

UNIVERSIDAD CENTROCCIDENTAL
“LISANDRO ALVARADO”
DECANATO DE CIENCIAS Y TECNOLOGÍAS
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

**DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA
ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA.**

BARQUISIMETO, JULIO 2011

UNIVERSIDAD CENTROCCIDENTAL
“LISANDRO ALVARADO”
DECANATO DE CIENCIAS Y TECNOLOGÍAS
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

**DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA
ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA**

Trabajo presentado como requisito parcial para optar al grado de:
Magister Scientiarum

Autor : Ing. Arelys Altagracia López M.

Tutora : Ing. Msc. Ennys H. Vivas S.

BARQUISIMETO, JULIO 2011

DEDICATORIA

A Dios todopoderoso por ser mi guía espiritual.

A mi Madre que donde quiera que esté aún me guía.

A mis hijas que me dieron la fuerza para salir de todas las adversidades, que este esfuerzo de constancia y voluntad sirva de ejemplo para ellas

A mí querido esposo por impulsarme a terminar esta investigación.

A mis hermanos, gracias por su apoyo.

A todas aquellas persona que me ayudaron de una u otra manera en la realización de esta investigación, mil gracias.

AGRADECIMIENTOS

En primer lugar doy un agradecimiento especial a Dios, que me guía, me protege y me da fuerza en todos los momentos de mi vida.

A mi madre (+) por enseñarme siempre que en la constancia está el éxito.

A esas grandes personas que son tan importantes para mí, gracias por existir.

A mi padre Leonzo por su apoyo y sabiduría, a mis hijas Emily y Ariadna que son mi razón de ser, mis hermanos por su apoyo y a mi querido esposo Pablo por siempre creer en mí y apoyarme. Le agradezco de corazón a la Ing. Ennys Vivas por la confianza, orientación, y la paciencia depositada, que Dios la bendiga.

A mis amigas Joseline, Libimar y Aimará, gracias por su ayuda y apoyo en todo momento.

A todas las personas que de una u otra manera me dieron ese empujón para seguir en esta investigación, gracias, esto no solamente queda en puras palabras sino que sale del corazón.

INDICE

LISTA DE CUADROS.....	v
LISTA DE GRÁFICOS	vi
LISTA DE FIGURAS.....	vii
RESUMEN	viii
INTRODUCCIÓN	1

CAPITULO

I EL PROBLEMA

Planteamiento del problema.....	3
OBJETIVOS	8
<i>General</i>	8
<i>Específicos</i>	8
Justificación e Importancia.....	8
Alcance y Limitaciones	10

II MARCO TEÓRICO

Antecedentes	11
Bases Teóricas	14
<i>Sistemas de Información</i>	14
<i>Seguridad de la Información</i>	15
<i>Análisis y Evaluación de Riesgo</i>	16
<i>Amenazas</i>	16
<i>Vulnerabilidades</i>	17
<i>Calculo de Riesgo</i>	18
<i>Tratamiento de Riesgos</i>	19
<i>Desarrollo del modelo de seguridad según el estándar internacional ISO/IEC</i> <i>27001:2005</i>	20
<i>Beneficios de implantar un SGSI</i>	25
<i>Serie de Normas ISO 27000</i>	26
<i>Modelos de Gestión de Riesgos</i>	27
DEFINICIÓN DE TÉRMINOS	34
Operacionalización de las Variables.....	38

III MARCO METODOLÓGICO

Naturaleza de la Investigación.....	40
Diseño de Investigación	41
<i>Fase I. Diagnóstico</i>	41
<i>Población y Muestra</i>	41
<i>Fase II. Estudio de Factibilidad</i>	45
<i>Fase III. Diseño del Proyecto</i>	46

<i>Aspectos Administrativos</i>	47
IV RESULTADOS	
Fase I. Diagnóstico.....	49
Resultados del Cuestionario	50
Resultados de la Entrevista.....	57
Resultados de la Observación Directa.....	59
Fase II. Factibilidad	65
Fase III: Diseño del Plan de Seguridad de la Información.	66
V CONCLUSIONES	
Conclusiones	93
Recomendaciones	94
REFERENCIAS BIBLIOGRÁFICAS	95
ANEXOS	98
A Cronograma de Actividades	99
B Cuestionario	100
C Formato de Validez del Instrumento(Cuestionario).....	101
D Resumen de Casos	102
E Acuerdo de Confidencialidad.....	103
F Autorizacion de Accesos Externo	108
G Procedimiento para Terminacion de Empleo.....	109
H Formato para Terminación de Empleo	110
I Formato Reporte de Vulnerabilidad	111
J Formato de Control de Usuarios	112
K Entrevista	113
L Formato de Validez del Instrumento(Entrevista)	115
M Formato de Control de Usuarios	116
CURRICULUM VITAE	117

LISTAS DE CUADROS

CUADROS	PAG
1. Clasificación de Vulnerabilidades.....	17
2. Operacionalización de las Variables.....	38
3. Usuarios de la red de la Alcaldía.....	42
4. Presupuesto	47
5. Ítem 1. Tiene usted conocimiento sobre lo que significa un plan de seguridad de información.....	50
6. Ítem 2. Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica de la Alcaldía.....	51
7. Ítem 3. Cree usted que se logrará un cambio positivo con la aplicación de este plan de seguridad de información en la plataforma tecnológica de la Alcaldía del Municipio Jiménez	51
8. Ítem 4. Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica de la alcaldía del Municipio Jiménez	52
9. Ítem 5. Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información en la Alcaldía del Municipio Jiménez.....	52
10. Ítem 6. Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones de esta alcaldía.....	53
11. Ítem 7. Actualmente existe un plan de recuperación ante desastres en la Alcaldía del Municipio Jiménez.....	53
12. Ítem 8. En la Alcaldía del Municipio Jiménez han realizado evaluación de riesgos relacionados con la información.....	54
13. Ítem 9. En la Alcaldía del Municipio Jiménez han realizado una evaluación de vulnerabilidades de la red.....	54
14. Ítem 10. La Alcaldía del Municipio Jiménez cuenta con software antivirus actualizado.....	55
15. Resultados de la Entrevista.....	57
16. Resultados de la Observación Directa.....	60
17. Actividades y Sub-actividades del Diseño del Plan de Seguridad.....	67
18. Realización de Análisis y Evaluación de Riesgo.....	73
19. Controles para el tratamiento de los Riesgos.....	76
20. Controles adicionales para el tratamiento de los Riesgos.....	77

LISTA DE GRÁFICOS

GRÁFICOS	PAG
1.-Importancia de la seguridad de la información.....	4
2.- Consideraciones para el manejo de los riesgos en la seguridad de la información.....	4

LISTA DE FIGURAS

FIGURAS	PP
1.- Fases del modelo PDCA.....	25
2.- Metodología de las Elipses para la Plataforma Tecnológica y Sistemas Administrativos.....	67
3.- Metodología para el Análisis y Evaluación de Riesgos.....	70

UNIVERSIDAD CENTROCCIDENTAL
“LISANDRO ALVARADO”
DECANATO DE CIENCIAS Y TECNOLOGÍA
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

**DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA
ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA**

Autora: Arelys A. López M.
Tutora: Ing. Msc. Ennys H. Vivas S.

RESUMEN

La presente investigación tiene como objetivo fundamental diseñar un Plan de Gestión de Seguridad de la Información en la Alcaldía del Municipio Jiménez del Estado Lara. La investigación se enmarcó desde el punto de vista metodológico en la modalidad de proyecto factible, apoyado en la investigación monográfica documental y de campo, el cual se dividió en tres (3) fases: (a) una primera fase de diagnóstico de la situación actual de la Alcaldía del Municipio Jiménez en relación a la seguridad de la información; (b) seguida por la evaluación de la factibilidad técnica, económica y financiera de la propuesta; (c) y por último el diseño del Plan de Seguridad de la Información de acuerdo a la norma ISO/IEC 27001:2005 aprobada por la Organización Internacional de Estandarización y por la Comisión Internacional Electrotécnica (de sus siglas en inglés ISO/IEC). La importancia del diseño de dicho plan permitió determinar los objetivos, procesos y procedimientos para el establecimiento de políticas de seguridad, así como de un conjunto de controles de seguridad que ayudarán a gestionar los riesgos en la Seguridad de la Información que maneja el organismo objeto de estudio, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten y generando resultados en concordancia con los objetivos y políticas requeridas para optimizar la Plataforma Tecnológica de la Alcaldía.

Palabras claves: Plan de Gestión de Seguridad de la Información, Políticas de Seguridad, Seguridad de la Información, Riesgos en la Seguridad de la Información.

INTRODUCCIÓN

Los sistemas basados en tecnologías de información cumplen un rol clave en la consecución de la misión de una organización, pues estas tecnologías no son más que aquellas que comprende el uso de un computador, una infraestructura de red e Internet, empleando datos e información, para generar conocimiento que satisfaga un conjunto de requerimientos específicos. Garantizar que este conocimiento es seguro, confiable y oportuno, depende de la calidad de los componentes que integran estas tecnologías de información. Esta calidad se mide en base a los tres principios de la seguridad como lo es la confidencialidad, integridad y disponibilidad, siendo importante resguardarlos de los potenciales riesgos a los que se puedan enfrentar.

Sobre la base de las consideraciones anteriores, se hace necesario contar con sistemas de Seguridad de la Información a fin de proteger la información de eventos inesperados y amenazas que generalmente son difíciles de controlar y gestionar.

Es así como nace el desarrollo de Sistemas de Gestión para la Seguridad de la Información (SGSI), el cual se usa para garantizar que la Seguridad de la Información es gestionada correctamente, bajo un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial, para lograr que ésta sea lo más segura posible para el logro de los objetivos generales.

Por lo antes expuesto, el objetivo principal de esta investigación es diseñar un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara, dentro del marco de la norma ISO/IEC 27000.

Esto con el fin de diseñar políticas, objetivos, procesos y procedimientos claros que permitan determinar y establecer controles de seguridad que ayuden a gestionar los riesgos en la Seguridad de la Información abarcando espacios físicos, procesos manuales y automáticos, elaboración de acuerdos de confidencialidad e integridad de la información y demás activos, gestión del personal, acceso de los usuarios a los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y

generar resultados en concordancia con los objetivos, funciones y responsabilidades de la Dirección de Informática de la Alcaldía requeridas para optimizar la plataforma tecnológica y por ende contribuir al logro de los objetivos generales del organismo objeto de estudio.

La siguiente investigación se estructura en cinco (5) capítulos a saber: el Capítulo Introductorio en el que se presenta el planteamiento del problema, objetivos general y específicos, justificación, importancia, alcance y limitaciones del estudio; el Capítulo II con el Marco Teórico en el cual se detalla toda la teoría sobre la que se sustenta esta investigación, con una presentación de los estudios anteriores (antecedentes) sobre la materia.

El Capítulo III donde se esboza la metodología que fue aplicada dentro de este estudio, prosiguiendo con los aspectos administrativos. Capítulo IV referido al análisis e interpretación de los resultados. Capítulo V el cual contiene las conclusiones en base a los objetivos planteados y recomendaciones del análisis de la investigación

Finalmente se presenta la bibliografía consultada y los anexos respectivos.

CAPÍTULO I

EL PROBLEMA

Planteamiento del problema

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles en el mercado. La posibilidad de interconectarse a través de las redes ha traído consigo el mejoramiento de la productividad en las organizaciones, además de la aparición de nuevas amenazas y riesgos para los sistemas de información, que pueden poner en juego la estabilidad y el futuro de las organizaciones. En el contexto de la norma ISO 27001:2005, un activo de información será: "...algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

Siendo la información uno de los activos que requiere ser protegida de forma adecuada frente a cualquier amenaza que ponga en peligro la continuidad del negocio. La importancia de mantener la Seguridad de la Información que manejan las organizaciones puede verse reflejada en la encuesta anual de Espiñeira, Sheldon y Asociados encuesta nacional 2006-2007 "Prácticas de Seguridad de la Información en empresas venezolanas" de allí se extrae el gráfico N° 1, donde se observa la importancia que asigna la gerencia a la seguridad informática. Dicha encuesta refleja que las organizaciones hoy día están preocupadas por el tema de seguridad, mientras que las pequeñas empresas no le dan mucha importancia.

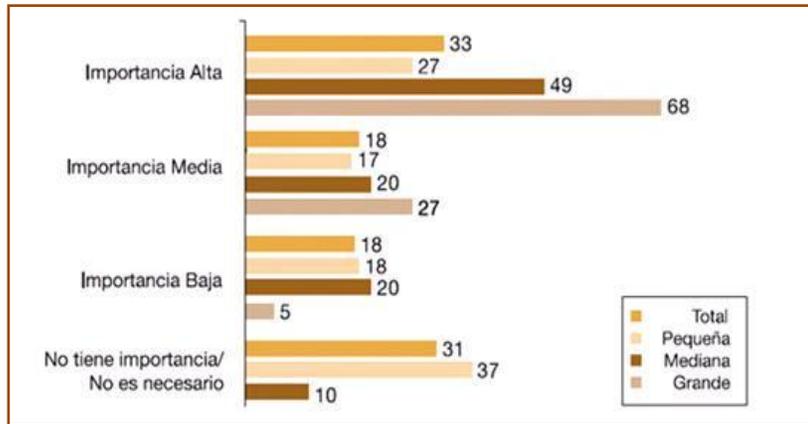


Gráfico N° 1. Importancia de la Seguridad de la Información.

En el Gráfico N° 2 se observa las consideraciones mencionadas por las empresas encuestadas para manejar con mayor efectividad los riesgos de Seguridad de Información, extraída de la mencionada encuesta de Espiñeira, Sheldon y Asociados.

Se inicia entonces, todo un proceso para gestionar la seguridad de la información, se establecen normas internacionales, se definen políticas locales que buscan garantizar integridad, confidencialidad y disponibilidad en la información. De allí que las organizaciones actuales están llamadas a diseñar políticas orientadas a gestionar el riesgo sobre la información y los sistemas que la procesan así como a diseñar sistemas eficientes para gerenciar el riesgo de tales sistemas.

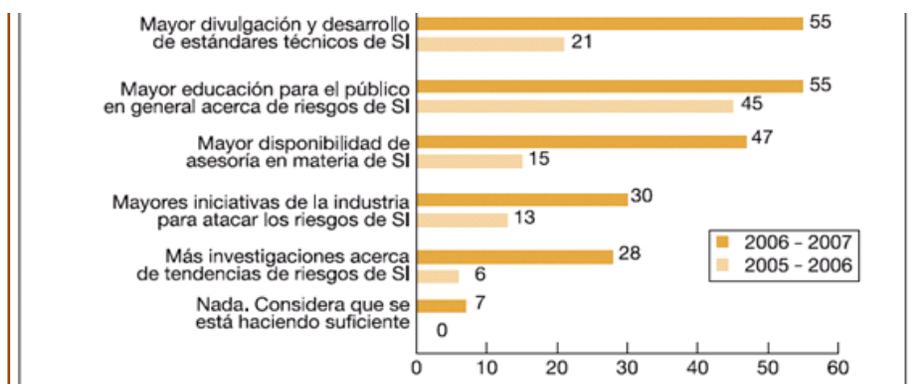


Gráfico N° 2. Consideraciones para el manejo de los riesgos en la seguridad de la información

Estos riesgos que afrontan las organizaciones hoy en día, tanto gubernamentales y no gubernamentales han llevado a que muchas desarrollen documentos y directrices que las orientan en el uso adecuado de estas destrezas tecnológicas, además de recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la organización.

En este sentido, el plan de gestión de seguridad de la información, surge como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información. Además, el proponer un Plan de Gestión de Seguridad de la Información requiere un alto compromiso con la organización, agudeza técnica, constancia para renovar y actualizar dicho plan en función del dinámico ambiente que rodea las organizaciones.

La norma ISO/IEC 27001 indica cómo implementar un sistema de gestión que garantice la Seguridad de la Información en una organización, esta norma establece que: “Los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar)” : realizar la evaluación de las amenazas, riesgos e impactos, en la fase **PLAN**, seleccionar e implementar los controles que reduzcan el riesgo a los niveles considerados como aceptables en la fase **DO** y cerrar y reiniciar el ciclo de vida con la recogida de evidencias y readaptación de los controles en la fase **CHECK** y **ACT**, según los nuevos niveles obtenidos y requeridos.

En Venezuela, es de gran preocupación la seguridad en materia de telecomunicaciones y del tratamiento de la información. Esto se evidencia con la Ley Orgánica de Ciencia, Tecnología e Innovación, publicada en gaceta oficial N° 38.242 del 03 de Agosto de 2005, la cual propone: “los principios orientadores en materia de ciencia, tecnología e innovación”, además menciona que el Ministerio de Ciencia y Tecnología coordinará las actividades en el área de tecnologías de información como

lo es: “Establecer políticas orientadas a resguardar la inviolabilidad del carácter privado y confidencial de los datos electrónicos obtenidos en el ejercicio de las funciones de los organismos públicos”.

Ahora bien, la Alcaldía del Municipio Jiménez es una institución del sector público que tiene como objetivo promover toda clase de actividades y prestar los servicios públicos que contribuyan a satisfacer las aspiraciones y necesidades de la colectividad, en el ámbito de su competencia de acuerdo a lo dispuesto en la Ley Orgánica de Régimen Municipal. Esto ha originado un crecimiento constante y sostenido de su plataforma tecnológica, además de sus activos, tales como la información, el hardware y software, equipos de computación, equipos de red y telecomunicaciones, recurso humano entre otros, y estos pueden estar expuestos a situaciones de inseguridad.

Cabe destacar que en entrevista informal con la Ingeniero Miledy Querales, Directora de Informática de la Alcaldía del Municipio Jiménez, se pudo constatar que existen varias deficiencias en los servicios de red que ofrece este organismo, que inciden directa o indirectamente en la seguridad de la Alcaldía, de su personal y de la infraestructura. Entre algunas de las deficiencias puntualiza las siguientes:(a) Carencia de un control de acceso efectivo a las instalaciones de la Alcaldía (b) Modificación de archivos por personas ajenas a la jefaturas de servicios; (c) Ausencia de un Control continuo de la administración de los sistemas de antivirus pertenecientes a la red; (d) Sustracción indebida de información por parte de los empleados que ya no ejercen funciones dentro de la institución; (e) Existencia de usuarios que acceden a información que no es de su competencia. Todo esto causa problemas como: acceso de personas no autorizadas a las instalaciones de la alcaldía, falta de continuidad en los procesos administrativos, presencia de virus en las computadoras de la alcaldía, pérdida de información requerida para la continuidad de los procesos administrativos, manejo de información por usuarios no autorizados, entre otros. Estas situaciones podrían gestionarse adecuadamente si se contase con un

plan de seguridad integral, lo que ayudaría a clarificar las acciones a tomarse en cuenta para minimizar los incidentes de seguridad

Un Plan de Gestión de Seguridad de la Información puede ayudar a la Alcaldía del Municipio Jiménez a estudiar los riesgos a los que está sometida toda su información, a evaluar que nivel de riesgo puede asumir y a implementar los controles que se consideren necesarios. También ayudaría a documentar las políticas y procedimientos relacionados, con un proceso continuo de revisión y mejora de todo el sistema.

Partiendo de la situación antes expuesta surgen las siguientes interrogantes: ¿Cuál es la situación actual de la Alcaldía del Municipio Jiménez en cuanto a seguridad de la información? ¿Cuáles aspectos se deben considerar para determinar si es viable técnica, económica y operativa, el diseño de un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez?, ¿Cuáles herramientas existen para diseñar un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez?

Para dar respuesta a las interrogantes planteadas se propone el diseño de un Plan de Gestión de Seguridad de la Información basado en normas o estándares internacionales, que tomen en cuenta la importancia de un sistema de seguridad y la fácil adecuación de este a los nuevos retos, redundando en un mejor funcionamiento de la alcaldía del municipio Jiménez del estado Lara.

OBJETIVOS

General

Diseñar un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara, de acuerdo al estándar internacional ISO/IEC 27001:2005.

