer los resultados.

ITEM	DESCRIPCION DE LA ACTIVIDAD	R/PT	RESPONSABLE
1.1	Preparación del informe de auditoría.		
2.1	Diseño del plan de recomendaciones para la Alcaldía Municipal de Ábrego.		J.A.A.B
3.1	Presentación de los resultados		

MARCAS O TILDES
GUA05: Guía de auditoría No. 5
J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor
M.R.S.R: Magreth Rossio Sanguino Reyes-Director Proyecto

Anexo 6. Evaluación a la seguridad física en las áreas seguras (ESF01).



**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS
DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE
EL ESTANDAR ISO/IEC 27001**



ENCUESTAS SOBRE SEGURIDAD FÍSICA

Aplicada a: Ing. JUAN PABLO ALVAREZ – Encargado del área de Sistemas

Objetivo: Encuesta realizada para recolectar información respecto a los controles de acceso a las áreas seguras.

1. ¿Existen perímetros de seguridad bien definidos para proteger las áreas que procesan información crítica y otros servicios de procesamiento de datos?
SI____ **NO**____
2. ¿Las áreas críticas cuentan con controles de acceso sólo para el personal autorizado?
SI____ **NO**____
3. ¿Se suministra seguridad para los equipos fuera de las instalaciones?
SI____ **NO**____
4. ¿Dentro de las instalaciones de la Alcaldía se cuenta con circuito cerrado de televisión?
SI____ **NO**____
5. ¿La Alcaldía cuenta con sistema de cámaras de vigilancia?
SI____ **NO**____
6. ¿Se realiza monitoreo a las áreas en donde están instaladas las cámaras de vigilancia?
SI____ **NO**____
7. ¿Se restringe el uso de dispositivos móviles en las áreas en donde se trabaje sistemas de información?
SI____ **NO**____
8. ¿Existe seguridad privada para las instalaciones de la alcaldía?
SI____ **NO**____

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

JUAN PABLO ALVAREZ
Encargado Área de Sistemas
Entrevistado

Anexo 7. Checklist binaria para la evaluación a la seguridad física en las áreas seguras (CHL01).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001
CHECK-LIST BINARIO



PT. No. **CHL01**

EMPRESA: Alcaldía Municipal de Ábrego
AREA: Seguridad Física
OBJETIVO: Evaluar los controles de acceso a las áreas seguras.

Elaboró: J.A.A.B. **Fecha:** 10-03-2014
Revisó: M.R.S.R. **Fecha:** 15-03-2014

ITEM	PREGUNTAS	S	N	R/PT	RESPONSABLE
1	¿Existen perímetros de seguridad bien definidos para proteger las áreas que procesan información crítica y otros servicios de procesamiento de datos?		X	AFO01	J.A.A.B.
2	¿Las áreas críticas cuentan con controles de acceso sólo para el personal autorizado?		X		
3	¿Se suministra seguridad para los equipos fuera de las instalaciones?		X	ENT02	
4	¿Dentro de las instalaciones de la Alcaldía Municipal se cuenta con circuito cerrado de televisión?		x		
5	¿La Alcaldía Municipal cuenta con sistema de cámaras de vigilancia?		X		
6	¿Se realiza monitoreo a las áreas en donde están instaladas las cámaras de vigilancia?		X		
7	¿Se restringe el uso de dispositivos móviles en las áreas en donde se trabaje sistemas de información?		X		
8	¿Existe seguridad privada para las instalaciones de la Alcaldía Municipal?		x		

MARCAS O TILDES

J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor

M.R.S.R: Magreth Rossio Sanguino Reyes - Directora Proyecto

AFO01: Archivo fotográfico No.1

ENT02: Entrevista No. 2

ANÁLISIS CUALITATIVO

Después que el ingeniero a cargo respondió a las preguntas de la encuesta, se evidenció lo siguiente:
Después de analizar las respuestas entregadas por el ingeniero, se puede concluir que los controles que posee la alcaldía municipal sobre la seguridad física, son deficientes ya que carecen de mecanismos y procedimientos que permitan restringir el acceso no autorizado tanto a equipos como a información confidencial.

Anexo 8. Archivo fotográfico N° 1. (AF001).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. **AFO01**

ARCHIVO FOTográfico No. 1



En estas imágenes se logra apreciar que las oficinas de la Alcaldía Municipal no cuenta con perímetros de seguridad que ayude a aislar a los funcionarios de cada oficina de las demás personas que utilizan los servicios que brinda la Alcaldía Municipal.

Anexo 9. Entrevista para verificar la existencia de controles de protección de los equipos fuera de las instalaciones (ESE06).



**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS
DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE
EL ESTANDAR ISO/IEC 27001**



ENCUESTAS SOBRE SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES DE LA ALCALDÍA MUNICIPAL

Aplicada a: Tilcia Avendaño Ropero – Encargado del área de Almacén

Objetivo: Encuesta realizada para recolectar información respecto a la seguridad de los equipos fuera de las instalaciones de la Alcaldía Municipal.

1. ¿Qué situaciones pueden motivar la autorización de la salida de equipos de cómputo de la Alcaldía Municipal?
.....
.....
2. ¿Existe algún formato o documento que registre esta autorización?
.....
.....
3. ¿Qué dependencia se encarga de manejar estos registros?
.....
.....
4. ¿Qué mecanismo de protección es implementado para preservar tanto la información como el equipo que sale de las instalaciones de la Alcaldía Municipal?
.....
.....
5. ¿Por cuánto tiempo permanecen los equipos de cómputo fuera de las instalaciones de la Alcaldía Municipal?
.....
.....
6. ¿Qué procedimiento se implementa cuando se da de baja a los equipos de cómputo?
.....
.....
7. ¿Qué pasa con la información contenida en esos equipos?
.....
.....

8. ¿Qué destino final tienen esos equipos?

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

TILCIA AVENDAÑO ROPERO
Encargado Área de Almacén
Entrevistado

Anexo 10. Evaluación a la seguridad física en los controles de protección contra amenazas externas e internas (ESF02).



**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS
DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE
EL ESTANDAR ISO/IEC 27001
ENCUESTAS SOBRE SEGURIDAD FISICA**



Aplicada a: Ing. JUAN PABLO ALVAREZ – Encargado del área de Sistemas

Objetivo: Encuesta realizada para recolectar información respecto a los controles para la protección de equipos contra amenazas externas e internas.

1. ¿Existen mecanismo de protección contra fallas de suministro eléctrico?

SI____ **NO**____

2. ¿La Alcaldía cuenta con dispositivos como (UPS, REGULADORES DE VOLTAJE O GENERADORES DE ENERGIA DE EMERGENCIA en caso de una falla de energía?

SI____ **NO**____

3. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

SI____ **NO**____

4. ¿La instalación eléctrica es independiente de la instalación de la red de datos?

SI____ **NO**____

5. ¿El cableado eléctrico y el de telecomunicaciones están protegidos contra interceptación o daño?

SI____ **NO**____

6. ¿El personal de la Alcaldía está capacitado en el manejo de extintores?

SI____ **NO**____

7. ¿Cuenta la Alcaldía con sistema de refrigeración para sus equipos de cómputo?

SI____ **NO**____

8. ¿Las instalaciones de la Alcaldía cuentan con sistemas de alarma contra incendios?

SI____ **NO**____

9. ¿En las áreas que utilizan sistemas informáticos, existen avisos formales de prohibición de ciertas actividades como No fumar, No consumir alimentos ni bebidas, entre otros

SI____ **NO**____

10. ¿La alcaldía presenta señalizaciones para marcar las salidas de emergencia?

SI____ **NO**____

11. ¿Actualmente existe un plan de contingencia en caso de una falla en los sistemas?

SI____ **NO**____

12. ¿Cómo se capacita al personal de la Alcaldía para que conozcan los planes de contingencia que existan dentro de la organización?

SI____ **NO**____

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

JUAN PABLO ALVAREZ
Encargado Área de Sistemas
Entrevistado

Anexo 11. CheckList binario para la evaluación a la seguridad física a los controles de protección contra amenazas externas e internas (CHL02).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001
CHECK-LIST BINARIO



PT. No. **CHL02**

EMPRESA: Alcaldía Municipal de Ábrego

AREA: Seguridad Física

OBJETIVO: Evaluar la existencia de controles utilizados para la protección de equipos contra amenazas externas e internas.

Elaboró: J.A.A.B.

Fecha:7-03-2014

Fecha:20-03-2014

Revisó: M.R.S.R.

ITE M	PREGUNTAS	S	N	R/PT	RESPONSABLE
1	¿Existen mecanismos de protección contra fallas de suministro eléctrico?		x		J.A.A.B.
2	¿La Alcaldía cuenta con dispositivos como (UPS, reguladores de voltaje o generadores de energía de emergencia en caso de una falla de energía?	X		<u>AFO08</u>	
3	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?		X		
4	¿La instalación eléctrica es independiente de la instalación de la red de datos?	X		<u>AFO06</u>	
5	¿El cableado eléctrico y el de telecomunicaciones están protegidos contra interceptación o daño?	X			
6	¿El personal de la Alcaldía está capacitado en el manejo de extintores?		X		
7	¿La Alcaldía Municipal cuenta con sistema de refrigeración para sus equipos de cómputo?		X	<u>AFO04</u>	
8	¿Las instalaciones de la Alcaldía cuentan con sistemas de alarma contra		X		

	incendios?				
9	¿Existen avisos formales de prohibición cuenta la alcaldía en las áreas de sus sistemas de información?		x		
10	¿La Alcaldía presenta señalizaciones para marcar las salidas de emergencia?	x		<u>AFO02</u>	
11	¿Actualmente existe un plan de contingencia en caso de una falla en los sistemas?		X		
12	¿Se capacita al personal de la Alcaldía para que conozcan los planes de contingencia que existan dentro de la organización?		X		
MARCAS O TILDES UTILIZADAS					
CHL02: Lista de Chequeo No. 2 AFO02: Archivo Fotográfico No. 2 AFO04: Archivo Fotográfico No. 4 AFO06: Archivo Fotográfico No. 6 AFO08: Archivo Fotográfico No. 8					

Anexo 12. Archivo fotográfico N° 8. (AF008).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ABREGO



PT. No. **AFO08**

ARCHIVO FOTOGRAFICO No. 8



En la imagen de la izquierda, se logra ver que las UPS que posee la Alcaldía Municipal se encuentran averiadas y se utilizan como multitomas para sus equipos, mientras que en el Centro de Convivencia Ciudadana presenta un dispositivo capaz de almacenar energía para un lapso de media hora.

Anexo 13. Archivo fotográfico N° 6 (AF006).

