ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TESIS DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: ANALISTA DE SISTEMAS

TEMA

Implementación de Políticas de Seguridad Informática para La M.I. Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002

Guayaquil - Ecuador

AUTORES
BARRAGÁN PAGUAY ISRAEL
GÓNGORA ZAMBRANO INGRID
MARTÍNEZ CÁRDENAS ERICKA

AÑO
2011

AGRADECIMIENTO

Al director de Proyecto, Mae. Víctor H. Muñoz Chachapolla, por ser nuestra guía con sus valiosos conocimientos que nos impartió en el Seminario, sirviéndonos de base para la realización de este proyecto.

Al Ing. Cesar Martínez Yagual, por su colaboración y tiempo dedicado durante la recolección de la información para la elaboración de este proyecto, y obtener así un trabajo de calidad y excelencia.

A cada uno de los docentes quienes a través de los años cursados nos enriquecieron con sus enseñanzas, impulsándonos así a la culminación de nuestra etapa estudiantil.

Barragán P. Israel
Góngora Z. Ingrid
Martínez C. Ericka

DEDICATORIA

A Dios por ser quien dio las fuerzas, sabiduría y entendimiento, permitiendo que llevemos a cabo este proyecto.

A nuestros padres y familiares, por el apoyo, la paciencia y compresión que supieron brindarnos en los momentos que más los necesitamos.

Barragán P. Israel
Góngora Z. Ingrid
Martínez C. Ericka

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

FIRMA DEL DIRECTOR DE LA TESIS Y MIEMBROS DEL TRIBUNAL

Mae. Víctor H. Muñoz Chachapolla
DIRECTOR DE PROYECTO

Mae. Enrique Salazar
DELEGADO

FIRMA DE LOS AUTORES DEL PROYECTO DE GRADUACIÓN

Barragán Paguay Israel Freddy

Góngora Zambrano Ingrid Natali

Martínez Cárdenas Ericka Elizabeth

RESUMEN

En el proyecto de titulación se pretende dar una adecuada solución de seguridad a la M. I. Municipalidad de Guayaquil, tomando como base estándares internacionales.

El primer capítulo presenta una introducción de lo que implica un Sistema de Gestión de Seguridad de la Información, es decir conceptos básicos, permitiendo tener una visión general y clara en donde se determina objetivos y acciones necesarias para conseguir que la entidad involucrada cuente con un conjunto de reglas y políticas para la seguridad y gestión de riesgos de la información.

En el segundo capítulo se presenta los antecedentes, objetivos y funciones desempeñadas dentro de la Muy Ilustre Municipalidad de Guayaquil en donde se implementaría las Políticas de Seguridad de acuerdo a las Normas ISO/IEC 27002 y descripción de los departamentos y/o áreas en que se divide y su organigrama principal.

El capítulo tres del manual presenta la metodología PDCA y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el Alcance que se desea establecer, indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro del Municipio de Guayaquil. Continuando con una breve descripción de las Políticas Generales que se deben aplicar en el área de Informática.

El capítulo cuatro del presente proyecto describe la metodología MAGERIT con el concepto y ventajas principales de su implementación. Se detalla el Inventario de Activos dentro del Departamento de Informática y de acuerdo al informe se realiza un exhaustivo Análisis de Riesgo con sus apropiados Criterios de Valorización.

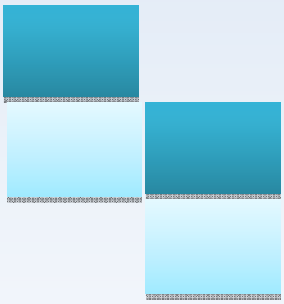
En el capítulo cinco se explica la Implementación de las Políticas, descripción y objetivos por cada una. Se especifica el Plan de tratamiento de Riesgos a utilizar para la gestión de Riesgos que se encontró en el Área de Informática.

Y por último el capítulo seis son las Estrategias de Difusión que se aplicara para llegar a difundir las Políticas dentro del Departamento. Se presenta los ANEXOS correspondientes al manual.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS



CAPÍTULO # 1

INTRODUCCIÓN Y NORMAS ISO PARA LA SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN SGSI

El presente documento establecerá los procedimientos y políticas de seguridad de la información dentro de la organización las cuales deben ser sustentadas por organismos que avalen la correcta implementación de dichos procedimientos.

Se conformó el grupo de trabajo con el objetivo de formular un modelo de política de Seguridad de la Información que sirva de punto de partida para la elaboración de las políticas correspondientes. Nuestro grupo de trabajo decidió basar el modelo en la norma ISO/IEC 27002, como un marco de referencia para la gestión de la seguridad de la información en una entidad, en este caso para la M.I. Municipalidad de Guayaquil.

Las presentes políticas de seguridad de la información se impondrán en cumplimiento con las disposiciones legales vigentes, con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la entidad establecida.

1.1. MARCO DE REFERENCIA

Seguridad de la Información

La seguridad de la información[1] se entiende como la preservación de las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

La seguridad es un proceso de mejora continua por lo que las políticas y procedimientos establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que puedan surgir eventualmente, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

[1] http://www.scd.com.ar/servicios_corporativos/que_comprende_la_auditoria_de_seguridad.html

1.2. ISO

La ISO (Organización Internacional de Normalización) [2] es una federación mundial de organismos nacionales de normalización (comités miembros de la ISO). La elaboración de las Normas Internacionales es normalmente confiada a los comités técnicos de la ISO. Cada miembro del comité interesado por un estudio tiene el derecho de formar parte del comité técnico creado para este efecto. Las organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con la ISO participan también en los trabajos.

Los proyectos de Normas Internacionales adoptadas por los comités técnicos son sometidos a los comités miembros para su aprobación, antes de su aceptación como Normas internacionales por el Consejo de la ISO. Las Normas Internacionales se aprueban de acuerdo con los procedimientos de la ISO y se requiere de la aprobación de 75% por lo menos, de los comités miembros que votan.

1.3. ESTÁNDAR

Publicación que recoge el trabajo en común de los comités de fabricantes, usuarios, organizaciones, departamentos de gobierno y consumidores, que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional con el objeto de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

1.3.1 ISO 27001

La ISO 27001 es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información. El objetivo fundamental es proteger la información de su organización para que no caiga en manos incorrectas o se pierda para siempre.

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

[2] http://seguridad.cai.es/paginas/paginafinal.asp?idNodo=225

1.4. SERIE ISO 27000

ISO ha reservado la serie de numeración 27000[3] para las normas relacionadas con sistemas de gestión de seguridad de la información. En el 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

- ISO27000 (términos y definiciones),
- ISO27002 (objetivos de control y controles),
- ISO27003 (guía de implantación de un SGSI),
- ISO27004 (métricas y técnicas de medida de la efectividad de un SGSI),
- ISO27005 (guía para la gestión del riesgo de seguridad de la información) y
- ISO27006 (proceso de acreditación de entidades de certificación y el registro de SGSI).

1.5. RELACIÓN DE LA NORMA ISO27001 CON OTROS ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Otros estándares internacionalmente aceptados y relacionados con seguridad de la información (COBIT3, NIST4, AS/NZ43605, entre otros), que la enfocan desde diferentes puntos de vista como controles de seguridad, buen gobierno, gestión de riesgo, etc.

Otras organizaciones solo pueden implementar un conjunto de buenas prácticas en seguridad de la información en base a modelos de gestión.

1.6. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un SGSI es un Sistema de Gestión de la Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System). Este sistema consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad para protegerse de ataques maliciosos o pérdidas de información.

La protección adecuada de la información en las empresas debería considerar aspectos organizativos y tecnológicos, examinando como las personas utilizan los activos de información y los recursos en el desempeño de su trabajo diario. Esta evaluación es de vital importancia para poder disponer de unas líneas básicas de referencia e introducir mejoras que demuestren ser efectivas.

[3] http://www.iso27000.es/iso27000.html#section3b

1.7. BENEFICIOS DE LA IMPLEMENTACIÓN DE UN SGSI

Podemos citar algunos de los aspectos positivos de la implementación de SGSI:

- **Protección del proceso de negocio**

  Conseguimos evitar interrupciones en el modelo de negocio, ya que se está asegurando la disponibilidad de los datos y del sistema de información. También se está preparado para recuperarse ante incidentes, garantizando la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

- **Mejora de la competitividad.**

  Cualquier mejora en la gestión de la organización redunda en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en nuestro negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

- **Cumplimiento legal**

  Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información o la privacidad. Gestionando de manera coordinada la seguridad tenemos un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

- **Mantener y mejorar la imagen corporativa.**

  Los clientes percibirán la organización como una empresa seria, responsable, comprometida con la mejora de sus procesos, productos y servicios. Es una poderosa herramienta de marketing (sobre todo si añadimos un sello tipo ISO27002).

1.8. JUSTIFICACIÓN DELA IMPLEMENTACIÓN DE UN SGSI

En la actualidad son muchos los factores a tener en cuenta para la implementación de un SGSI, la seguridad de la información es un área que día a día va adquiriendo más protagonismo en los presupuestos e inversiones empresariales. Los planes de contingencia y de continuidad del negocio cobran especial relevancia a la hora de abordar cualquier proyecto. Ya son muchos y muy frecuentes los escenarios donde la pérdida de información puede ocasionar daños importantes en los desarrollos corporativos.

A lo anterior se suman los ataques externos que vulneran el funcionamiento correcto de los sistemas, incluso la interrupción esporádica de ciertos sistemas y servicios, puede ocasionar importantes pérdidas económicas.

Los virus informáticos, el "hacking" o los ataques de negación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) constituye un modelo de gestión que establece unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El objetivo de estos Sistemas de Gestión es identificar los riesgos a los que está sometida su información y asumirlos, minimizarlos, transferirlos o controlarlos mediante una sistemática definida, documentada y conocida por todos, que se analiza y mejora constantemente.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que el SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

Un Sistema de Gestión de la Seguridad de la Información ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir, disminuyendo vulnerabilidades e incrementando el valor de sus activos.

1.9. COMPONENTES PRINCIPALES DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Alcance del SGSI.- Identificación clara de las relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

Política de Seguridad del SGSI.- En la Norma ISO 27002 se nos indica los contenidos mínimos que debe incluir. No debemos confundir la Política del SGSI con la Política de Seguridad de la Información de nuestra organización (que según la Norma estaría incluida en la anterior), si bien, ambas políticas pueden ser definidas en un documento único. La Política de Seguridad del SGSI debe ser aprobada por la dirección y distribuida entre todo el personal afectado. Es decir, que la Política de Seguridad del SGSI es un documento que debe ser sometido a periódicas revisiones y actualizaciones.

Estándares, Procedimientos, y Guías que soportan el SGSI.- Aquellos documentos y mecanismos que regulan el propio funcionamiento del SGSI. Documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Metodología de Análisis de Riesgos.- Son varias las herramientas disponibles en el mercado para realizar un Análisis de Riesgos. En cualquier caso, son herramientas complejas, y dependiendo de la estructura de nuestra organización puede resultar más óptimo encomendar esta tarea a alguna consultora externa. El Análisis de Riesgos consiste en la identificación de los activos (datos, hardware, software, servicios, personal, etc.) de valor de nuestra organización y la determinación del riesgo asociado a cada uno en base a las amenazas y vulnerabilidades que los rodean. El objetivo del Análisis de Riesgo es obtener una visión global del riesgo al que se encuentran expuestos nuestros activos, en función de la probabilidad de que una amenaza pueda llegar a materializarse y el impacto que causaría en la organización.

Selección de controles para el tratamiento del riesgo

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce como el Plan de Tratamiento del Riesgo (PRT) que es un documento o conjunto de ellos, de vital importancia para el SGSI. El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, que recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones.

Para el tratamiento de riesgos existen cuatro estrategias

1. **Reducción del riesgo.-** Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.
   Al identificar los controles a ser implantados es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas.

2. **Aceptación del riesgo.-** Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el conto de implementar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo y vivir con las consecuencias si el riesgo ocurriese.

3. **Transferencia del riesgo.-** Es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora.
   Hay que tener en cuenta, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales aplicaran dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto debe ser muy bien analizada para así poder identificar con precisión cuanto del riesgo actual está siendo transferido.