Específicos

1. Diagnosticar la situación actual de la Alcaldía del Municipio Jiménez del Estado Lara en relación a la seguridad de la información.
2. Determinar la factibilidad técnica, económica y operativa del Plan de Gestión de Seguridad de la Información de acuerdo a la norma ISO/IEC 27001:2005
3. Diseñar un Plan de Gestión de Seguridad de la Información, de acuerdo a la norma ISO/IEC 27001:2005 para Dirección de Informática de la Alcaldía Del Municipio Jiménez Del Estado Lara.

Justificación e Importancia

La importancia de la Seguridad de la Información se viene tratando desde hace algunos años en las organizaciones, las cuales hacen grandes inversiones en sistemas y dispositivos de seguridad como: firewalls, antivirus, sistemas de respaldo entre otros; Sin embargo, esto no es suficiente para considerar que un sistema es seguro en relación a la integridad, la disponibilidad y la confidencialidad de la información que se maneja. De allí que los mecanismos de seguridad necesitan de un Plan de Gestión de la Seguridad que los integre a las políticas generales de la institución, considerando a la organización como un todo.

Un Plan de Gestión de Seguridad de la Información permite maximizar los esfuerzos desarrollados para asegurar la organización en todos sus niveles, apoya el cumplimiento del marco legal, aporta una metodología para el análisis y gestión del riesgo y garantiza la implantación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.

Es así como la Alcaldía del Municipio Jiménez se beneficiaría con el diseño de un Plan de Gestión de Seguridad de la Información pues éste permitirá establecer políticas, procedimientos, objetivos y procesos claros que permitan determinar y establecer controles de seguridad que ayuden a tratar los riesgos en la Seguridad de la Información comprendiendo espacios físicos, procesos automáticos y manuales, gestión del personal, usuarios de los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y generar resultados en concordancia con las políticas y objetivos generales de la Alcaldía.

Alcance y Limitaciones

Esta investigación busca proponer el diseño de un Plan de Gestión de Seguridad de la Información en la Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara, de acuerdo al estándar internacional ISO/IEC 27001:2005, evaluando así las amenazas, riesgos e impactos, precedida por un diagnóstico de la situación actual de la seguridad de la información, que permita un análisis comparativo de los controles a ser implantados o requeridos en la Alcaldía Del Municipio Jiménez, respecto a los controles planteados en la norma.

Debido a que la norma suma 133 controles entre todas las secciones, se propone limitar este estudio de acuerdo necesidades propias de la alcaldía a algunos dominios de control, como son: (a) Organización de la Seguridad de la Información, (b) Control de Acceso, (c) Seguridad Física y Ambiental, (d) Gestión de Activos, (e) Gestión de las comunicaciones y Operaciones, (f) Seguridad de los Recursos Humanos y (g) Gestión de Incidentes en la seguridad de la Información.

La limitación de la investigación a los siete (7) dominios mencionados es pertinente, puesto que están relacionados intrínsecamente con los tres principios básicos de la seguridad como lo son: la confidencialidad, integridad y disponibilidad, además de abordar las tres (3) áreas críticas de cualquier organización como son los activos, seguridad física y ambiental, y el control de acceso. Por otro lado, la norma propone dos fases adicionales al diseño y establecimiento del SGSI como lo son la revisión y el mantenimiento, lo que permitirá adicionar dominios y objetivos de control a medida en que se vayan identificando como necesarios.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes

El término seguridad informática es una generalización para un conjunto de tecnologías que ejecutan ciertas tareas relativas a la seguridad de los datos. ISO, en su norma 7498, define la seguridad informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene. El bien máspreciado por cualquier institución es la información y de ahí que se han desarrollado protocolos y mecanismos adecuados, para preservar su seguridad

A continuación se hará referencia a trabajos de investigación realizados con anterioridad que apoyan, como antecedentes, al diseño de un Plan de Gestión de Seguridad de la Información en la Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara, basado en el estándar ISO/IEC 27001:2005.

Díaz, N. (2005) realizó una tesis titulada: *“Diseño e Implantación de un Esquema de Seguridad para el Intercambio de Información de FARMASALUD”*. Entre los objetivos de la investigación se encuentran el de diseñar una estrategia integral de seguridad para protección y detección de intrusos que permita resguardar la confidencialidad y la integridad de la información, y Proponer un plan de monitoreo interno y administración de los recursos informáticos defendidos que hacen parte del sistema de seguridad.

El proyecto concluye con el diseño de un esquema de seguridad más sólido y eficiente que sustenten un intercambio de información confiable y seguro,

principalmente con sus asociados del grupo corporativo.

Este trabajo de grado permite orientar el desarrollo de esta investigación para la Alcaldía del Municipio Jiménez, porque el diseño del esquema de seguridad propuesto está basado en la norma ISO 17799, equivalente a la norma ISO 27001, que es el estándar sugerido en esta investigación.

Méndez, J. (2006) realizó un trabajo especial titulado: “*Estudio de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local*”, donde plantea la investigación de las metodologías de seguridad más cercanas a lo especificado en los estándares internacionales de la seguridad, además de identificar los elementos claves que deben formar parte de una implantación de seguridad en WLAN.

El proyecto concluye con dos esquemas metodológicos complementarios, contentivos de las mejores prácticas de seguridad tanto para el ámbito global de la organización como para el entorno específico de las redes inalámbricas de área local, mediante una combinación integral de las perspectivas necesarias para la implantación de una cultura de seguridad organizacional.

El trabajo sirve de marco de referencia para la investigación ya que la metodología usada consta de una colección de documentos que pueden ser clasificados como mejores prácticas generales para el control y seguridad de las Tecnologías de Información y Comunicación. Tiene que ver con la Seguridad de la Información y la metodología sugerida es equivalente (ISO/IEC 17799), lo que permite evaluar el proceso que se siguió durante el establecimiento de dicha metodología y orientar el desarrollo de esta investigación.

Por su parte, Mujica, M. (2007) presentó una tesis titulada: “*Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica Antonio José de Sucre, Sede Rectoral*”. La metodología sugerida por el autor está basada en las normas ISO/IEC 27001:2005 e ISO/IEC 17799:2005, lo que ayuda en la implementación del Plan de Seguridad que la Institución (UNEXPO) necesitaba para controlar y gestionar los incidentes de seguridad.

Los objetivos específicos del estudio eran: (a) Diagnosticar la situación actual de la seguridad informática. (b) Determinar la factibilidad operativa, técnica y económica de diseñar el Plan de Seguridad. (c) Diseñar el Plan de Seguridad Informática. (d) Evaluar el diseño del Plan de Seguridad.

La tesis tiene relación con esta propuesta ya que la solución planteada tiene que ver con la implementación de la metodología sugerida en la norma (ISO/IEC 27001), lo que permite evaluar el proceso que se siguió para el diseño del plan de seguridad para la UNEXPO y orientar el desarrollo de esta investigación para la Alcaldía del municipio Jiménez.

Villena, M. (2007) presentó una tesis titulada: “*Sistema de Gestión de Seguridad de Información para una Institución Financiera*”. Esta tesis tenía como objetivos específicos los siguientes: (a) Establecer los principales lineamientos para implementar un modelo de Sistema de Gestión de Seguridad de Información (SGSI) en una institución financiera. (b) Asegurar que la tecnología de información usada esté alineada con la estrategia de negocio. (c) Establecer los niveles de responsabilidades para que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización. Este proyecto está basado en el modelo de Mc. Cumber. A partir del modelo citado, la investigación cubrirá todos aquellos lineamientos a tener en cuenta en relación a estándares, normas, procedimientos y medidas tecnológicas que aseguren la confidencialidad, integridad, y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión, además del aspecto de detección de accesos no autorizados a la información

El trabajo de grado tiene relación directa con esta propuesta ya que la solución planteada tiene que ver con la Seguridad de la Información y la metodología sugerida basado en el modelo de Mc. Cumber, plantea que se debe resguardar la confidencialidad, integridad, y disponibilidad de la información de manera similar a la norma (ISO/IEC 27001), lo que permite evaluar el proceso que se siguió durante el

establecimiento del Sistema de Gestión de Seguridad de la Información en la entidad bancaria y de esa forma orientar el desarrollo de esta investigación.

Mendoza, R. (2009), realizó una tesis titulada: “*Sistema de Gestión para la Seguridad de la Información Caso: Centro de Tecnología de Información y Comunicación del Decanato de Ciencias y Tecnología - UCLA*”, en el cual planteó los problemas presentados en el Centro de Tecnología de Información y Comunicación del Decanato de Ciencias y Tecnología en cuanto al manejo de la seguridad de la información. Los objetivos del proyecto eran: dar lineamientos metodológicos, y de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, en el CTIC.

El proyecto concluye con el cumplimiento de los controles propuestos en la norma ISO/IEC 27002, lo que permitió el descubrimiento de las vulnerabilidades, así como el manejo y control de los riesgos, lo que se relaciona directamente con esta propuesta ya que se basó en la aplicación de un SGSI según la norma ISO 27001:2005, que es el mismo estándar sugerido en esta investigación.

Bases Teóricas

El presente sección tiene como finalidad reseñar los aspectos teóricos relacionados con el diseño de un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara.

Sistemas de Información

Según Vittoriano (2008) la información es considerada como: “insumo fundamental que actúa como facilitador para los objetivos de la organización, con base en ella se desarrolla su negocio y es un elemento vital para el desarrollo modelo

de negocio de la organización”. En el contexto de la norma ISO 27001:2005, un activo de información será: “...algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”.

Soto, L. (2007) define Sistema de Información como:

El sistema de personas, registros de datos y actividades que procesa los datos y la información en cierta organización, incluyendo manuales de procesos o procesos automatizados. El Sistema de Información basado en computadoras es el campo de estudio de las tecnologías de información; de cualquier manera, éstas difícilmente deberían tratarse como tema aparte del enorme Sistema de Información del cual forman parte. (p. 26)

Seguridad de la Información

La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información (SI) como:

La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización. Además, también pueden estar involucradas otras propiedades como son: la autenticidad, la responsabilidad, el no-repudio y la confiabilidad.

Es decir, estos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación.

Confidencialidad. La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Para garantizar la integridad de la información el remitente debe estar siempre autenticado. Esta se puede ver afectada por problemas de hardware, software, virus o personas malintencionadas.

Disponibilidad. Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran

Análisis y Evaluación de Riesgo

Daltabuit, E. y otros (2007), definen el análisis de riesgos como la selección de los mecanismos de protección, que permiten estimar las pérdidas potenciales de información, y ayudan a reducirlo facilitando la selección de los mismos. Como lo señala Puig et al., 2008, el documento que de esta etapa se derive, será el que se implantará durante la primera fase del SGSI y sus acciones serán de corto, mediano y largo plazo.

Para Muñoz (2004), la metodología de análisis y gestión de riesgos de los sistemas de información es el núcleo de las actuaciones relacionadas con el análisis, la evaluación y la gestión del riesgo. Esta metodología analiza los riesgos, identifica las amenazas y su impacto, y gestiona el riesgo basado en: (a) Elementos (activos, amenazas, vulnerabilidades, riesgos, impactos, salvaguardas), (b) Eventos (estáticos, dinámicos organizativos, dinámicos físicos), (c) Procesos (planificación, análisis de riesgos, gestión de riesgos, selección de salvaguardas).

Amenazas

De acuerdo con la normas ISO 27000, se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización. Alexander y otros (2007), coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etcétera.

- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.
- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware ó de red.

Luego de identificadas todas las amenazas, se evalúa su probabilidad de ocurrencia. El resultado de esta evaluación permitirá identificar las amenazas de mayor a menor concurrencia y la decisión sobre cuales atacar y cuales descartar de acuerdo con criterios técnicos, legales y de costos.

Vulnerabilidades

Las vulnerabilidades están asociadas a debilidades de los activos de información. De acuerdo con Alexander (ob.cit) la vulnerabilidad en el contexto de los sistemas de información es considerada como la ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición.

De acuerdo con la norma ISO 17799-2005, las vulnerabilidades son clasificables según como lo indica el Cuadro N° 1.

Cuadro N° 1. Clasificación de Vulnerabilidades

Recursos Humanos	Controles de acceso	Seguridad Física y ambiental	Gestión de operaciones y comunicación	Mantenimiento, desarrollo y adquisición de sistemas de información.
Falta de capacitación en temas de seguridad	Falta de políticas de escritorio	Controles de acceso físico no adecuados	Interfaces complicadas para los usuarios	No hay protección de llaves criptográficas
Falta de mecanismos de monitoreo	Segregación inapropiada de redes	Ubicación de áreas críticas en zonas de altos riesgo	Inadecuado manejo de controles de cambios	falta de políticas en el uso de criptografía

Falta de políticas de uso de medios de telecomunicaciones	Falta de protección de equipos de telecomunicaciones	Falta de programas de renovación de equipos	Inadecuada gestión de redes	Falta de validación de datos procesados
No eliminación de accesos al retirar los empleados	Políticas débiles para el manejo de claves	Descuidos con los equipos	Falta de mecanismos de aseguramiento de envío de mensajes o datos	Falta de ambientes para pruebas
Falta de control de activos devueltos al finalizar los contratos		Falta de regulación del voltaje	Carencia de segregación de tareas	Falta de documentación de software
Desmotivación de empleados			Falta de protección de redes públicas	Malas prácticas en procesos de pruebas de ensayo

Según Granada (2009) las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información. Esto es lo que para expertos en temas de seguridad de información se conoce como la relación causa-efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será el de integrar estos elementos para analizar y definir los niveles de riesgo que luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

Calculo de Riesgo

Una vez se listan y clasifican los activos y se identifican las amenazas y vulnerabilidades, se procede al cálculo del riesgo. Este cálculo utilizará valores cuantitativos pues el valor de un activo de información se tasa en el impacto en

pérdidas económicas que el mismo genera si es vulnerado. Para Daltabuit (2007), el análisis de riesgo se puede realizar de 2 formas:

- Análisis cuantitativo. Basado en la métrica y el cálculo de valores que determinen el costo-beneficio, su cálculo demanda un gran esfuerzo, pero permiten la comparación de valores.

- Análisis cualitativo. Es más ágil, pero sus resultados son más subjetivos los cuales no se basan en cifras y contienen análisis sencillos. No permiten la comparación de valores más allá del orden relativo.

Tratamiento de Riesgos

A partir del informe de evaluación de riesgos se procede a examinar cual es el tratamiento más adecuado para cada uno de los riesgos que han sido identificados.

Siguiendo los lineamientos de la norma ISO 27001:2005, el tratamiento de riesgos comprende los siguientes enfoques:

Determinar si el riesgo es aceptable o si requiere un tratamiento, en cuyo caso se identificará una de las siguientes alternativas: (a) Reducir el riesgo a un nivel aceptable, implantando algún control (combinación de personas, procesos y herramientas), (b) Aceptar el riesgo porque no es posible realizar un tratamiento o porque éste resulta demasiado costoso, (c) Evitar el riesgo, o (d) Transferir el riesgo a una tercera parte (Por ejemplo, Compañías de Seguros).

En caso de que se decida mitigar el riesgo se debe definir que controles del SGSI se deben implementar. Además, si se considera necesario se pueden seleccionar controles específicos adicionales.

Para definir los controles a implementar en base al análisis de riesgo se deben realizar los siguientes pasos:

1. Preparar un documento de Declaración de Aplicabilidad (DDA), en el que se detalle la relación de controles que se van a implantar.
2. Establecer el nivel de riesgo aceptable para la Organización.

3. Obtener la aprobación de la dirección a la DDA y a los riesgos no cubiertos.
4. Formular un plan de tratamiento de riesgos en el que se establecerán las acciones necesarias para conseguir mitigar los riesgos a un nivel aceptable y para implantar los controles que se consideren necesarios según requerimiento de la norma ISO/IEC 27001:2005 en sus numerales 4.2.1.f, g y h.
5. Preparar los procedimientos necesarios para la implantación de controles.

Desarrollo del modelo de seguridad según el estándar internacional ISO/IEC 27001:2005

La implementación de este modelo de seguridad requiere de unas políticas claras y la ejecución de todas aquellas actividades tendientes a gestionar el riesgo.

Definición de las políticas de seguridad

Luego de establecer el alcance del SGSI, será necesario definir y documentar la política de seguridad.

Según Daltabuit & Vázquez et al., (2007), “concebir y redactar la política recae sobre los responsables del funcionamiento de la misma (...) el elemento fundamental de estos documentos es que expresan el consenso de quienes conocen mejor que nadie los principios operativos, económicos y éticos que conducirán al éxito colectivo”.

En opinión de Howard (Citado en Tipton y Krause, 2007) la política incluirá los siguientes principios básicos: (a) Reconocimiento y concientización de la importancia de la Seguridad de la Información para los resultados del negocio, (b) Señalar el riesgo al que están expuestos los sistemas de información y a su vez el efecto inmediato sobre las operaciones del negocio, (c) Seguimiento estricto a las normas legales y los estándares internacionales para el manejo seguro de la información, (d) Coparticipación, compromiso y co-responsabilidad de todos los miembros de la organización de manera individual y como organización, (e) Visión de largo plazo

pero con capacidad de autoevaluación y reajuste. Tal como lo concluye Steer (2008), estas políticas se convierten entonces en una declaración expresa de la intención de conseguir algo que contribuye a la seguridad de la información, definiendo que necesita protegerse y cómo hacerlo, oponiéndose a las amenazas identificadas y satisfaciendo las exigencias de Seguridad de la Información que definen las normas legales y los estándares internacionales.

De acuerdo con Puig et al., (2008), la política de seguridad tendrá como mínimo los siguientes elementos:

1. Una definición de Seguridad de la Información y sus objetivos globales.
2. El establecimiento del objetivo de la dirección que soporte los objetivos y principios de la seguridad de la información.
3. Una explicación detallada de las políticas, principios, normas y requisitos más importantes para la organización:

Desarrollo de procedimientos para la Gestión de la Seguridad de la Información

Todas las amenazas y las vulnerabilidades evidenciadas hay que enfrentarlas, lo que requiere una planificación constante de las diferentes alternativas de solución por lo tanto, luego de haber sido definidas las políticas de seguridad de la información, se elaborarán los procedimientos de seguridad para soportar el SGSI y el modelo de seguridad diseñado.

Para Alexander et, al. (2007), el desarrollo de procedimientos para la gestión de Seguridad de la Información se traduce en el desarrollo de políticas, normas y procedimientos y junto a ellos la aplicación de salvaguardas y controles que verifican y garantizan que cada amenaza tiene su respuesta adecuada.

La definición de estos procedimientos de gestión de seguridad facilita la transferencia de conocimiento que en el futuro ayudará en la aplicación de mejoras al sistema de gestión por cuenta del personal interno de la organización.

Todo este conjunto de políticas y procedimientos de seguridad para establecer un SGSI, deben estar alineados con el estándar ISO/IEC 27001:2005 que se compone de 11 dominios:

- 1) Política de seguridad
- 2) Organización de la seguridad de la información
- 3) Administración de recursos
- 4) Seguridad de los recursos humanos
- 5) Seguridad física y del entorno
- 6) Administración de las comunicaciones y operaciones
- 7) Control de acceso
- 8) Adquisición, desarrollo y mantenimiento de sistemas de información
- 9) Administración de los incidentes de seguridad
- 10) Administración de la continuidad de negocio
- 11) Cumplimiento (requerimientos legales, estándares, técnico y auditorías)

Durante la ejecución del proyecto se debe considerar el desarrollo de los siguientes procedimientos esenciales en seguridad, indicados por el estándar ISO/IEC 27001:2005, a saber: (a) Control de: Documentos, de Registros, de acceso, (b) Proceso de auditorías internas, (c) Acciones Preventivas (Salvaguardas técnicas, físicas, medidas de organización), (d) Acciones Correctivas, (e) Proceso de revisión Gerencial, (f) Gestión de: Incidentes de seguridad, de copias de respaldo de Información, de RR.HH. (Políticas de personal, Administración de Usuarios y Contraseñas), (g) Control de Cambios, (h) Inventario y Clasificación de Activos de información, (i) Seguridad de los Medios e Información en Tránsito

Plan de Concientización en Seguridad de la información

Esta fase comprende las actividades necesarias para establecer la estrategia de sensibilización y divulgación de políticas y procedimientos para la Gestión de la

Seguridad de la Información, con el propósito de establecer al interior de la organización un grado de compromiso y concientización con respecto al SGSI.