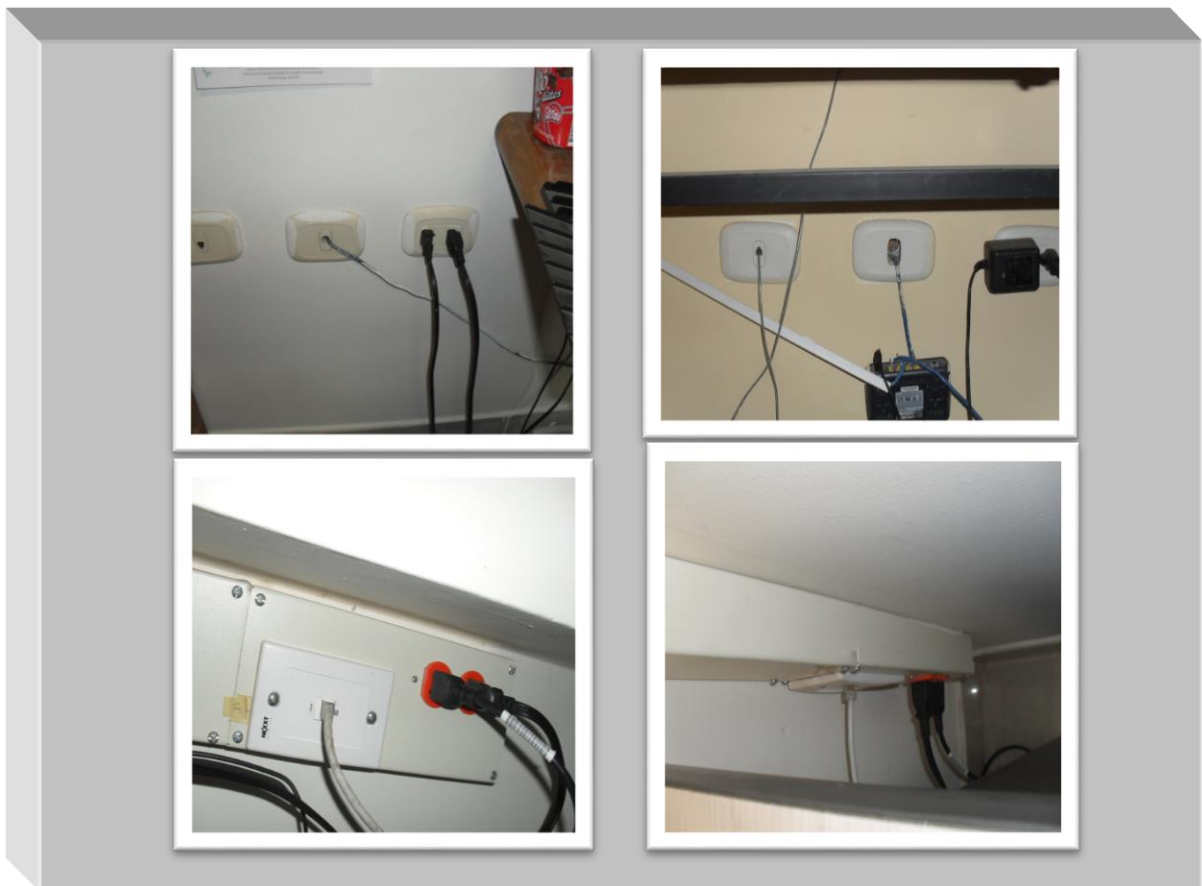


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. **AFO06**

ARCHIVO FOTográfico No. 6



En estas imágenes se puede observar que tanto en la Alcaldía Municipal como en el Centro de Convivencia Ciudadana existe independencia tanto en la red eléctrica como en la red de telecomunicaciones, con la diferencia en que la Alcaldía la separación está dentro de las paredes mientras que en el Centro de Convivencia la separación se emplea canaletas.

Anexo 14. Archivo Fotográfico N° 4 (AF004).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS
SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. AFO04

ARCHIVO FOTOGRAFICO No. 4



Tanto en la Alcaldía Municipal como en el Centro de Convivencia Ciudadana no presentan sistemas de aire acondicionado, solamente utilizan ventiladores para su uso personal. Cabe resaltar que solo la oficina de planeación y obras civiles y el despacho de la personerera cuentan con sistema de aire acondicionado.

Anexo 15. Archivo Fotográfico N° 2 (AF002).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO





PT. No. AFO02

ARCHIVO FOTOGRAFICO No. 2



En la Alcaldía Municipal se ven reflejados las señalizaciones que indican las salidas de emergencia pero también se pudo observar que aparte de la entrada principal existe una salida de emergencia pero es demasiado estrecha y permanece siempre con candado.

Anexo 16. Formato de verificación seguridad física respecto a los controles para la protección de los equipos contra amenazas externas e internas (FVE02).

		UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS					
PT. No. <u>FVE02</u>							
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander Área o Proceso: Controles de protección contra amenazas externas e internas. Fecha Elaboración: <u>19/05/2014</u> Fecha Revisión: <u>26/05/2014</u>							
Objetivo Verificar la existencia y eficacia de los controles utilizados para la protección contra amenazas externas e internas.							
No.	ACTIVIDAD	SI	NO	R/PT	OBSERVACIONES	AUDITOR	
1	Extintores	X		<u>AFO03</u>	La Alcaldía Municipal dentro de sus instalaciones cuenta con dos extintores, uno por cada piso con su respectivo manual de uso. En cambio el Centro de Convivencia al ser una edificación moderna no cuenta con extintores en sus instalaciones.	J.A.A.B.	
2	Alarmas contra incendios		X		Tanto la Alcaldía Municipal como el centro de		

					convivencia no cuenta con sistemas de alarmas contra incendios que den alerta a incendios dentro de sus instalaciones.
3	Detectores de humo		X		No se observan detectores de humo dentro de las instalaciones de la Alcaldía Municipal como en el centro de convivencia.
4	UPS en los equipos que manejan información crítica		x	<u>AFO08</u>	La Alcaldía Municipal solamente cuenta con una de menor capacidad solamente en la dependencia de tesorería, ya que al averiarse lo utilizan como un multitomas, mientras que el centro de convivencia cuenta en sus instalaciones con una ups de una mayor capacidad para que al momento de que ocurra una

					falla de energía la información que se procesa en los equipos de cómputo no se pierda o se dañe.
5	Cableado eléctrico con la normativa correspondiente		X	<u>AFO10</u>	El cableado eléctrico de la Alcaldía Municipal se encuentra separado del cableado de red de datos pero no se ha cambiado dicha norma por mucho tiempo, mientras que en el centro de convivencia la instalación eléctrica maneja una normativa actual, ya que se trata de un edificio nuevo, pero la instalación eléctrica no está bajo tierra, sino que es pasado por encima del edificio mediante tubos metálicos.
6	Cableado de datos con la normativa correspondiente		x	<u>AFO11</u>	El cableado de red que es utilizado en la Alcaldía Municipal

					es de categoría 5 y 6 y no se utiliza canaletas que le briden protección contra interferencias, mientras que en el centro de convivencia se utiliza solamente categoría 6 y son introducidas en cada dependencia por medio de canaletas, ya que dentro de cada canaleta hay una división tanto de la red eléctrica como la de datos.
7	Independencia del cableado eléctrico y de datos	X		<u>AFO06</u>	Tanto las instalaciones de la Alcaldía Municipal como las del Centro de Convivencia el cableado de red y eléctrico está instalado de forma independiente con sus respectivas tomas, pero en el centro de convivencia maneja

					dos tipos de cableado eléctrico, uno para los equipos de cómputo y otro para el edificio.
8	Pararrayos		X		Tanto la Alcaldía Municipal como el Centro de Convivencia no cuentan con pararrayos para proteger sus equipos de cómputo a causa de descargas eléctricas.
9	Suministro alterno de corriente eléctrica (planta eléctrica)		X		No se cuenta actualmente con una planta eléctrica para satisfacer las necesidades en caso de que existan fallas de energía.
10	Prohibición formal de ingerir comidas y bebidas cerca de los equipos de cómputo		X		No se observan avisos que indiquen la prohibición de ingerir comidas y bebidas cerca a los equipos de cómputo tanto de la alcaldía municipal como en el centro de

					convivencia.
11	Prohibición formal de fumar en las áreas de procesamiento de datos	X			La Alcaldía Municipal dentro de sus políticas, se implementa la política de no fumar en las oficinas, pero no se ven avisos que indiquen dicha política. Estos avisos se observan fuera de las dependencias.
12	Avisos formales sobre la utilización correcta de los equipos de cómputo		X		No existen avisos que indiquen a los funcionarios de la Alcaldía Municipal el correcto uso de los equipos de cómputo.
13	Refrigeración de equipos		X	<u>AFO04</u>	Solamente una sección de la dependencia de planeación y la oficina del despacho de la personería cuentan con sistema de refrigeración de aire acondicionado, algunas dependencias cuentan con ventiladores.

14	Control de humedad		X		Dentro de las instalaciones de la Alcaldía Municipal no se ve reflejado dispositivos que marquen la humedad en cada dependencia tanto en los equipos donde se procesa información como dispositivos de red con que se cuenta.
15	Especificación ruta de evacuación		X		La ruta de evacuación del edificio de la Alcaldía Municipal es la misma para ir a la salida de emergencia.
16	Salidas de emergencia		X	<u>AFO02</u>	La salida de emergencia esta con su respectiva señalización pero a su vez es demasiado estrecha y siempre está cerrada con candado. No existe cámara de vigilancia para esta salida. El centro de convivencia dentro

					de sus instalaciones no se encuentran señalizaciones para marcar las salidas de emergencia	
MARCAS O TILDES UTILIZADAS						
<p>CHL02: Lista de Chequeo No. 2 AFO02: Archivo fotográfico No. 2 AFO03: Archivo fotográfico No. 3 AFO04: Archivo fotográfico No. 4 AFO06: Archivo fotográfico No. 6 AFO08: Archivo fotográfico No. 8 AFO10: Archivo fotográfico No. 10 AFO11: Archivo fotográfico No. 11 J.A.A.B. Jhon Alexander Álvarez Bayona - Auditor M.R.S.R. Magreth Rossio Sanguino Reyes-Directora proyecto</p>						

Anexo 17. Archivo fotográfico N° 3 (AF003).

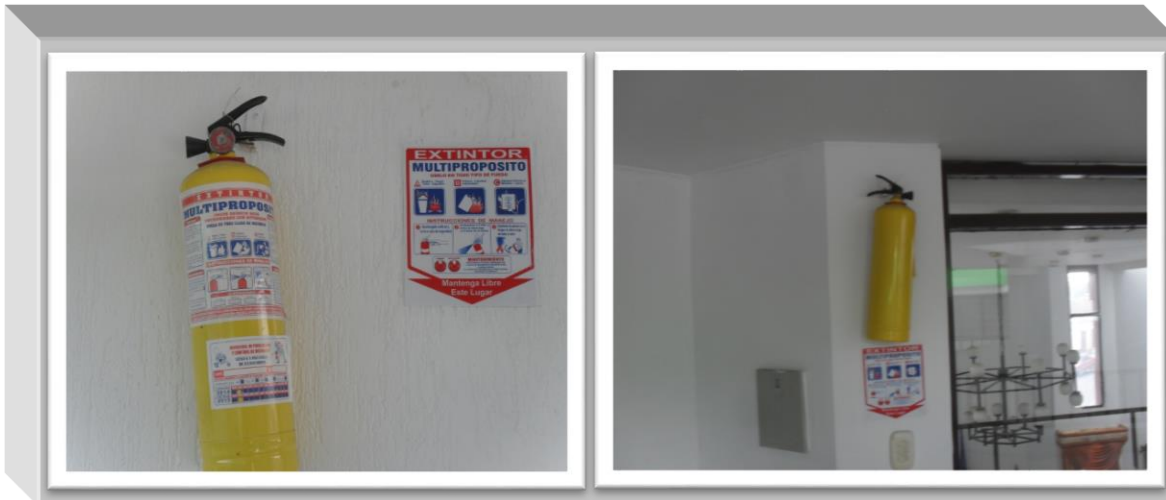


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. AFO03

ARCHIVO FOTOGRAFICO No. 3



Solamente la Alcaldía Municipal cuenta con extintores para sus instalaciones uno por cada piso, mientras que el Centro de Convivencia carece de extintores.

Anexo 18. Archivo fotográfico N° 10 (AF010).