4. **Evitar el riesgo.-** La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican para así poder evitar la ocurrencia del riesgo.
   Las maneras habituales para implementar esta opción son:
   - Dejar de conducir ciertas actividades.
   - Desplazar activos de información de un área riesgosa a otra.
   - Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

Informe de evaluación de riesgos.-Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Gestión del Riesgo.- Implica clasificar los riesgos en aceptables y no aceptables. Lógicamente, la Gestión del Riesgo debe enfocarse hacia los riesgos que la organización no está dispuesta a aceptar, y se debe clarificar el tratamiento que se va a emplear hasta alcanzar un nivel de riesgo aceptable.

Registros.- Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de Aplicabilidad.- Es el documento final que muestra la selección de los controles aplicables que conforman el SGSI. En la Declaración de Aplicabilidad debe quedar bien claro, y de forma razonada cuáles son los controles de la Norma ISO que se van a implantar y cuáles no se estima oportuno. También debe realizarse una breve descripción de cada uno de ellos y el estado en que se encuentran en la actualidad.

Es muy importante recalcar en que el SOA es parte esencial de un SGSI, y que como todos los documentos que hacen parte de este sistema requiere ser actualizado periódicamente debido a la adición de nuevos servicios en la Organización.

Control de documentos.- Todos los documentos requeridos serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- ✓ Aprobar documentos y prioridades o clasificación de empleo.
- ✓ Revisiones, actualizaciones y re aprobaciones de documentos.
- ✓ Asegurar que los cambios y las revisiones de documentos sean identificados.
- ✓ Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- ✓ Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- ✓ Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- ✓ Asegurar que los documentos de origen externo sean identificados.
- ✓ Asegurar el control de la distribución de documentos.
- ✓ Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

CAPÍTULO # 2

ANTECEDENTES DELA INSTITUCIÓN

2. ANTECEDENTES DE LA M. I. MUNICIPALIDAD DE GUAYAQUIL

2.1 INTRODUCCIÓN

La M. I. Municipalidad de Guayaquil, es una entidad administrativa que agrupa una sola localidad, como es el caso de la ciudad de Guayaquil. Esta institución se rige principalmente en lo que prescribe la Constitución Política de la República y en la Ley de Régimen Municipal en que establece la autonomía funcional, económica y administrativa de la Entidad.

El cabildo debe cumplir las necesidades peculiares de acuerdo a los servicios públicos a prestarse y responderá a una estructura que permita tener todas y cada una de las funciones que a ella competen, para el mejor cumplimiento de las mismas.

La Municipalidad desea laborar bajo una guía de Manual de Seguridad de Informática, que sirven de base para el funcionamiento, actualización y evaluación de los Sistemas con que la entidad cuenta.

2.2 FUNCIONES Y OBJETIVOS GENERALES

A la Municipalidad le corresponde, cumpliendo con los fines que le son esenciales, satisfacer las necesidades colectivas del vecindario, especialmente las derivadas de la convivencia urbana cuya atención no compete a otros organismos gubernativos; sin embargo cooperará con apego a la Ley, a la realización de los fines del Estado.

Normar a través de Ordenanzas, dictar Acuerdos y Resoluciones, determinar la política a seguir y fijar las metas en cada una de las ramas propias de la Administración Municipal.

Para alcanzar los objetivos propuestos y cumplir las funciones encomendadas, la M. I. Municipalidad de Guayaquil [4]desarrolla las siguientes estrategias:

- Procurar el ordenamiento urbanístico de la ciudad, mejorar e incrementar los servicios públicos de la comunidad, a la vez que mantener en buen estado los existentes.

- Ejercer un estricto control en materia de higiene, salubridad y asistencia social, propender la elevación del nivel cultural de los vecinos del Cantón.

[4]http://www.guayaquil.gob.ec/

- Alcanzar el mayor rendimiento de las fuentes de financiamiento, procurar a la vez el ordenamiento racional y lógico del costo municipal.

- Propender a mejorar el sistema económico-administrativo del Cabildo para fortificar las finanzas y alcanzar una eficiente racionalización administrativa.

- Coordinar su acción con otros organismos de la Ciudad y de la provincia, con la finalidad de optimizar recursos y encontrar una verdadera solución a los problemas del Cantón.

- Sistematizar a través del procedimiento electrónico de datos, las distintas áreas de la Corporación, a fin de encontrar mayor eficiencia y servicio para la comunidad.

La M. I. Municipalidad está compuesta por los siguientes departamentos:

1. **Dirección de Medio Ambiente:**

Esta división es la encargada de asesorar a la Alcaldía en la emisión de políticas, normas y estrategias de gestión municipal relativas al medio ambiente, planificar, supervisar, y coordinar las actividades relacionadas con la preservación del Medio Ambiente, en la jurisdicción cantonal.

2. **Dirección de Asesoría Jurídica:**

Asesorar al nivel directivo y ejecutivo y a los demás directivos de la Municipalidad en asuntos de orden jurídico; programar, organizar, dirigir, coordinar y controlar las actividades relacionadas con estudios jurídicos, patrocinio legal y contrataciones de la Entidad.

3. **Dirección de Asesoría Jurídica:**

La Dirección de Control de Gestión tendrá como misión asesorar y aplicar métodos de control, evaluación y seguimiento al Sistema de Control interno implementando en las Fundaciones y Corporaciones Municipales.

4. **Dirección de Recursos Humanos:**

Establecer y aplicar las políticas relativas a la administración de personal, aprobadas por el Concejo Cantonal o el Alcalde. Cumplir y hacer cumplir las políticas de reclutamiento y selección determinadas en el Reglamento de Personal, así como velar porque se cumpla con lo dispuesto en éste y en el Reglamento Orgánico y Funcional de la Municipalidad.

5. **Dirección de Informática:**

Planificar y desarrollar sistemas automatizados de información. Asesorar a las diferentes dependencias municipales en los campos de su especialización. Supervisar el adecuado funcionamiento de los sistemas implantados.

6. **Dirección Administrativa:**

Cumplir y hacer cumplir las Leyes; Ordenanzas, Reglamentos, Acuerdos y Resoluciones Municipales; y aquellas disposiciones emanadas del Concejo Cantonal y el Alcalde. El departamento es responsable del funcionamiento, mantenimiento y conservación de las instalaciones, dependencias y mobiliario tanto interno como externo de la M.I. Municipalidad de Guayaquil. Implantar los diferentes programas de Seguridad Industrial en las áreas que ameriten protección.

7. **Dirección de Secretaría General:**

Tramitar informes, certificaciones, correspondencia y demás documentos. Dar fe de los actos del Concejo y de la Alcaldía, asegurando oportunidad y reserva en el manejo de la documentación oficial, y certificar la autenticidad de copias, compulsas o reproducciones.

8. **Dirección de Obras Públicas General:**

Programar y ejecutar las obras que emprende la municipalidad, ya sea por administración directa, por contrato o por concesión, desde su inicio hasta la entrega coordinando con las empresas de servicio público, la mejor y eficiente ejecución de las obras de infraestructura, para el beneficio de la comunidad.

9. **Dirección de Justicia y Vigilancia:**

Cumplir y hacer cumplir las leyes, ordenanzas, reglamentos, acuerdos y resoluciones municipales dentro de la esfera de sus funciones; organizar y administrar la acción de vigilancia y control municipales; velar por una adecuada administración interna.

10. **Dirección de Terrenos y Servicios Parroquiales:**

Cumplir y hacer cumplir las Leyes; Ordenanzas, Reglamentos, Acuerdos y Resoluciones Municipales; y aquellas disposiciones emanadas del Concejo Cantonal y el Alcalde, que tengan que ver con el control y ejecución de las normas municipales en la comunidad.

2.3 ORGANIGRAMA DE LA INSTITUCIÓN

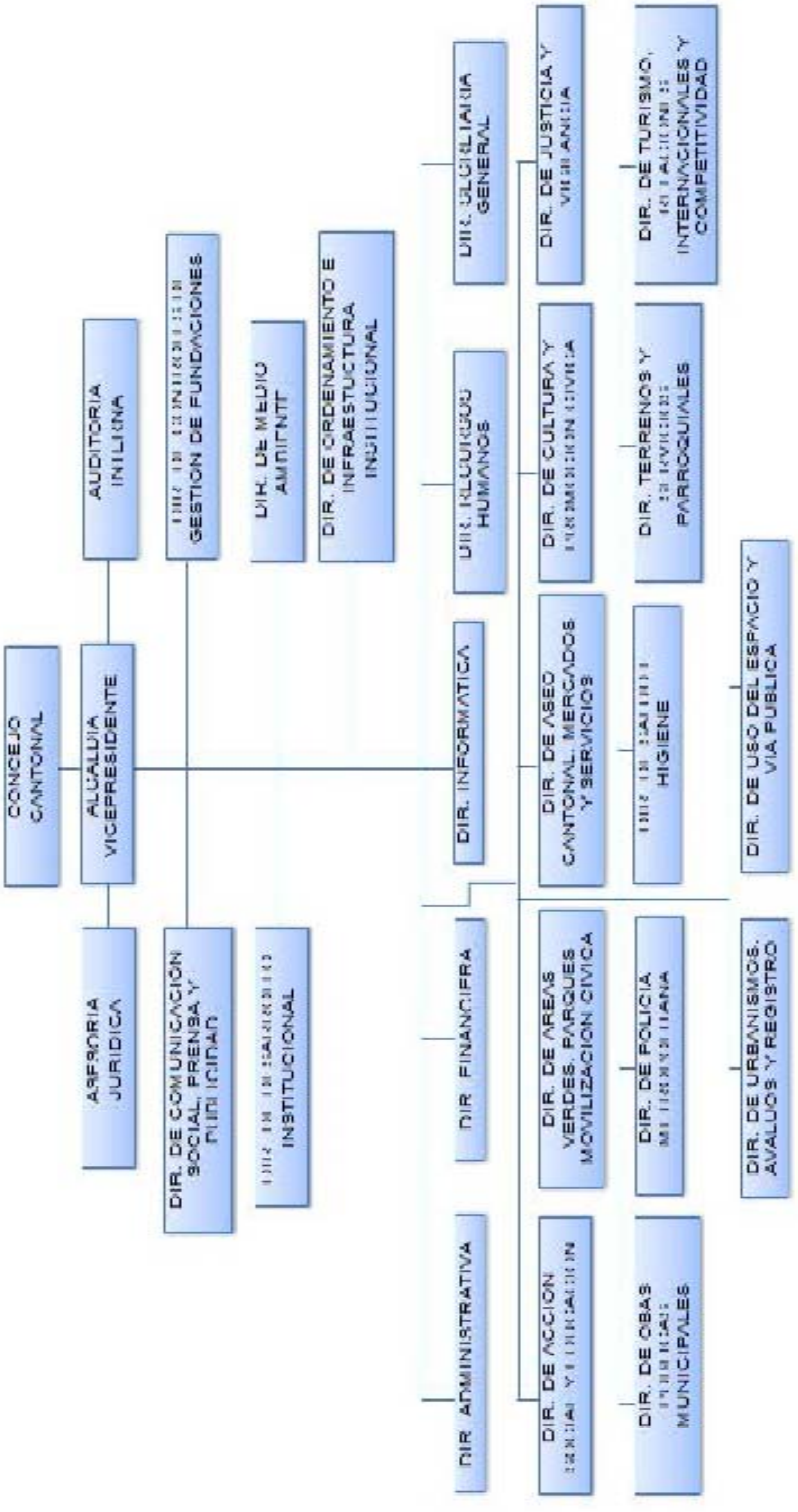
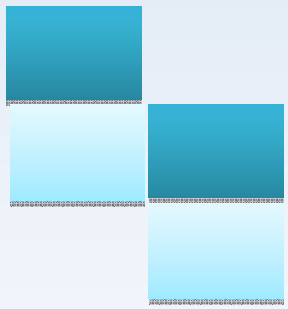


Figura 2-1: Organigrama de la M.I. Municipalidad de Guayaquil



CAPÍTULO # 3

PLANEACIÓN PARA LA IMPLEMENTACIÓN DE POLÍTICAS SEGURIDAD DE INFORMACIÓN

3. PLANEACIÓN

3.1 MODELO PDCA

Todos los Sistemas de Gestión de la Seguridad de la Información se basan en la necesidad de que la Seguridad de la Información esté en continua evolución y que, además, dicha evolución esté documentada y justificada.