Las actividades de concientización no solo se deben orientar hacia los temas de seguridad sino que es importante que se refuercen mediante la divulgación del mismo a través de talleres, cursos entre otros. Un criterio igualmente importante es la respuesta de la audiencia frente a los diferentes medios de difusión o divulgación de los contenidos.

Existen diferencias en el aprendizaje de las personas que deben ser contempladas a la hora de diseñar una campaña de concientización. Un enfoque muy eficaz consiste en determinar para una audiencia dada los siguientes criterios:

- El estilo preferido de aprendizaje.
- El nivel de conocimiento actual

El Monitoreo y control al SGSI

El rápido avance en el desarrollo de la tecnología impacta los planes de Seguridad de la Información en cualquier organización y ello hace que los mecanismos de seguridad implementados puedan dañarse con el paso del tiempo. Un plan de monitoreo ayudará como lo precisa Alexander et al., (2007) a revelar el nivel de deterioro en el que se encuentra el SGSI y a definir las acciones correctivas necesarias.

“El monitoreo y el control de riesgos involucra la ejecución de los procesos de la administración del riesgo para responder a los eventos que comprometen la seguridad de la información” (Del Carpio, 2006, p. 107).

La revisión es un ejercicio práctico con resultados métricos orientados a calcular el nivel de eficiencia en la respuesta del SGSI. Los procedimientos para llevar a cabo este monitoreo y la revisión están detalladas en la ISO 27001:2005, su ejecución debe ayudar a:

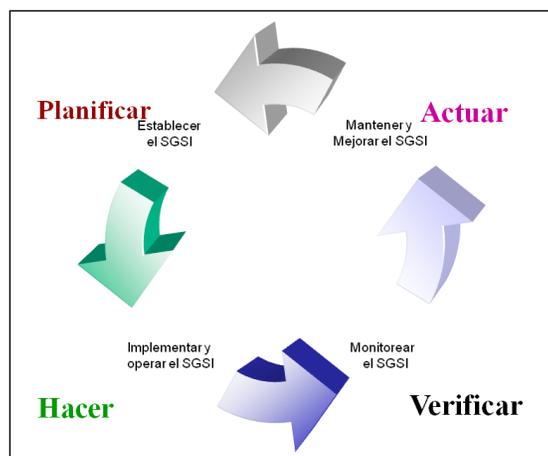
- Detectar errores

- Identificar las fallas de seguridad
- Controlar que las actividades de seguridad se realicen de acuerdo a lo establecido
- Definir las acciones a implementar para corregir errores y fallas.

Un SGSI varía según el tipo de organización. Sin embargo, y de acuerdo con Alexander (2007), el procedimiento para la implementación y mantenimiento del SGSI debe seguir un ciclo de mejora continua en 4 pasos: Planear, hacer verificar y actuar. Este es el esquema propuesto por la norma ISO/IEC 27001:2005.

En la fase **PLAN** se realiza la evaluación de las amenazas, riesgos e impactos. En la fase **DO**, se seleccionan e implementan los controles que reduzcan el riesgo a los niveles considerados como aceptables y en **CHECK** y **ACT** se cierra y reinicia el ciclo de vida con la recogida de evidencias y readaptación de los controles según los nuevos niveles obtenidos y requeridos. Este proceso cíclico permite la mejor adaptación de la seguridad al cambio continuo que se produce en la empresa y su entorno, como se observa en la figura 1.

Figura 1. Fases del modelo PDCA.



Fuente: ISO27000.es

El propósito de un SGSI no es garantizar la seguridad (que nunca podrá ser absoluta) sino garantizar que los riesgos de la Seguridad de la Información son conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

Beneficios de implantar un SGSI

Según Kwell (2008) los beneficios de implantar un sistema de gestión de Seguridad de la Información son: (a) Establecimiento de una metodología de gestión de la seguridad clara y estructurada, (b) Reducción del riesgo de pérdida, robo o corrupción de información, (c) Los clientes tienen acceso a la información a través medidas de seguridad, (d) Los riesgos y sus controles son continuamente revisados, (e) Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial, (f) Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar, (g) Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad, (h) Confianza y reglas claras para las personas de la organización, (i) Reducción de costos y mejora de los procesos y servicio, (j) Aumento de la motivación y satisfacción del personal,

(k)Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías

Serie de Normas ISO 27000

- ISO 27000: Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido.
- ISO 27001. Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.
- ISO 27002: Desde el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. No es certificable.
- ISO 27003: Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
- ISO 27004: Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
- ISO 27005: Consistirá en una guía de técnicas para la gestión del riesgo de la Seguridad de la Información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.
- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.
- ISO 27007: Consistirá en una guía de auditoría de un SGSI.
- ISO 27011: Consistirá en una guía de gestión de Seguridad de la Información específica para telecomunicaciones.
- ISO 27031: Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- ISO 27032: Consistirá en una guía relativa a la ciberseguridad.
- ISO 27033: Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante Gateway, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.
- ISO 27034: Consistirá en una guía de seguridad en aplicaciones.
- ISO 27799: Es un estándar de gestión de Seguridad de la Información en el sector.

Modelos de Gestión de Riesgos

La selección de la metodología y de la herramienta requiere una investigación, que tomando los parámetros adecuados, servirán de guía en la elección de la herramienta más favorable, al final lo importante no es tanto cuáles son los pasos a seguir para la formulación del modelo como la estimación de qué aspectos son los que se pueden definir. Tomado de las comparaciones metodológicas provistas por ENISA en <http://www.enisa.europa.eu/rmra/comparison.html>

A continuación se presenta una breve descripción de las metodologías allí nombradas.

MICROSOFT THREAT MODELLING

Este modelo consta de cinco pasos que a continuación se describen:

1. Identificar los Objetivos
 - Los objetivos se pueden clasificar en :
 1. Objetivos de Identidad

2. Objetivos Financieros
3. Objetivos de reputación
4. Objetivos de integridad y confidencialidad
5. Objetivos de disponibilidad

2. Evaluación del sistema

- ◆ Una vez que se han declarado los objetivos se debe analizar el diseño del sistema para identificar los componentes, los flujos de información y los límites de confianza.

3. Descomponer el sistema

- ◆ Implica identificar las características y los módulos con impacto en la seguridad que deben ser evaluados.

4. Identificar las amenazas

- ◆ Se parte del hecho de que es imposible identificar amenazas que no son conocidas. Por lo tanto, concentrándose en los riesgos conocidos, se realiza una identificación basada en el empleo de herramientas de BugTraq.

5. Identificar las vulnerabilidades

- ◆ Además de saber qué tipo de amenaza es el que se puede identificar, es preciso clasificar quién es el posible atacante. Se propone la siguiente clasificación:
 - ◆ Descubrimiento accidental
 - ◆ Malware automático
 - ◆ Atacante curioso

- ◆ Script Kiddies
- ◆ Atacante Motivado
- ◆ Crimen organizado

STRIDE/DREAD

- ◆ STRIDE es una metodología para identificar amenazas conocidas. Establece seis categorías:

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of service
- Elevation of privilege

- ◆ DREAD es un modelo que permite establecer un grado de riesgo que permite ordenar los riesgos mediante la evaluación de cinco categorías.

- ◆ Propone una expresión que se traduce en un índice, aplicando la siguiente expresión:

$$Risk_Dread = \frac{(DAMAGE + REPRODUCTIBILITY + EXPLOTABILITY + AFFECTEDUSER + DISCOVERABILITY)}{5}$$

- ◆ **Damage Potential** *Si la amenaza se materializa, ¿cuánto daño puede causar?*
- ◆ **Reproducibility** *¿Cómo de fácil es reproducir el exploit?*
- ◆ **Exploitability** *¿Qué se necesita para materializar la amenaza?*
- ◆ **Affected Users** *¿Cuántos usuarios se ven afectados?*

- ◆ *Discoverability* ¿Cómo es fácil de descubrir esta amenaza?

TRIKE

- ◆ Es un modelo similar al propuesto desde Microsoft.
- ◆ Existen sin embargo diferencias. TRIKE propone una aproximación a la descripción del riesgo que no aúna los ataques, las amenazas y las vulnerabilidades.
- ◆ Al contrario, permite distinguir unos de otros construyendo un sistema experto para toma de decisiones.

AS/NZS 4360

- ◆ El Australian/New Zealand Standard es simple, muy flexible e iterativo.
- ◆ Proporciona una serie de conjuntos de tablas de riesgos como ejemplos, pero permite desarrollar y adaptar su propio modelo a las organizaciones.
- ◆ El modelo se resume en cinco puntos.
 - Establecer el contexto
 - Identificar los riesgos
 - Analizar los riesgos
 - Evaluar los riesgos
 - Habilitar contramedidas.

CVSS

El departamento de Homeland Security (DHS) del gobierno de EEUU estableció que el denominado grupo “NIAC Vulnerability Disclosure Working Group”, que incorporaba a Cisco Systems, Symantec, ISS, Qualys, Microsoft, CERT/CC y eBay.

Uno de los resultados de este grupo ha sido el CVSS – Common Vulnerability Scoring System.

CVSS no es un modelo en sí, sino que permite normalizar las notificaciones de seguridad asignándole una métrica única a las amenazas descubiertas. La definición de la métrica es muy compleja y su cálculo implica tener en cuenta factores software y de entorno. La evaluación de estos factores obliga a utilizar una tabla para determinar el grado de criticidad de las amenazas conocidas. De hecho la sobrecarga que supone calcular el índice CVSS sobre una aplicación determinada aumenta factorialmente con cada amenaza que se estima.

CVSS no encuentra ni reduce la superficie de ataque. Tampoco enumera los riesgos para un programa determinado. Lo que proporciona es una aproximación técnica, estandarizada, abierta y ordenada de una vulnerabilidad específica.

OCTAVE

Se trata de un modelo muy complejo originario de la Carnegie Mellon University en colaboración con el CERT. Se centra en la evaluación del riesgo organizativo y no técnico. Aunque es útil en la gestión de grandes organizaciones es demasiado costoso y no proporciona medidas para mitigar los efectos de las amenazas. Es más bien un decálogo de buenas costumbres.

MAGERIT

Se trata de una metodología promovida por el CSAE (Consejo Superior de administración electrónica) que persigue una aproximación metódica al análisis de riesgos. Se trata por tanto de una metodología para auxiliar en tarea de toma de decisiones en entornos críticos. Los objetivos de la aplicación de este modelo son:

Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de paralizarlos a tiempo

Ofrecer un método sistemático para analizar tales riesgos

Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Su aplicación se estructura en cinco niveles:

- Modelo de valor
- Modelo de riesgos
- Estado de los riesgos
- Informe de insuficiencias
- Plan de seguridad

CRAMM

CRAMM - (CCTA (Central Computer and Telecommunications Agency) Risk Analysis and Management Method). Esta es una propuesta creada por la CCTA de Reino Unido. Actualmente está en su quinta versión, y está estructurada en tres etapas. Cada etapa utiliza unos cuestionarios que permiten identificar y analizar los riesgos del sistema. La última etapa propone contramedidas para los riesgos.

- ◆ Etapa 1: Establecimiento de objetivos
 - Definir los límites del estudio.
 - Identificar y valorar los activos del sistema.
 - Determinar el valor de los datos del sistema a través de entrevistas con el personal acerca del potencial daño empresarial que tendría la falta de disponibilidad, su destrucción, falta de confidencialidad o su modificación.
 - Identificar y valorar los activos software del sistema.
- ◆ Etapa 2: Evaluación de riesgos
 - Identificar y valorar el tipo y nivel de amenazas que podrían afectar al sistema.
 - Evaluar la exposición del sistema frente a estas amenazas.

Combinar ambos aspectos con la valoración de los activos para determinar una medida del riesgo.

- ◆ Etapa 3: Identificación y Selección de contramedidas
 - Se propone una librería de contramedidas agrupadas en 70 grupos lógicos para facilitar su aplicación.

Metodología de la Elipse

Según Alexander (2.006), Para identificar los activos de información se puede utilizar la metodología de las elipses, “la cual una vez determinado el alcance se decide el proceso que se evaluará. Con esto se trata de visualizar con mucha precisión los distintos subprocesos que componen al alcance. Esto se determina en la elipse concéntrica, el paso siguiente sería determinar los usuarios y dueños de esos procesos, el segundo paso en la metodología, es el de identificar en la elipse intermedia las distintas interacciones de los subprocesos de la elipse concéntrica, tienen con otros procesos de la organización. Seguidamente, también se deben identificar con la elipse concéntrica. La elipse externa, se identifican aquellas organizaciones extrínseca a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse concéntrica.”

DEFINICIÓN DE TÉRMINOS

A

- **Ataques:** Los ataques de red recaen sobre vulnerabilidades directamente relacionadas con los protocolos y sus implementaciones.
- **Administrador de Red:** Es la persona encargada de la administración de la red. Entre sus actividades incluye la administración, mantenimiento y monitoreo de los equipos de comunicaciones y servidores que conforman la red: switches, routers, firewalls, etc.

B

- **Backup(Respaldo) :** Copia de seguridad. Acción de copiar documentos, archivos o ficheros de tal forma que puedan recuperarse en caso de fallo en el sistema.
- **Base de Datos:** Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos.

C

- **Clave de Acceso:** Es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa

determinado, un terminal o computador personal (PC), un punto en la red, etc. Muchas veces se utiliza la terminología inglesa (password) para referirse a la clave de acceso.

- **Contraseña de Usuario:** Una contraseña de usuario o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicitan una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

D

- **Datos: (Data):** Hechos conceptos, instrucciones o caracteres representados de un manera apropiada para que sean comunicados, transmitidos o procesados por ser humanos o por medios automáticos y a los cuales se le asigna un significado.
- **Derechos de Acceso de los Usuarios:** Es el conjunto de permisos o privilegios dados a un usuario para acceder a un determinado recurso. A mayor permiso para un usuario, mayores posibilidades para manipular el recurso.
- **Directorio:** Es una estructura jerárquica que almacena información sobre recursos (o de forma más general, objetos) en la red. El directorio se implementa normalmente como una base de datos optimizada para operaciones de lectura (soporta búsquedas de grandes cantidades de información) y con capacidades de exploración.

E

- **Enlace:** Conexión o ruta de comunicaciones dedicada punto a punto o conmutada.

F

- **Firewalls:** (Pared de Fuego). Dispositivo diseñado para proveer seguridad en la periferia de una red. Se trata de cualquier programa (Software) ó dispositivo (Hardware) que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve más allá del firewall.
- **Fraudes:** Engaño hacia un tercero, abuso de confianza, dolo, simulación, etc. En seguridad es una herramienta, para llevar a cabo toda clase de estafas sobre los usuarios más confiados.

H

- **Hacker:** Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.
- **Hubs:** Concentradores. Retransmiten cualquier paquete que llegue a uno de sus puertos a sus otros puertos.

I

- **Intrusos:** Persona que ingresa a un sistema sin autorización.
- **ISO:** (International Organization for Standardization):

P

- **Políticas de Seguridad:** Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños informáticos.
- **Propietario de la Información:** Persona o Dependencia responsable de los datos.

R

- **Red:** Se tiene una red cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

S

- **Servidores (Hardware):** Equipos centralizadores y de enlaces para la constitución de redes, de diferentes magnitudes, en interacción con PCs, routers, hubs, proxys, etc.
- **Sistema Operativo:** Es un conjunto de programas que administran los recursos del computador como discos duros, memorias, control de periféricos como monitor, teclados, etc.

U

- **Usuarios Finales:** Los usuarios finales son aquellos que hacen uso de los servicios y recursos que brinda la red.
- **Usuario Básico:** Aquel que puede acceder únicamente a los recursos de la Red e Internet.
- **Usuario Avanzado:** Aquel con capacidad de administrar los recursos del equipo y que además tiene acceso a los recursos de red e Internet.

Operacionalización de las Variables

Las dimensiones sobre las que se analizó el objeto de estudio es un subconjunto de los dominios de control propuestos en la norma ISO/IEC 27001:2005 de los cuales se toma: (a) Gestión de Incidentes en la Seguridad de la Información, (b) Control de Acceso, (c) Seguridad Física y Ambiental y (d) Gestión de Activos

Estas dimensiones junto con el objeto de estudio conforman las variables de estudio, que por ser un modelo de tipo causal, donde las dimensiones definen y miden el grado de satisfacción de la Seguridad de la Información se deben clasificar como dependiente e independientes, a saber:

Variable Dependiente : Seguridad de la Información

Variables Independientes : Gestión de Activos., Seguridad Física y Ambiental.
Control de Acceso, Gestión de Incidentes.

A su vez cada dimensión (variable independiente) tiene uno o más indicadores los cuales fueron seleccionados de un subconjunto de los objetivos de control de la norma quedando especificados en el cuadro N° 2.

Cuadro N° 2. Operacionalización de las Variables

<i>Variables de Estudio</i>	<i>Dimensión</i>	<i>Indicadores</i>	<i>Instrumento</i>
“DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA”	Seguridad de la Información	<ul style="list-style-type: none"> • Gestión de Incidentes en la Seguridad de la Información <div style="display: inline-block; vertical-align: middle; margin-left: 10px;"> } Reportes de Eventos, de Debilidades Responsabilidades y procedimientos </div> • Control de Acceso <div style="display: inline-block; vertical-align: middle; margin-left: 10px;"> } De los Usuarios A: las redes, los sistemas operativos, a las aplicaciones Controles de entrada </div> 	✓ Encuestas

		<ul style="list-style-type: none"> • Seguridad Física Ambiental y <ul style="list-style-type: none"> físicos Seguridad de las oficinas Protección contra amenazas externas y ambientales • Gestión de Activos de <ul style="list-style-type: none"> Gestión de los equipos Inventario, propiedad y uso de los activos Clasificación de la información 	<ul style="list-style-type: none"> ✓ Entrevista ✓ Observación Directa
--	--	--	---

Fuente: el Autor.

CAPÍTULO III

MARCO METODOLÓGICO

Parella y Martins (2004) expresan que en toda investigación es indispensable que los hechos estudiados, las relaciones establecidas y los resultados obtenidos sean certificaciones importantes con respecto al problema investigado y los nuevos conocimientos que reúnan la consolidación de su validez. Cumple un proceso que aplica métodos científicos donde se procura obtener información relevante y fidedigna para entender, verificar, corregir y aplicar conocimientos.

En esta etapa del trabajo se persigue garantizar la exactitud y la confiabilidad de los datos recolectados. Para ello se debe seguir un proceso ordenado que permita el logro de los objetivos. Este proceso es lo que se conoce como “Marco Metodológico”.

Naturaleza de la Investigación

El diseño de un Plan de Gestión de Seguridad de la Información para la Dirección de Informática de la Alcaldía del Municipio Jiménez está enmarcado dentro de la modalidad de Estudio de Proyecto Factible apoyado en la investigación monográfica documental y de campo, de acuerdo al “Manual para la Elaboración de Trabajo Conducentes a Grado Académico de Especialización, Maestría y Doctorado” aprobado por el Consejo Universitario de la UCLA en su Sesión N° 1353.

Este manual indica que: “Se entenderá por estudios de proyectos una proposición sustentada en un modelo viable para resolver un problema práctico planteado, tendente a satisfacer necesidades institucionales o sociales y pueden referirse a la formulación de políticas, programas, tecnología, métodos y procesos”.

Diseño de Investigación

El proceso de investigación, se realizó a través de las tres fases fundamentales en la formulación de un proyecto factible: Fase I, Diagnóstico; Fase II, Estudio de Factibilidad y Fase III, Diseño del Proyecto según el manual aprobado por la UCLA. A continuación se especifican estas fases.

Fase I. Diagnóstico

En esta fase se realizó un análisis de la situación actual de la Alcaldía del Municipio Jiménez con el objeto de recolectar información suficiente sobre la Seguridad de la Información que maneja actualmente y así determinar sus deficiencias en cuanto a la misma. Esto permite proponer un Plan de Gestión de la Seguridad de la Información para manejar el riesgo y mejorar la Seguridad de la Información que produzca resultados en concordancia con las políticas y objetivos generales de la Alcaldía.

Este análisis toma en cuenta los Controles y Objetivos de Control de la Norma ISO/IEC 27002:2005 aplicados a través de técnicas e instrumentos metodológicos al personal que trabaja en la Alcaldía del Municipio Jiménez.