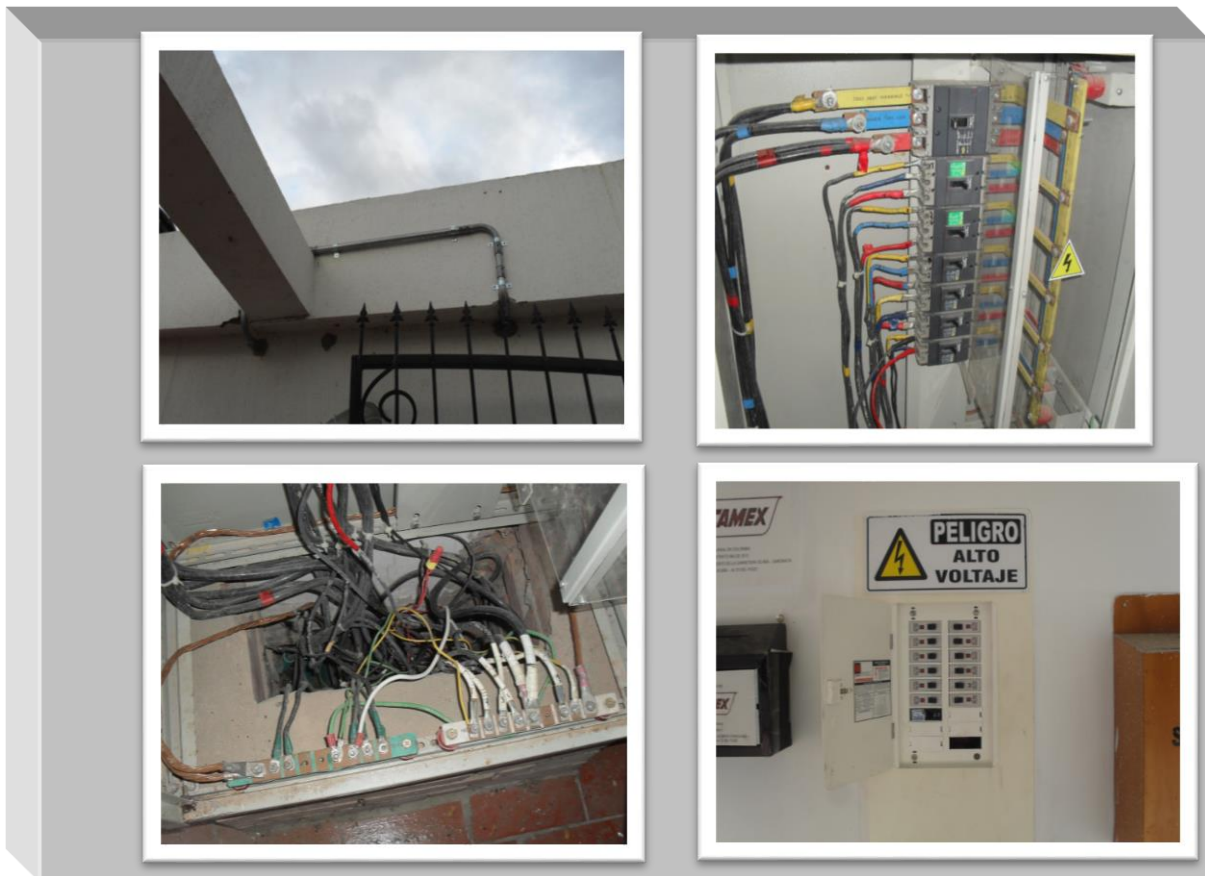


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS
SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. AFO10

ARCHIVO FOTOGRAFICO No. 10



La red eléctrica del Centro de Convivencia es regulada, lo que significa que la red cableada de los equipos es diferente de la del edificio, empleando para su organización la utilización de canaletas, mientras que en la Alcaldía Municipal la red eléctrica está separada e instalada dentro de las paredes del edificio.

Anexo 19. Archivo fotográfico N° 11 (AF011).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. **AF011**

ARCHIVO FOTográfico No. 11



Las siguientes imágenes corresponden a los dispositivos de red que están implementados tanto en la Alcaldía Municipal como en el Centro de Convivencia, pero se puede observar que dichos dispositivos no se encuentran en habitaciones especiales para evitar el acceso a personal no autorizado a estos dispositivos, lo cual generaría que las comunicaciones dentro de estos edificios se vean altamente perjudicados.

Anexo 20. Evaluación a la seguridad lógica (ESL03).



**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACION FISICA Y LOGICA DE LOS SISTEMAS DE
INFORMACION DE LA ALCALDIA MUNICIPAL DE
ABREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001**



ENCUESTAS SOBRE SEGURIDAD LOGICA

Aplicada a: Ing. JUAN PABLO ALVAREZ – Encargado del área de Sistemas

Objetivo: Encuesta realizada para recolectar información acerca sobre la seguridad lógica de los sistemas de información de la Alcaldía Municipal.

1. ¿Se restringe el uso de equipos de cómputo solo al personal autorizado por la Alcaldía?

SI _____ **NO** _____

2. ¿Los sistemas de información que están presentes en la Alcaldía cuentan con un sistema de contraseñas para su ingreso?

SI _____ **NO** _____

3. ¿Los empleados cuentan con claves únicas y exclusivas para cada sistema?

SI _____ **NO** _____

4. ¿Las personas que laboran en la Alcaldía son conscientes de la importancia de la información que tienen bajo su responsabilidad?

SI _____ **NO** _____

5. ¿Existe algún tipo de control para el acceso a los sistemas?

SI _____ **NO** _____ ¿Cuál (es)? _____

6. ¿Se capacita periódicamente a los empleados para el buen uso de sus sistemas?

SI _____ **NO** _____

7. ¿Se realizan copias de seguridad de la información que se genere dentro de las instalaciones de la Alcaldía?

SI _____ **NO** _____

8. ¿Los sistemas de cómputo de la Alcaldía cuentan con programas de detección de intrusos?

SI _____ **NO** _____

9. ¿Los equipos de cómputo cuentan con software antivirus?

SI _____ **NO** _____

10. ¿Realizan diariamente actualizaciones a las bases de datos de los antivirus que poseen los equipos de cómputo?

SI _____ **NO** _____

11. ¿Existen restricciones para instalar aplicaciones desde cualquier equipo?

SI _____ **NO** _____

12. ¿El software que está instalado en los equipos de cómputo de la Alcaldía cuenta con su respectiva licencia de uso?

SI _____ **NO** _____

13. ¿Se atienden las fallas que presenta los sistemas de información?

SI _____ **NO** _____

14. ¿La Alcaldía cuenta con políticas de seguridad de la información debidamente documentadas?

SI _____ **NO** _____

15. ¿Utilizan dispositivos extraíbles para guardar las copias de seguridad?

SI _____ **NO** _____

16. ¿Existe software anti espía instalado en los equipos de cómputo?

SI _____ **NO** _____

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

JUAN PABLO ALVAREZ
Encargado Área de Sistemas
Entrevistado

Anexo 21 CheckList binario para la evaluación a la seguridad lógica (CHL03).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001
CHECK-LIST BINARIO



PT. No. **CHL03**

EMPRESA: Alcaldía Municipal de Ábrego
AREA: Seguridad Lógica
OBJETIVO: Evaluar la seguridad lógica y los controles para el acceso a los sistemas de información de la Alcaldía Municipal.

Elaboró: J.A.A.B.

Fecha: 22-03-2014

Revisó: M.R.S.R.

Fecha: 26-03-2014

ITEM	PREGUNTAS	S	N	R/PT	RESPONSABLE
1	¿Se restringe el uso de equipos de cómputo solo al personal autorizado por la Alcaldía?	X		AFO07	J.A.A.B.
2	¿Los sistemas de información que están presentes en la Alcaldía cuentan con un sistema de contraseñas para su ingreso?	X		AIM01	
3	¿Los empleados cuentan con claves únicas y exclusivas para cada sistema?	X			
4	¿Las personas que laboran en la Alcaldía están conscientes de la importancia de la información que ellos manipulan?		X		
5	¿Existen algún tipo de control para el acceso a los sistemas?		X		
6	¿Se capacita periódicamente a los empleados para el buen uso de sus sistemas?		X		
7	¿Se realiza copias de seguridad de la información que se genere dentro de las instalaciones de la Alcaldía?	X		AIM03	
8	¿Los sistemas de cómputo de la Alcaldía cuentan con programas de detección de intrusos?		X		
9	¿Los equipos de cómputo cuentan con software antivirus?	X			
10	¿Realizan diariamente actualizaciones a las bases de datos de los antivirus		X	AIM05	

	que posee los equipos de cómputo?			
11	¿Existen restricciones a la hora de instalar aplicaciones sin previa autorización?		X	
12	¿El software que está instalado en los equipos de cómputo de la Alcaldía presenta licencias?		X	
13	¿Se atienden las fallas que les ocurran al software?		X	
14	¿La Alcaldía cuenta con políticas de seguridad de información y están documentadas?		X	
15	¿Utilizan dispositivos extraíbles para guardar las copias de seguridad?		X	
16	<p>¿Qué tipo de software antiespía presenta los equipos de cómputo?</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor CHL03: Lista de Chequeo No. 3 AFO07: Archivo Fotográfico No. 7 AIM01: Archivo de Imágenes No. 1 AIM03: Archivo de Imágenes No. 3 AIM05: Archivo de Imágenes No. 5</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>ANALISIS CUALITATIVO</p> <p>Después de analizar las respuestas dadas por el ingeniero a cargo del área de sistemas de la Alcaldía Municipal, se puede concluir que los controles en cuanto a la seguridad lógica son aceptables, pero a su vez necesitan mejorar tanto los controles que posean actualmente como de implementar más controles que ayuden a mitigar fallas que se presenten con lo relacionado a la seguridad lógica.</p> </div>		X	

Anexo 22. Archivo fotográfico N° 7 (AF007).

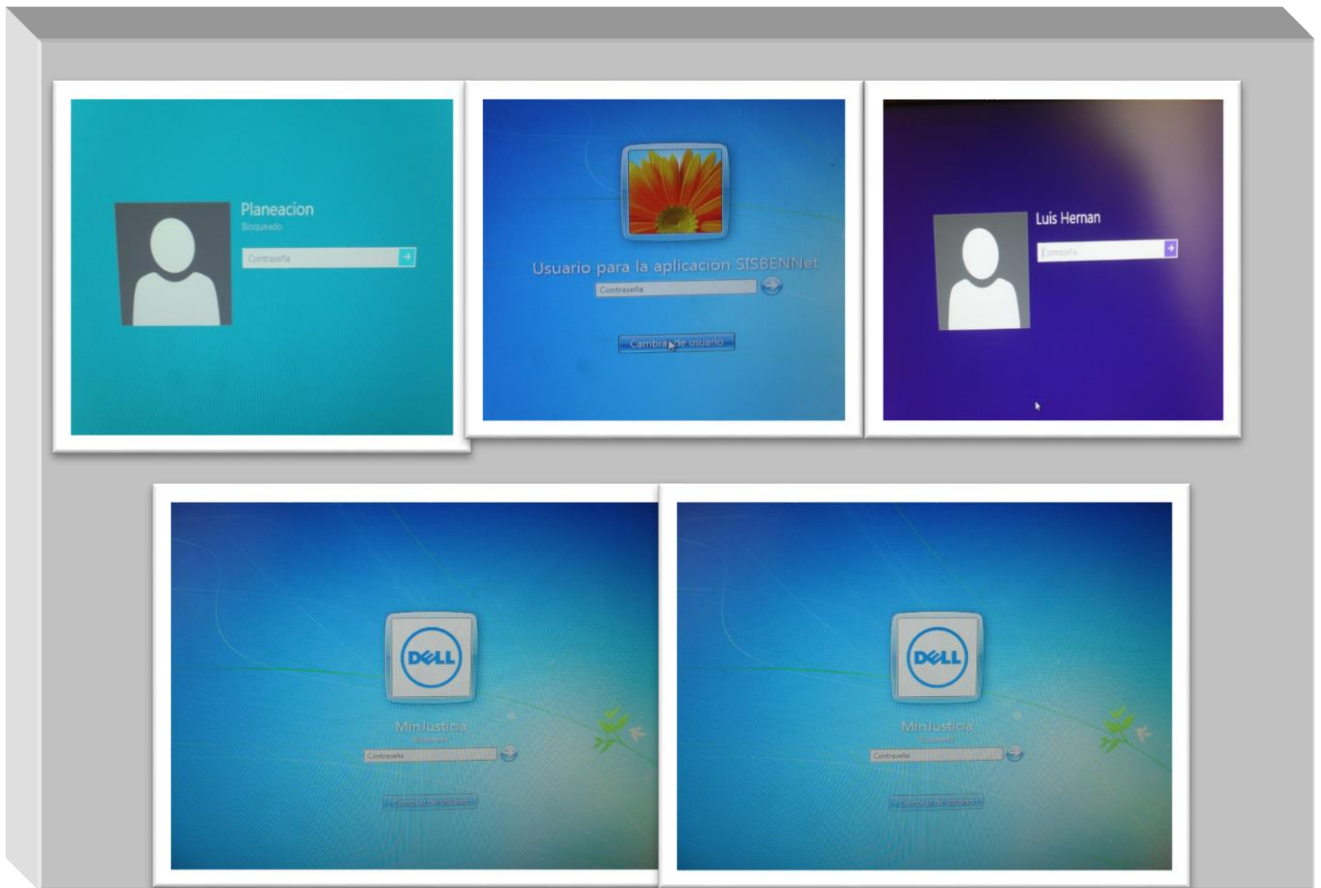


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ABREGO



PT. No. AFO07

ARCHIVO FOTográfico No. 7



En estas imágenes se puede observar que todos los equipos de cómputo tanto de la Alcaldía Municipal como los del Centro de Convivencia presentan sistemas de autenticación a la hora de encender los equipos y cada funcionario tiene su propia clave para el ingreso a cada equipo.