La norma ISO/IEC 27002 proporciona un conjunto de recomendaciones sobre qué medidas a tomar en la empresa para asegurar los Sistemas de Información. Los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva aplicaremos para la gestión del riesgo analizado.

El modelo **PDCA**, es una estrategia de mejora continua de la calidad implementada en cuatro pasos detallados a continuación.

3.1.1. PLANIFICAR

Planificación de la gestión del servicio:

1. Definir el alcance del ITSM (Gestión De Servicios De Tecnología De La Información).
2. Definir las políticas de gestión de servicios.
3. Establecer los objetivos y requisitos.
4. Definir los procesos.
5. Definir enfoque de riesgos para alcanzar objetivos.
6. Roles, responsabilidades (general por proceso).
7. Definir los recursos, equipamiento, presupuestos, herramientas.
8. Como se va a gestionar, auditar y mejorar el ITSM.

3.1.2. HACER

Implementar la gestión y provisión del servicio

1. Definir e implantar el plan de gestión del servicio.
2. Implantar los procesos (documentos, responsables, registros, indicadores, entradas y salidas).
3. Implantar el sistema de gestión.

3.1.3. VERIFICAR

Monitorizar, medir y verificar

1. Desarrollar procedimientos de monitorización.
2. Revisar regularmente el ITSM.
3. Revisar objetivos y plan de gestión del servicio.
4. Auditar internamente el ITSM.

3.1.4. ACTUAR

Mantener el ITSM y desarrollar la mejora continua

1. Identificar e implantar las mejoras.
2. Adoptar acciones correctivas y preventivas.
3. Verificar que las mejoras cumplen su objetivo.

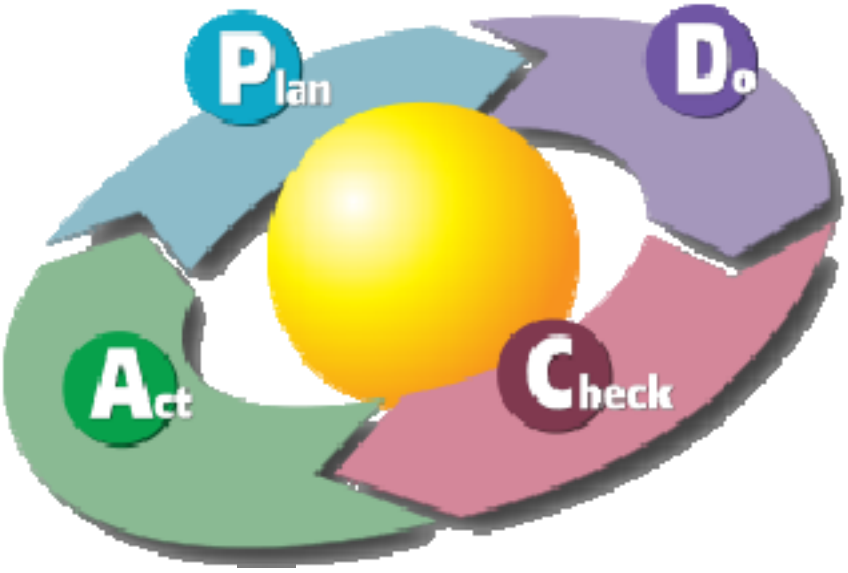


Figura 3-1: Modelo PDCA

3.2 ALCANCE

3.2.1 NORMA ISO/IECE 27002

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales. **(ANEXO 1)**

Figura 3-2: Dominios Norma ISO 27002

3.3 ALCANCE DE LAS POLÍTICAS DE SEGURIDAD

En la actualidad muchos son los aspectos a tener en cuenta para garantizar que se cumplan con las expectativas requeridas, es decir una serie de normativas que cuiden hasta el mínimo, para que todo resulte un éxito. Por lo tanto, es necesario disponer de todos los recursos para certificar la seguridad de la información, como lo es en el caso de una entidad del gobierno; como La M.I. Municipalidad de Guayaquil, que maneja información tal de los empleados, proveedores, tecnología, ciudadanos (clientes), etc.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

La implementación del Manual de Políticas de Seguridad para La M.I. Municipalidad de Guayaquil, corresponde al departamento de Informática, el cual tiene a su cargo las siguientes funciones:

a) Apoyar computacionalmente las actividades de todos las Direcciones, Departamentos y otras unidades de la Municipalidad, preocupándose del desarrollo de programas como de la actualización de todo su equipo.

b) Mantener y administrar las redes, sistemas y equipos computacionales de la Municipalidad.

c) Prestar soporte a usuarios en todo lo relativo a la plataforma computacional de la Municipalidad.

d) Supervisar todo proyecto informático que fuere contratado a terceros y ser la contraparte técnica de los sistemas computacionales arrendados.

e) Controlar las concesiones que le correspondan de acuerdo a su participación en la elaboración de las especificaciones técnicas y que le sean atingentes a la naturaleza de sus funciones.

f) Velar por la integridad de la información almacenada en equipos computacionales de propiedad municipal, además de elaborar y ejecutar los planes de contingencia necesarios en caso de pérdida de dicha información.

g) Preparar, ayudar a interpretar y entregar la información estadística a las unidades municipales que lo requieran.

h) Recopilar, actualizar y mantener datos e información estadística Comunal y Regional, necesaria para la Municipalidad, con la finalidad de que ésta sea útil en la toma de decisiones.

i) Crear y administrar las bases de datos que sean relevantes para la toma de decisión y para el conocimiento de la comunidad.

j) Coordinar el accionar de las distintas dependencias municipales de manera de ir integrando y correlacionando información y bases de datos.

k) Cumplir otras tareas que el Administrador Municipal le encomiende, de acuerdo a la naturaleza de sus funciones y del Marco Legal.

3.4 OBJETIVO GENERAL

Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

3.5 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad que se plantean en este documento, se basan en un análisis estratégico. Estas políticas representan directrices generales de alto nivel que deben ser adoptadas por el personal de la Municipalidad.

3.5.1. POLÍTICAS GENERALES

1. Para acceder a la Red Municipal se requiere que el usuario cuente con una clave, la misma que es de su absoluta responsabilidad.

2. Los usuarios solo pueden ingresar a los terminales autorizados, conocidos como PC., en los casos que no tenga un terminal bajo su cargo, o no exista uno específico en ésa área solicitará la asignación respectiva, con el formulario “Solicitud de Acceso al Sistema”.

3. Las claves se cambiarán máximo en 45 días. Pudiendo hacerlo el usuario antes de ése tiempo cuando lo crea conveniente.

4. Las claves que no se utilizan en un plazo máximo de 90 días serán eliminadas del sistema. Se exceptúan los casos de permisos por maternidad, o enfermedad.

5. Solo en casos especiales podrán tener hasta dos sesiones simultáneamente, previa autorización del director.

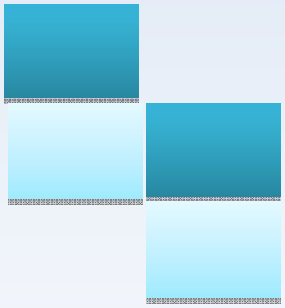
6. No podrán permanecer en las instalaciones de Informática personal sin autorización.

7. Los usuarios, dueños de las aplicaciones clasificaran su información en pública y privada.

8. Cuando una persona dejaré de pertenecer a la institución, entregará las llaves, y copias de manuales a su cargo, así como los bienes respectivos siguiendo el procedimiento establecido por Control de Bienes.

9. La Dirección de Recursos Humanos, comunicará la renuncia o salida de empleados a la Dirección de Informática para la eliminación de la clave.

10. Los usuarios son responsables del cuidado y protección de los equipos asignados, así como del uso o mal uso de la clave de acceso.



CAPÍTULO # 4

ANÁLISIS DE RIESGO

4. METODOLOGÍA DE CONTROL DE RIESGO

Previa la identificación, análisis y evaluación de vulnerabilidades es necesario realizar una revisión de varias metodologías de riesgos para seleccionar la más adecuada acorde la realidad de la empresa y de esta manera analizar las vulnerabilidades actualmente presentes en la corporación.

4.1. METODOLOGÍA DE RIESGOS

Hay varios métodos para realizar el análisis de riesgo, cada método tiene sus propias características, así como sus ventajas y desventajas para seleccionar un método de análisis de riesgos que se ajuste a las características de la empresa.

4.1.1. MAGERIT

Es la metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones publicas promovido por el consejo superior de informática. Materia define los procedimientos para guiar a la administración paso a paso en el establecimiento de la protección necesaria y como respuesta a su dependencia creciente respecto de las técnicas electrónicas, informáticas y telemáticas. Los objetivos son:

1. Analizar los riesgos que soportan un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. El análisis de riesgo permite identificar las amenazas que asechan a los distintos componentes pertenecientes o relacionados con el sistema de información (activos), para determinar la vulnerabilidad del sistema entre esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización. Se tiene así una medida del riesgo que corre el sistema analizado.

2. Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados, mediante la gestión de riesgos.

3. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo.

4. Ofrecer un método sistemático para analizar tales riesgos.

5. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

6. Apoyar la preparación a la Organización para procesos de evaluación, auditoria, certificación, o acreditación según corresponda el caso.

4.2. VENTAJAS

Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

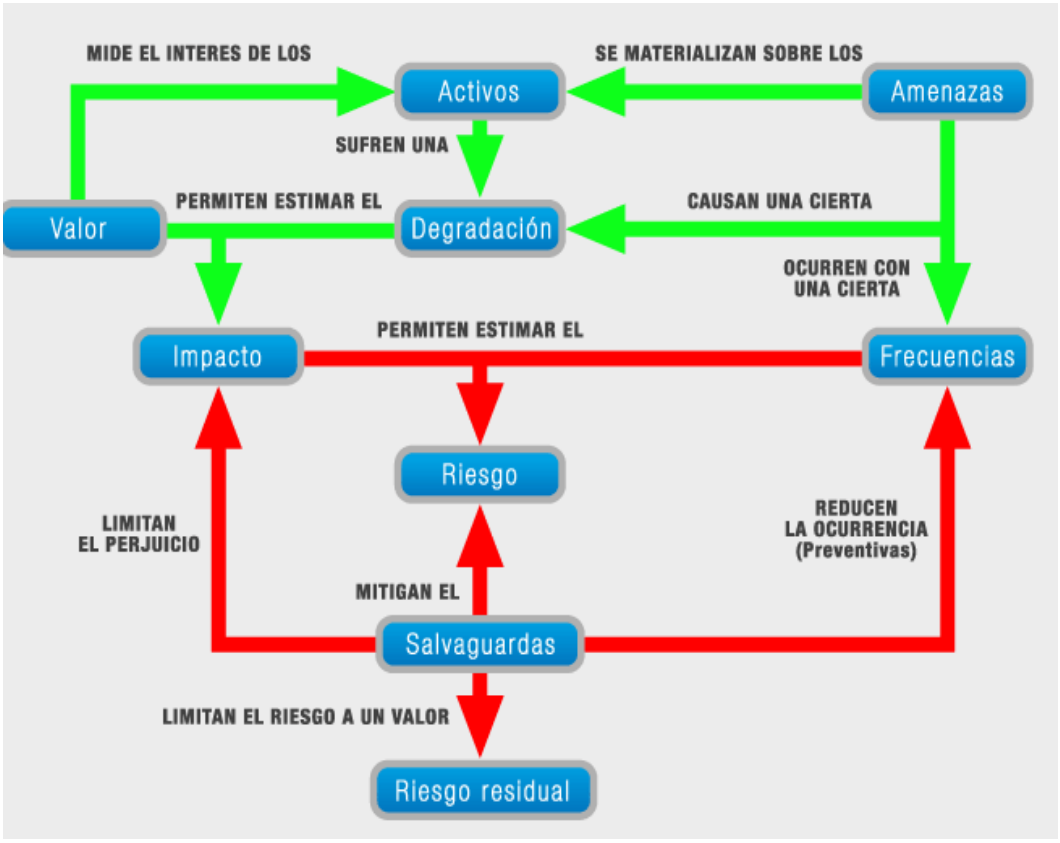


Figura 4-1: Metodología Magerit

4.3. INVENTARIO DE ACTIVOS

N°	ACTIVO
1	DomainController
2	Active Directory
3	Exchange Server
4	Dataprotector
5	Isa Server
6	Isa Server Informática
7	Sharepoint
8	HelpDesk
9	Ultimus – Desarrollo
10	Ultimus – Producción
11	ON – BASE
12	Aplicaciones – Desarrollo – SQL
13	Aplicaciones – Testing – SQL
14	Aplicaciones – Producción – SQL
15	Base de Datos – Desarrollo – SQL
16	Base de Datos – Testing
17	Base de Datos – Producción – SQL
18	Base de Datos – Producción – SQL
19	Base de Datos – Oracle – Desarrollo -
20	Base de Datos – Producción
21	Base de Datos – Terminal de Transferencia de Víveres
22	Claves de usuarios
23	SMS

Tabla 4-1: Inventario de Activos

4.4. ANÁLISIS Y EVALUACIÓN DE RIESGOS

4.4.1. CRITERIOS DE VALORIZACIÓN

A continuación se explicará las escalas utilizadas para la valoración del riesgo, el límite de tolerancia del riesgo y el criterio. Para la valoración de riesgos se identificarán y evaluarán los activos basados en las necesidades de la organización. La organización debe determinar un criterio para la determinación de los tres elementos que son: confidencialidad, integridad, disponibilidad.