Población y Muestra

Balestrini, M. (1998) indica que: “Una población o universo puede referirse a un conjunto de elementos de los cuales se pretenden indagar y conocer sus características, o una de ellas, y para el cual serán válidas las conclusiones obtenidas en la investigación...”.

Para efectos de esta investigación la población viene dada por los cuarenta (40) usuarios de la red de la Alcaldía, distribuidos en los distintos departamentos los

cuales son los que actualmente comparten los recursos y utilizan el sistema administrativo, así como también los servicios de internet, correo electrónico, entre otros.

De acuerdo a lo expuesto por Ary, W. (1996): “...si la población posee pequeñas dimensiones, debe ser seleccionada en su totalidad, para así reducir el error en la muestra”, de esta manera la muestra representada en este caso por el total de la población se presenta en el cuadro N° 3.

Cuadro N° 3 Usuarios de la Red de la Alcaldía.

Direcciones o Departamentos	Cantidad
Informática	2
Presupuesto	3
Administración	2
Hacienda	6
Despacho	1
Auditoría	2
Sala	2
Desarrollo Social	2
Servicios Generales	3
Servicios Contables	4
Tesorería	4
Recursos Humanos	5
Sindicatura	2
Control y Gestión	2
Total	40

Fuente: el autor

Técnicas e Instrumentos de Recolección de Datos

Para Ugel (2005) “La recolección de datos es un proceso meticuloso y difícil, pues requiere un instrumento de medición que sirva para obtener la información

necesaria para estudiar un aspecto o el conjunto de aspectos de un problema”. En este caso se prevé usar para recolectar los datos son: encuestas o cuestionario, entrevistas y observación directa.

La encuesta es definida por Zapata (2005) como un conjunto de técnicas destinadas a reunir, de manera sistemática, datos sobre determinado tema o temas relativos a una población, a través de contactos directos o indirectos con los individuos o grupos de individuos que integran la población estudiada.

De acuerdo a los objetivos perseguidos por la presente investigación, se diseñó un cuestionario para comprobar que el problema existe y censar la posibilidad de aceptación del diseño de un Plan de Gestión de Seguridad de la Información.

De igual manera la entrevista se usó para obtener datos sobre el problema específico de esta investigación tomando en cuenta lo planteado por Ugel (ob.cit) “En la entrevista una persona (el encuestador) solicita información a otra (el sujeto investigado o encuestado) para obtener datos sobre un problema específico, es decir, debe haber un intercambio verbal entre dos personas.” La modalidad de esta técnica será no estructurada para poder realizar preguntas abiertas dejando de esta manera mayor libertad al sujeto entrevistado y al investigador.

Ugel (ob.cit) define a la Observación directa como:

El fenómeno en estudio es una técnica bastante objetiva de recolección; con ella puede obtenerse información aun cuando no existía el deseo de proporcionarla y es independiente de la capacidad y veracidad de las personas a estudiar; por otra parte, como los hechos se estudian sin intermediarios, se evitan distorsiones de los mismos, sin embargo, debe cuidarse el entrenamiento del observador, para que la observación tenga validez científica.

Cabe mencionar que la observación directa y la entrevista contemplan los Controles y Objetivos de Control contenidos en la Norma ISO/IEC 27002:2005, para así proponer el diseño de un plan de gestión de Seguridad de la Información para la dirección de informática de la alcaldía del municipio Jiménez, basado en la Norma ISO/IEC 27001:2005.

Para recolectar los datos que se requieren para complementar la verificación de que el problema existe, se utilizó la técnica de observación directa, no participante y sistemática en la realidad objeto de estudio.

Validez y Confiabilidad del Instrumento

Para Bernal (2006) “Un instrumento de medición es válido cuando se mide aquello lo cual está destinado”. Para determinar si se está midiendo realmente lo esperado y así darle validez al instrumento en esta investigación, ellos son sometidos a la evaluación de tres expertos en el área y un metodólogo.

Por su parte se dice que un instrumento es confiable si: “se miden fenómenos o eventos una y otra vez con el mismo instrumento de medición ¿se obtienen los mismos resultados u otros similares? Si la respuesta es afirmativa, se dice que el instrumento es confiable” Bernal (ob.cit)

Para efectos de esta investigación la confiabilidad se determina a través del método de Kurder-Richardson (K-R₂₀), el cual permite obtener una medida del grado de homogeneidad de los ítems del instrumento, así como también su consistencia interna del mismo. El modelo de Kuder-Richardson (K-R₂₀), es aplicable en los instrumentos de ítems dicotómicos en los cuales existen respuestas: correctas e incorrectas, verdaderas y falsas, sí y no; el cual se representa de la siguiente manera:

$$\Gamma_{tt} = \left(\frac{k}{k-1} \right) * \left(\frac{v_t - \sum pq}{v_t} \right)$$

Donde:

r_{tt} = Es el coeficiente de confiabilidad KR₂₀.

K= es el numero de ítems de la escala

v_t = es la varianza total de la prueba.

p= es la proporción de las respuestas que corresponden a una de las dos categorías.

q= es 1-p

$\sum pq$ = es la sumatoria de la varianza individual de los ítems.

El índice de confiabilidad debe ser menor o igual a uno (1) para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la exactitud y objetividad en los resultados.

Fase II. Estudio de Factibilidad

Según Senn, J. (1987) “la factibilidad es la posibilidad de que el Plan sea beneficioso para la organización”. En este sentido, para la propuesta se hace necesario determinar la factibilidad operativa, técnica, financiera y económica.

Factibilidad Operativa

Según Mendoza, R. (2009): “la prueba de factibilidad cuestiona, si el sistema trabajará cuando se desarrolle, instale y aplique”. Al trabajo se le deben hacer tres (3) cuestionamientos: 1º Un nuevo sistema puede ser demasiado complejo para los usuarios de la organización o los operadores del sistema. En este caso, los usuarios pueden ignorarlo o usarlo de tal forma que cause errores. 2º Un nuevo sistema puede hacer que los usuarios se resistan a él, como consecuencia de una técnica de trabajo,

miedo a ser desplazados, interés en el sistema antiguo u otras razones. 3° Un nuevo sistema puede introducir cambios demasiado rápido que impidan que el personal pueda adaptarse a él ó aceptarlo.

Factibilidad Técnica

Según Mendoza, R. (2009): “Ésta factibilidad analiza la relación entre medios y fines”. La pregunta básica es: ¿Son los medios y estrategias que se proponen adecuados para el logro de los fines y objetivos buscados? En esta investigación se evalúa si el equipo y/o software están disponibles y si se tienen las capacidades técnicas requeridas para cada alternativa del diseño considerado. De igual manera se consideró si la organización tiene el personal con experiencia técnica suficiente para diseñar, implantar, operar y mantener el sistema propuesto.

Factibilidad Económica

Según Mendoza, R. (2009): “En ésta Factibilidad relaciona con la disponibilidad de recursos humanos, materiales y financieros. Pretende definir, mediante comparación, los beneficios y los costos estimados de un proyecto, para determinar si es recomendable su implementación y posterior operación. En el desarrollo de un sistema, los beneficios financieros deben igualar o exceder los costos de inversión para la empresa.

Fase III. Diseño del Proyecto

Cumplidos los requisitos estipulados por las Fases I y II y de acuerdo a lo requerido en esta fase se realizan las siguientes actividades, tomando como referencia la norma ISO/IEC 27001:2005:

1. Definir el alcance del SGSI.
2. Definir las Políticas
3. Definir el enfoque de valuación de riesgos.

4. Identificar los riesgos.
5. Analizar y evaluar cada riesgo.
6. Identificar y evaluar las opciones para el tratamiento de los riesgos.
7. Seleccionar los objetivos de Control y Controles para el tratamiento de riesgos.

Aspectos Administrativos

En esta sección se definen los tres (3) recursos más importantes de toda investigación: humanos, financieros y tiempo.

Para el diseño de un Plan de Gestión de Seguridad de la Información para la Alcaldía del Municipio Jiménez del Estado Lara, se cuenta con los siguientes recursos: (a) **Humanos**. Todos los usuarios de la red de la alcaldía a los cuales se les aplicó el instrumento. El investigador también es parte el recurso humano así como el metodólogo y los dos expertos que validaron el instrumento. (b) **Financieros**. Los recursos económicos asociados al proyecto, (ver cuadro N° 4). (c) **Tiempo**. Se controla mediante un cuadro de “Cronograma de Actividades” en el cual se especifican las actividades realizadas en función del tiempo de ejecución. Se representa mediante un Diagrama de Gantt, (ver el anexo A).

Cuadro N° 4. Presupuesto.

<i>ITEM</i>	<i>ACTIVIDADES PRINCIPALES EN LAS QUE SE UTILIZA</i>	<i>CANT.</i>	<i>COSTO UNITARIO</i>	<i>COSTO TOTAL</i>
Computador portátil	Transcripción de la información, elaboración de instrumentos,	1	Bs 6.000,00	Bs 6.000,00
Impresora multifuncional		1	Bs 800,00	Bs 800,00
Libros	Consulta y estudio de temas relacionados con la investigación.	3	Bs 100,00	Bs 300,00
Resmas de papel bond	Reproducción de instrumentos y material de referencia, toma de notas, levantamiento de información.	3	Bs 40,00	Bs 120,00
Cartucho color		2	Bs 180,00	Bs 360,00
Cartucho negro		2	Bs 120,00	Bs 240,00

Fotocopias		300	Bs 0,25	Bs 75,00
Encuadernado		5	Bs 12,00	Bs 60,00
Empastado		5	Bs 120,00	Bs 600,00
Internet banda ancha	Consultas electrónicas	1	Bs 140,00	Bs 140,00
<i>TOTAL</i>				Bs 8.695,00

CAPITULO IV

RESULTADOS DEL ESTUDIO

En este capítulo se desarrollaron las fases descritas en el capítulo anterior.

Fase I: Diagnóstico

La recolección de los datos se hizo mediante la aplicación del cuestionario “DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA” encontrado en el Anexo “B” el cual constó de diez (10) ítems cerrados para medir actitudes y opiniones. Dicho cuestionario fue aplicado a todo el personal de la alcaldía del Municipio Jiménez, que trabaja con los sistemas de información. Esto con el fin de corroborar el estado de la seguridad de la información y la posibilidad de aceptación del Diseño del Plan de Seguridad de la Información.

Validez y confiabilidad de los instrumentos

Para evaluar el contenido de los instrumentos utilizados, se siguió el procedimiento sugerido, es decir, se sometió a la validez de criterios por juicio de expertos a través del formato para la validación del instrumento, presentado en el Anexo “C”. Dichos instrumentos fueron aplicados a la Lcda. Msc. Morely Bullones, la Lcda. Luzmary Pérez y La Ing. Miledy Querales.

Para efectos de la confiabilidad del instrumento “cuestionario” se le aplicó el método de Kuder-Richardson ($K-R_{20}$) el cual es conveniente cuando se usan preguntas dicotómicas. Una vez realizado los cálculos pertinentes a los valores correspondientes se obtuvo un $K-R_{20} = 0,7676$, lo cual se traduce en que el instrumento es de “Fuerte confiabilidad” según se establece en la fase de validez y

confiabilidad de los instrumentos de la presente investigación (ver pág. 44), además se considera que cada pregunta tiene igual importancia para el investigador.

Resultados de la aplicación del Cuestionario

Ítem 1.

A continuación se muestra en el cuadro N° 5 la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿Tiene usted conocimiento sobre lo que significa un Plan de Seguridad de Información?, y el porcentaje correspondiente

Cuadro N° 5

Item 1	SI	NO	TOTAL
frecuencia	26	14	40
%	65	35	100

Según se observa en el Cuadro N° 5 el 65 % de la población encuestada afirman que tienen conocimiento acerca de lo que significa el Plan de Seguridad de la Información, mientras que el 35 % manifiestan que desconocen dichos planes. Aun cuando la diferencia no es significativa se hace imprescindible el adiestramiento de todo el personal que labora en la Alcaldía en el tema de seguridad. Todo esto para lograr comprender todas las acciones que deben establecerse dentro de lo que es un Plan de Seguridad de la Información.

Ítem 2.

A continuación se muestra en el cuadro N° 6 la cantidad de respuestas afirmativas y negativas en relación a la interrogante ¿Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica de la Alcaldía? y el porcentaje correspondiente

Cuadro N° 6

Item 2	SI	NO	TOTAL
frecuencia	38	2	40
%	95	5	100

En el cuadro N° 6 se observa que, existe un clara tendencia del 95% de los encuestados los cuales opinan que el Plan de Seguridad a implementarse en la alcaldía permitirá mejorar y ampliar la calidad tecnológica, actualizando la plataforma existente.

Ítem 3.

A continuación en el cuadro N° 7 se muestra la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿Cree usted que se logrará un cambio positivo con la aplicación de este plan de seguridad de información en la plataforma tecnológica de la Alcaldía del Municipio Jiménez? y su porcentaje correspondiente.

Cuadro N° 7

Se puede observar en el cuadro N° 7 que el 95% de los encuestados considera que la aplicación del plan de seguridad de la información, logrará cambios positivos a nivel tecnológico en la alcaldía del Municipio Jiménez.

Ítem 4.

Item 3	SI	NO	TOTAL
frecuencia	34	6	40
%	95	5	100

A continuación se muestra en el cuadro N° 8 la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica de la alcaldía del Municipio Jiménez? y su porcentaje correspondiente.

Cuadro N° 8

Item 4	SI	NO	TOTAL
frecuencia	33	7	40
%	82,5	17,5	100

El cuadro 8, muestra que el 82,5%, de los encuestados manifiestan su aprobación a la implementación del Plan de Seguridad de la Información en la alcaldía del municipio Jiménez, para mejorar la calidad de la información que se maneja.

Ítem 5.

En el cuadro N° 9 se muestra la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información en la Alcaldía del Municipio Jiménez?, y su porcentaje correspondiente.

Cuadro N° 9

Item 5	SI	NO	TOTAL
frecuencia	27	13	40
%	67,5	32,5	100

En el cuadro 9 se observa que el 67,5%, de los encuestados están de acuerdo en que en la alcaldía exista un programa para la sensibilización del personal, lo cual es un factor preponderante para el éxito de la implementación de un Plan de Seguridad de Información.

Ítem 6.

En el cuadro 10 se puede observar la cantidad de respuestas afirmativas y negativas en relación a la interrogante ¿Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones de esta alcaldía?

Cuadro N° 10

Item 6	SI	NO	TOTAL
frecuencia	35	5	40
%	87,5	12,5	100

Como se muestra en el cuadro 10 el 87,5%, de los encuestados están dispuestos a colaborar con la implementación del Plan de Seguridad de la Información en la alcaldía del municipio Jiménez, para obtener mejoras en la plataforma tecnológica.

Ítem 7.

En el cuadro 11 se puede observar la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿Sabe usted si existe un plan de recuperación ante desastres en la Alcaldía del Municipio Jiménez? Con su porcentaje correspondiente.

Cuadro N° 11

Item 7	SI	NO	TOTAL
frecuencia	18	22	40
%	45	55	100

Nótese en el cuadro N° 11 que el 55% de los encuestados opina que no existe una estrategia de recuperación ante desastre, lo que significa que en la alcaldía desconocen si se cuenta con un plan de recuperación para aplicaciones críticas y así proporcionar la continuidad de negocio.

Ítem 8.

En el cuadro N° 12 se puede observar la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿En la Alcaldía del Municipio Jiménez han realizado evaluación de riesgos relacionados con la información?, con su porcentaje correspondiente

Cuadro N° 12

Item 8	SI	NO	TOTAL
frecuencia	13	27	40
%	32,5	67,5	100

Se observa en el cuadro N° 12, que el 67,5% opina que la alcaldía no cuenta con el análisis de riesgos relativo a los sistemas de información lo cual constituye una pieza importante para la selección de controles a aplicar e incluso la base para elaborar el Plan de Seguridad de la Información.

Ítem 9.

En el cuadro N° 13 se puede observar la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿En la Alcaldía del Municipio Jiménez han realizado una evaluación de vulnerabilidades de la red? y su porcentaje correspondiente.

Cuadro N° 13

Item 9	SI	NO	TOTAL
frecuencia	12	28	40
%	30	70	100

En el cuadro N° 13, se observa que el 70%, de los encuestados manifiesta que la alcaldía no cuenta con el análisis de vulnerabilidad, lo cual es una debilidad en la seguridad de la información, pues permite que una amenaza pueda afectar a un activo.

Ítem 10.

En el cuadro N° 14 se puede observar la cantidad de respuestas afirmativas y negativas en relación a la interrogante: ¿La Alcaldía del Municipio Jiménez cuenta con software antivirus actualizado? y su respectivo porcentaje.

Cuadro N° 14

Item 10	SI	NO	TOTAL
frecuencia	10	30	40
%	25	75	100

En el cuadro N° 14, se observa una tendencia del 75%, que opina que la alcaldía no posee antivirus actualizado, lo cual es muy importante para evitar daños a la información y los procesos.

De los resultados obtenidos a través de la encuesta se puede apreciar que:

En relación a la necesidad al diseño del Plan de Gestión de Seguridad de la Información se pudo observar que:

- Un 65% del personal de la Alcaldía tiene conocimiento acerca del Plan de Seguridad de la Información mientras que el 35% manifiestan el desconocimiento de dicho Plan.
- Un 95 % de los encuestados coinciden en que el diseño del Plan de Seguridad de la Información permitirá mejorar y ampliar la calidad tecnológica, además logrará cambios positivos a nivel tecnológico en la alcaldía del Municipio Jiménez.
- Un 82,5% del personal que labora en la Alcaldía está de acuerdo con el Diseño del Plan de Seguridad de la Información para mejorar la calidad de la información que se maneja.
- Un 67,5%, de los encuestados están de acuerdo en que exista un programa para la sensibilización del personal, en cuanto a Seguridad de Información.

En relación a los problemas existentes en cuanto a la Seguridad de la Información se pudo observar que:

- Un 55% de los encuestados opina que no existe una estrategia de recuperación ante desastre, lo que significa que en la alcaldía no cuenta con un sistema o plan de contingencia en caso de desastre.
- Un 67,5% opina que la alcaldía no cuenta con el análisis de riesgos relativo a los sistemas de información lo cual constituye una pieza importante para la selección de controles a aplicar e incluso la base para elaborar el Plan de Seguridad de la Información
- Un 70%, de los encuestados manifiesta que la alcaldía no cuenta con el análisis de vulnerabilidad.
- Un 75%, de los encuestados opina que la alcaldía no posee antivirus actualizado, lo cual es muy importante para evitar daños a la información y los procesos.