Anexo 23. Archivo de imágenes N° 3 (AIM03).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS
SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. **AIM01**

ARCHIVO DE IMÁGENES No. 1



Las siguientes imágenes corresponden a los sistemas de autenticación de los sistemas de información que presenta actualmente la Alcaldía Municipal.

Anexo 24. Archivo de imágenes N° 5 (AIM05).

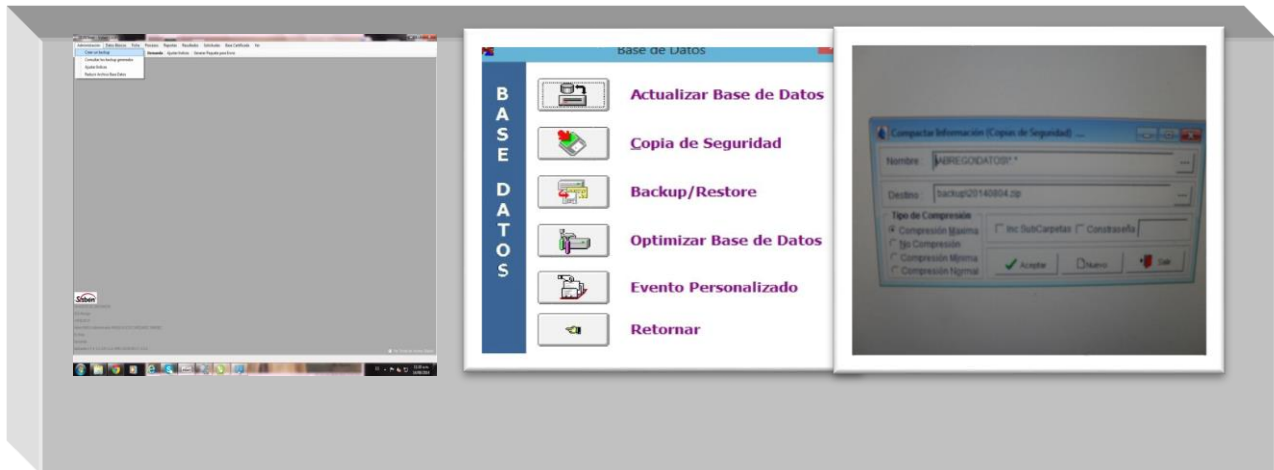


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. AIM03

ARCHIVO DE IMÁGENES No. 3



Se observa los sistemas de información que generan copias de seguridad de la información que poseen, cabe resaltar que estos son las aplicaciones que son propias de la Alcaldía Municipal, ya que las demás aplicaciones son plataformas web y están centralizadas en Bogotá.

Anexo 25. Archivo de imágenes No 5 (AIM05).

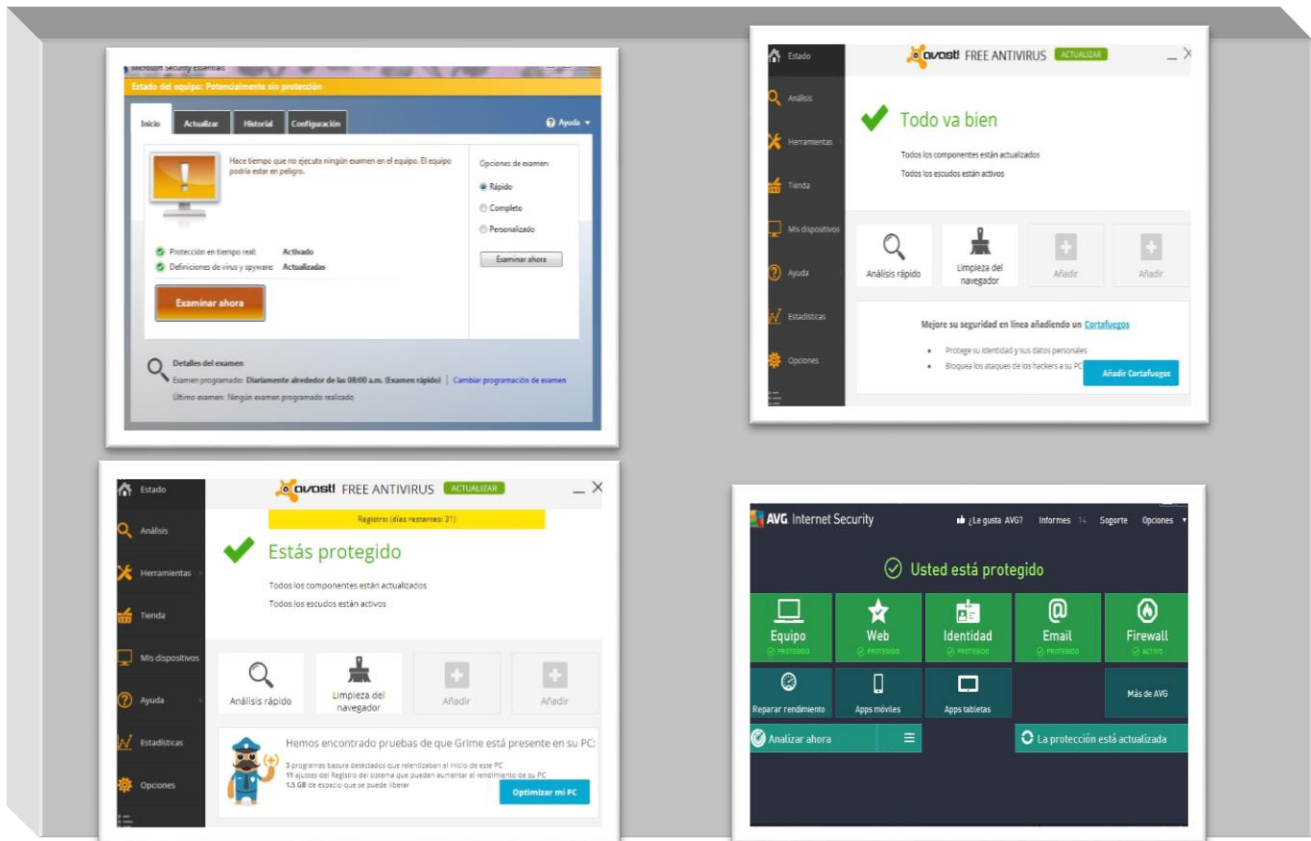


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS
SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO



PT. No. **AIM05**

ARCHIVO DE IMAGENES No. 5



En estas imágenes se muestran los diferentes programas antivirus que poseen los equipos de cómputo de la Alcaldía Municipal y el Centro de Convivencia, además algunos equipos tiene sus antivirus en periodo de prueba.

Anexo 26. Formato de verificación seguridad lógica (FVE03).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ABREGO



PT. No. **FVE03**

Empresa: Alcaldía Municipal de Ábrego, Norte de Santander Área o Proceso: Seguridad Lógica	Fecha Elaboración: <u>22/04/2014</u> Fecha Revisión: <u>26/04/2014</u>
---	---

Objetivo
 Evaluar la seguridad lógica y los controles para el acceso a los sistemas de información de la Alcaldía Municipal.

No.	ACTIVIDAD	SI	NO	R/PT	OBSERVACIONES	AUDITOR
1	Autenticación para ingreso a los equipos de computo	X		<u>AFO07</u>	Los equipos de cómputo tanto de la Alcaldía Municipal como los del centro de convivencia poseen sistema de autenticación para ingresar a los equipos.	J.A.A.B.
2	Autenticación sistema de información alcaldía municipal	X		<u>AIM01</u>	Cada sistema de información que posee la Alcaldía Municipal cuenta con claves de acceso a dichos sistemas, los cuales son dados por los proveedores de estos sistemas. El	

					centro de convivencia no cuenta con sistemas de información en ninguna de sus dependencias.
4	Copias de seguridad	X		<u>AIM03</u>	Los funcionarios que manipulan sistemas de información en la Alcaldía Municipal generan diariamente copias de seguridad, incluso varios funcionarios realizan varias copias diarias de la información que manipularon. Pero algunos funcionarios no guardan las copias de seguridad en memorias sino que los deja dichos archivos en los mismos equipos.
5	Antivirus actualizado	X		<u>AIM05</u>	Los funcionarios que trabajan con equipos de cómputo realizan de forma automática la actualización de los antivirus, pero

					hay unos equipos que poseen estos programas antivirus de periodo de prueba.
6	Licencias sistemas operativos			X	Solamente los equipos que están instalados en el centro de convivencia presentan licencias de sus sistemas operativos, el cual es Windows 7 professional.
7	Programas de detección de intrusos			X	Ningún equipo de cómputo de la Alcaldía Municipal o del centro de convivencia presenta programas de detección de intrusos.
8	Políticas de seguridad de la información			X	Tanto la Alcaldía Municipal como en el centro de convivencia no poseen políticas de seguridad para la protección de la información que se genera en dichas instalaciones.

9	Utilización de dispositivos extraíbles para almacenar copias de seguridad generados por los sistemas de información	X			Las dependencias que trabajan con sistemas de información, utilizan dispositivos como memorias y cd's para el almacenamiento de las copias de seguridad generados por dichos sistemas.
10	Licencias sistemas de información	X			Cada sistema de información utilizado para facilitar los servicios de la Alcaldía Municipal, cuenta con sus respectivas licencias otorgadas por los proveedores de dichos sistemas de información.
MARCAS O TILDES UTILIZADAS					
FVE03: Formato de verificación No. 1 AFO07: Archivo Fotográfico No. 7 AIM01: Archivo de Imágenes No. 1 AIM03: Archivo de Imágenes No. 3 AIM05: Archivo de Imágenes No. 5 J.A.A.B. Jhon Alexander Álvarez Bayona – Auditor					

Anexo 27. Evaluación al servicio de mantenimiento de equipos (EME04).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL
ESTANDAR ISO/IEC 27001



ENCUESTA SOBRE MANTENIMIENTO DE EQUIPOS

Aplicada a: Ing. JUAN PABLO ALVAREZ – Encargado del área de Sistemas

Objetivo: Encuesta realizada para recolectar información acerca sobre el servicio de mantenimiento de equipos de la Alcaldía municipal.

1. ¿Existe un plan de mantenimiento preventivo a los equipos de cómputo de la Alcaldía Municipal?

2. ¿Cómo se lleva a cabo el mantenimiento preventivo a los equipos de cómputo?

3. ¿Quién es el encargado de realizar el mantenimiento preventivo de los equipos de cómputo?

4. ¿Cada cuánto se realiza el mantenimiento a los equipos de cómputo de la Alcaldía Municipal?

5. ¿Cómo es el proceso de notificación de las fallas en los equipos de cómputo y a quién se notifican?

6. ¿Cuánto tiempo tardan dichas solicitudes en ser atendidas?

7. ¿Cuánto tiempo tardan los equipos en ser reparados o solucionados los problemas con las aplicaciones de software?

8. ¿Cómo se realiza el mantenimiento a las aplicaciones de software instaladas en los equipos de cómputo, especialmente a aquellas que soportan la información crítica de la Alcaldía Municipal?

9. ¿Cómo se lleva el registro del mantenimiento tanto de hardware como de software en la Alcaldía Municipal de Ábrego?

10. ¿Se realizan copias de respaldo de la información de los equipos de cómputo antes de realizar el mantenimiento?

11. ¿Cuáles son las fallas más frecuentes reportadas por los usuarios de los equipos de cómputo?

12. ¿Qué procedimiento implementa el área de sistemas, para el caso en el que se presente algún inconveniente con un equipo de cómputo o en su defecto con una aplicación de software, y el equipo o la aplicación necesiten ser retirados?

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

JUAN PABLO ALVAREZ
Encargado Área de Sistemas
Entrevistado

Anexo 28. CheckList al servicio de mantenimiento de equipos (CHL04).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ABREGO – ISO/IEC 27001



PT. No. **CHL04**

EMPRESA: Alcaldía Municipal de Ábrego
AREA: Seguridad Física
OBJETIVO: Verificar la existencia de planes de mantenimiento de equipos.