Confidencialidad	Clase	Descripción
1	Pública	Puede ser revelado y proporcionado a terceras personas.
2	Uso interno	Puede ser revelado y proporcionado. Si el contenido fuera revelado no tendría mucho efecto en las operaciones.
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas.

Tabla 4-2: Criterio de Valorización - Confidencialidad

Integridad	Clase	Descripción
1	No necesaria	Usado solo para consultas.
2	Necesaria	Si el contenido fuese falsificado habría problemas, pero no afectarían mucho a las operaciones.
3	Importante	Si la integridad se perdiera, habría un efecto fatal en las operaciones.

Tabla 4-3: Criterio de Valorización – Integridad

Disponibilidad	Clase	Descripción
1	Bajo	Si la información no estuviese disponible no habría efectos en las operaciones.
2	Mediano	Si la información no estuviese disponible, habría algún efecto en las operaciones. Sin embargo métodos alternativos pueden ser usados en las operaciones.
3	Alto	Si la información no llegara a estar disponible cuando sea necesitada, habría un efecto fatal en las operaciones.

Tabla 4-4: Criterio de Valorización - Confidencialidad

Nivel	Valor	Descripción
3	Alto	Existe una gran probabilidad de que ocurra, por lo menos una vez.
2	Media	Podría ocurrir con alguna probabilidad.
1	Bajo	Es un fenómeno que ocurre rara vez en el año.

Tabla 4-5: Criterio de Valorización - Ocurrencia

Nivel	Valor	Descripción
1	Nula	No hay Vulnerabilidad.
2	Baja	Sí hay controles y son suficientes.
3	Media	Hay algunos controles.
4	Alta	No hay controles o no son suficientes.

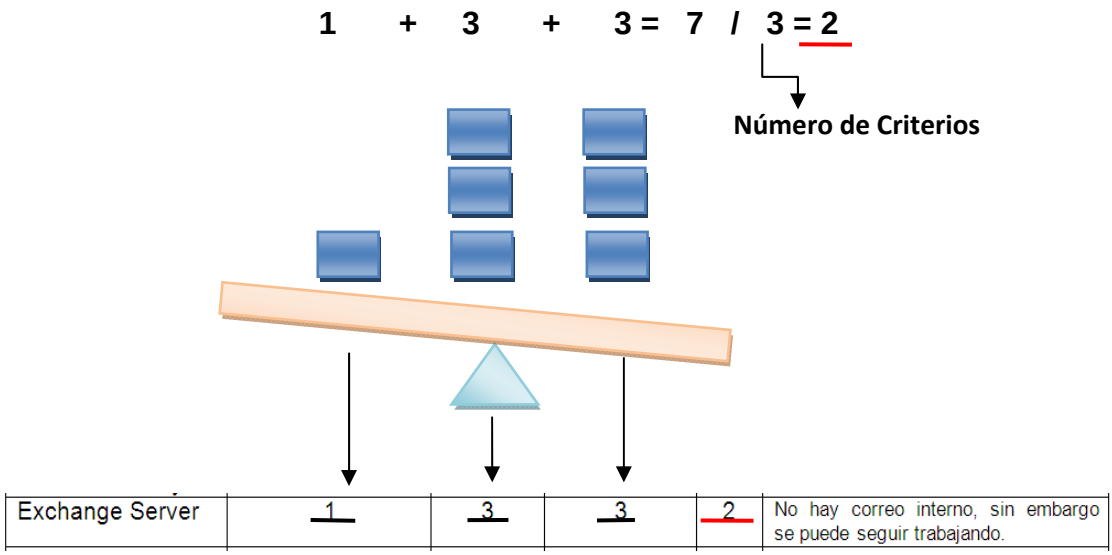
Tabla 4-6: Criterio de Valorización - Vulnerabilidad

Nivel	Valor	Descripción
1	Insignificante	Impacto muy bajo - No requiere acción.
2	Menor	Efectos menores en el negocio - No requiere acción.
3	Poco Significativo	Algún efecto negativo - No se considera necesario tomar acción.
4	Significativo	Efecto negativo en el negocio. Estos riesgos son considerados aceptables.
5	Importante	Tendrían serios efectos negativos en el negocio.
6	Mayor	Tendrían efectos negativos mayores en el negocio, y deberían ser reducidos en todas las circunstancias.

Tabla 4-7: Criterio de Valorización - Riesgo

4.4.2. CÁLCULO DE TASACIÓN DE ACTIVOS

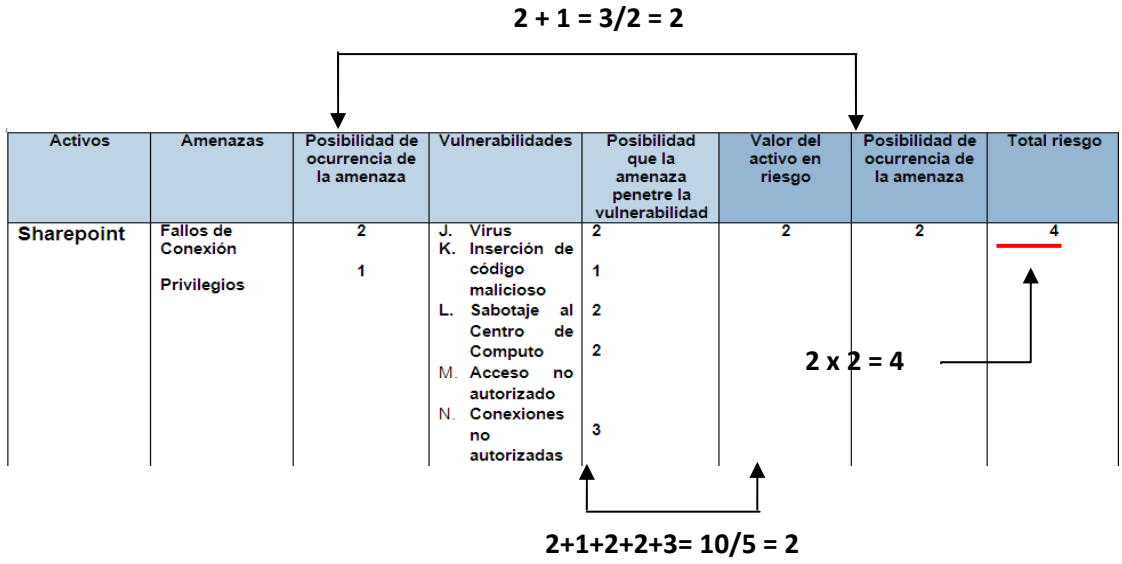
La tasación del activo se calcula de la siguiente forma:



Exchange Server	1	3	3	2	No hay correo interno, sin embargo se puede seguir trabajando.

4.4.3. CÁLCULO DE RIESGO

El nivel de riesgo del activo se calcula de la siguiente forma:



Activos	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor del activo en riesgo	Posibilidad de ocurrencia de la amenaza	Total riesgo
Sharepoint	Fallos de Conexión Privilegios	2 1	J. Virus K. Inserción de código malicioso L. Sabotaje al Centro de Computo M. Acceso no autorizado N. Conexiones no autorizadas	2 1 2 2 3	2	2	4

4.5. TASACIÓN DE ACTIVOS

Activo	Confidencialidad	Integridad	Disponibilidad	Total	Justificación
Domain Controller	3	3	3	3	Porque si esta caído el DomainController no hay sistema para el Municipio.
Active Directory	3	3	3	3	No existe validación a la red.
Exchange Server	1	3	3	2	No hay correo interno, sin embargo se puede seguir trabajando.
SMS	1	2	1	1	No es crítico, porque solo se suspenden las actualizaciones vía red.
Datapro-tector	1	3	3	2	Se suspenden los respaldos.
Isa Server	3	3	3	3	No hay internet.
Isa Server Informática	2	2	2	2	No hay internet para el departamento de Informática.
Sharepoint	3	3	3	3	No se puede revisar los documentos publicados.
HelpDesk	1	1	1	1	No se puede reportar problemas, pero se los puede manejar por correo interno.
Ultimus – Desarrollo	1	1	1	1	Actualmente el sistema está en etapa terminada.
Ultimus – Producción	2	2	3	2	Afecta solo a los Departamentos involucrados.
ON – BASE	1	3	2	2	Afecta solo a los Departamentos involucrados.
Aplicaciones – Desarrollo–SQL	1	3	2	2	Los cronogramas de Desarrollo se atrasan.
Aplicaciones – Testing – SQL	1	1	1	1	No es crítico.

Tabla4-2: Tasación de Activos

Activo	Confidencialidad	Integridad	Disponibilidad	Total	Justificación
Aplicaciones – Producción – SQL	3	3	3	3	No se pueden correr las aplicaciones de producción.
Base de Datos – Desarrollo – SQL	2	2	2	2	Se retrasan los cronogramas de Desarrollo.
Base de Datos – Testing	1	1	1	1	No es crítico.
Base de Datos – Producción – SQL	3	3	3	3	No se puede correr las aplicaciones de producción.
Base de Datos – Oracle – Desarrollo	1	1	3	2	Se retrasan los cronogramas de Desarrollo.
Base de Datos – Producción	3	3	3	3	No se puede correr las aplicaciones de producción.
Base de Datos – Terminal de Transferencia de Víveres	3	3	3	3	No se puede correr las aplicaciones de producción.
Claves de usuarios	**3**	**3**	**3**	3	No se puede tener acceso a la Red.