Resultados de la Entrevista

La entrevista mostrada en el Anexo “K” fue aplicada a la Directora de Recursos Humanos y la Directora de Informática de la Alcaldía, pues se requería información gerencial que solo ellos manejan. Esto se realizó con el fin de corroborar el estado de la seguridad informática, y de los controles pertinentes a la seguridad de la información, en este sentido, se obtuvieron como resultado las siguientes respuestas para cada una de las preguntas analizadas en la Cuadro N° 15:

Cuadro N° 15. Resultados de la Entrevista

<i>Pregunta</i>	<i>Respuesta de la Directora de Informática</i>	<i>Comentario</i>
1.- ¿Considera usted que deben existir políticas de seguridad para la plataforma tecnología de la Alcaldía del Municipio Jiménez?	Si	Las políticas de seguridad deben estar documentadas y ser de conocimiento de los empleados que sean afectados por estas políticas.
2.- ¿Existe un documento que defina las políticas de seguridad de información de la Alcaldía del Municipio Jiménez?	No se tiene	Se debe consolidar toda la información referente a políticas de seguridad, ya que este es un elemento de control dentro del funcionamiento de la seguridad de información.
3.- ¿Conoce usted alguno de los estándares de seguridad de información?	No	Es imprescindible que el personal que labora en el área de tecnología, tenga conocimientos del área de seguridad, pues se debe comprender todas las acciones que deben establecerse en un plan de seguridad de información.
4.- ¿El manejo de la Información de la Organización está en manos del personal que tiene responsabilidad directa sobre ella?	No.	Un elemento indispensable para establecer confidencialidad es tener clara la importancia de la información.
5.- ¿Indique si la institución posee	No	Un programa para sensibilizar a los

programas dirigidos a sensibilizar a los empleados sobre la Seguridad de la Información?		empleados es factor predominante a la hora de aplicar un plan de seguridad de información.
6.- ¿Existe un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información, relacionada con la Alcaldía?	No se tiene pues en oportunidades se llevan información fuera de la institución y no se sabe que sucede con ella.	En este ítem se evidencia que no existe tal acuerdo, documento muy importante a la hora de evaluar responsabilidades.
7.- ¿En la institución han realizado pruebas de penetración perimetral?	NO	La prueba de penetración consiste en evaluar la seguridad de los sistemas accesibles desde Internet (routers exteriores, firewall, servidores web, de correo, de noticias, etc), intentando penetrar en ellos y de esta forma alcanzar zonas de la red de una empresa como puede ser la red interna o la DMZ.
<i>Pregunta</i>	<i>Respuesta de la Directora de Recursos Humanos</i>	<i>Comentario</i>
1.- ¿El manejo de la Información de la Organización está en manos del personal que tiene responsabilidad directa sobre ella?	No, a veces ésta es manipulada por pasantes o personal contratado temporalmente.	Un elemento indispensable para establecer confidencialidad es tener clara la importancia de la información.
2.- ¿Indique si la institución posee programas dirigidos a sensibilizar a los empleados sobre la Seguridad de la Información?	No	Un programa para sensibilizar a los empleados es factor predominante a la hora de aplicar un plan de seguridad de información.
3.- ¿Existe un documento donde los empleados, acuerden la confidencialidad de la información, relacionada con la Alcaldía?	No se tiene.	En este ítem se evidencia que no existe tal acuerdo, documento muy importante a la hora de evaluar responsabilidades.
4.- ¿Existe un documento donde estén definidas las	No se tiene.	Se puede evidenciar que no se tiene este documento el

responsabilidades para la terminación o cambio de empleo para los empleados, de la Alcaldía?		cual es muy importante a la hora de evaluar responsabilidades.
---	--	--

Resultados de la Observación Directa

La observación directa se realizó usando los objetivos de control estipulados en el estándar ISO/IEC 27001:2005, con el fin de corroborar el estado de la seguridad informática en la Alcaldía, a continuación se detalla en la Cuadro N° 16 los aspectos considerados y observados.

Cuadro N° 16. Observación Directa en base a los Controles

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Manejar la Seguridad de la Información dentro de la organización.		
A.6.2 Entidades externas		
Objetivo: Mantener la Seguridad de la Información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados y/o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	<u>Observación Directa:</u> No existe análisis de riesgo, no se maneja la criticidad de las aplicaciones, datos o servicios que maneja la Alcaldía, hecho corroborable en el cuestionario(ítems 8)
A.7 Gestión de activos		
A.7.1 Responsabilidad por los activos		
Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	<u>Observación Directa:</u> la Alcaldía posee inventarios sobre los activos tangibles que esta maneja pero no está estandarizado, además no se cuenta con el inventario de los servicios de información.
A.7.2 Clasificación de la información		
Objetivo: Asegurar que la información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	<u>Observación Directa:</u> No existen lineamientos de clasificación, existe desconocimiento en cuanto a la clasificación de la información vital para la Alcaldía, hecho corroborable en la entrevista (Preg. 4)
A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo		
Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus		

responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	<u>Observación Directa:</u> si existen roles mas no se cumplen con las responsabilidades establecidas, pues personal externo a la institución tienen acceso a información confidencial sin que exista un compromiso establecido en caso de pérdida o robo de la misma. Hecho corroborable en la entrevista (Preg. 4)
A.8.1.3	Términos y condiciones de empleo	<u>Observación Directa:</u> los empleados de la Alcaldía no mantienen un acuerdo de confidencialidad de datos, no existe una clausula en los contratos para ello, pues en oportunidades se ha dado el caso que empleados que son notificados de su despido de la institución borran información y no se toman medidas en contra de esas personas. Hecho corroborable en la entrevista (Preg. 4)
A.8.2 Durante el empleo Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	<u>Observación Directa:</u> No existe gestión de responsabilidades, ya que no existen políticas de seguridad establecidas por tanto el personal externos no tiene compromiso establecido con dichas políticas, hecho corroborable en la entrevista (Preg. 1).
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	<u>Observación Directa:</u> No están definidas claramente las responsabilidades para realizar la terminación o cambio del empleo, ya que el personal de la institución que es notificado de su despido borra información y no se toman medidas en contra de ellos.
A.9 Seguridad física y ambiental		
A.9.1 Áreas seguras Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	<u>Observación Directa:</u> no existe tal perímetro de seguridad física, pues en oportunidades se ha violado la seguridad perimetral sin que se haya tomado medidas para evitarlo, además no

		<p>hay cuarto de servidores, no hay cuarto de cableado principal, se violenta las normas de cableado estructurado, no hay cableado certificado, todo esto está documentado a continuación fotográficamente:</p>
 <p>Foto N°1: el cableado eléctrico expuesto.</p>	 <p>Foto N° 2: Router expuesto y cableado sin canalización.</p>	 <p>Foto N° 3: Servidor sin respaldo y expuesto, al igual que el Firewall.</p>
 <p>Foto N°4: el cableado eléctrico expuesto, sin resguardo.</p>	 <p>Foto N° 5: Router expuesto y cableado sin canalización.</p>	 <p>Foto N° 6: cableado sin rack ni canalización.</p>
<p>A.9.2 Seguridad del equipo</p> <p>Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización</p>		
A.9.2.1	Ubicación y protección del equipo	<p><u>Observación Directa:</u> No existe plan de contingencia, ya que los equipos están expuestos sin que tenga acceso solo personal autorizado. Hecho demostrado fotográficamente en el control A.9.1.1</p>
<p>A.10 Gestión de las comunicaciones y operaciones</p>		
<p>A.10.1 Procedimientos y responsabilidades operacionales</p> <p>Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información</p>		
A.10.1.1	Procedimientos de operación documentados	<p><u>Observación Directa:</u> No existen normas y procedimientos, pues en oportunidades se han robado medios de procesamiento sin medidas para repercutir esto.</p>
<p>A.10.2 Gestión de la entrega del servicio de terceros</p> <p>Objetivo: Implementar y mantener el nivel apropiado de Seguridad de la Información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.</p>		
A.10.2.1	Entrega del servicio	<p><u>Observación Directa:</u> No existe documentación que asegure que los terceros implementen, operen y mantengan los controles de seguridad.</p>

A.10.3 Planeación y aceptación del sistema		
Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	<u>Observación Directa:</u> No existe monitoreo de consumo de los recursos que permita realizar proyecciones de su uso asegurando el desempeño de los sistemas.
A.10.4 Protección contra software malicioso y código móvil		
Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	<u>Observación Directa:</u> Existe antivirus en las estaciones de trabajo, sin embargo en aquellas que no se encuentran en red la actualizaciones las realiza una persona utilizando un pendrive.
A.10.5 Respaldo (backup)		
Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	Backup o respaldo de la información	<u>Observación Directa:</u> se hacen respaldos de la data del sistema administrativo a diario pero no se cuenta con respaldo fuera de la institución, por lo que en una oportunidad un alto funcionario fue despedido, borro la información y no se contaba con respaldo de dicha información.
A.10.6 Gestión de seguridad de redes		
Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	<u>Observación Directa:</u> no existe, porque existen recursos compartidos a los que tienen acceso los equipos que se encuentran dentro de la red sin que haya restricciones para algunos usuarios.
A.10.7 Gestión de medios		
Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	<u>Observación Directa:</u> No existen procedimientos normados para el manejo de información en medios removibles.
A.10.8 Intercambio de información		
Objetivo: Mantener la Seguridad de la Información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	<u>Observación Directa:</u> No existen procedimientos para aquellas organizaciones externas a la institución que maneja información vital de la alcaldía.
A.10.9 Servicios de comercio electrónico		

Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.10 Monitoreo		
Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	Registro de auditoría	<u>Observación Directa:</u> No existen el monitoreo para el control de accesos a usuarios.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso		
Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	<u>Observación Directa:</u> No existen el monitoreo , por tanto no existe las políticas para el control de accesos.
A.11.2 Gestión del acceso del usuario		
Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a la los sistemas de información.		
A.11.2.1	Inscripción del usuario	<u>Observación Directa:</u> Existe un procedimiento de registro a través de un memorándum pero no se establece los permisos pertinentes a ciertos usuarios(por ejemplo: acceso a pasantes o personal contratado temporalmente.
A.11.3 Responsabilidades del usuario		
Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
A.11.3.1	Uso de clave	<u>Observación Directa:</u> existen las claves sin embargo son compartidas por algunos usuarios que las transfieren.
A.11.4 Control de acceso a redes		
Objetivo: Evitar el acceso no autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	<u>Observación Directa:</u> No existen porque los usuarios no se les proporciona restricciones de acuerdo a la función que cumplen(por ejemplo: los usuarios pueden ver información de dependencias que no son donde laboran).
A.11.5 Control de acceso al sistema de operación		
Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	<u>Observación Directa:</u> Existen, solo que todos usan la misma clave.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información		

Objetivo: Asegurar que la información de los eventos y debilidades en la Seguridad de la Información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	<u>Observación Directa:</u> No existe, pues que una vez que el hecho ocurre es informado mucho después que ocurre.
A.13.2 <i>Gestión de incidentes y mejoras en la seguridad de la información</i> Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	<u>Observación Directa:</u> No existe pues no se toman medidas inmediatas cuando ocurre un incidente de seguridad.

Conclusiones generales de la fase de Diagnóstico

1. En la Alcaldía no existen Políticas de Seguridad de la Información, que permita salvaguardar los activos de información de la institución y la infraestructura, de los riesgos a los que se encuentran expuestos.
2. La Alcaldía no cuenta con controles en cuanto a seguridad física y control de acceso, por lo que la institución y los activos de información están expuestos a amenazas y riesgo.
3. No existen procedimientos de gestión normados en cuanto al manejo de usuarios, claves, roles y responsabilidades.
4. La Alcaldía no dispone de un Plan de Gestión de Seguridad de la Información.
5. No utilizan sistemas de respaldo de la información vital para la institución, por lo que es recurrente la pérdida de información por parte del personal tanto interno como externo a ésta.
6. La Alcaldía no cuenta con seguridad perimetral por lo que la red está expuesta a vulnerabilidades.

Factibilidad Técnica

La viabilidad técnica de esta propuesta está garantizada, ya que:

1. La norma ISO/IEC 27001:2005 es, en sí misma, un modelo extenso y detallado, en el cual se especifican las etapas que se deben cumplir para la implantación de un SGSI.

2. Existe una gran cantidad de metodologías y herramientas para el Análisis y la Gestión del Riesgo que facilitan dicho análisis.
3. En el país (Venezuela) operan empresas que ofrecen capacitación en la norma ISO/IEC 27001:2005.
4. La Alcaldía del Municipio Jiménez cuenta con personal capacitado para liderar este proyecto.
5. La Alcaldía del Municipio Jiménez cuenta con el equipo informático suficiente (computadoras y periféricos) para el desarrollo de esta propuesta.

Factibilidad Económica

La factibilidad económica de esta propuesta está garantizada, ya que:

1. La Alcaldía del Municipio Jiménez, consciente de los beneficios de apoyar la Seguridad de la Información, aprueba la elaboración del Diseño del Plan de Seguridad de la Información, hecho corroborable en el Cuestionario y la Entrevista
2. Existen metodologías y herramientas gratuitas para llevar a cabo el diseño, la instalación y operación de un SGSI, como por ejemplo: ELIPSE, EBIOS, MAGERIT e ISO27001.
3. La Alcaldía del Municipio Jiménez cuenta con personal que está en la disposición y en la capacidad de formarse en el diseño, implantación, operación y monitoreo del SGSI.

Factibilidad Operativa

La factibilidad operativa está garantizada, ya que:

1. Existe muy buena disposición por parte de la Alcaldía del Municipio Jiménez, para mejorar la Seguridad.
2. El personal de la Dirección de Informática de la Alcaldía del Municipio Jiménez, tiene experiencia en el área de computación y están familiarizados con los aspectos de la seguridad tecnológica.
3. El personal de la Alcaldía del Municipio Jiménez está consciente de los incidentes de seguridad que han ocurrido y han solicitado mejorar la seguridad física y el control de acceso a las instalaciones.

4. El personal de la Alcaldía del Municipio Jiménez ha colaborado en el desarrollo de este trabajo de seguridad y sus observaciones han sido de gran ayuda.

Fase III: Diseño del Plan de Seguridad de la Información.

En concordancia con la norma ISO/IEC 27001:2005 se realizaron las actividades y sub-actividades que se detallan en la Cuadro N° 17:

Cuadro N° 17. Actividades y Sub-actividades del Diseño del Plan de Seguridad

<i>DISEÑO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN</i>	
1.- Definición del SGSI	<ul style="list-style-type: none"> ✓ Identificación del alcance del SGSI ✓ Definición de la Política de Seguridad del SGSI.
2.- Evaluación de riesgos.	<ul style="list-style-type: none"> ✓ Definición de una metodología para la clasificación de los riesgos. ✓ Identificación y tasación de activos. ✓ Evaluación de la posibilidad de que las amenazas y vulnerabilidades ocurran. ✓ Cálculo de los riesgos de seguridad.
3.- Tratamiento de los riesgos	<ul style="list-style-type: none"> ✓ Selección de controles para reducir el riesgo a nivel aceptable.

1) Definición del SGSI

✓ Identificación del alcance del SGSI

Para definir el alcance del sistema de gestión de Seguridad de la Información en la Dirección de Informática de la Alcaldía se usó el método de las elipses, con el cual se trata de visualizar con mucha precisión los distintos procesos y subprocesos; que componen el alcance. Luego se deben listar los activos de información relacionados con estos procesos. En el contexto de la norma ISO 27001:2005, un activo de información será: "...algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger". Con base a los procesos definidos en la figura N° 3, se listan los activos de información asociados a cada dependencia de la Alcaldía definidos con los

usuarios y dueños de esos procesos, componentes críticos tales como software, hardware e infraestructuras que soportan dichos procesos.

- Activos de Información (*Dirección de Informática*). Bases de datos, documentos del sistema, manuales de usuario, procedimientos documentados, información archivada en medios digitales o impresos.
- Documentos legales (*Sindicatura*). Contratos con proveedores, contratistas, Empleados, Obreros relacionados con los procesos críticos.
- Activos de Software (*Dirección de Informática*). De aplicación, del sistema operativo, nuevos desarrollos que puedan exponer información crítica de la Institución.
- Activos de Hardware (*Dirección de Informática*). Servidores de aplicación, de base de datos, web, de respaldo, PC.
- Servicios (*Dirección de Informática*). De red (TCP/IP, FW, Router, Switch, Acces Point).
- Personas (Recursos Humanos). Empleados, Obreros.
- Otros. Objetivos Generales de la Institución.

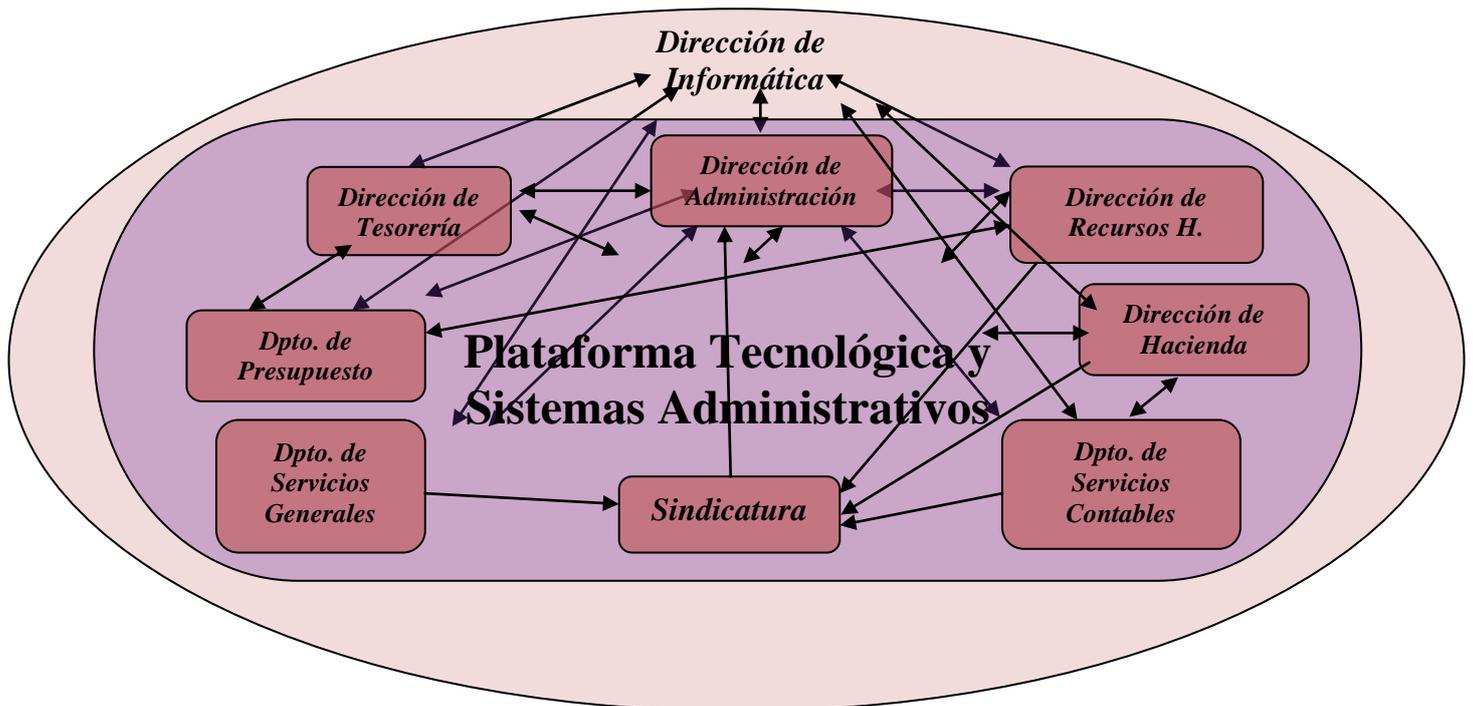


Figura 3. Metodología de las Elipses para Plataforma Tecnológica y Sistemas Administrativos.
Fuente: El Autor

ALCANCE DEL PLAN DE GESTION DE SEGURIDAD DE LA
INFORMACION

DECLARACIÓN

El Plan de Gestión de Seguridad de la Información de la Alcaldía del Municipio Jiménez abarca todas las áreas, procesos, servicios e información vital para garantizar la disponibilidad de los servicios que la Alcaldía presta, tanto a nivel interno como a nivel del Municipio; asegurando la confidencialidad, integridad y disponibilidad de los servicios y los sistemas de información de la Alcaldía. Por ello, se hará énfasis en aquellos activos que, por su valor en relación a la disponibilidad de los sistemas de información y los servicios puedan ser susceptibles a sufrir riesgos de seguridad, y a su vez puedan comprometer el objetivo general de la Alcaldía.

OBJETIVOS

- (a) Garantizar la disponibilidad de los Sistemas de Información administrativos.*
- (b) Garantizar el funcionamiento de estos sistemas y así apoyarlos con las actividades de Soporte Técnico.*
- (c) Minimizar el hurto de parte y piezas de los equipos de computación que se utilizan para el manejo de los sistemas de información administrativos.*

Según lo indicado en el Diseño del Plan de Gestión de Seguridad de la Información, se muestra a continuación las políticas respectivas.

*POLÍTICA DEL PLAN DE GESTION DE SEGURIDAD DE LA
INFORMACION*

DECLARACIÓN.

Los servicios que la Alcaldía presta, la información que permite prestar dichos servicios, las aplicaciones y equipos que lo sustentan, las instalaciones físicas que hospedan los Sistemas de Información y el personal vinculado directamente con la prestación de dichos servicios deben permanecer principalmente disponibles, sin menoscabo de la integridad y de la confidencialidad necesaria para que los servicios se mantengan funcionando. Como norte de acción se velará porque los contribuyentes y público en general reciban un servicio oportuno, adecuado y de calidad que satisfaga sus demandas y que redunde en beneficio de los objetivos generales de la Alcaldía del Municipio Jiménez.