Elaboró: J.A.A.B. **Fecha:** 27-03-2014
Revisó: M.R.S.R. **Fecha:** 02-04-2014

ITEM	PREGUNTAS	R/PT	RESPONSABLE
1	¿Existe un plan de mantenimiento preventivo a los equipos de cómputo de la Alcaldía Municipal?		J.A.A.B.
RTA	La Alcaldía Municipal no cuenta actualmente con un plan para el mantenimiento preventivo a los equipos de cómputo.		
2	¿Cómo se lleva a cabo el mantenimiento preventivo a los equipos de cómputo?		
RTA	Mediante hojas de registro de las fallas presentadas en los equipos de cómputo.		
3	¿Quién es el encargado de realizar el mantenimiento preventivo de los equipos de cómputo?		
RTA	El ingeniero de soporte es el encargado de realizar el mantenimiento preventivo a los equipos de cómputo.		
4	¿Cada cuánto se realiza el mantenimiento a los equipos de cómputo de la Alcaldía Municipal?		
RTA	El mantenimiento preventivo a los equipos de cómputo tanto de la Alcaldía Municipal como a los del centro de convivencia se realiza 2 veces al año.		
5	¿Cómo se notifica las fallas que se vean reflejadas con el mantenimiento de los equipos de cómputo?		
RTA	Se llama mediante el almacenista al ingeniero de soporte para notificar las fallas que		

	posean a los equipos de computo.		
6	¿Cómo se atienden las fallas encontradas en el mantenimiento de equipos de cómputo?		
RTA			
7	¿Se realizan copias de respaldo de la información de los equipos de cómputo antes de realizar el mantenimiento?		
RTA	Si se realizan copias de respaldo de la información de los equipos de cómputo.		
8	¿Qué tipo de fallas se encuentran en el mantenimiento de los equipos de cómputo de la Alcaldía?		
RTA	Virus.		

MARCAS O TILDES

J.A.A.B: Jhon Alexander Álvarez Bayona- Auditor
--

M.R.S.R: Magreth Rossio sanguino Reyes- Directora Proyecto

Anexo 29. Evaluación a la red de datos (ERD05).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL
ESTANDAR ISO/IEC 27001



ENCUESTAS SOBRE LA RED DE DATOS

Aplicada a: Ing. JUAN PABLO ALVAREZ – Encargado del área de Sistemas

Objetivo: Encuesta realizada para la recolección de información correspondiente a la red de datos de la Alcaldía municipal

1. ¿La Alcaldía en su red de datos cuenta con su propio correo institucional para la transferencia de información confidencial?

2. ¿Qué servicios son soportados por la red de datos de la Alcaldía Municipal?

3. ¿Qué restricciones hay a la hora de transferir información por la red de datos?

4. ¿Qué servicios están restringidos en la red? ¿Qué mecanismos utilizan?

5. ¿Las instalaciones de la red de datos cuentan con normas técnicas de cableado estructurado?

6. ¿La conexión de datos es independiente de la conexión eléctrica?



7. ¿A quién recurren en caso de que se presente una falla en la red de datos?

8. ¿Qué tipo de tecnología es utilizada en la red de datos de la Alcaldía?

JHON ALEXANDER ALVAREZ
Estudiante encargado Auditoría
Entrevistador

JUAN PABLO ALVAREZ
Encargado Área de Sistemas
Entrevistado

Anexo 30. CheckList para evaluar la red de datos (CHL05).

 <p style="text-align: center;">UNIVERSIDAD FRANCISCO DE PAULA SANTANDER FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS EVALUACIÓN FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO, MEDIANTE EL ESTANDAR ISO/IEC 27001 CHECK-LIST DE RANGO</p> 								
								PT. No. CHL05
EMPRESA: Alcaldía Municipal de Ábrego AREA: Red de datos OBJETIVO: Realizar un CheckList binario para evaluar lo relacionado a la red de datos en la Alcaldía Municipal								
Elaboró: <u>J.A.A.B.</u>							Fecha: 03-04-2014	
Revisó: <u>M.R.S.R</u>							Fecha: 06-04-2014	
ITEM	PREGUNTAS	O	B	R	M	D	R/PT	RESPONSABLE
1	¿La Alcaldía en su red de datos cuenta con su propio correo institucional para la transferencia de información confidencial?		X					J.A.A.B
2	¿Qué servicios son soportados por la red de datos de la Alcaldía Municipal?		X					
3	¿Qué restricciones hay a la hora de transferir información por la red de datos?				X			
4	¿Las instalaciones de la red de datos cuentan con normas técnicas de cableado estructurado?			X				
5	¿Qué tipo de intranet se trabaja		x					

	dentro de las instalaciones de la Alcaldía?							
6	¿A quién recurren en caso de que se presente una falla en la red de datos?			X				
7	¿Qué tipo de tecnología es utilizada en la red de datos de la Alcaldía?			X				
8	¿La conexión de datos es independiente de la conexión eléctrica?		X					
<p>J.A.A.B: Jhon Alexander Álvarez Bayona- auditor M.R.S.R: Magreth Rossio Sanguino Reyes - Director Proyecto CHL05: Lista de chequeo No. 5 O: Optimo=5 B: Bueno=4 R: Regular=3 M: Malo=2 D: Deficiente=1</p>								

Después de aplicar el procedimiento de evaluación del Checklist para la seguridad de la red de datos, se obtuvo el siguiente resultado.

Cantidad de Ítem = 8

Ítem 1 = 4

Ítem 6 = 3

Ítem 2 = 4

Ítem 7 = 3

Ítem 3 = 2

Ítem 8 = 4

Ítem 4 = 3

Ítem 5 = 4

Subtotal = Σ Ítem 1 hasta Ítem 8

Subtotal = 27

Total = Subtotal / Cantidad de ítems

Total = 27 / 8

Total = 3.375 \approx 3.3

Por lo anteriormente descrito en la fórmula, se puede concluir que La Seguridad de la red de datos de la Alcaldía Municipal de Ábrego, Norte de Santander, es **Regular**, puesto que la alcaldía municipal presenta fallas en los controles que les permita implementar protección a la red de datos y de soportar los servicios que son utilizados en la red.

Anexo 31. Encuesta para verificar la protección de los equipos fuera de las instalaciones (ENC01).



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE
INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ABREGO – ISO/IEC 27001



PT No. **ENC01**

EMPRESA: Alcaldía Municipal de Ábrego
AREA: Seguridad Física
OBJETIVO: Verificar la existencia de controles para la seguridad de los equipos fuera de las instalaciones de la Alcaldía Municipal.

Elaboró: J.A.A.B.

Fecha: 20-05-2014

Revisó: M.R.S.R.

Fecha: 23-05-2014

ITEM	PREGUNTAS	R/PT	RESPONSABLE
1	¿Qué situaciones pueden motivar la autorización de la salida de equipos de cómputo de la Alcaldía Municipal?		J.A.A.B.
	RTA: Cuando hay falla del sistema, también cuando algún funcionario necesita terminar algún trabajo.		
2	¿Existe algún formato o documento que registre esta autorización?	FSE08	
	RTA: Si poseen un formato para registrar las autorizaciones de retiro de equipos.		
3	¿Qué dependencia se encarga de manejar estos registros?		
	RTA: Almacén y gestión documental.		
4	¿Qué mecanismo de protección es implementado para preservar tanto la información como el equipo que sale de las instalaciones de la Alcaldía Municipal?		
	RTA: No se implementa ningún mecanismo para preservar tanto equipos como información.		
5	¿Por cuánto tiempo permanecen los equipos de cómputo fuera de las instalaciones		

de la Alcaldía Municipal?

RTA:

Los equipos de cómputo pueden estar por fuera de las instalaciones 12 horas o más.

6 ¿Qué procedimiento se implementa cuando se da de baja a los equipos de cómputo?

RTA:

Por el momento no se ha dado de baja ningún equipo de cómputo.

7 ¿Qué pasa con la información contenida en esos equipos?

RTA:

La información se guarda en memorias USB o en CD-DVD.

8 ¿Qué destino final tienen esos equipos?

RTA:

Los pocos equipos que presentan fallas el ingeniero los arregla en cada dependencia.

Anexo 32. Archivo de imágenes N° 4. (AIM04).

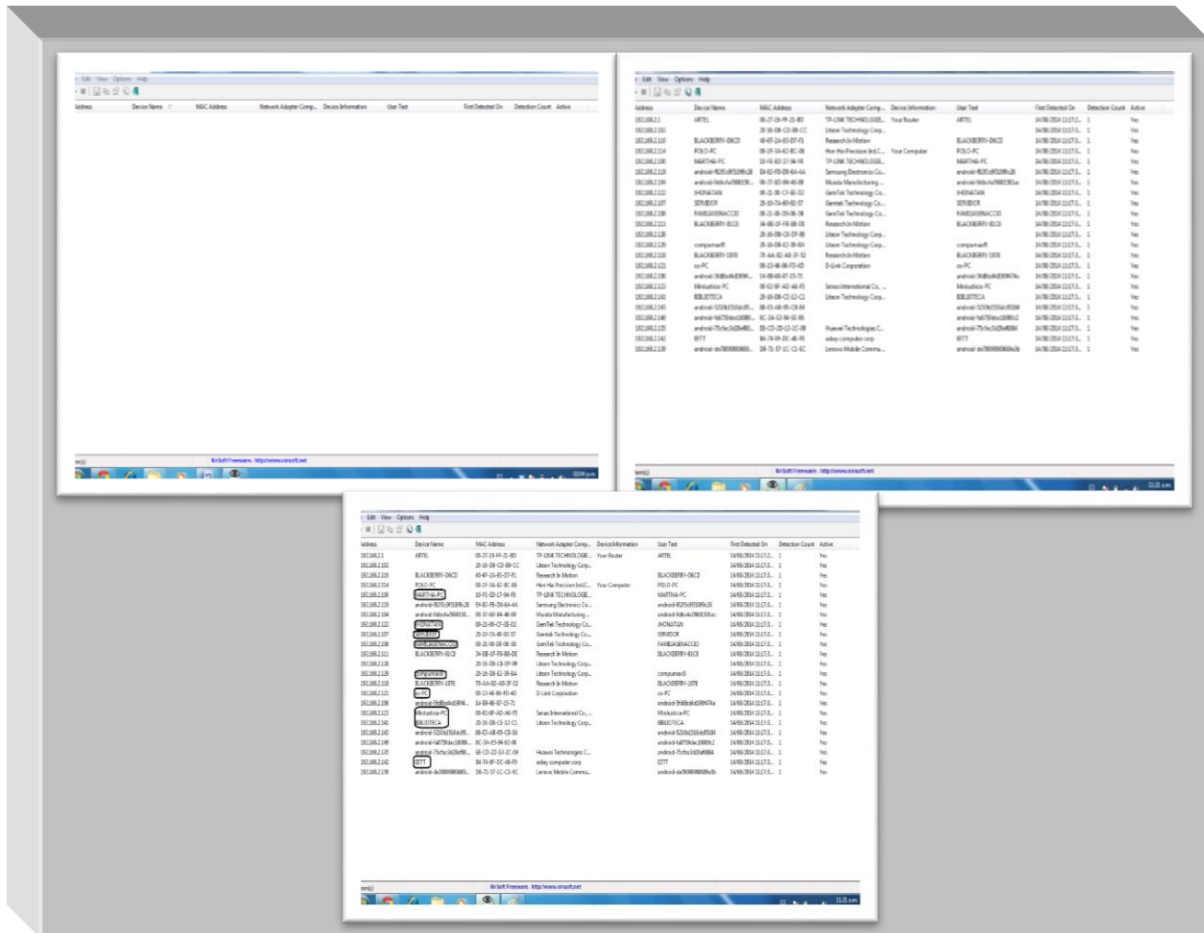


**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS
SISTEMAS DE INFORMACIÓN DE LA
ALCALDÍA MUNICIPAL DE ÁBREGO.**



PT. No. **AIM04**

ARCHIVO DE IMAGENES No. 4



Mediante el uso de una herramienta llamada Wireless Network Watcher versión 1.32, lo cual consiste en hacer un barrido de direcciones IP para verificar los dispositivos que ingresan sin autorización.

Anexo 33. Archivo de imágenes No. 2 (AIM02).