Tabla4-2: Tasación de Activos

4.6. ANÁLISIS Y EVALUACIÓN DE RIESGOS

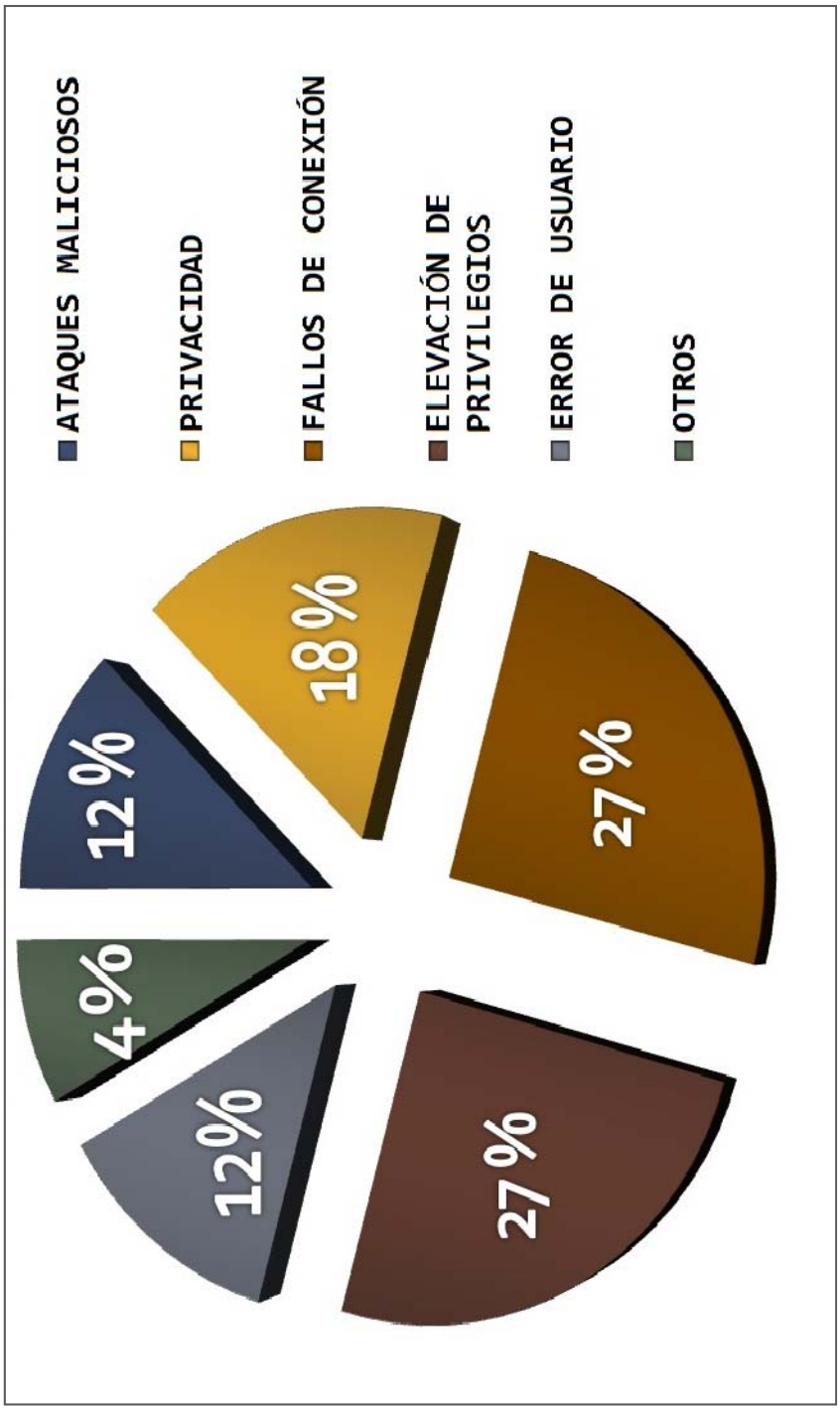


Figura 4-2: Amenazas a los Activos

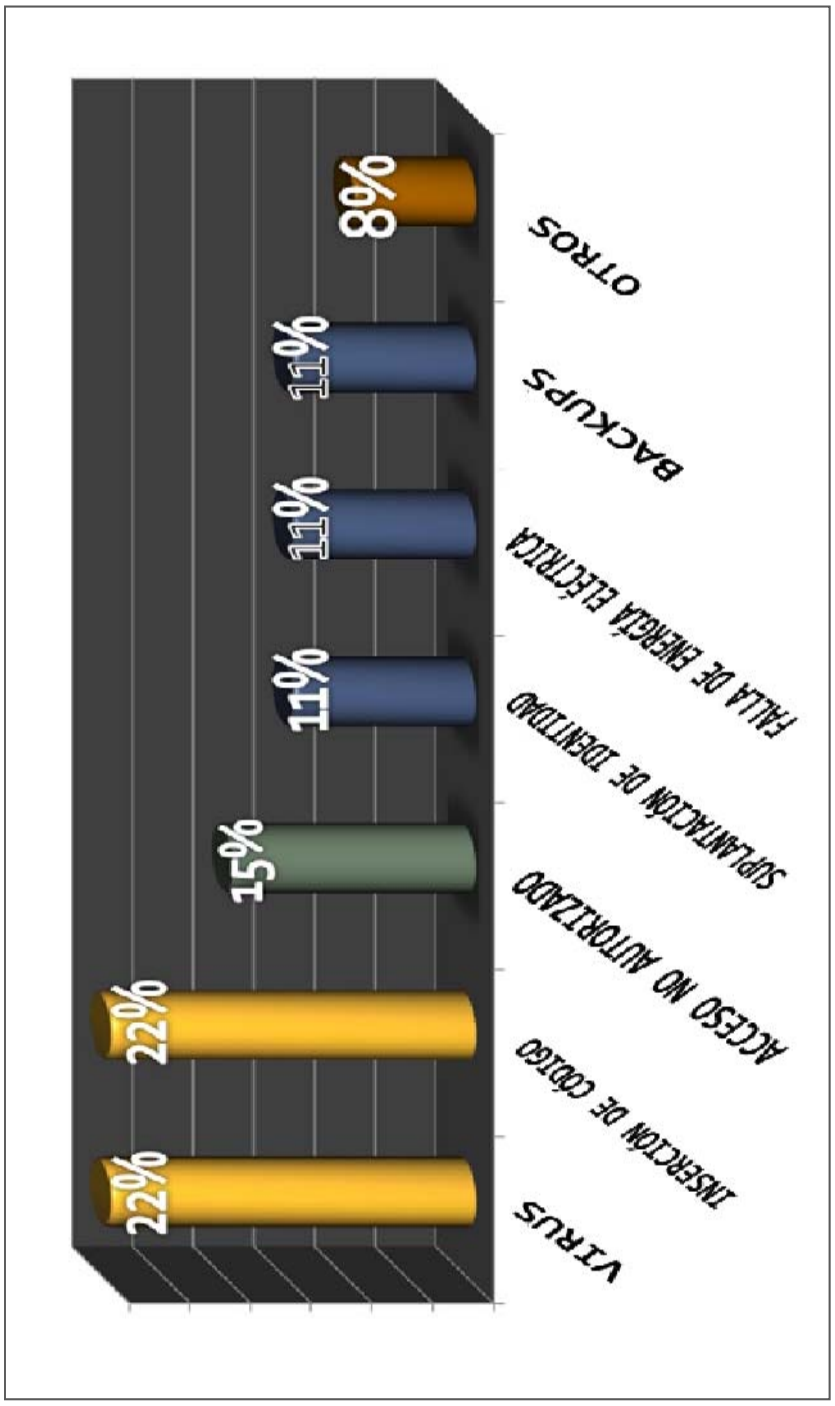


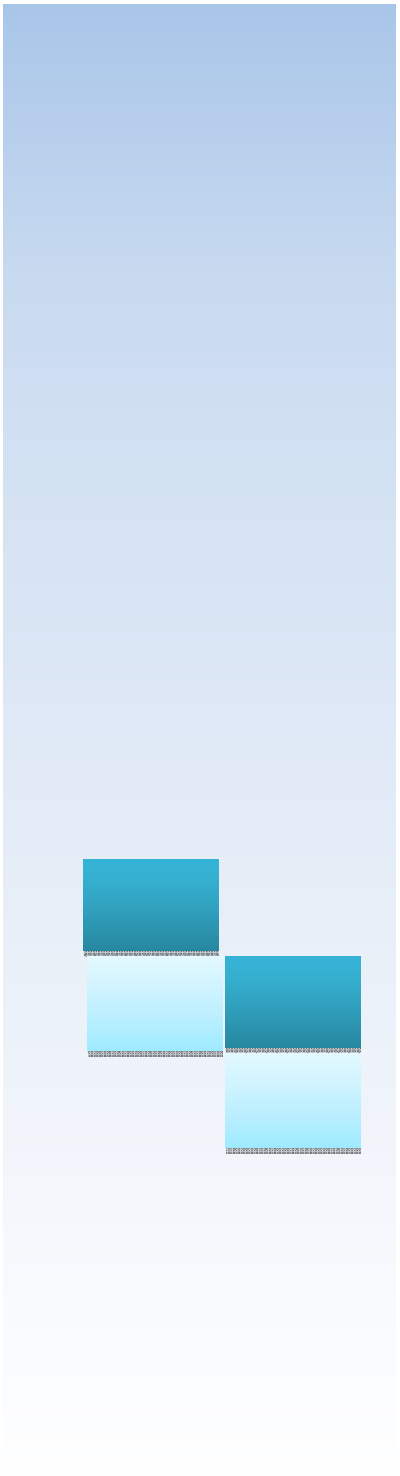
Figura 4-3: Vulnerabilidades de los Activos

Activos	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor del activo en riesgo	Posibilidad de ocurrencia de la amenaza	Total riesgo
DomainController	Ataques Maliciosos	1	A. Virus B. Inserción de código malicioso	2 2	1	2	2
	Privacidad	1	C. Sabotaje al Centro de Computo	1			
	Fallos de Conexión	2	D. Falla del hardware	2			
Isa Server	Ataques Maliciosos	1	E. Virus F. Denegación de servicios	2 1	1	2	2
	Fallos de Conexión	1	G. Inserción de código malicioso	2			
	Elevación de privilegios	2	H. Sabotaje al Centro de Computo I. Acceso no autorizado	1 2			

Tabla4-3: Análisis de Riesgo

Activos	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor del activo en riesgo	Posibilidad de ocurrencia de la amenaza	Total riesgo
Base de Datos – Producción – SQL	Plagio	1	A. Deficiencia organizativa	2	3	2	6
	Alteración	2	B. Acceso no autorizado	2			
	Privacidad	1	C. Falta de Criptografía	3			
	Perdida de Información	2	D. No tener backups	3			
Claves de usuarios	Alteración	1	E. Acceso no autorizado	2	3	2	6
	Privacidad	2	F. Control de Documentos	3			
			G. Suplantación de la identidad del usuario	3			
			H. Abuso de privilegios de acceso	3			

Tabla 4-4: Análisis de Riesgo



CAPÍTULO # 5

IMPLEMENTACIÓN DE POLÍTICAS SEGURIDAD DE INFORMACIÓN

5. PLAN DE TRATAMIENTO DE RIESGO

El análisis y evaluación riesgo nos permitió valorizar el riesgo y conocer cuáles son los activos de información que tienen mayor exposición por lo tanto conocer donde enfocar los recursos de la organización.

El riesgo tiene 4 opciones de tratamiento que son:

•Reducir, con la aplicación de contramedidas o salvaguardas especificadas controles del Anexo A de la norma.

•Evitar, dejando de realizar la actividad que produce el riesgo.

•Transferir, a un tercero como por ejemplo una aseguradora o una tercerización de servicios.

•Aceptar, que consiste en asumir la responsabilidad de correr dicho riesgo.

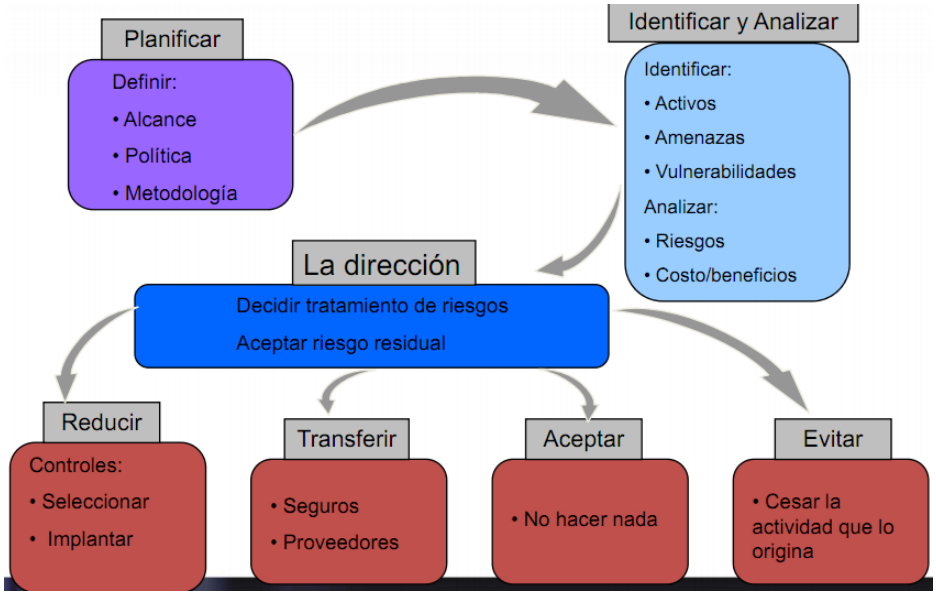


Figura5-1: Plan de Tratamiento de Riesgo

El objetivo de este punto es tomar cual debe ser la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro de Análisis de Riesgo y los Criterios de Valorización.