OBJETIVOS

- (a) Asegurar que los contribuyentes y público en general, tengan acceso a los servicios que se prestan dentro de La Alcaldía.*
- (b) Asegurar la veracidad y la completitud de la información necesaria para prestar los servicios que presta la Alcaldía.*
- (c) Garantizar que la información que la Alcaldía maneja o que está contenida en los equipos de computación, sólo sea accedida por sus propietarios o por personal autorizado.*

2) Definir el enfoque de Evaluación de riesgo

Existen muchas metodologías de evaluación de riesgos explicadas en el capítulo II (pág. 45), pero se usó la metodología de la elipse porque dado que los activos de información abarcan diferentes elementos, es importante que se tenga claro cuáles son los activos y sus diferentes clasificaciones, y con el método de elipses se puedan categorizar e identificar dichos activos de forma más exacta.

3) Identificación, Análisis y Evaluación de riesgo

Una vez identificados todos los activos de información comprendidos en el alcance, utilizando la metodología de las elipses, se procede a establecer el SGSI, siguiendo las pautas del estándar ISO 27001:2005 en su sección 4.2.1, donde se establece que el análisis y evaluación de riesgo se debe efectuar de forma disciplinada y sistemática, para determinar cuáles de los activos deben ser protegidos para mitigar su riesgo, así como también determinar cuál es el riesgo residual (riesgo con el cual la institución está decidida a convivir), los pasos a seguir en la aplicación de esta metodología se muestra a continuación en la figura N° 4:

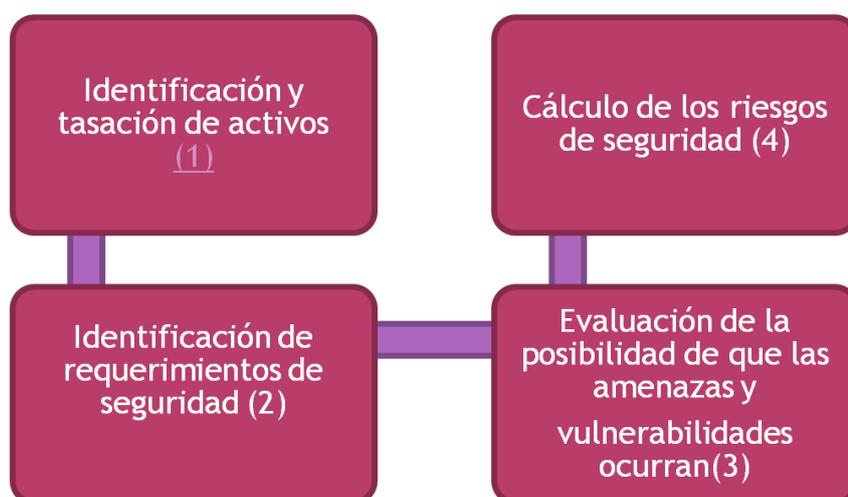


Figura N° 4. Metodología para el Análisis y Evaluación de Riesgo

Fuente: El Autor.

El Cuadro N° 5 muestra la información que se obtuvo del análisis y evaluación de riesgo: (1) Identificación y tasación de activos, la identificación se elaboró mediante el análisis de la Figura 3 a través de las elipses. La tasación se realizó en función de su impacto a su confidencialidad, integridad y disponibilidad con una escala cualitativa entre Alto (A), Medio (M) y Bajo (B). En el cuadro N° 18 se realiza un resumen de todos los activos a los que se le realizó tasación, por la sensibilidad de la información se muestra en forma detallada la tasación de los sistemas administrativos y la plataforma tecnológica, (2) Identificación de requerimientos de seguridad: Estos son los contemplados una vez realizada la tasación. Son los que dieron como resultado Alto (A) en la columna “Total” de tasación, identificados en el cuadro N° 18, (3) Evaluación de la posibilidad de que las amenazas y vulnerabilidades ocurran. Esto se llevó a cabo a través de la técnica de lluvia de ideas aplicada al personal involucrado en los procesos, descritos en la Figura 3 Pág. 67, (4) Cálculo de los riesgos de seguridad: Esto fue establecido haciendo el promedio del “Valor Activo” y la “Posible Ocurrencia” dando como resultado “Total General” identificados el cuadro N° 18.

Finalmente se concluyó siguiendo de manera sistemática la metodología, lo que sirvió para identificar los activos que están más expuestos a riesgo y así poder tomar los controles respectivos.

Cuadro N° 18. Realización del Análisis y Evaluación de Riesgo

Activos	Tasación de Activos			Total	Amenazas	PO	Vulnerabilidad	PEV	VA	PO	Total
	Confidencialidad	Integridad	Disponibilidad								
<i>Base de Datos del Sistema</i>	A	A	A	A	<i>Plagio</i>	<i>M</i>	<i>Deficiencia de envío</i>	<i>B</i>	A	M	M
					<i>alteración</i>	<i>B</i>	<i>Desconocimiento</i>	<i>M</i>			
					<i>Privacidad</i>	<i>A</i>	<i>Acceso no autorizado</i>	<i>A</i>			
					<i>Respaldo</i>	<i>A</i>	<i>falta de control de respaldo</i>	<i>A</i>			
<i>Servidor</i>	A	A	A	A	<i>Plagio</i>	<i>M</i>	<i>Acceso no autorizado</i>	<i>A</i>	A	A	A
					<i>Respaldo</i>	<i>B</i>	<i>falta de control de respaldo</i>	<i>A</i>			
					<i>alteración</i>	<i>M</i>	<i>Desconocimiento</i>	<i>B</i>			
					<i>Privacidad</i>	<i>A</i>	<i>Acceso no autorizado</i>	<i>M</i>			
<i>Pc`s de Informática</i>	A	A	A	A	<i>Falta de seguridad</i>	<i>M</i>	<i>Control de acceso</i>	<i>A</i>	A	A	A
					<i>fallos técnicos,</i>	<i>A</i>	<i>energía eléctrica</i>	<i>A</i>			
					<i>errores de usuario,</i>	<i>M</i>	<i>falta de políticas</i>	<i>A</i>			
					<i>falta de seguridad</i>	<i>A</i>	<i>Acceso no autorizado</i>	<i>B</i>			

<i>Sistema Administrativo (SIGESP)</i>	A	A	A	A	<i>Errores de Código</i>	B	<i>Personal no calificado</i>	B	M	A	A
					<i>Código malicioso</i>	M	<i>control de acceso</i>	A			
					<i>fallos técnicos</i>	A	<i>energía eléctrica</i>	A			
					<i>errores de usuario</i>	M	<i>mal entrenamiento</i>	A			
					<i>Fallas de seguridad.</i>	A	<i>falta de políticas</i>	A			
<i>Información vital para la Institución</i>	A	A	A	A	<i>alteración</i>	M	<i>Deficiencia de envío</i>	M	A	M	M
					<i>Privacidad</i>	B	<i>Acceso no autorizado</i>	M			
					<i>Respaldo</i>	A	<i>falta de control de respaldo</i>	A			

Fuente: El Autor

Leyenda: A.....Alto, M.....Medio, B....Bajo.

PO: Posible Ocurrencia

PEV: Posible Explotación de Vulnerabilidad.

VA: Valor del Activo

Opciones para el tratamiento del riesgo

Seleccionar los objetivos de control para el tratamiento de los riesgos.

Luego de identificar, estimar y cuantificar los riesgos, se deben determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, para enfrentarlos de la manera más eficaz.

En la cláusula 4.2.1 (g) de la norma plantea de manera muy precisa que se deben seleccionar objetivos de control y controles apropiados del estándar ISO 27001:2005: (a) Aplicar controles apropiados. (b) Aceptar riesgos consistente y objetivamente. (c) Evitar los riesgos. (d) Transferir los riesgos, y la selección se debe justificar sobre la base de las conclusiones del análisis y evaluación de los riesgos. En general, aquellos riesgos cuya tasación esté estimada como de baja frecuencia, se puede asumir el riesgo y tratarlo más tarde. Por el contrario, los que se estiman de alta frecuencia o tasación ALTA es donde se debe tomar medidas. De las opciones propuestas por la norma se decidió tomar las 2 primeras, por lo que en este caso serán controlados o asumidos. En consecuencia, se deben proponer controles para gestionar los riesgos calificados como tasación ALTA. Estos controles se toman de la ISO/IEC 27002:2005; sin embargo, la norma aclara que los controles propuestos no son exclusivos y podrían adoptarse otro tipos de controles.

Tomando en consideración lo planteado a continuación se muestra en el cuadro N° 19 los controles a implantar para el tratamiento de los riesgos, en aquellos activos donde la tasación resultó Alta. Además en el cuadro N° 20 se muestra una serie de controles para el tratamiento en general en base a los controles de aquellos activos cuya tasación resultó BAJA o MEDIA.

Cuadro N° 19. Controles para el tratamiento de los riesgos.

Activos	Tasación de Activos			Total	Amenazas	PO	Vulnerabilidad	PEV	VA	PO	Total	Controles Propuestos	Clausula
	Confidencialidad	Integridad	Disponibilidad										
Servidor	A	A	A	A	Plagio	M	Acceso no autorizado	A	A	A	A	7.1.3 Uso aceptable de los activos	Gestión de activos.
					Respaldo	B	falta de control de respaldo	A				8.2.3 Proceso Disciplinario	Seguridad ligada a los recursos humanos.
					alteración	M	Desconocimiento	B				11.1.1 Política de control de acceso	Control de Acceso.
					Privacidad	A	Acceso no autorizado	M				11.2.x, 11.3.x, 11.5.x	
Pc`s de Informática	A	A	A	A	Plagio	M	Control de acceso	A	A	A	A	9.1.2 Control físico de ingreso, 9.1.3 Seguridad en las oficinas, 9.2.1 Ubicación y protección del equipo.	Seguridad física y ambiental
					fallos técnicos,	A	energía eléctrica	A				10.1.2 Gestión de Cambios, 10.10.1 Registro de auditoría, 10.10.5 Registro de fallas	Gestión de comunicaciones y operaciones.
					errores de usuario,	M	falta de políticas	A				11.5.3 Sistema de gestión de contraseñas	Control de Acceso.
					falta de seguridad	A	Acceso no autorizado	B				11.1.1 Política de control de A.	Control de Acceso.

Cuadro N° 20. Controles adicionales para el tratamiento de los riesgos.

A.5.1 Política de seguridad de información		
Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información		
A.5.1.1	Documentar política de seguridad de información	Acción: Todos los documentos generados serán entregados a la gerencia de Operaciones para que se encargue de divulgarlo en el resto del personal. Se planteó las políticas de seguridad generales para la plataforma tecnológica de la Alcaldía descritas en la Fase III del diseño.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Manejar la Seguridad de la Información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Acción
	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.	
A.6.1.2	Coordinación y Asignación de responsabilidades de la seguridad de información	Acción
	Descritas en la Fase III del diseño del Plan de Seguridad Informático.	
A.6.1.3	Acuerdos de confidencialidad	Acción
		Se entregó a la Alcaldía un modelo de acuerdo de confiabilidad de la información. <u>Solución Alternativa:</u> Ver anexo E.
A.6.2 Entidades externas		
Objetivo: Mantener la Seguridad de la Información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados y/o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Acción:
	<u>Acción:</u> Descritas en la Fase III del diseño del Plan de Seguridad Informático.	
A.7 Gestión de activos		
A.7.1 Responsabilidad por los activos		
Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.		
	Inventarios de activos	Acción

		Se Creó un formato estandarizado para el control de los activos, debido a que existe inventario mas no existía un formato unificado, además de la sugerencia de que usen el sistema de registro de activos(SIGESP). Descritas en la Fase III del diseño del Plan de Seguridad Informático.
A.8 Seguridad de los Recursos Humanos		
	A.8.1 Antes del empleo Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.	
A.8.1.1	Roles y responsabilidades Acción: Descritas en la Fase III del diseño del Plan de Seguridad Informático.	
	A.8.2 Durante el empleo Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.	
A.8.2.1	Gestión de responsabilidades Acción: Se sugiere la capacitación de uno de los ingenieros de la dirección de informática en Seguridad de la Información para que este personal luego multiplique los conocimientos al resto del equipo.	
	A.8.3 Terminación o cambio del empleo. Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.	
A.8.3.1	Responsabilidades de terminación	Acción: Es necesario crear un procedimiento de terminación de empleo e incluir dentro de los procesos el respaldo y eliminación de las cuentas de acceso a la persona que ya no labora en la institución. Ver anexo G. Se creó un formato de eliminar los niveles de acceso o cualquier otro dispositivo de red cuando se haya terminado el empleo. Ver anexo H
A.9.1 Áreas seguras		
Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización		
A.9.1.1	Perímetro de seguridad física	Se debe delimitar el área de la oficina. Para ello se propone colocar alarmas, de igual colocar sensores de presencia en las cercanías de los equipos susceptibles, para evitar que intrusos interfieran en la seguridad de estos y demás equipos de red. Descritas en la Fase III del diseño del Plan de Seguridad Informático.
A.9.2.1	A.9.2 Seguridad del equipo	

	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización	
	Ubicación y protección del equipo <ul style="list-style-type: none"> • Acción: Se deben reducir peligros ambientales sobre todo en los equipos que se encuentran en áreas exteriores. Sólo debe permitirse acceso al personal autorizado • Descritas en la Fase III del diseño del Plan de Seguridad Informático. 	
A.9.2.2	Servicios públicos Control <ul style="list-style-type: none"> • El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. Se debe coordinar con los entes de CORPOELEC el cronograma de racionamiento del servicio eléctrico y así evitar daños a los equipos. 	
A.9.2.3	Seguridad en el cableado Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la interceptación o daño. Se deben colocar tuberías para la protección del cableado, esto se propuso en la fase II del diseño.	
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	<u>Acción:</u> se crearon los siguientes formatos: formato de control de vulnerabilidades ver anexo I.
	A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de Seguridad de la Información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.	
A.10.2.1	Entrega del servicio Acción: Se deben controlar los cambios en los medios y sistemas de procesamiento de la información. Esto se propuso en la fase II del diseño.	
A.10.3 Planeación y aceptación del sistema		
Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad Acción: Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas de los sistemas durante su desarrollo y antes de su aceptación.	
	Solución Alternativa Descritas en la Fase III del diseño del Plan de Seguridad Informático.	
A.10.4.1	A.10.4 Protección contra software malicioso y código móvil Objetivo: Proteger la integridad del software y la información.	
	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados
	Alternativa de solución: Incorporar en para el firewall reglas para los virus conocidos y software malicioso.	

	Además de la actualización del software del mismo.	
A.10.5.1	A.10.5 Respaldo (backup) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	
	Backup o respaldo de la información	Control Se deben adquirir un sistema de respaldo, además de realizar copias de respaldo de la información y software esencial, se deben probar regularmente.
	Solución Propuesta: Descritas en la Fase II factibilidad.	
A.10.6.1	A.10.6 Gestión de seguridad de redes Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte	
	Controles de red	Acción: sugerir a la gerencia coordine con las empresas proveedoras para la revisión de los contratos de todos los acuerdos de niveles de servicios y así evaluar los niveles de seguridad que estos puedan ofrecer
A.10.7.1	A.10.7 Gestión de medios Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.	
	Gestión de los medios removibles	Control: Incluir a los medios removibles dentro de los activos Acción: Investigar cómo se puede detectar de forma automática la inclusión de un medio removible dentro de la red de la Alcaldía.
A.10.8.1	A.10.8 Intercambio de información Objetivo: Mantener la Seguridad de la Información y software intercambiados dentro de una organización y con cualquier entidad externa.	
	Procedimientos y políticas de información y software	Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas
		Aplicar el formato de acuerdos de confidencialidad de la información
	Alternativa propuesta: aplicar el formato de acuerdos de confidencialidad propuesto para los empleados, para terceros como aliados comerciales y contratistas. Ver anexo E	
A.11.1 Control de acceso		
A.11.1.1	Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información	
	Política de control de acceso Acción Se elaboraron Normas y procedimientos, se puede observar en la Fase III del diseño del Plan de Seguridad Informático.	
	A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información	
A.11.2.1	Inscripción del usuario Control: procedimiento formal para la inscripción de los usuarios dentro de la red. Para ello se creó un Formato de Control de usuarios. Ver anexo J	

	<p>Gestión de privilegios</p> <p>Control: Se debe restringir y controlar la asignación y uso de los privilegios. Para ello se realizó el formato de control de usuarios Ver Anexo J</p>	
A.11.2.3	<p>Gestión de la clave del usuario</p> <p>Control: La asignación de claves se debe controlar a través de un proceso de gestión de inscripción del usuario</p> <p>Acción: Se deben crear usuarios por cada persona que labora en la institución. Ver Anexo J</p>	
A. 13 Gestión de incidentes en la seguridad de la información		
	<p>A.13.1 Reporte de eventos y debilidades en la seguridad de la información</p> <p>Objetivo: Asegurar que la información de los eventos y debilidades en la Seguridad de la Información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.</p>	
A.13.1.1	<p>Reporte de eventos en la seguridad de la información</p> <p>Acción: Formato de reporte de incidencias</p>	
	<p>Generar un formato estándar para el reporte de vulnerabilidades. Ver Anexo N° 20</p>	
	<p>A.13.2 Gestión de incidentes y mejoras en la seguridad de la información</p> <p>Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información</p>	
A.13.2.1	<p>Responsabilidades y procedimientos</p>	<p>Control: Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.</p>
	<p>Solución Alternativa:</p> <p>Sugerir a la gerencia tomar acciones y amonestaciones para incidencias de seguridad de la información. Incluyendo acción de seguimiento contra una persona u organización después de un incidente en la Seguridad de la Información donde se involucre una acción legal (sea civil o criminal). Ver anexo "E"</p>	

Políticas de Seguridad de la Información.

I. Justificación:

Este manual de políticas de seguridad fue elaborado de acuerdo al análisis de riesgos y de vulnerabilidades en las dependencias de la Alcaldía del Municipio Jiménez, por consiguiente el alcance de estas políticas, se encuentra sujeto a la institución.

II. Objetivos.

Objetivo General.

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la institución.

Objetivos Específicos:

Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de la Dirección de Informática en la administración del riesgo. Compromiso de todo el personal de la institución con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

Todos los empleados se convierten en interventores del sistema de seguridad.

III Responsabilidades

Es responsabilidad de la Dirección de Informática, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, revistas internas) de los Procedimientos de Seguridad. Asimismo, es responsabilidad del supervisor inmediato capacitar a sus empleados en lo relacionado con los Procedimientos de Seguridad.

IV Definición de políticas de seguridad informática

Cada Institución debe tener un conjunto mínimo de medidas de seguridad informática que garantice la integridad de la data, la información y los equipos que conforman la plataforma tecnológica sobre la que se procesan los procedimientos administrativos y operativos que la rigen.

Las políticas aquí presentadas han sido definidas por la Dirección de Informática de la Alcaldía de Jiménez con el propósito de establecer el adecuado comportamiento que debe tener cada uno de los usuarios, sin excepción, en el manejo de los componentes tecnológicos y la información soportada por la infraestructura informática de la Institución.

PS-01 ACCESO FÍSICO:

Todos los funcionarios que laboran para la Alcaldía de Jiménez (fijos y contratados) deben tener acceso sólo a la información estrictamente necesaria para el desarrollo de sus actividades. En el caso de los sistemas automatizados deberá solicitarse dicho acceso por escrito a la Dirección de Informática.

Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial de alcaldía.

Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

IDENTIFICADORES DE USUARIO Y CONTRASEÑAS

- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

RESPONSABILIDADES PERSONALES

1. La información que es soportada por la infraestructura de tecnología informática de la Alcaldía de Jiménez pertenece a la misma, a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable del Departamento o Dirección que genera esa

información. La propiedad de la información no va en contra del carácter público de la misma, esto significa, que la información generada por la Alcaldía de Jiménez deberá estar disponible en el evento que sea requerida por personal interno o externo a la institución, cuya solicitud atienda al proceso formal de requisición de la información. En caso de divulgación no autorizada de la información de propiedad de la Alcaldía de Jiménez se generarán sanciones a las personas que lo realicen.

2. Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
3. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
4. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
5. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.
6. El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
7. La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
8. En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
9. En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.
10. Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación,

destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

11. Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.
12. Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
13. Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
14. Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
15. Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

SALIDA DE INFORMACIÓN

1. Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.
2. Además, en la salida de datos especialmente protegidos (como son los datos de carácter personal para los que el Reglamento requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

USO APROPIADO DE LOS RECURSOS

- Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de

Comunicación Electrónica están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Queda Prohibido

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de ALCALDÍA.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por alcaldía tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

DEL SOFTWARE

- Todo el personal que accede a los Sistemas de Información de la alcaldía debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

- Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- También tiene prohibido borrar cualquiera de los programas instalados legalmente.

Administración de Cambios

Todo cambio que afecte la plataforma tecnológica debe ser solicitado por escrito ante la Dirección de Informática por los usuarios de la información y aprobado formalmente por esta Dirección. Bajo ninguna circunstancia, un cambio puede ser aprobado, realizado e implantado por la misma persona o área de trabajo.

PS-02 Almacenamiento y Respaldo de la Información:

La información soportada por la infraestructura de tecnología informática de la Alcaldía de Jiménez deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad. El área dueña de la información en conjunto con la Dirección de Informática definirá la estrategia a seguir para el respaldo de la información.

PS-03 Confidencialidad de la Información:

Toda la información generada y procesada en la Alcaldía de Jiménez y cualquiera de sus entes paramunicipales, es de propiedad y uso del área que la genera. Es potestad y obligación de dicha área clasificar la información dentro de los criterios que la Alcaldía de Jiménez establezca en sus normas de seguridad. Para la clasificación de la información se deberá tener en cuenta el grado de confidencialidad requerido en su manejo, entendiéndose por confidencial aquella información cuyo conocimiento por parte de usuarios no autorizado implique riesgos para la institución; aquella información técnica y/o institucional, que incluye entre otros, los documentos, dibujos, bocetos o diseños, proyectos, materiales, prototipos o muestras divulgadas o distribuidas. Las partes se comprometen a tratar toda información confidencial como tal, para utilizarla exclusivamente con fines institucionales en los procesos administrativos de la oficina correspondiente, sin divulgarla a terceros y sin ponerla a disposición del público, ni accesible de cualquier forma, así como

tampoco copiar ni reproducir, salvo con el consentimiento previo por escrito de la parte encargada de divulgar la información, ningún elemento o documento entregado que contenga en parte o en su totalidad, información confidencial.

PS-04 Lineamientos para la Adquisición de Bienes Informáticos

- Toda adquisición de tecnología informática se efectuará a través de un Comité, que está conformado por el personal de la Administración de Informática.
- La adquisición de Bienes de Informática en la alcaldía, quedará sujeta a los lineamientos establecidos en este documento.
- La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad.
- Para la adquisición de Hardware se observará lo siguiente:
 - ✓ El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de alcaldía.
 - ✓ Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
 - ✓ Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
 - ✓ La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática de alcaldía, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.
 - ✓ Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en

procesamiento.

- ✓ Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en alcaldía, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- ✓ Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- ✓ Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.
- ✓ En lo que se refiere a los servidores, equipos de comunicaciones, concentradores de medios (HUBS) y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones al vencer su período de garantía.
- ✓ En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones. Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización de la dirección de informática.
- ✓ En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones del artículo siguiente.
- ✓ Para la adquisición de Software base y utilitarios, la dirección de informática dará a conocer periódicamente las tendencias con tecnología de punta vigente. En casos excepcionales, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante la dirección de informática. Todos los productos de Software que se adquieran

deberán contar con su licencia de uso, documentación y garantía respectivos.

- ✓ Todos los productos de Software que se utilicen a partir de la fecha en que entre en vigor el presente ordenamiento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con el debido licenciamiento.
- ✓ Para la operación del software de red en caso de manejar los datos Alcaldía mediante sistemas de información, se deberá tener en consideración lo siguiente.
 - Toda la información institucional deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
 - El acceso a los sistemas de información, deberá contar con los privilegios ó niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
 - Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
 - Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CDs de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, la Unidad de Informática recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.

- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.
- Para la prestación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:
 - Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.

PS-05 Lineamientos para la Información

- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:
 - ✓ Información histórica para auditorias.
 - ✓ Información de interés de la Alcaldía
 - ✓ Información de interés exclusivo de alguna área en particular.
- Los jefes de área responsables de la información contenida en los departamentos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones

emergentes con dicha información tomando las medidas de seguridad pertinentes.

- Se establecen tres tipos de prioridad para la información: (a) Información vital para el funcionamiento del área, (b) Información necesaria, pero no indispensable en el área, (c) Información ocasional o eventual.
- En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.
- La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.
- El respaldo de la información ocasional o eventual queda a criterio del área.
- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento.
- Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.
- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.
- Ningún colaborador en proyectos de software y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial de la alcaldía tanto ahora como en el futuro.

PS-06 Plan de Contingencias Informáticas

La Administración de Informática creará para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- ◆ Continuar con la operación del área con procedimientos informáticos

alternos.

- ◆ Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- ◆ Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- ◆ Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- ◆ Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- ◆ Ejecutar pruebas de la funcionalidad del plan.
- ◆ Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

PS-07 Responsabilidad de los Funcionarios en el Cumplimiento de la Normatividad referente a Seguridad Informática

Todas las personas que laboran para la Alcaldía de Jiménez, son responsables por el cumplimiento de estas políticas para la seguridad informática. Todos los usuarios de los sistemas son responsables del manejo adecuado de la información y mediante el cumplimiento de estas políticas, se comprometen a respetar su carácter de confidencialidad e integridad. Los responsables de la información se encargarán de definir los accesos a la información y aprobar cambios a los aplicativos en concordancia con la normatividad de seguridad informática vigente.

En general, se requiere el fiel cumplimiento de las políticas de seguridad aquí establecidas para garantizar la integridad de la data e información de la Alcaldía de Jiménez como Institución. La sanción correspondiente a estos delitos se interpretará y regirá conforme a la Ley Especial contra Delitos Informáticos promulgada en gaceta oficial N° 37.313 de fecha 30/10/2001 y la Ley sobre Mensajes de Datos y Firmas Electrónicas promulgada en gaceta oficial N° 37.148 de fecha 28/02/2001.

CONCLUSIONES

Con en el presente trabajo se pudo evidenciar que la Alcaldía del Municipio Jiménez carece de políticas y controles eficientes en cuanto a: la seguridad de la red, resguardo de la información y manejo de los riesgos a los que está expuesta.

Se demostró que existe la factibilidad técnica, económica y operativa para diseñar el Plan de Seguridad de la Información.

El Diseño propuesto, permitirá brindar un esquema de seguridad más sólido y eficiente en el uso de los Sistemas de Información una vez implantado.

Cabe destacar que la Seguridad de la Información no depende única y exclusivamente del Diseño del Plan de Gestión de Seguridad faltaría la implantación, evaluación y mejoras a dicho plan.

RECOMENDACIONES

- ❖ Designar dentro de la estructura organizativa un ente que se responsabilice por la ejecución del Plan de Seguridad de la Información diseñado en este trabajo.

- ❖ Extender el Plan de Gestión de Seguridad de la Información presentado a los dominios no estudiados en este trabajo con la finalidad de definir completamente los riesgos a los que está sometida la información de la alcaldía del Municipio Jiménez y así tratarlos adecuadamente.

- ❖ Se hace indispensable mantener actualizada las normas, procedimientos y políticas de acuerdo a la dinámica en que vayan surgiendo nuevas estrategias de ataque contra los sistemas y sus activos de información, en concordancia con lo planteado por la norma que establece que se debe revisar y monitorear el plan de Gestión de Seguridad de la Información.

REFERENCIAS BIBLIOGRÁFICAS

Alexander, A (2.006). Análisis del riesgo y el sistema de gestión de información: el enfoque ISO 27001:2005. Disponible en: www.eficienciagerencial.com (consultado agosto 2006).

Ary, W. 1996. *Metodología de la Investigación*. Ediciones Roalg. Madrid. España.

Alexander, A. G. (2007). *Diseño de un sistema de gestión de seguridad de la información*. Bogotá. Colombia. Ediciones Alfaomega.

Balestrini, M. 1998. *Cómo se elabora el Proyecto de Investigación en Venezuela*. Ediciones Consultores Asociados, Servicio Editorial. Caracas. Venezuela.

Barrios, M. 2005. *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctoral*. Ediciones FEDUPEL. Caracas. Venezuela.

Bernal, C. 2006. *Metodología de la investigación para administración, economía humanidades y ciencias sociales*. Segunda edición. Pearson educación de México, México.

Corletti, A. 2006. *Análisis de ISO-27001:2005. Artículos de seguridad informática*. URL:<http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005>. (Consulta: abril, 13, 2009).

Daltabuit, E., Hernández, L., Mallen, G. & Vásquez, J. (2007). *La seguridad de la información*. Mexico. Ediciones Limusa.

Del Carpio, G. 2006. *Análisis del riesgo en la administración de proyectos de tecnología de información*, [Versión electrónica], Industrial Data, 1 (9), 104-107

ENISA. Agencia para la Seguridad de la Información de la Red Europea. URL: <http://www.enisa.europa.eu>. (Consulta: abril 15, 2010).

Espiñeira, Sheldon y Asociados. 2005. *Encuesta nacional 2006-2007: Prácticas de Seguridad de la Información en empresas venezolanas*. URL: <http://www.pwc.com/ve/es/encuestas/assets/practicas-2006-2007.pdf>. (Consulta: mayo 01, 2010).

Granada, Cesar. 2009. *Gestión de Seguridad de la Información en el sector bancario. Especialización en Gerencia de Sistemas y Tecnología*. Colombia.

ISO27000.es. *El Portal de ISO 27000 en español*. URL: <http://www.iso27000.es/>. (Consulta: octubre 23, 2010).

Jesús, M. 2006. *“Estudio de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local”*. Trabajo Especial de grado. Universidad Metropolitana. Caracas. Venezuela

KWell - Empresa líder de Servicios de Seguridad y Gestión de Riesgos Tecnológicos 2008. URL: <http://www.kwell.net/kwell/index.php>. (Consulta: marzo 02, 2010).

López, A. 2008. Su portal: *El Portal de ISO 27000 en español*. (ISO27000.es). URL: <http://www.iso27000.es/sgsi.html>. (Consulta: mayo 03, 2008).

Mujica, M. 2007. *Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” Sede Rectoral*. Trabajo de grado. Universidad Centroccidental “Lisandro Alvarado”. Barquisimeto. Venezuela.

Nelly, R. 2005. *“Diseño e Implantación de un Esquema de Seguridad para el Intercambio de Información de FARMASALUD”* Trabajo de grado. Universidad Metropolitana. Caracas. Venezuela.

Ozz, E. (2001). *Administración de Sistemas de Información (2ª ed)*. México: Thomson Learning.

Parella y Martins (2004). *Metodología de la Investigación Cualitativa*. Caracas.FEDUPEL

Puig, T. 2008. *Implantación de un sistema de gestión de seguridad*. URL: <http://www.mailxmail.com/curso/empresa/gestiondeseguridad>. (Consulta: marzo 15,2009).

Rosendo, M. 2009. *Sistema de gestión para la Seguridad de la Información caso: centro de tecnología de información y comunicación del decanato de ciencias y tecnología - UCLA*. Trabajo de grado. Universidad Centroccidental “Lisandro Alvarado”. Barquisimeto. Venezuela.

Senn, J. 1987. *Análisis y diseño de sistemas de información*. Ediciones McGraw-Hill. México.

Soto, L. 2007. *Sistemas de Información*. URL: <http://www.mitecnologico.com/Main/ConceptoSistemaInformacion>. (Consulta: mayo 20, 2008).

Ugel, E. 2005. *Técnicas de Recolección de Datos*. Departamento de medicina. Universidad Centroccidental Lisandro Alvarado. URL: <http://www.ucla.edu.ve/dmedicin/departamentos/medicinapreventivasocial/SEB/investigacion/recoleccion.pdf>. (Consulta 06, marzo 2011).

Universidad Centroccidental “Lisandro Alvarado”. Las Normas de Seguridad Informática y de Telecomunicaciones UCLA. 2005. Sesión Ordinaria N° 1647. URL: http://www.ucla.edu.ve/telecom/NORMAS_de_seguridad_INF_y_de_telecomunicaciones_UCLA.pdf. (Consulta: Noviembre 20, 2010).

Ugel, E. 2005. *Técnicas de Recolección de Datos*. Departamento de medicina. Universidad Centroccidental Lisandro Alvarado. URL: <http://www.ucla.edu.ve/dmedicin/departamentos/medicinapreventivasocial/SEB/investigacion/recoleccion.pdf>. Consulta 06, marzo 2011.

Vásquez, F. 1996. *Ordenación del territorio*. Servicio de publicaciones universidad de murcia.

Velásquez M., Mauricio A. 1998. *Ceros y unos: La economía de la información*. Informática al día, 111, 19-23.

Vittoriano, E. (2008, Agosto). *La información como activo*. (Latin America CACS) Santiago. Chile. 2008.

Villena, M. 2007. *Sistema de Gestión de Seguridad de Información para una Institución Financiera*. Trabajo de grado. Pontificia Universidad Católica del Perú. Facultad de ciencias e ingeniería. Lima. Perú.

Zapata, O. 2005 *Herramientas para elaborar tesis e investigaciones socioeducativas*. Editorial Pax. México DF, México.

ANEXOS

Anexo "A". Cronograma de Actividades.

ACTIVIDADES	MES 1				MES 2				MES 3				MES 4			
	jul-11				agos-11				sep-11				oct-11			
SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Elaboración del instrumento para el diagnóstico	X	X	X													
Validación del instrumento		X	X	X												
Aplicación del instrumento					X	X										
Análisis e interpretación de los resultados							X	X								
Conclusiones del estudio diagnóstico								X	X							
Factibilidad Operativa									X							
Factibilidad Técnica									X							
Factibilidad económica									X							
Evaluación de las Herramientas para la Elaboración del Plan										X						
Elaboración del diseño de un plan de gestión de seguridad de la información.											X	X	X	X	X	X

Anexo "B". Cuestionario

CUESTIONARIO N° 1
DIAGNÓSTICO DEL ESTADO ACTUAL DE LA DE SEGURIDAD DE LA
INFORMACIÓN EN LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL
ESTADO LARA

1. ¿Tiene usted conocimiento sobre lo que significa un plan de seguridad de información?

SI ___ NO ___

2. ¿Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica de la Alcaldía?

SI ___ NO ___

3. ¿Cree usted que se logrará un cambio positivo con la aplicación de este plan de seguridad de información en la plataforma tecnológica de la Alcaldía del Municipio Jiménez?

SI ___ NO ___

4. ¿Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica de la alcaldía del Municipio Jiménez?

SI ___ NO ___

5. ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información en la Alcaldía del Municipio Jiménez?

SI ___ NO ___

6. ¿Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones de esta alcaldía?

SI ___ NO ___

7. ¿Sabe usted si existe un plan de recuperación ante desastres en la Alcaldía del Municipio Jiménez?

SI ___ NO ___

8. ¿En la Alcaldía del Municipio Jiménez han realizado evaluación de riesgos relacionados con la información?

SI ___ NO ___

9. ¿En la Alcaldía del Municipio Jiménez han realizado una evaluación de vulnerabilidades de la red?

SI ___ NO ___

10. ¿La Alcaldía del Municipio Jiménez cuenta con software antivirus actualizado?

SI ___ NO ___

Anexo “C”. Validez del Instrumento

**UNIVERSIDAD CENTROCCIDENTAL “LISANDRO ALVARADO”
 DECANATO DE CIENCIAS Y TECNOLOGIA
 POSTGRADO EN CIENCIAS DE LA COMPUTACION
 MENCIÓN REDES DE COMPUTADORAS
 “DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
 INFORMACIÓN.CASO: DIRECCIÓN DE INFORMÁTICA DE LA
 ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA.”**

Formato de Validación del Instrumento (CUESTIONARIO)

Ciudadano (a): _____

Para efectos de la evaluación correspondiente a los ítems planteados en el instrumento se determinará la validez en los siguientes términos:

- a) **Pertinencia:** Es la correspondencia del ítem con el aspecto a evaluar;
- b) **Claridad:** se refiere a la redacción precisa y sencilla del ítem
- c) **Congruencia:** entendida como la lógica interna del ítem.

Se le agradece seleccionar una de las 2 posibles opciones (Si/No) para cada ítem con el objetivo de señalar el grado de pertinencia, claridad y congruencia de los mismos.

OPINION DEL EXPERTO

Ítem	<i>Pr</i>		<i>Cl</i>		<i>Cn</i>		<i>D</i>		<i>M</i>		<i>E</i>		<i>I</i>	
	<i>SI</i>	<i>NO</i>	<i>SI</i>	<i>N</i>	<i>SI</i>	<i>NO</i>	<i>SI</i>	<i>N</i>	<i>SI</i>	<i>N</i>	<i>SI</i>	<i>NO</i>	<i>SI</i>	<i>NO</i>
				<i>O</i>				<i>O</i>		<i>O</i>				
1	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
2	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>
3	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
4	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
5	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
6	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
7	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
8	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
9	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>
10	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>	<input type="checkbox"/>	X <input type="checkbox"/>

Leyenda: **Pr:** Pertinencia; **Cl:** Claridad; **Cn:** Congruencia; **D:** Dejar; **M:** Modificar; **E:** Eliminar; **I:** Incluir otro ítem.

Observaciones generales: _____

Firma del experto/ CI:

Anexo “D”. Resúmenes de casos.

ITEMS	1	2	3	4	5	6	7	8	9	10
INDIVIDUOS										
1	1	1	0	1	0	1	1	0	0	0
2	0	1	1	1	0	1	1	0	0	0
3	0	1	1	1	0	0	1	0	0	0
4	1	1	0	1	0	0	0	0	0	0
5	0	1	0	1	0	1	1	0	0	0
6	1	1	1	1	1	1	0	0	0	1
7	0	1	0	1	1	1	0	0	0	0
8	0	1	1	1	1	1	0	0	0	0
9	1	1	1	1	1	1	0	1	1	0
10	0	1	1	1	1	1	0	0	0	0
11	1	1	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	0	1	1	0
13	1	1	1	0	1	1	1	1	1	0
14	1	1	1	0	1	1	0	0	0	0
15	1	1	1	0	1	1	0	0	0	0
16	0	1	1	0	1	1	1	0	0	0
17	0	1	1	0	1	1	0	0	0	0
18	1	1	1	0	1	1	1	0	1	0
19	0	0	1	1	1	1	0	0	0	0
20	0	1	1	1	1	1	0	0	0	0
21	1	1	1	1	0	1	0	0	0	0
22	0	1	1	1	0	1	0	0	0	0
23	1	1	1	1	1	1	0	0	0	0
24	1	1	1	1	1	1	0	0	0	0
25	1	0	0	0	0	0	0	0	0	0
26	1	1	1	1	0	1	0	0	0	0
27	0	1	0	1	0	0	0	1	0	0
28	0	1	1	1	0	1	0	0	0	0
29	0	1	1	1	0	1	0	0	0	0
30	1	1	1	1	0	1	0	0	0	0
31	1	1	1	1	1	1	1	1	0	0
32	1	1	1	1	1	1	1	1	0	0
33	1	1	1	1	1	1	1	0	0	1
34	1	1	1	1	1	1	1	0	1	1
35	1	1	1	1	1	1	1	1	1	1
36	1	1	1	1	1	1	1	1	1	1
37	1	1	1	1	1	1	1	1	1	1
38	1	1	1	1	1	1	1	1	1	1
39	1	1	1	1	1	0	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1



Anexo “E”. Acuerdo de Confidencialidad.

ACUERDO DE CONFIDENCIALIDAD

ENTRE: _____ (*Nombre de la Empresa*)

Y: _____ (*Nombre del Trabajador, Contratista o Empresa contratada*)

Este Acuerdo de Confidencialidad entre los contratantes, se regulará por las siguientes cláusulas:

1. TIEMPO ESTABLECIDO DEL ACUERDO

Este Acuerdo de Confidencialidad comienza (*con la firma del Contrato Laboral o Comercial o retroactivamente al principio de la relación cuando se firmó el Contrato*) y permanecerá vigente mientras esté vigente el Objeto por el cual se inició la relación, manteniéndose inclusive durante las prórrogas sin necesidad de firmar un nuevo Acuerdo de Confidencialidad.