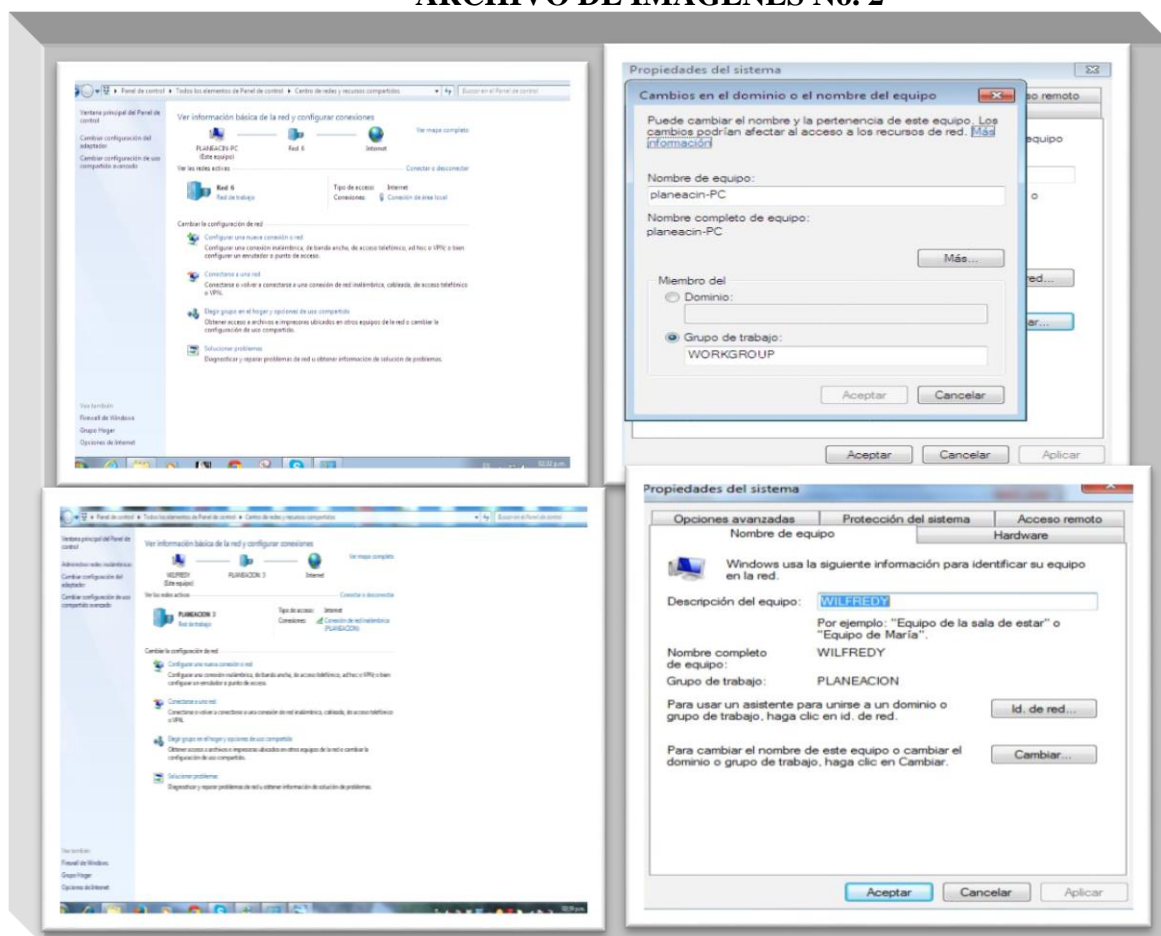


UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS
EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE
LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA
MUNICIPAL DE ÁBREGO





PT. No. AIM02

ARCHIVO DE IMÁGENES No. 2



En estas imágenes se ven las diferentes ubicaciones de red que poseen los equipos de cómputo tanto de la Alcaldía Municipal como los del Centro de Convivencia.



Anexo 34. Hallazgos seguridad física (HAZ01).

 <p style="text-align: center;"> UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001 </p> 			
			PT. No. <u>HAZ01</u>
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander			
Área o Proceso: red de datos		Fecha: <u>18/05/2014</u>	
REF.	SITUACION	CAUSAS	SOLUCIÓN
1	Los equipos al conectarse a la red cableada tienen tres (3) opciones para configurar su red: como red pública, red privada o red doméstica, la alcaldía no tiene definido una política a la hora de definir a qué grupo se deben conectar los empleados en la red.	Falta de conocimiento de los empleados de la Alcaldía Municipal a la hora de configurar a qué tipo de red desean conectarse (red pública, red doméstica. red pública).	Se recomienda emplear políticas de autenticación a la hora de conectarse a la red, ya sea que se configure en una red pública o en una red privada dependiendo de la situación. También se recomienda configurar los equipos para que se identifiquen en una red privada ya que brinda mayor seguridad y confiabilidad que una red pública. Se recomienda asignar a cada dependencia una ubicación de red específica para sus equipos, evitando que otras dependencias tengan la misma ubicación en la red provocando alguna falla en la seguridad.
2	Se pudo evidenciar que existen equipos y otros dispositivos móviles que no pertenecen a la Alcaldía Municipal y que se encuentran conectados de forma permanente a la red inalámbrica de la	Teniendo en cuenta que debido a que no existe personal del área de sistemas de forma permanente en la Alcaldía y para evitar traumatismos en los	1 Se recomienda cambiar la configuración de los router's a un protocolo estático y realizar el registro de los equipos que necesiten trabajar con las conexiones inalámbricas existentes.

	misma.	accesos a Internet por parte de los entes reguladores, la configuración de los router's se realizó de forma dinámica a través del protocolo DHCP. De igual manera, la divulgación desmesurada de las claves de acceso a las conexiones inalámbricas ha permitido que usuarios externos puedan tener acceso a dicha red.	2. Cambiar periódicamente las claves de acceso a las conexiones inalámbricas.
3	<p>1. Tanto la Alcaldía Municipal como el centro de convivencia cuentan con un switch para cada instalación, pero dichos dispositivos no son administrables, por tal motivo no se puede acceder a ellos y poder configurarlos de manera óptima. Además el dispositivo de red de la Alcaldía Municipal se encuentra abierto y visible al público al igual que el del centro de convivencia con la diferencia de que dicho dispositivo se encuentra en su gabinete con llave.</p> <p>2. El diseño de la red cableada tanto de la Alcaldía Municipal como en el centro de convivencia no se les entregó los diseños de la red cableada, para verificar el tipo de cableado, los protocolos empleados y si se utilizó estándares actualizados para el diseño de redes cableadas.</p> <p>3. El cableado utilizado actualmente por</p>	<p>1. Falta de conocimiento acerca de dispositivos que pueden ser administrables.</p> <p>2. Falta de interés por parte de los administradores de la Alcaldía Municipal y del centro de convivencia de solicitar la documentación para observar como fue el diseño de sus redes.</p> <p>3. Poco conocimiento sobre los estándares de cableado de red de datos empleados actualmente.</p>	<p>1. Adquirir dispositivos de red que sean administrables para poder subnetear la red cableada y administrar mejor los servicios que se trabajen por este medio.</p> <p>2. Verificar mediante un especialista en diseño de redes, el estado actual de sus redes tanto de la Alcaldía Municipal como del Centro de Convivencia y posteriormente se genere documentación de lo que se encuentre.</p> <p>3. Cambiar el tipo de cableado de red utilizado actualmente en estas instalaciones, para pasar al cableado utp categoría 7 y a su vez el cambio de los conectores para dicho cable, ya que brinda mayor protección contra interferencias y se maneja mayores velocidades de transmisión.</p>

<p>la Alcaldía Municipal para la red cableada es utp de categoría 5E y 6, el cual se encuentra sin una buena organización desde el punto en donde se encuentra el dispositivo de red hasta las demás dependencias, por otra parte el cableado utilizado en el centro de convivencia es utp de categoría 6 y dicho cable es pasado a las demás dependencias por medio de canaletas.</p>		
<p style="text-align: center;">ELABORADO POR: JHON ALEXANDER ALVAREZ BAYONA Auditor</p>		<p style="text-align: center;">REVISADO POR MAGRETH ROSSIO SANGUINO REYES Directora proyecto</p>



Anexo 35. Hallazgos seguridad lógica (HAZ02).

 <p style="text-align: center;">UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 			
			PT. No. <u>HAZ02</u>
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander			
Área o Proceso: seguridad física		Fecha: <u>20/05/2014</u>	
REF.	SITUACION	CAUSAS	SOLUCIÓN
1	<p>1. No poseen perímetro de seguridad como barreras que bloqueen el ingreso a terceros o áreas de recepción a cada dependencia.</p> <p>2. Existe solamente un formato para registrar los equipos de cómputo que son sacados de las instalaciones de la alcaldía municipal y del centro de convivencia, tanto la seguridad del equipo como de la información almacenada corren por cuenta de la persona que solicita dicho equipo.</p> <p>3. No se observa cámaras de vigilancia tanto en las dependencias que se maneja información crítica como en las afueras de las instalaciones.</p>	<p>No existe voluntad por parte de la Alcaldía Municipal, para planear e implementar controles más efectivos respecto al acceso físico en las instalaciones de la Alcaldía Municipal.</p>	<p>Implementar políticas de seguridad para el acceso físico, como entradas con autenticación de usuarios, barreras que limiten el acceso a terceros a los equipos e información de cada dependencia, también de la utilización de cámaras de vigilancia en cada dependencia como dentro de las instalaciones de la Alcaldía Municipal y del Centro de Convivencia, así mismo, de implementar áreas de recepción para llevar una mejor organización y garantizar seguridad a las actividades realizadas en dichas dependencias.</p>
2	<p>Después de revisar tanto la información suministrada por el ingeniero, como de la verificación de la información dada, estos son los hallazgos que se observaron:</p> <p>1. Tanto la Alcaldía Municipal como el Centro de Convivencia cuenta con</p>	<p>El poco conocimiento de los administradores de la alcaldía municipal, en cuanto a mejorar controles existentes o de implementar controles mejores para la seguridad de sus</p>	<p>Se recomienda diseñar, construir, implementar y capacitar un plan de contingencia en que se detallen las actividades que ayuden a garantizar el buen funcionamiento tanto sus sistemas de cómputo como de su infraestructura,</p>

<p>dispositivos como ups y reguladores de voltaje, pero las ups de la Alcaldía Municipal están averiadas y se utilizan como multitomas, mientras que la ups que se encuentra en el centro de convivencia está en buen estado y tiene capacidad para soportar energía por media hora.</p> <p>2. La Alcaldía Municipal dentro de sus instalaciones cuenta con dos extintores, uno por cada piso con su respectivo manual de uso. En cambio el Centro de Convivencia al ser una edificación moderna no cuenta con extintores en sus instalaciones.</p> <p>3. La Alcaldía Municipal como el Centro de Convivencia cuenta con independencia tanto el cableado eléctrico como el cableado de telecomunicaciones, pero en el centro de convivencia la red eléctrica es regulada ya que la instalación eléctrica para los equipos de cómputo es independiente de la instalación eléctrica del edificio.</p> <p>4. No se cuenta con alarmas contra incendios, así como de sistemas de detección de humo, tampoco se cuenta con avisos formales de no ingerir comidas si manipulan equipos de cómputo, del manejo apropiado de dichos equipos.</p> <p>5. Solamente una sección de la dependencia de planeación y la oficina del</p>	<p>equipos de amenazas externas e internas, ya que se ve que no se le presta mayor atención a esto por falta de conocimiento de estos temas.</p>	<p>incorporando mecanismos que minimicen daños de los equipos por causas de fluido eléctrico o por incendios.</p> <p>Además de empelar avisos formales que ayuden mejoran los avisos que se utiliza actualmente como a los que no se presentan allí.</p> <p>Implementar extintores para las instalaciones del centro de convivencia. La Alcaldía Municipal debe adoptar mejores dispositivos para contrarrestar falas en el suministro eléctrico.</p> <p>Implementar sistemas de refrigeración de aire acondicionado para las dependencias y tanto de la Alcaldía Municipal como las del Centro de Convivencia, para mitigar los daños a los equipos por exponerse a temperaturas altas.</p> <p>Adquirir pararrayos para evitar daños a los equipos de cómputo por descargas eléctricas</p>
---	--	---