5.1. IMPLEMENTACIÓN DE PLAN DE TRATAMIENTO DE RIESGO

Activo	Amenazas	Tratamiento	Objetivo del Control	Control	Justificación
DomainController	Ataques Maliciosos	Reducir	8.2	8.2.2	Instruir a los empleados sobre la políticas implementadas
			8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
	Privacidad		9.2	9.2.1	Proteger e hardware y reducir amenazas y peligros ambientales
			9.2	9.2.4	Asegurar la continua disponibilidad del hardware
	Fallos de Conexión		10.4	10.4.1	Proteger de intrusiones maliciosas
Isa Server	Ataques Maliciosos	Transferir	7.1	7.1.3	Uso correcto del sistema
			8.1	8.1.1	Definir roles y responsabilidades sobre el activo.
			8.2	8.2.2	Instruir a los empleados sobre la políticas implementadas
			8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
			10.4	10.4.1	Proteger de intrusiones maliciosas
	Fallos de Conexión		11.2	11.2.1	Ejecutar un procedimiento forma para la inscripción y des-inscripción para otorgar acceso.
			11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegics.
	Elevación de privilegios		11.2	11.2.3	Permitira controlar a través de un proceso de gestion formal la asignación de claves.
			10.4	10.4.1	Proteger de intrusiones maliciosas a los datos
			11.1	11.1.1	Revisión de la política de control de acceso.
			11.2	11.2.1	Ejecutar un procedimiento forma para la inscripción y des-inscripción para otorgar acceso.
			11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegics.

Tabla5-1: Plan de Tratamiento de Riesgo

Activo	Amenazas	Tratamiento	Objetivo del Control	Control	Justificación
SharePoint	Fallos de Conexión	Reducir	8.1	8.1.1	Definir roles y responsabilidades sobre el activo.
			8.2	8.2.2	Instruir a los empleados sobre la políticas implementadas
			8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
	Privilegios		10.4	10.4.1	Proteger de intrusiones maliciosas
			11.2	11.2.1	Ejecutar un procedimiento forma para la inscripción y des-inscripción para otorgar acceso.
			11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegios.
			11.2	11.2.3	Permitirá controlar a través de un proceso de gestión formal la asignación de claves
Aplicaciones – Producción– SQL	Error de funcionamiento	Reducir	8.1	8.1.1	Definir roles y responsabilidades sobre el activo.
	Códigos Maliciosos		8.2	8.2.2	Instruir a los empleados sobre la políticas Implementadas
	Fallos Técnicos		8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
	Errores de Usuario		10.4	10.4.1	Proteger de intrusiones malicinsas
			11.1	11.1.1	Revisión de la política de control de acceso.
	Falta de Seguridad		11.2	11.2.1	Ejecutar un procedimiento forma para la inscripción y des-inscripción para otorgar acceso.
	Falta mantenimiento		11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegios.

Tabla 5-2: Plan de Tratamiento de Riesgo

Activo	Amenazas	Tratamiento	Objetivo del Control	Control	Justificacion
Base de Datos Producción – SQL	Plagio	Reducir	8.2	8.2.2	Instruir a los empleados sobre la políticas implementadas
	Alteración		8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
	Privacidad		10.4	10.4.1	Proteger de intrusiones maliciosas a los datos
			11.1	11.1.1	Revisión de la política de control de acceso.
	Perdida de Información		11.2	11.2.1	Ejecutar un procedimiento forma para la inscripción y des-inscripción para otorgar acceso.
			11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegios
Claves de usuarios	Alteración	Reducir	8.1	8.1.1	Definir roles y responsabilidades sobre el activo.
			8.2	8.2.1	Para que los empleados estén claramente informados sobre sus roles y responsabilidades
			0.2	0.2.2	Instruir a los empleados sobre la políticas implementadas
			8.2	8.2.3	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad
			11 2	11 2 1	Ejecutar un procedimiento forma para la inscripción y des inscripción para otorgar acceso.
	Privacidad		11.2	11.2.2	Restringir y controlar la asignación y uso de los privilegios.
			11.2	11.2.3	Permitira controlar a través de un proceso de gestión formal la asignación de claves.
			11 2	11 2 4	Revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
			11.3	11.3.1	Para que los usuarios mantengan la confidencialidad dentro del sistema.

Tabla 5-3: Plan de Tratamiento de Riesgo

AMENAZA	CONTROL	TRATAMIENTO
ATAQUES MALICIOSOS	10.4.1 Controles contra códigos maliciosos. A.11.2. A.11.3. A.11.4.	REDUCIR
PRIVACIDAD	11.1.1 Política de control de acceso. 11.2.1 Registro de Usuario. 11.2.3 Gestión de claves secretas de usuario. 11.2.4 Revisión de los derechos de acceso del usuario. A.1.1. A.1.2. A.1.3. A.1.12. A.3.4. A.3.5. A.11.5.	REDUCIR
FALLOS DE CONEXIÓN	9.2.1 Ubicación y protección del equipo. 9.2.4 Mantenimiento de los equipos. A.3.8. A.6.1.	REDUCIR
ELEVACIÓN DE PRIVILEGIOS	11.2.2 Gestión de privilegios. 11.3.1 Uso de claves secretas. A.1.6. A.2.3. A.3.2. A.3.9. A.3.2.	REDUCIR
ERROR DE USUARIO	8.1.1 Roles y responsabilidades. 7.1.3 Uso aceptable de los activos. 8.2.2 Conocimiento, educación y capacitación en Sistemas de información. 8.2.3 Proceso disciplinario. A.1.16. A.1.12. A.4.4. A.4.6.	REDUCIR

Tabla 5-4: Controles contra Riesgos

5.2. DESARROLLO DEL SOA (DECLARACIÓN DE APLICABILIDAD)

SOA Describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.

ISO 27002:2005 Controls		Controles Actuales	Observaciones (justificación de exclusión)	Controles seleccionados y las razones para la selección				Observaciones (descripción general de la aplicación)
				LR	CO	BPBI	ERA	
Cláusula	Sec	Objetivo de control						
Política de Seguridad	5.1	Políticas de Seguridad de la Información						
	5.1.1	Documento de Política de Seguridad de la Información						
		Políticas Generales	☒ Si existe		☒			Se implementaran políticas para el correcto comportamiento del departamento de informática.
		Seguridad a nivel físico		☒				
		Seguridad a nivel lógico		☒		☒		Políticas para asignación de accesos y administración de los sistemas.
		Seguridad a nivel de sistemas		☒				Políticas para el correcto uso y tanibulación de las aplicaciones de sistemas.
		Respaldo y recuperación de información		☒				Políticas para establecer tiempos de respaldo y normas de recuperación en caso de que se pierda la información.
		Accesos Remotos		☒				Definir políticas para terceros, que tendrán acceso a la información
		Seguridad de WWW		☒				El personal solo podrá tener acceso a paginas establecidas.
		Control de Virus Uso de Software		☒				Definir políticas para protección de información antes amenazas de virus y/o uso de software incorrecto
		Equipos de Computación		☒				
		Manipulación de PC						Políticas para la tanibulación de los equipos de computación, mantenimiento y actualizaciones que se realice al mismo.
		Mantenimiento de equipos						
		Actualización de equipos						
		Seguridad de los equipos de computación					☒	
		Sanciones		☒				Se aplicaran sanciones por el no cumplimiento de las políticas establecidas.

Tabla 5-5: SOA

Responsabilidad de los Activos	7.1	**Responsabilidad sobre los activos**									
		7.1.3 Uso aceptable de los activos					X	X	X	X	Uso correcto del sistema.
Seguridad ligada a los recursos humanos	8.1	**Antes del empleo**									
		8.1.1 Roles y responsabilidades					X	X	X	X	Definir roles y responsabilidades sobre el activo.
	8.2	**Durante el empleo**									
		8.2.2 Concientización, educación y capacitación en SI					X	X	X	X	Instruir a los empleados sobre políticas implementadas.
		8.2.3 Proceso disciplinario					X	X	X	X	Para ejecutar un proceso disciplinario formal para los empleados que cometan un incumplimiento de seguridad.
Seguridad física y del entorno	9.2	**Seguridad de los equipos**									
		9.2.1 Ubicación y protección del equipo					X	X	X	X	Proteger el hardware y reducir amenazas y peligros ambientales.
		9.2.4 Mantenimiento de los equipos					X	X	X	X	Asegurar la continua disponibilidad del hardware.
Gestión de comunicaciones y operaciones	10.4	**Protección contra el código malicioso y descargable**									
		10.4.1 Controles contra códigos maliciosos					X	X	X	X	Proteger de intrusiones maliciosas.
Control de Acceso	11.1	**Requisitos del negocio para el control de acceso**									
		11.1.1 Política de control de acceso					X	X	X	X	Revisión de la política de control de acceso.
	11.2	**Gestión de acceso de usuario**									
		11.2.1 Registro de Usuario					X	X	X	X	Ejecutar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso.
		11.2.2 Gestión de privilegios					X	X	X	X	Restringir y controlar la asignación y uso de los privilegios.
		11.2.3 Gestión de claves secretas de usuario					X	X	X	X	Permitir control a través de un proceso de gestión formal la asignación de claves.
		11.2.4 Revisión de los derechos de acceso de usuario					X	X	X	X	Revisar los cerrojos de acceso de los usuarios a intervalos regulares, utilizando un proceso formal.
	11.3	**Responsabilidad de usuario**									
		11.3.1 Uso de claves secretas					X	X	X	X	Para que los usuarios mantengan la confidencialidad de un dispositivo del sistema.

Tabla 5-6: SOA

5.3. POLÍTICAS DE SEGURIDAD

OBJETIVO:

Proporcionar dirección y apoyo directivo para brindar seguridad de la información.

El nivel directivo debe establecer una dirección y política clara, demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

5.2.1. POLÍTICAS GENERALES

A.1.1 Para acceder a la Red Municipal se requiere que el usuario cuente con una clave, la misma que es de su absoluta responsabilidad.

A.1.2 Los usuarios solo pueden ingresar a los terminales a los cuales estén autorizados, conocidos como PC., en los casos que no tenga un terminal bajo su cargo, o no exista uno específico en ésa área solicitará la asignación respectiva, con el formulario “Solicitud de Acceso al Sistema”.

A.1.3 Las claves se cambiarán máximo en 45 días. Pudiendo hacerlo el usuario antes de ése tiempo cuando lo crea conveniente.

A.1.4 Las claves que no se utilizan en un plazo máximo de 90 días serán eliminadas del sistema. Se exceptúan los casos de permisos por maternidad o enfermedad.

A.1.5 Solo en casos especiales podrán tener hasta dos sesiones simultáneamente, previa autorización del director del área en que el usuario se encuentre.

A.1.6 No podrán permanecer en las instalaciones de Informática personal sin autorización.

A.1.7 Los ambientes de Desarrollo, Producción estarán plenamente definidos.

A.1.8 Los programadores no podrán acceder a los datos de producción. Solo en los casos de “standby”, emergencia o “links” de lecturas, sujetándose a lo establecido en el Reglamento de Seguridad Informática *(Anexo 3)*.

A.1.9 Los usuarios, dueños de las aplicaciones clasificaran su información en pública y privada.

La Información Pública estará disponible para todas las direcciones, y la Privada solo para el personal de la misma dirección, siguiendo el procedimiento de "Solicitud de Acceso al Sistema".

A.1.10 Los manuales originales de software propiedad de la Municipalidad estarán bajo custodia del Jefe de Seguridad Informática.

A.1.11 Los jefes de áreas solicitaran una copia de los manuales que de acuerdo a sus funciones les correspondan.

A.1.12 Cuando una persona deje de pertenecer a la institución, entregará las llaves, y copias de manuales a su cargo, así como los bienes respectivos siguiendo el procedimiento establecido por Control de Bienes.