Asimismo, si el contrato inicial termina y se inicia después un nuevo contrato pero con el mismo objeto del contrato anterior, este Acuerdo de Confidencialidad tomará vigencia sin necesidad de firmar uno nuevo.

2. REPRESENTACIÓN Y GARANTÍAS

El _____ (*Trabajador o Contratista*) representa y garantiza que su relación con la Empresa no causará o requerirá que ello viole cualquier obligación a, el acuerdo, o la confianza relacionada con confidencialidad, el secreto de fabricación y la información propietaria con cualquier otra persona, empresa o entidad. Más aun, el _____ (*Trabajador o Contratista*) reconoce que una condición de esta relación consiste en que no ha traído y no traerá o usará en el desempeño de sus deberes en la Empresa cualquier información propietaria o confidencial de un antiguo Empleador o Contratante sin la autorización escrita de aquel Empleador o Contratante. La violación de esta condición causa la terminación automática de la relación _____ (*Laboral o Comercial*) desde el tiempo de violación. Si el _____ (*Trabajador o Contratista*) considera que tiene investigaciones o invenciones anteriores a la firma de este Acuerdo de Confidencialidad que serán excluidas de este acuerdo, se deberán anotar en la parte trasera de este documento o en uno aparte firmado por las partes. Con esto. El _____ (*Trabajador o Contratista*) libera a la Empresa de cualquier reclamación por parte del _____ (*Trabajador o Contratista*) por cualquier empleo por la Empresa de cualquier invención antes hecha o concebida por El _____ (*Trabajador o Contratista*).

3. CONFIDENCIALIDAD

- a. El _____ (*Trabajador o Contratista*) reconoce que la Empresa contratante ha hecho, o puede poner a su disposición ciertas listas de clientes, datos de precios, fuentes de suministro, técnicas, información computarizada, mapas, los métodos, producto de diseño, la información, y/o Información Propietaria de, o autorizado a, la Empresa o sus clientes, incluyendo sin restricción, secretos de fabricación, invenciones, patentes, y materiales con derechos de autor (_____ *mas todo lo que se considere Material o Información Confidencial*).
- b. El _____ (*Trabajador o Contratista*) reconoce que esta información tiene un valor económico, real o potencial, que no es generalmente dado a conocer al público o a los otros que podrían obtener el valor económico de su descubrimiento o empleo y que esta información es sujeta a un esfuerzo razonable por la Empresa de mantener su secreto y confidencialidad. Asimismo, el _____ (*Trabajador o Contratista*) no hará ninguna duplicación u otra copia del Material Confidencial.
- c. El _____ (*Trabajador o Contratista*) devolverá inmediatamente se le solicite por parte de la Empresa, todo material confidencial que se le haya solicitado. El _____ (*Trabajador o Contratista*) notificará a la Empresa cualquier descubrimiento que haya hecho, considerándose esto, como parte del Material Confidencial. El _____ (*Trabajador o Contratista*) se compromete a no utilizar información o Material Confidencial finalizado la relación _____ (*Laboral o Comercial*).

4. INFORMACIÓN CONSIDERADA DE LA EMPRESA

- a. Para el objetivo de este Acuerdo, también se considerará como Material Confidencial cualquier información, observación, datos, material escrito, registro, documento, dibujo, fotografía, disposición, programas de computador, software, multimedia, programas fijos, invención, descubrimiento, mejora, desarrollo, instrumento, máquina, aparato, aplicación, diseño, trabajo de paternidad literario, logo, sistema, idea promocional, lista de clientes, necesidad del cliente, práctica, información de precios, procesos, pruebas, concepto, fórmulas, métodos, información de mercado, técnicas, secreto de fabricación, producto y/o la investigación relacionada con el desarrollo de investigación real o previsto, productos, organización, control de comercialización, publicidad, negocio o fondos de Empresa, sus afiliados o entidades relacionadas. (_____ y todo lo que considere necesario incluir).
- b. Todo lo anterior, es y será de la Empresa incluso después de terminada la relación con el _____ (*Trabajador o Contratista*).
- c. El _____ (*Trabajador o Contratista*) cumplirá con las medidas de seguridad que tome la Empresa para proteger la confidencialidad de cualquier Información reservada o secreta de la Empresa.
- d. El _____ (*Trabajador o Contratista*) irrevocablemente designa al Gerente o quien haga sus veces en la Empresa para realizar todos los actos necesarios para obtener

- y/o mantener patentes, derechos de autor y derechos similares a cualquier Información exclusiva de la Empresa, según la normas _____ (*Colombianas*) e Internacionales.
- e. Cualquier uso para una patente, el registro de derechos de autor o el derecho similar registrado por el _____ (*Trabajador o Contratista*) dentro de un año después de la terminación de este Acuerdo será supuesto a relacionarse con la Información creada por el _____ (*Trabajador o Contratista*) durante el término de este Acuerdo, a no ser que el _____ (*Trabajador o Contratista*) pueda demostrar de otra manera con la certeza razonable.
- f. La Empresa puede disponer libremente de toda su información y Material Confidencial, por lo que el _____ (*Trabajador o Contratista*) no tendrá ninguna autoridad para ejercer cualquier derecho o privilegios en lo que concierne a la Información perteneciente exclusivamente a la Empresa poseída por o asignada a esta última conforme a este Acuerdo y las leyes _____ (*Colombianas*)

5. LABOR CONTRATADA

- a. El _____ (*Trabajador o Contratista*) reconoce que todos los trabajos de autoría llevados a cabo por la Empresa son sujetos a la dirección de la Empresa y su control y dichos trabajos constituyen una función contratada de conformidad al Contrato _____ (*Laboral o Comercial*).
- b. Toda la Información o Material Confidencial, creada, inventada, concebida o descubierto por el _____ (*Trabajador o Contratista*) que este sujeto a derechos de autor explícitamente, como se considera, por el _____ (*Trabajador o Contratista*), corresponde a trabajos propios de la labor contratada y son de propiedad de la Empresa.

6. ASIGNACIÓN

- a. La empresa poseerá como su propiedad exclusiva , y el _____ (*Trabajador o Contratista*) está de acuerdo con asignar, transferir, y transportar y o sus candidatos autorizados todo su derecho, título e interés a y a todas y cualquier dichas "ideas" que estén relacionadas en general con el negocio de la Empresa, incluyendo, pero no limitado con cualquier invención, procesos, mejoras, ideas, obras de arte registrables como propiedad literaria, marcas registradas, derechos de autor, fórmulas, la tecnología de la fabricación, acontecimientos, escrituras, otros, registrables como propiedad literaria, patentables o in patentable, desde la fecha de este Acuerdo o la fecha del primer contrato celebrado con la Empresa y hasta la terminación de la relación _____ (*Laboral o Comercial*) con el _____ (*Trabajador o Contratista*) .
- b. El _____ (*Trabajador o Contratista*) por la presente asigna a la Empresa todas las entregas y libera a la Empresa, cualquier afiliado de Empresa y sus oficiales respectivos, directores y empleados, de y contra cualquier y todas las reclamaciones, demandas, responsabilidades, gastos, y los gastos de el _____ (*Trabajador o Contratista*), provenientes, o relacionando con, cualquier Información de Propiedad.

7. PREMIOS O COMISIONES (Optativo)

- a. La Empresa pagará al _____ (*Trabajador o Contratista*) un premio consistente en _____ (*efectivo, especie, etc.*) sobre la Investigación o Creación del _____ (*Trabajador o Contratista*).

8. NO COMPETIR

El _____ (*Trabajador o Contratista*) está de acuerdo con no contratar con terceros en cualquier actividad que compita con cualquier actividad de Empresa durante el curso de su relación _____ (*Laboral o Comercial*). Para los objetivos de este párrafo, la actividad competitiva abarca la formación o la planificación de formar una entidad de negocio que, como se puede considerar, sea competitiva con cualquier negocio de la Empresa. Esto no impide al _____ (*Trabajador o Contratista*) buscar u obtener el empleo u otras formas de relaciones de negocio con un competidor después de la terminación de empleo con la Empresa mientras que tal competidor existiese antes de la terminación de la relación con la Empresa y el _____ (*Trabajador o Contratista*) de ninguna manera estuvo implicado con la organización o la formación de tal competidor.

9. OPORTUNIDADES DE NEGOCIO

Durante las condiciones de este Acuerdo, si el _____ (*Trabajador o Contratista*) se da cuenta de cualquier proyecto, inversión, empresa, negocio u otra oportunidad o similar relacionado con el mismo campo comercial de la Empresa, o cualquier proyecto, inversión, empresa, o el negocio de Empresa, entonces el _____ (*Trabajador o Contratista*) notificará la Empresa inmediatamente por escrito de tal Oportunidad y usará los esfuerzos de buena fe del _____ (*Trabajador o Contratista*) para hacer que la Empresa tuviese la oportunidad de explorar, invertir dinero en, participar en, o de otra manera afiliarse a tal Oportunidad.

10. SOLICITACIÓN DE EMPLEADOS

El _____ (*Trabajador o Contratista*) conviene que terminado el Contrato que dio origen a este Acuerdo de Confidencialidad, no inducirá o intentará contratar a los trabajadores de la Empresa para crear un nuevo negocio que compita en el mismo ramo mercantil.

11. SOLICITACIÓN DE CLIENTES DESPUÉS DE TERMINACIÓN DE ACUERDO

Por el término de _____ (*días, meses o año*), de terminada la relación con la Empresa, el _____ (*Trabajador o Contratista*) no va a, directamente o indirectamente, dar a conocer a cualquier persona, firma o corporación los nombres o las direcciones de cualquiera de los clientes de Empresa o cualquier otra información que les pertenece, o visitarán, buscarán clientes, se llevarán, o intentarán visitar, buscar clientes, o llevarse cualquier cliente de Empresa sobre quien el _____ (*Trabajador o Contratista*) se halla contactado o con quien el _____ (*Trabajador o Contratista*) se dio por enterado durante el tiempo de este Acuerdo, para sí o para cualquier otra persona, firma, o corporación.

12. SANCIONES POR VIOLAR EL ACUERDO DE CONFIDENCIALIDAD

EL _____ (*Trabajador o Contratista*) que viole alguna de las disposiciones antes mencionadas en relación con lo que se considera objeto de la Confidencialidad, ocasionará el pago de una multa de \$ _____, sin perjuicio de las demás acciones laborales, comerciales y penales a que haya lugar para la reclamación de indemnización de perjuicios ocasionados con la violación a la Confidencialidad aquí suscrita.

13. Conciliación y Arbitraje

En caso de cualquier controversia en este Acuerdo, los firmantes se comprometen a llevar las diferencias ante un Centro de Conciliación o un Tribunal de Arbitramento antes de iniciar cualquier acción legal ante jueces. Los gastos de las diligencias de Conciliación o Tribunal de Arbitramento será sufragado por la parte solicitante.

Hasta aquí este Acuerdo de Confidencialidad.

Se firma en dos ejemplares que serán entregados a los firmantes, a los _____ días del mes de _____ del año _____.

Firmas:



Anexo "F". Autorización de Accesos Externos

Lugar y Fecha: ____/____/____/____

**AUTORIZACIÓN DE ACCESOS A PERSONAL EXTERNO A LA
ALCALDIA**

Nombres: _____, _____

Apellidos: _____, _____

Cedulas: _____, _____

Tipo de Cambio a realizar:

Observaciones:

Atentamente:

Nombre y apellido: _____

(Por la Dirección de Informática)

C.I: _____

Firma y Sello: _____



Anexo “G”. Procedimiento Normado para terminación de empleado

Propósito General:

Establecer la normativa para el respaldo de la información en caso de la terminación del empleo o trabajo realizado en la Alcaldía del Municipio Jiménez.

Actores:

Supervisor de seguridad

Empleado saliente.

Dirección de Recursos Humanos.

Este procedimiento de terminación de empleo describe, específicamente, el esquema a seguir cuando un empleado termina la relación laboral con la Alcaldía del Municipio Jiménez

El procedimiento será el siguiente:

1. El departamento de RRHH de la Alcaldía del Municipio Jiménez, debe informar la Dirección de Informática que un empleado dejará sus actividades laborales, por las causas que fuesen: despido, termino de contrato o renuncia voluntaria.
2. El representante de la Dirección de Informática procede a respaldar de forma inmediata la información de Correos, documentos e informes de la persona.
3. El empleado firma el formato de terminación de empleo (Anexo H).
4. El formato debidamente llenado es entregado a recursos humanos y la dirección de RRHH No debe entregar el pago de la liquidación del empleado hasta no tener este formato.



Anexo "H". Formato para terminación de empleo

Fecha: __/__/__

NOMBRE DEL EMPLEADO: _____

APELLIDO DEL EMPLEADO: _____

LOGIN QUE USABA:

PASSWORD QUE USABA: _____

FECHA DE NOTIFICACION:

FECHA DE RESPALDO:



Anexo "I". Formato Reporte de Vulnerabilidades

Fecha: __/__/__

Reporte de vulnerabilidades

Numero de Caso: _____

Jefatura o dirección donde se observó la falla: _____

Describe vulnerabilidad: _____

Memoria Fotográfica: _____

Nombre de persona que levanta vulnerabilidad: _____

Firma



Anexo "K". Entrevista

**UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
MAESTRIA EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORA**

ENTREVISTA

Fecha: ____/____/____

**DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA
ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA**

1.- ¿Considera usted que deben existir políticas de seguridad para la plataforma tecnológica de la Alcaldía del Municipio Jiménez?

Si []

No []

2.- ¿Existe un documento que defina las políticas de seguridad de información de la Alcaldía del Municipio Jiménez?

Si []

No []

3.- ¿Conoce usted alguno de los estándares de seguridad de información?

Si []

No []

4.- ¿El manejo de la Información de la Organización está en manos del personal que tiene responsabilidad directa sobre ella?

Si []

No []

5.- ¿Indique si la institución posee programas dirigidos a sensibilizar sobre la Seguridad de la Información para todos los empleados?

Si []

No []



6.- ¿Existe un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información, relacionada con la Alcaldía?

Si []

No []

7.- ¿En la institución han realizado pruebas de penetración perimetral?

Si []

No []

8.- ¿Existe un documento donde estén definidas las responsabilidades para la terminación o cambio de empleo para los empleados, de la Alcaldía?

Si []

No []

Agradeciendo cordialmente su colaboración. Atentamente,

Ing. Arelys López.



Anexo “L”. Validez del Instrumento

**UNIVERSIDAD CENTROCCIDENTAL “LISANDRO ALVARADO”
DECANATO DE CIENCIAS Y TECNOLOGIA
POSTGRADO EN CIENCIAS DE LA COMPUTACION
MENCION REDES DE COMPUTADORAS
“DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN.CASO: DIRECCIÓN DE INFORMÁTICA DE LA
ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA.”**

Formato de Validación del Instrumento (ENTREVISTA)

Ciudadano (a): _____

Para efectos de la evaluación correspondiente a los ítems planteados en el instrumento se determinará la validez en los siguientes términos:

- a) **Pertinencia:** Es la correspondencia del ítem con el aspecto a evaluar;
- b) **Claridad:** se refiere a la redacción precisa y sencilla del ítem
- c) **Congruencia:** entendida como la lógica interna del ítem.

Se le agradece seleccionar una de las 2 posibles opciones (Si/No) para cada ítem con el objetivo de señalar el grado de pertinencia, claridad y congruencia de los mismos.

OPINION DEL EXPERTO

Ítem	<i>Pr</i>		<i>Cl</i>		<i>Cn</i>		<i>D</i>		<i>M</i>		<i>E</i>		<i>I</i>	
	<i>SI</i>	<i>NO</i>												
1	<input type="checkbox"/>													
2	<input type="checkbox"/>													
3	<input type="checkbox"/>													
4	<input type="checkbox"/>													
5	<input type="checkbox"/>													
6	<input type="checkbox"/>													
7	<input type="checkbox"/>													
8	<input type="checkbox"/>													

Leyenda: **Pr:** Pertinencia; **Cl:** Claridad; **Cn:** Congruencia; **D:** Dejar; **M:** Modificar;
E: Eliminar; **I:** Incluir otro ítem.

Observaciones generales: _____

Firma del experto/ CI:



Anexo "M". Planilla para la identificación de activos

Plan de Gestión de Seguridad de la Información

Planilla para Identificación de Activos por Dirección o Jefatura

Indicaciones: Utilice esta planilla para describir cada uno de los activos de información Vitales para su dirección o Jefatura, que sean relevantes para la prestación del servicio que usted como director o jefe presta.

Nombre del Servicio que usted presta:

Descripción del servicio:

Listado de activos Vitales.

- | | |
|----------|-----------|
| 1) _____ | 9) _____ |
| 2) _____ | 10) _____ |
| 3) _____ | 11) _____ |
| 4) _____ | 12) _____ |
| 5) _____ | 13) _____ |
| 6) _____ | 14) _____ |
| 7) _____ | 15) _____ |
| 8) _____ | 16) _____ |

Eventos Profesionales

- **Modulo Uno Software Libre** en la Academia de Software Libre del Estado Lara Septiembre-Diciembre 2006.
- **Certificado Modulo Cero Software Libre** en la Academia de Software Libre del Estado Lara Junio-Agosto 2006.
- **Componente Docente** (Modalidad en Línea), en la universidad Fermín Toro. Julio 2006.
- **XXV Festival Juvenil Regional de la Ciencia**, en calidad de participante. Desde el 22-06 al 24-06-1994.Tocuyo.
- **II Jornadas de Internet**. Desde el 22-06 al 26-06-1998. Universidad Centroccidental “Lisandro Alvarado”, Decanato de Ciencia y Tecnología. Barquisimeto.
- **VIII Jornadas Infociencias 2000** “Una Ventana Hacia La Innovación Tecnológica”
En Calidad de: Participante. Hotel Barquisimeto Hilton. 13 y 14 de Octubre 2000
- **X Jornadas de Infociencias 2001**. “Tecnología para La Sociedad del Conocimiento”
En Calidad de: Participante. Hotel Príncipe. 08 y 09 de Noviembre 2001.
- **XII Jornadas de Infociencias 2003**. “Una puerta Abierta a la Innovación Tecnológica”
En Calidad de: Participante. Hotel Príncipe. 3 y 4 de Abril 2003.
- **XIII Jornadas de Infociencias 2003**. “Explorando Horizontes Tecnológicos”
En Calidad de: Participante. Auditorio Ambrosio Oropeza. 02 y 03 de Octubre 2003.
- **XIV Jornadas de Infociencias 2004**. “Una Visión al conocimiento Tecnológico”
En Calidad de: **Coordinador de Documentación del proyecto SIGESA**. Hotel príncipe. 15 y 16 de Abril 2004.
- **Asistente Técnico en Mantenimiento de Micros**. IUTEPAL Maracay convenio Morán .Abril 2002-Julio 2003.

Perfil Profesional

- Especialista proactivo, dinámico con capacidad e iniciativa para plantear alternativas de solución eficientes ante circunstancias críticas.
- Alto sentido de la responsabilidad, puntualidad y cooperación.
- Capacidad para trabajar en equipo y mantener buenas relaciones interpersonales.
- Adaptabilidad para trabajar bajo presión y habilidad para el aprendizaje autodidacta.
- Habilidad para negociar con el cliente en el levantamiento de especificaciones técnicas para definir la factibilidad y alcance de un proyecto.
- Coordinación de Grupos de Trabajo.

**Conocimientos
Técnicos**

- Análisis, diseño, desarrollo, mantenimiento de Redes LAN, MAN y WAN.
- Análisis, diseño, desarrollo, puesta en producción y mantenimiento de Aplicaciones, Sitios y Páginas Web.
- Conocimientos del estándar J2EE para desarrollo de aplicaciones web.
- Conocimientos en la instalación, configuración y administración del Servidor Web Apache bajo ambiente Windows.
- Análisis, diseño y desarrollo de sistemas de información, bajo las metodologías Estructurada y Orientada a Objeto.
- Diseño, creación y mantenimiento de Bases de Datos relacionales y documentales.
- Manejo de Utilitarios Web: Flash, DreamWeaver, MS FrontPage, Adobe Photoshop, CorelDraw en cualquiera de sus versiones.
- Manejo de sistemas de Capta huellas, Sistema de postulaciones, y Sistema de Totalización para Elecciones Nacionales.