<p>despacho de la personería cuentan con sistema de refrigeración de aire acondicionado, algunas dependencias cuentan con ventiladores.</p> <p>6. La salida de emergencia esta con su respectiva señalización pero a su vez es demasiado estrecha y siempre está cerrada con candado. No existe cámara de vigilancia para esta salida. El Centro de Convivencia dentro de sus instalaciones no se encuentra señalizaciones para marcar las salidas de emergencia.</p> <p>7. Dentro de las instalaciones de la Alcaldía Municipal no se ve reflejado dispositivos que marquen la humedad en cada dependencia tanto en los equipos donde se procesa información como dispositivos de red con que se cuenta.</p> <p>8. Tanto la Alcaldía Municipal como el Centro de Convivencia no cuentan con pararrayos para proteger sus equipos de cómputo a causa de descargas eléctricas.</p> <p>9. Actualmente la Alcaldía Municipal no posee un plan de contingencias documentado.</p>		
<p style="text-align: center;">ELABORADO POR:</p> <p style="text-align: center;">JHON ALEXANDER ALVAREZ BAYONA Auditor</p>	<p style="text-align: center;">REVISADO POR</p> <p style="text-align: center;">MAGRETH ROSSIO SANGUINO REYES Directora proyecto</p>	

Anexo. 36. Hallazgos red de datos (HZA03)

 <p style="text-align: center;">UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 			
			PT. No. HAZ03
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander			
Área o Proceso: red de datos		Fecha: 28/05/2014	
REF.	SITUACION	CAUSAS	SOLUCIÓN
1	Los funcionarios que manipulan sistemas de información en la Alcaldía Municipal generan diariamente copias de seguridad, incluso varios funcionarios realizan varias copias diarias de la información que manipularon. Pero algunos funcionarios no guardan las copias de seguridad en memorias sino que los deja dichos archivos en los mismos equipos.	Falta de interés y conocimientos por parte de los funcionarios de la Alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.	Modificar el procedimiento de copias de seguridad mediante la contratación de un data center.
2	Los antivirus de algunas equipos de cómputo son descargados por internet, lo cual significa que tiene un periodo de prueba de un mes para su uso, después de esto no se actualizan.	Falta de interés y conocimientos por parte de los funcionarios de la Alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de	Adquisición de licencias de software antivirus para garantizar la protección de los equipos de cómputo frentes a fallas producidas por agentes maliciosos transportados por memorias o por navegar o descargar contenido por internet

		implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.	
3	Solamente los equipos que están instalados en el Centro de Convivencia presentan licencias de sus sistemas operativos, el cual es Windows 7 professional.	Falta de interés y conocimientos por parte de los funcionarios de la alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.	Adquirir licencias de sistema operativo para los equipos de la Alcaldía Municipal, para brindar un mejor comportamiento del equipo de cómputo en las actividades realizadas en dicho equipo
4	Ningún equipo de cómputo de la Alcaldía Municipal o del Centro de Convivencia presenta programas de detección de intrusos, solamente cuenta con la protección de los programas antivirus.	Falta de interés y conocimientos por parte de los funcionarios de la alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.	Implementar dentro de los equipos de cómputo sistemas de protección contra intrusos en las diferentes dependencias que posea la Alcaldía Municipal y el Centro de Convivencia.
5	Tanto la Alcaldía Municipal como en el Centro de Convivencia no poseen políticas	Falta de interés y conocimientos por parte de los	Diseñar, construir e implementar políticas de seguridad de la información

	<p>de seguridad para la protección de la información que se genera en dichas instalaciones.</p>	<p>funcionarios de la Alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.</p>	<p>que se genere en los sistemas de información usados en la Alcaldía Municipal.</p>
<p>ELABORADO POR: JHON ALEXANDER ALVAREZ BAYONA Auditor</p>		<p>REVISADO POR MAGRETH ROSSIO SANGUINO REYES Directora proyecto</p>	

Anexo 37. Prueba sustantiva N° 1 (PSU01).

		UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001			
PT. No. <u>PSU01</u>					
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander				Fecha realización: <u>05/05/2014</u>	
Área o Proceso: Red de Datos					
OBJETIVO					
Verificar la existencia y eficiencia de los controles de acceso a la red cableada que soporta los servicios de la Alcaldía Municipal a través de pruebas sustantivas.					
TÉCNICA EMPLEADA: Observación					
TIPO DE PRUEBA		Cumplimiento ____	Sustantiva <u> x </u>	Doble Finalidad ____	
PROCEDIMIENTO A EMPLEAR					
<ol style="list-style-type: none"> 1. Ingresar a cada equipo de la red para verificar su identificación en la misma. 2. Verificar el (los) grupo(s) de trabajo al que pertenece cada equipo. 3. Verificar la existencia de sistemas de login a cada uno de los equipos de la red de datos. 					
RECURSOS:					
Acceso a los equipos de cómputo.					
RESULTADOS DE LA PRUEBA					
HALLAZGOS					R/PT
Los equipos al conectarse a la red cableada tienen tres (3) opciones para configurar su red: como red pública, red privada o red doméstica, la alcaldía no tiene definido una política a la hora de definir a qué grupo se deben conectar los empleados en la red.					<u>AIM02</u>
CAUSA					
Falta de conocimiento de los empleados de la Alcaldía Municipal a la hora de configurar a qué tipo de red desean conectarse (red pública, red doméstica, red pública).					

SITUACIÓN DE RIESGO QUE GENERA

Pérdida de información, ya que puede existir la posibilidad de que varias dependencias tengan la misma ubicación de red lo que ocasiona que se puedan ver dentro de la red.

RECOMENDACIONES DE AUDITORIA

Se recomienda emplear políticas de autenticación a la hora de conectarse a la red, ya sea que se configure en una red pública o en una red privada dependiendo de la situación. También se recomienda configurar los equipos para que se identifiquen en una red privada ya que brinda mayor seguridad y confiabilidad que una red pública.

Se recomienda asignar a cada dependencia una ubicación de red específica para sus equipos, evitando que otras dependencias tengan la misma ubicación en la red provocando alguna falla en la seguridad.



ELABORADO POR:

JHON ALEXANDER ALVAREZ BAYONA
Auditor

REVISADO POR

MAGRETH ROSSIO SANGUINO REYES
Directora proyecto

Anexo 38. Prueba sustantiva N° 2 (PSU02).

	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001			
PT. No. PSU02				
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander Área o Proceso: Red de Datos Fecha: <u>10/05/2014</u>				
OBJETIVO Verificar la existencia y eficiencia de los controles de acceso a la red inalámbrica de la Alcaldía Municipal de Ábrego a través de pruebas sustantivas.				
TÉCNICA EMPLEADA: Análisis del entorno de conexión inalámbrica mediante software				
TIPO DE PRUEBA	Cumplimiento ____	Sustantiva <u> x </u>	Doble Finalidad ____	
PROCEDIMIENTO A EMPLEAR <ol style="list-style-type: none"> 1. Ejecutar la aplicación Wireless Network Watcher versión 1.71 en un equipo que se conecte a la red inalámbrica que posea la Alcaldía. 2. Realizar un análisis de los equipos que estén ingresando a la red inalámbrica, escaneando por direcciones IP y mostrando en una interfaz sencilla los equipos conectados, el nombre, la MAC, la clase de adaptador, etc. 3. Verificar la existencia de sistemas de logueo en los equipos de la red inalámbrica de la Alcaldía. 				
RECURSOS: Wireless Network Watcher version 1.71				
RESULTADOS DE LA PRUEBA				
HALLAZGOS			R/PT	
Se pudo evidenciar que existen equipos y otros dispositivos móviles que no pertenecen a la Alcaldía Municipal y que se encuentran conectados de forma permanente a la red inalámbrica de la misma.			<u>AIM04</u>	
CAUSA Teniendo en cuenta que debido a que no existe personal del área de sistemas de forma permanente en la Alcaldía y para evitar traumatismos en los accesos a Internet por parte de los entes reguladores, la configuración de los router's se realizó de forma				

dinámica a través del protocolo DHCP. De igual manera, la divulgación desmesurada de las claves de acceso a las conexiones inalámbricas ha permitido que usuarios externos puedan tener acceso a dicha red.

SITUACIONES DE RIESGO QUE GENERA

1. Pérdida de información por el bajo rendimiento de la señal en las conexiones inalámbricas a la hora de enviar información entre dependencias.
2. Posibilidad de accesos no autorizados a información confidencial.
3. Pérdida de integridad de la información.

RECOMENDACIONES DE AUDITORIA

1. Se recomienda cambiar la configuración de los router's a un protocolo estático y realizar el registro de los equipos que necesiten trabajar con las conexiones inalámbricas existentes.
2. Cambiar periódicamente las claves de acceso a las conexiones inalámbricas.

ELABORADO POR:

JHON ALEXANDER ALVAREZ BAYONA



Auditor

REVISADO POR

MAGRETH ROSSIO SANGUINO REYES



Directora proyecto

Anexo 39. Prueba sustantiva N° 3. (PSU03).

 <p>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 	
PT. No. PSU03	
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander Área o Proceso: Red de Datos	Fecha realización: <u>14/05/2014</u>
OBJETIVO Realizar un análisis del entorno de red cableada que posee la Alcaldía Municipal, mediante pruebas sustantivas.	
TÉCNICA EMPLEADA: Observación	
TIPO DE PRUEBA	Cumplimiento ____ Sustantiva <u> x </u> Doble Finalidad ____
PROCEDIMIENTO A EMPLEAR 1. Identificar los dispositivos instalados tanto para la Alcaldía Municipal como en el centro de convivencia. 2. Revisar si presentan estándares para el cableado de red usado actualmente por estas organizaciones.	
RECURSOS: acceso a las instalaciones de la Alcaldía Municipal y el centro de convivencia.	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	R/PT
1. Tanto la alcaldía municipal como el centro de convivencia cuentan con un switch para cada instalación, pero dichos dispositivos no son administrables, por tal motivo no se puede acceder a ellos y poder configurarlos de manera óptima. Además el dispositivo de red de la Alcaldía Municipal se encuentra abierto y visible al público al igual que el del centro de convivencia con la diferencia de que dicho dispositivo se encuentra en su gabinete con llave. 2. El diseño de la red cableada tanto de la Alcaldía Municipal como en el centro de convivencia no se les entrego los diseños de la red cableada, para verificar el tipo de cableado, los protocolos empleados	<u>AFO11</u>



<p>y si se utilizó estándares actualizados para el diseño de redes cableadas.</p> <p>3. El cableado utilizado actualmente por la Alcaldía Municipal para la red cableada es utp de categoría 5E y 6, el cual se encuentra sin una buena organización desde el punto en donde se encuentra el dispositivo de red hasta las demás dependencias, por otra parte el cableado utilizado en el centro de convivencia es utp de categoría 6 y dicho cable es pasado a las demás dependencias por medio de canaletas.</p>	
<p>CAUSA</p> <ol style="list-style-type: none"> 1. Falta de conocimiento acerca de dispositivos que pueden ser administrables. 2. Falta de interés por parte de los administradores de la Alcaldía Municipal y del centro de convivencia de solicitar la documentación para observar como fue el diseño de sus redes. 3. Poco conocimiento sobre los estándares de cableado de red de datos empleados actualmente. 	
<p>SITUACIÓN DE RIESGO QUE GENERA</p> <p>Daño a equipos, ya que en el caso de la Alcaldía Municipal el dispositivo no se encuentra en un sitio seguro y al estar abierto es propenso a daño tanto de cableado como del mismo dispositivo.</p>	
<p>RECOMENDACIONES DE AUDITORIA</p> <ol style="list-style-type: none"> 1. Adquirir dispositivos de red que sean administrables para poder subnetear la red cableada y administrar mejor los servicios que se trabajen por este medio. 2. Verificar mediante un especialista en diseño de redes, el estado actual de sus redes tanto de la alcaldía municipal como del centro de convivencia y posteriormente se genere documentación de lo que se encuentre. 3. cambiar el tipo de cableado de red utilizado actualmente en estas instalaciones, para pasar al cableado utp categoría 7 y a su vez el cambio de los conectores para dicho cable, ya que brinda mayor protección contra interferencias y se maneja mayores velocidades de transmisión. 	
<p>ELABORADO POR:</p> <p>JHON ALEXANDER ALVAREZ BAYONA Auditor</p>	<p>REVISADO POR:</p> <p>MAGRETH ROSSIO SANGUINO REYES Directora Proyecto</p>

Anexo 40. Prueba sustantiva N° 4 (PSU04).