A.1.13 La Dirección de Recursos Humanos, comunicará la renuncia o salida de empleados a la Dirección de Informática para la eliminación de claves de acceso.

A.1.14 Para paso de programas del ambiente de Desarrollo a Producción y viceversa se seguirá lo establecido en el procedimiento del Reglamento de Seguridad Informática "Capitulo 3 Seguridades Lógicas" *(*Anexo 3*)*.

A.1.15 La depuración del espacio en disco del sistema la realizaran conjuntamente las áreas involucradas como Base de Datos, Seguridades y Producción. Los usuarios son responsables del cuidado y protección de los equipos asignados, así como del uso o mal uso de la clave de acceso.

A.1.16 Los usuarios son responsables de la información guardada en sus discos duros, para lo cual deben seguir los procedimientos de respaldos de información establecidos.

A.1.17 Los operadores son responsables de notificar cualquier anomalía que se presente en el Centro de Cómputo durante la ausencia de los Jefes respectivos, y notificarán cualquier desperfecto en las instalaciones eléctricas, equipos de aire acondicionado, para su mantenimiento preventivo o correctivo.

A.1.18 Todas las PC de escritorio o laptop deberán tener activado la clave de encendido.

A.1.19 Todos los terminales deben tener activado el salva pantalla con clave de encendido a los 5 minutos máximo.

A.1.20 La información o papelería no utilizada en el Centro de Cómputo debe ser triturada.

A.1.21 Para ingresar o sacar hardware o software de propiedad de la Institución se requiere de autorización escrita del Director, Sub- Director o del correspondiente Jefe del departamento de Informática.

A.1.22 Para los contratos con terceros se incluirá una cláusula de confidencialidad de la información.

A.1.23 Para la instalación de algún software, se requiere de la licencia respectiva, y en caso de no poseerla no podrá realizar dicha instalación.

5.2.2. POLÍTICAS DE SEGURIDAD A NIVEL FÍSICO

A.2.1 El ingreso al Centro de Cómputo es restringido. Sólo personal autorizado por la Dirección pueden ingresar al Centro de Cómputo.

A.2.2 No se podrá fumar en ningún área de informática.

A.2.3 Sólo personal autorizado puede ingresar después de las horas normales de trabajo, así como los fines de semana y feriados.

A.2.4 En caso de algún incidente de incendio, corto circuito, o casos fortuitos o de fuerza mayor que se presente en el Centro de Cómputo se comunicará inmediatamente al personal respectivo.

A.2.5 Se prohíbe tomar café o comer cerca de los equipos de computación.

A.2.6 Se deben revisar los extintores de incendios cada año, para ser cambiados o recargados.

A.2.7 Las cintas de respaldos deben estar en cajas fuertes seguras y contra incendios.

A.2.8 Todos los equipos hardware y los correspondientes software deben estar asegurados contra robos, destrucción y en forma general contra cualquier siniestro.

A.2.9 El área de Informática estará vigilada las 24 horas del día con personal externo a la Dirección.

A.2.10 Las llaves a lugares restringidos estarán en poder del Director de informática o la persona delegada por él.

A.2.11 Durante el mantenimiento preventivo o correctivo de los equipos estará presente el Jefe de Producción, o el Supervisor de Producción o un delegado de ésta área.

5.2.3. POLÍTICAS DE SEGURIDADES A NIVEL LÓGICO

A.3.1 Las funciones de los operadores estarán reguladas por un menú. No deben trabajar desde el "prompt" del Sistema Operativo.

A.3.2 La administración del menú de los operadores estará bajo la responsabilidad del Departamento de Producción.

A.3.3 Los problemas que se presenten el área del Centro de Cómputo serán registradas en una bitácora electrónica. Y notificada lo más pronto posible a las áreas involucradas.

A.3.4 Los reportes generados en el área del Centro de Cómputo serán entregados únicamente al destinatario.

A.3.5 Los reportes de "logs", o rastros de auditorías solo deben ser entregados al Departamento de Auditoria de Sistemas.

A.3.6 La instalación y mantenimiento del Sistema Operativo es responsabilidad del Jefe de Producción o su delegado.

A.3.7 La instalación y actualizaciones de la Base de Datos es responsabilidad del Administrador de la Base de Datos.

A.3.8 Las Seguridades lógicas de la red están a cargo del Jefe de Redes o de su delegado.

A.3.9 La creación de claves de acceso a los sistemas y la entrega de dichas claves es responsabilidad del Jefe de Seguridad Informática.

A.3.10 Se dará claves de los sistemas a usuarios que se encuentran entrenados en los mismos, previa verificación del Jefe de Desarrollo, que ha recibido el listado de los usuarios que recibieron la inducción.

A.3.11 Para asignar opciones a usuarios se seguirá el procedimiento "Solicitud de Acceso al Sistema", siendo el responsable de las mismas el usuario solicitante, es decir el Jefe del departamento en que se requiere el permiso.

A.3.12 El acceso a los sistemas por parte de los usuarios será a través de un menú, es decir de acuerdo a las funciones que le correspondan. Es responsabilidad de los usuarios notificar la suspensión de su clave o eliminación de opciones no utilizadas o que no le correspondan a sus funciones.

5.2.4. POLÍTICAS DE SEGURIDADES A NIVEL DE SISTEMAS

A.4.1 Los programas de ingreso de información deben contemplar rutinas de validación de datos.

A.4.2 Los programas que permiten ingreso, modificación, eliminación de información deben generar registros para Auditoria, conteniendo usuario, fecha, hora, terminal, tipo de transacción, observaciones, etc.

A.4.3 Los sistemas deberán contemplar las agrupaciones por roles de funciones como por ejemplo: Directores, Sub-Directores, Jefes, Supervisores, Revisores, Digitadores, Analistas, Auxiliares, etc.

A.4.4 El sistema debe contemplar la recuperación de la información en caso de que una transacción falle por error de programación, error del usuario etc.

A.4.5 El desarrollo de los sistemas se sujetarán a los estándares establecidos en ésta área.

A.4.6 Se realizarán reuniones periódicas con los usuarios dueños de la aplicación para asegurar el cumplimiento de los objetivos establecidos y alcance del sistema.

A.4.7 En caso de opciones con datos privados, el sistema debe contemplar la ejecución desde un determinado terminal o nivel de usuario.

A.4.8 La documentación de los sistemas debe contemplar las tablas a las que se tiene acceso, así como los diferentes permisos de lectura, inserción, actualización o eliminación.

A.4.9 Una vez terminado el sistema, se deben entregar al área de Seguridades los Diagramas Funcionales, la Base de Datos y los respectivos Modelos Entidad – Relación. Se sujetara a lo establecido en el Procedimiento de Implementación de los Sistemas.

A.4.10 Al final del desarrollo del sistema se generarán los siguientes documentos:

Manual Técnico del Sistema.
Manual del Usuario, y
Manual del Operador.

A.4.11 Al realizar la entrega del Sistema, se firmará un acta de entrega/ recepción del mismo, en el que se indicará una cláusula que contenga “Los datos son de propiedad del usuario y tienen la responsabilidad de protegerlos”.

5.2.5. POLÍTICAS DE RESPALDOS Y RECUPERACIÓN DE INFORMACIÓN

A.5.1 El tiempo en que se realizaran los respaldos serán establecidos según su relevancia. Se seguirá según lo señalado en el Reglamento de Seguridad Informática *(*Anexo 3*).*

A.5.2 Los respaldos serán en cintas separadas para la: Base de Datos, Programas, Usuarios, "Logs Files" y Archivos del Sistema Operativo.

A.5.3 Los respaldos semanales se los mantendrá en lugares externos y seguros.

A.5.4 Los respaldos mensuales no rotaran y se convertirán en archivos permanentes.

A.5.5 Las cintas para uso diario rotaran cada 8 días, debiendo tenerse 8 juegos de cintas.

A.5.6 Las cintas semanales rotaran cada 4 semanas, debiendo tener el mismo número de juegos de cintas.

A.5.7 Las cintas deben estar etiquetadas con la siguiente información básica: Año, mes, día, hora, información que contiene y comentarios.

A.5.8 La información histórica que se mantendrá en línea será hasta dos años. Los demás datos se los mantendrá en servidores o directorios especiales.

A.5.9 Las cintas serán actualizadas cada cierto periodo de tiempo, de acuerdo a las disponibilidades de equipo y necesidades, por el Supervisor de Producción.

5.2.6. POLÍTICAS RELACIONADAS A LOS EQUIPOS DE COMPUTACIÓN

A.6.1 Todos los equipos (computadores, estaciones de trabajo y equipo accesorio), que esté conectado a la red, o que en forma autónoma se tenga y que sea propiedad de la institución, debe sujetarse a las normas y procedimientos de instalación de la Dirección de Informática.

A.6.2 La Dirección de Informática en coordinación con el Departamento de Control de Bienes deberá tener un registro de todos los equipos propiedad de la Institución.

A.6.3 El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, y su correspondiente control de acceso.

A.6.4 Las áreas de Soporte Técnico y Soporte a Usuario son las responsables de la instalación, reubicación, reasignación y todo aquello que implique movimientos de equipos.

A.6.5 La protección física de los equipos es responsabilidad de su custodio y corresponde notificar los movimientos en caso de que existan a las autoridades correspondientes (departamento de Soporte Técnico, Control de bienes y otros de competencia).

5.2.7. POLÍTICAS DE MANTENIMIENTO DE EQUIPOS.

A.7.1 Al departamento de Soporte Técnico y de Usuarios, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico necesario.

A.7.2 Se contrataran compañías externas para que se encarguen del mantenimiento preventivo y correctivo de las máquinas y equipos que no estén en garantías con los proveedores, en especial de los servidores y equipos de red.

A.7.3 No se dará mantenimiento a equipos que no son de propiedad de la institución.

A.7.4 Ningún usuario final podrá efectuar el mantenimiento de los equipos a su cargo, aunque éste sea el mantenimiento básico.

5.2.8. POLÍTICAS DE ACTUALIZACIÓN DE LOS EQUIPOS.

A.8.1 Todos los equipos (computadores personales, estaciones de trabajo, y demás relacionados) y los de comunicaciones que son de propiedad de la institución deberán ser actualizados tendiendo a conservar e incrementar la calidad del servicio que prestan, mediante la mejora sustantiva de su desempeño.

5.2.9. POLÍTICAS DE ACCESOS REMOTOS

A.9.1 Para el caso especial de acceso a los recursos por parte de terceros deberán ser autorizados por la Dirección de Informática en conjunto con la Dirección propietaria de los datos que están vinculados.

A.9.2 El usuario de estos servicios deberá sujetarse a las normas y políticas internas establecidas.

5.2.10. POLÍTICAS DEL WWW

A.10.1 La Dirección de Informática es la responsable de instalar y administrar el o los servidores WWW. Es decir, sólo se permite servidores de páginas autorizadas por la Dirección.

5.2.11. POLÍTICA DE CONTROL DE VIRUS, USO DE SOFTWARE

A.11.1 Está prohibido el uso de programas sin licencias no autorizadas por la Institución.

A.11.2 Se debe mantener en forma residente un anti-virus instalado en su computador y la actualización en línea de las nuevas versiones que se liberen.

A.11.3 Ejecutar el anti-virus antes de utilizar cualquier disco removible o fichero recibido que provenga de otro usuario, ya sea de la empresa o del exterior.

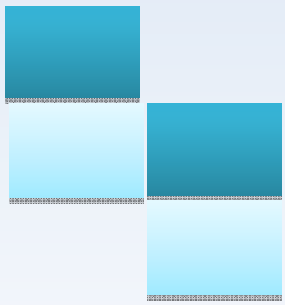
A.11.4 Proteger contra escritura todos los discos removibles.

5.2.12. SANCIONES.

S.1.1 Cualquier violación a las políticas y normas de seguridad deberá ser sancionado de acuerdo lo establecido en el Reglamento de Personal.

S.1.2 Las sanciones también pueden contemplar la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

S.1.3 Todas las acciones en las que se comprometa la seguridad y que no estén previstas en esta política deberán ser revisadas por la Dirección de Informática para una resolución de acuerdo a las leyes vigentes.