 <p>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 	
PT. No. PSU04	
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander. Área o Proceso: seguridad física(áreas seguras)	Fecha realización: <u>18/05/2014</u>
Objetivo Evaluar la existencia de controles de acceso a las áreas seguras de las instalaciones de las Alcaldía Municipal de Ábrego a través de lista de chequeo y de corroborar la información obtenida mediante formato de verificación.	
TÉCNICA EMPLEADA: revisión información obtenida por la utilización de listas de chequeo.	
TIPO DE PRUEBA	Cumplimiento ____ Sustantiva <u>x</u> Doble Finalidad ____
PROCEDIMIENTO A EMPLEAR:	
<ol style="list-style-type: none"> 1. Realizar encuesta al ingeniero a cargo del área de sistemas, para obtener información respecto a los controles de acceso físico. 2. Verificar la información entregada por el ingeniero revisando las instalaciones de la alcaldía municipal. 	
RECURSOS	
<ol style="list-style-type: none"> 1. Respuestas entregadas por el ingeniero con la ayuda de la encuesta. 2. Evidencias fotográficas. 	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	R/PT
Tanto la Alcaldía Municipal como en el centro de convivencia presentan fallas en sus controles de acceso, los cuales dichas fallas se reflejan en lo siguiente: <ol style="list-style-type: none"> 1. No poseen perímetro de seguridad como barreras que bloqueen el ingreso a terceros o áreas de recepción a cada dependencia. 	<u>CHL01</u> <u>FVE01</u>

<p>2. Existe solamente un formato para registrar los equipos de cómputo que son sacados de las instalaciones de la alcaldía municipal y del centro de convivencia, tanto la seguridad del equipo como de la información almacenada corren por cuenta de la persona que solicita dicho equipo.</p> <p>3. No se observa cámaras de vigilancia tanto en las dependencias que se maneja información crítica como en las afueras de las instalaciones.</p>	
<p>CAUSA</p>	
<p>No existe voluntad por parte de la Alcaldía Municipal, para planear e implementar controles más efectivos respecto al acceso físico en las instalaciones de la Alcaldía Municipal.</p>	
<p>SITUACIÓN DE RIESGO QUE GENERA</p>	
<p>La deficiencia en los controles para el acceso físico a las instalaciones , puede provocar pérdidas tanto de equipos como de información, provocando que se suspenda las actividades soportadas por dichos activos que posee la Alcaldía Municipal.</p>	
<p>RECOMENDACIONES DE AUDITORIA</p>	
<p>Implementar políticas de seguridad para el acceso físico, como entradas con autenticación de usuarios, barreras que limiten el acceso a terceros a los equipos e información de cada dependencia, también de la utilización de cámaras de vigilancia en cada dependencia como dentro de las instalaciones de la Alcaldía Municipal y del centro de convivencia, así mismo, de implementar áreas de recepción para llevar una mejor organización y garantizar seguridad a las actividades realizadas en dichas dependencias.</p>	
<p>ELABORADO POR:</p> <p>JHON ALEXANDER ALVAREZ BAYONA Auditor</p>	<p>REVISADO POR:</p> <p>MAGRETH ROSSIO SANGUINO REYES Directora Proyecto</p>

Anexo 41. Prueba sustantiva N° 5 (PSU05).

 <p>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 	
PT. No. PSU05	
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander.	Fecha realización: <u>24/05/2014</u>
Área o Proceso: Seguridad física (protección contra amenazas externas e internas)	
Objetivo Evaluar la existencia y eficacia de los controles utilizados para la protección contra amenazas externas e internas, por medio de listas de chequeo y de corroborar la información obtenida mediante formato de verificación.	
TÉCNICA EMPLEADA: revisión información obtenida por la utilización de listas de chequeo.	
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva <u>x</u> Doble Finalidad ___
PROCEDIMIENTO A EMPLEAR: <ol style="list-style-type: none"> 1. Realizar encuesta al ingeniero a cargo del área de sistemas, para obtener información respecto a los controles empleados para la protección de amenazas tanto externas como internas. 2. Tomar evidencias de lo observado dentro de las instalaciones. 	
RECURSOS <ol style="list-style-type: none"> 1 Respuestas entregadas por el ingeniero con la ayuda de la encuesta. 2 Evidencias fotográficas. 	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	R/PT
Después de revisar tanto la información suministrada por el ingeniero, como de la verificación de la información dada, estos son los hallazgos que se observaron: <ol style="list-style-type: none"> 1. Tanto la alcaldía municipal como el centro de convivencia cuenta con dispositivos como ups y reguladores de voltaje, pero las ups de la alcaldía municipal están averiadas y se utilizan como multitomas, mientras que la ups que se encuentra en el centro de convivencia está en buen estado y tiene 	<u>CHL02</u> <u>FVE02</u>

<p>capacidad para soportar energía por media hora.</p> <ol style="list-style-type: none"> 2. La Alcaldía Municipal dentro de sus instalaciones cuenta con dos extintores, uno por cada piso con su respectivo manual de uso. En cambio el centro de convivencia al ser una edificación moderna no cuenta con extintores en sus instalaciones. 3. La alcaldía municipal como el centro de convivencia cuenta con independencia tanto el cableado eléctrico como el cableado de telecomunicaciones, pero en el centro de convivencia la red eléctrica es regulada ya que la instalación eléctrica para los equipos de cómputo es independiente de la instalación eléctrica del edificio. 4. No se cuenta con alarmas contra incendios, así como de sistemas de detección de humo, tampoco se cuenta con avisos formales de no ingerir comidas si manipulan equipos de cómputo, del manejo apropiado de dichos equipos. 5. Solamente una sección de la dependencia de planeación y la oficina del despacho de la personería cuentan con sistema de refrigeración de aire acondicionado, algunas dependencias cuentan con ventiladores. 6. La salida de emergencia esta con su respectiva señalización pero a su vez es demasiado estrecha y siempre está cerrada con candado. No existe cámara de vigilancia para esta salida. El centro de convivencia dentro de sus instalaciones no se encuentran señalizaciones para marcar las salidas de emergencia. 7. Dentro de las instalaciones de la Alcaldía Municipal no se ve reflejado dispositivos que marquen la humedad en cada dependencia tanto en los equipos donde se procesa información como dispositivos de red con que se cuenta. 8. Tanto la Alcaldía Municipal como el centro de convivencia no cuentan con pararrayos para proteger sus equipos de cómputo a causa de descargas eléctricas. 9. Actualmente la alcaldía municipal no posee un plan de contingencias documentado. 	
CAUSA	
<p>El poco conocimiento de los administradores de la alcaldía municipal, en cuanto a mejorar controles existentes o de implementar controles mejores para la seguridad de sus equipos de amenazas externas e internas, ya que se ve que no se le presta mayor atención a esto por falta de conocimiento de estos temas.</p>	
SITUACIÓN DE RIESGO QUE GENERA	
<p>Al no tener conocimiento de los riesgos de no poseer controles para la seguridad de los equipos contra amenazas internas y externas, provocaría tanto daño a los equipos, por no poseer los mecanismos de protección adecuados en caso de fallas de</p>	

suministro eléctrico o de propagación de incendios, así mismo, de pérdida de información al no poseer y capacitar un plan de contingencia para el caso de que sus sistemas de información fallen por alguna eventualidad.

RECOMENDACIONES DE AUDITORIA

Se recomienda diseñar, construir, implementar y capacitar un plan de contingencia en que se detallen las actividades que ayuden a garantizar el buen funcionamiento tanto sus sistemas de cómputo como de su infraestructura, incorporando mecanismos que minimicen daños de los equipos por causas de fluido eléctrico o por incendios.

Además de empelar avisos formales que ayuden mejoran los avisos que se utiliza actualmente como a los que no se presentan allí.

Implementar extintores para las instalaciones del centro de convivencia.

La Alcaldía Municipal debe adoptar mejores dispositivos para contrarrestar falas en el suministro eléctrico

Implementar sistemas de refrigeración de aire acondicionado para las dependencias y tanto de la Alcaldía Municipal como las del centro de convivencia, para mitigar los daños a los equipos por exponerse a temperaturas altas.

Adquirir pararrayos para evitar daños a los equipos de computo por descargas eléctricas



ELABORADO POR:

JHON ALEXANDER ALVAREZ BAYONA
Auditor

REVISADO POR:

MAGRETH ROSSIO SANGUINO REYES
Directora Proyecto

Anexo 42. Prueba sustantiva No. 6 (PSU06).

 <p>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA FACULTAD DE INGENIERIAS PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS EVALUACIÓN DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE ÁBREGO – ISO/IEC 27001</p> 	
PT. No. PSU06	
Empresa: Alcaldía Municipal de Ábrego, Norte de Santander. Área o Proceso: Seguridad lógica	Fecha realización: <u>28/05/2014</u>
Objetivo Verificar la eficiencia de los controles implementados para la seguridad lógica de los sistemas de información de la Alcaldía Municipal mediante listas de chequeo y corroborar la información recolectada mediante formatos de verificación	
TÉCNICA EMPLEADA: Observación.	
TIPO DE PRUEBA	Cumplimiento ___ Sustantiva <u>x</u> Doble Finalidad ___
PROCEDIMIENTO A EMPLEAR: <ol style="list-style-type: none"> 3. Realizar encuesta al ingeniero a cargo del área de sistemas, para obtener información respecto a los controles de acceso físico. 4. Verificar la información entregada por el ingeniero revisando las instalaciones de la Alcaldía Municipal. 	
RECURSOS <ol style="list-style-type: none"> 1 Respuestas entregadas por el ingeniero con la ayuda de la encuesta. 3 Evidencias fotográficas. 	
RESULTADOS DE LA PRUEBA	
HALLAZGOS	R/PT
1. Los funcionarios que manipulan sistemas de información en la Alcaldía Municipal generan diariamente copias de seguridad, incluso varios funcionarios realizan varias copias diarias de la información que manipularon. Pero algunos funcionarios no guardan las copias de seguridad en memorias sino que los deja dichos archivos en los mismos equipos.	<u>CHL03</u> <u>FVE03</u>

<ol style="list-style-type: none"> 2. Los antivirus de algunas equipos de cómputo son descargados por internet, lo cual significa que tiene un periodo de prueba de un mes para su uso, después de esto no se actualizan. 3. Solamente los equipos que están instalados en el centro de convivencia presentan licencias de sus sistemas operativos, el cual es Windows 7 Professional. 4. Ningún equipo de cómputo de la Alcaldía Municipal o del centro de convivencia presenta programas de detección de intrusos, solamente cuenta con la protección de los programas antivirus. 5. Tanto la Alcaldía Municipal como en el centro de convivencia no poseen políticas de seguridad para la protección de la información que se genera en dichas instalaciones. 	
CAUSA	
Falta de interés y conocimientos por parte de los funcionarios de la alcaldía Municipal de los riesgos que puedan surgir de no mejorar sus actuales controles de seguridad lógica y así mismo de implementar nuevos controles que mitiguen el impacto que generaría a sus sistemas algunas fallas en alguno de sus controles de seguridad lógica.	
SITUACIÓN DE RIESGO QUE GENERA	
Pérdida de integridad, confidencialidad y accesibilidad de la información crítica generada por los sistemas de información que actualmente maneja la Alcaldía Municipal.	
RECOMENDACIONES DE AUDITORIA	
<p>Adquirir licencias de sistema operativo para los equipos de la Alcaldía Municipal, para brindar un mejor comportamiento del equipo de cómputo en las actividades realizadas en dicho equipo</p> <p>Adquisición de licencias de software antivirus para garantizar la protección de los equipos de cómputo frente a fallas producidas por agentes maliciosos transportados por memorias o por navegar o descargar contenido por internet.</p> <p>Implementar dentro de los equipos de cómputo sistemas de protección contra intrusos en las diferentes dependencias que posea la alcaldía municipal y el centro de convivencia.</p> <p>Diseñar, construir e implementar políticas de seguridad de la información que se genere en los sistemas de información usados en la Alcaldía Municipal.</p> <p>Modificar el procedimiento de copias de seguridad mediante la contratación de un data center.</p>	
<p style="text-align: center;">ELABORADO POR:</p> <p style="text-align: center;">JHON ALEXANDER ALVAREZ BAYONA Auditor</p>	<p style="text-align: center;">REVISADO POR:</p> <p style="text-align: center;">MAGRETH ROSSIO SANGUINO REYES Directora Proyecto</p>