CAPÍTULO # 6

Estrategias de Difusión, Conclusiones y Recomendaciones

6. ESTRATEGIAS DE DIFUSIÓN

6.1. COMUNICACIONES ESCRITAS:

- Enviar memorándums a todos los empleados informando los nuevos cambios en políticas de seguridad informática.
- Entregar a todo el personal un tríptico con la información más relevante de las nuevas políticas.
- Realizar evaluaciones periódicas al personal para conocer que tan bien se conoce las nuevas políticas.

6.2. REUNIONES:

Organizar reuniones informativas a diferentes niveles empresariales en la cual se dará a conocer información detallada de las nuevas políticas y procedimientos de seguridad.

6.3. BOLETÍN INFORMATIVO*:*

Consiste en una pequeña publicación mensual en donde se puede encontrar información de acontecimientos importantes de reuniones y cambios de puestos de trabajo o novedades de la organización.

6.4. COMUNICACIÓN ELECTRÓNICA:

Difundir la información mediante el sistema de correo electrónico interno de empresa. Dicha información debe de ser puntual.

6.5. COMUNICACIONES INFORMALES*:*

Comúnmente llamados como rumores de la oficina, consiste en intercambios de información que se producen de manera espontánea entre los empleados de la oficina sin que se haya programado un encuentro sino que este surge espontáneamente.

7. CONCLUSIONES

1. La forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en casos de incidentes.

2. La seguridad de la información no es una responsabilidad únicamente del área de tecnología, debe fluir desde la alta gerencia hacia todos los procesos de negocios.

3. Un comité de seguridad de la información compuesto por cada jefe de área genera más compromiso para hacer cumplir las políticas de seguridad de la información.

4. La organización debe entender la seguridad como un proceso que nunca termina.

5. Es de gran importancia limitar la asignación de privilegios, por lo que deberán estar perfectamente identificados y asignarse en base a la necesidad de uso. Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios.

8. RECOMENDACIONES

1. Crear un Comité de Seguridad, Un Equipo de Seguridad de Información y un Equipo de Tecnología de la Información.

2. Habilitar un Centro de Cómputo alterno – en un lugar distante al edificio principal donde funciona el Centro de Cómputo actual.

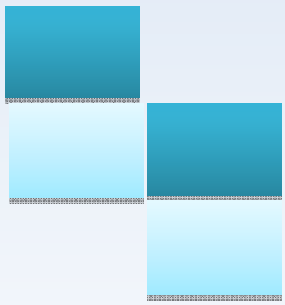
3. Para los usuarios de alto riesgos (cajeros, administradores, directores etc.), adquirir equipos con reconocimiento de huellas digitales.

4. Capacitar al personal municipal en el conocimiento básico de seguridades de la información prevención de virus, ingenierita social, respaldos de información etc.

5. Evaluar la posibilidad de adquirir Forefront Client Security y Forefront Server Security Management Console para obtener mayor protección, control y gestión de la seguridad de la estructura tecnológica.

6. Efectuar un Ethical Hacking para verificar las seguridades a nivel de la red.

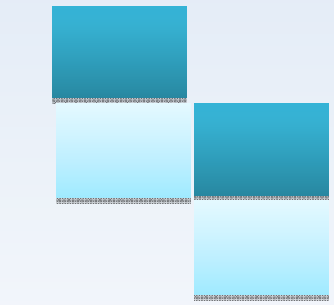
7. Planificar la realización de un simulacro de incendio y evacuación del personal de informática.



GLOSARIO

9. GLOSARIO

ATINGENTES. -Tocante o perteneciente.
ISMS. - Information Security Management System (inglés).
ISO.- Organización Internacional de Normalización.
ITSM.- Gestión De Servicios De Tecnología De La Información.
PRT.- Plan de Tratamiento de Riesgo.
SGSI.- Sistema de Gestión de la Seguridad de la Información.
HACKING.- virus informático.
SOA.- Arquitectura a Orientada a Servicios.



ANEXO

10. ANEXO 1

10.1 DISTRIBUCIÓN DE LOS DOMINIOS DE LA NORMA ISO 27002[5]

10.1.1 POLÍTICA DE SEGURIDAD

1.1 Política de seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

1.1.1 Documento de la política de seguridad de la información

Control: El documento de la política de seguridad de la información debe ser aprobado por la gerencia, publicado y comunicado a todos los empleados y las partes externas relevantes. Esta política de seguridad de la información se debe comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector.

1.1.2 Revisión de la política de seguridad de la información

Control: La política de seguridad de la información debe ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad. Se debe mantener un registro de la revisión gerencial. Se debe obtener la aprobación de la gerencia para la política revisada.

10.1.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1.2 Organización interna

Objetivo: Manejar la seguridad de la información dentro de la organización. Se debe establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debe aprobar la política de seguridad de la información, asignar los roles de seguridad, coordinar y revisar la implementación de la seguridad en toda la organización.

[5] http://iso27002.es/

1.2.1 Compromiso de la gerencia con la seguridad de la información

Control: La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información. La gerencia debe identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, revisar y coordinar los resultados de la consultoría a través de toda la organización.

1.2.2 Coordinación de la seguridad de la información

Control: Las actividades de la seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes. Si la organización no utiliza grupos inter-funcionales separados; por ejemplo, porque dicho grupo no es apropiado para el tamaño de la organización; las acciones arriba descritas deben ser realizadas por otro organismo gerencial adecuado o un gerente individual.

1.2.3 Asignación de las responsabilidades de la seguridad de la información

Control: Todas las responsabilidades de la seguridad de la información deben estar claramente definidas.

1.2.4 Autorización de proceso para facilidades procesadoras de información.

Control: Un proceso de la gerencia para la autorización de facilidades nuevas de procesamiento de información, debe ser definido e implementado.

1.2.5 Acuerdos de confidencialidad

Control: Se deben identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la organización para proteger la información.

1.2.6 Contacto con las autoridades

Control: Se deben mantener los contactos apropiados con las autoridades relevantes.

1.2.7 Contacto con grupos de interés especial

Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

1.2.8 Revisión Independiente de la Seguridad de la Información

Control: Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.

1.3 Grupos o personas externas

Objetivo: Mantener la seguridad de la información y los medios de procesamientos de información de la organización que son ingresados, procesados, comunicados a, o manejados por grupos externos. La seguridad de la información y los medios de procesamiento de la información de la organización no deben ser reducidos por la introducción de productos y servicios de grupos externos.

1.3.1 Identificación de los riesgos relacionados con los grupos externos

Control

Se deben identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se deben implementar controles apropiados antes de otorgarles acceso.

1.3.2 Tratamiento de la seguridad cuando se lidia con clientes

Control

Se deben tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

1.3.3 Tratamiento de la seguridad en acuerdos con terceros

Control

Los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o medios de procesamiento de información de la compañía, o agregan productos o servicios a los medios de procesamiento de información deben abarcar todos los requerimientos de seguridad relevantes.

10.1.3 GESTIÓN DE ACTIVOS

1.4 Responsabilidad por los activos

Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales. Todos los activos deben ser inventariados y contar con un propietario nombrado. Los propietarios deben identificar todos los activos y se debe asignar la responsabilidad por el mantenimiento de los controles apropiados.

1.4.1 Inventario de los activos

Control

Se deben identificar todos los activos y se debe elaborar y mantener un inventario de todos los activos importantes.

1.4.2 Propiedad de los activos

Control

Toda la información y los activos asociados con los medios de procesamiento de información deben ser propiedad de una parte designada de la organización.

1.4.3 Uso aceptable de los activos

Control

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

1.5 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección apropiado. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información. La información tiene diversos grados de confidencialidad e importancia.

1.5.1 Lineamientos de clasificación

Control

Se debe clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.

1.5.2 Etiquetado y manejo de la información

Control

Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

10.1.4 SEGURIDAD DE RECURSOS HUMANOS

1.6 Antes del empleo

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Las responsabilidades de seguridad deben ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.

1.6.1 Roles y responsabilidades

Control

Se deben definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

1.6.2 Investigación de antecedentes

Control

Los chequeos de verificación de antecedentes de todos los candidatos para empleo, contratistas y terceros deben llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes; y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

1.6.3 Términos y condiciones del empleo

Control

Como parte de su obligación contractual; los usuarios empleados, contratistas y terceros deben aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.

1.7 Durante el empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

1.7.1 Responsabilidades de la gerencia

Control

La gerencia debe requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.

1.7.2 Conocimiento, educación y capacitación en seguridad de la información

Control

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas deben recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

1.7.3 Proceso disciplinario

Control

Debe existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.

1.8 Terminación o cambio de empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada. Se deben establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

1.8.1 Responsabilidades de terminación

Control

Se deben definir y asignar claramente las responsabilidades de realizar la terminación del empleo o el cambio de empleo.

1.8.2 Devolución de los activos

Control

Todos los usuarios empleados, contratistas y terceras personas deben devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato acuerdo.

1.8.3 Retiro de los derechos de acceso

Control

Los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información deben ser retirados a la terminación de su empleo, contrato o acuerdo, o deben ser reajustados de acuerdo al cambio.

10.1.5 SEGURIDAD FÍSICA Y AMBIENTAL

1.9 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

1.9.1 Perímetro de seguridad física

Control

Se deben utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

1.9.2 Controles de ingreso físico

Control

Las áreas seguras deben protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

1.9.3 Asegurar las oficinas, habitaciones y medios

Control

Se debe diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios.

1.9.4 Protección contra amenazas externas e internas

Control

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

1.9.5 Trabajo en áreas aseguradas

Control

Se debe diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

1.9.6 Áreas de acceso público, entrega y carga

Control

Se deben controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, si fuese posible, deben aislarse de los medios de procesamiento de información para evitar el acceso no autorizado.

1.10 Seguridad de los equipos

Objetivo: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización. Se debe proteger el equipo de amenazas físicas y ambientales. La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-autorizado a la información y proteger contra pérdida o daño. Esto también debe considerar la ubicación y eliminación del equipo.

1.10.1 Ubicación y protección del equipo

Control

Se debe ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.

1.10.2 Servicios públicos de soporte

Control

Se debe proteger el equipo de fallas de energía y otras interrupciones causadas por fallasen los servicios públicos de soporte.

1.10.3 Seguridad del cableado

Control

El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información deben protegerse contra la intercepción o daño.

1.10.4 Mantenimiento de los equipos

Control

Se debe mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.

1.10.5 Reutilización o retirada segura de los equipos

Control

Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

1.10.6 Retirada de materiales propiedad de la empresa

Control

Se deben chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

10.1.6 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

1.11 Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información. Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados. Cuando sea apropiado, se debe implementar la segregación de funciones para reducir el riesgo de negligencia o mal uso deliberado del sistema.

1.11.1 Documentación de los procedimientos de operación.

Control

Los procedimientos de operación se deben documentar, mantener y poner a disposición de todos los usuarios que los necesiten. Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.

1.11.2 Segregación de los deberes

Control

Lasfunciones y áreas de responsabilidad deben estar segregadas para reducir las oportunidades de una modificación no-autorizada, uso no-intencional o mal uso de los activos de la organización.

1.11.3 Separación de los medios de desarrollo, prueba y operación

Control

Los medios de desarrollo, prueba y operación deben estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.

1.12 Gestión de la entrega del servicio de terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

1.12.1 Entrega del servicio

Control

Se debe asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.

1.12.2 Monitoreo y revisión de los servicios de terceros

Control

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y se deben llevar a cabo auditorías regularmente.

1.12.3 Manejo de cambios en los servicios de terceros

Control

Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos.

1.13 Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas en el sistema. Se requiere de planeación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido. Se deben realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

1.13.1 Gestión de la capacidad

Control

Se debe monitorear, afinar el uso de los recursos y se deben realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

1.13.2 Aceptación del sistema

Control

Se debe establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas y se deben realizar pruebas adecuadas del sistema(s) durante el desarrollo y antes de su aceptación.

1.14 Protección contra el código malicioso y móvil

Objetivo: Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

1.14.1 Controles contra códigos maliciosos

Control

Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se deben implementar procedimientos para el apropiado conocimiento del usuario.

1.14.2 Controles contra códigos móviles

Control

Donde se autorice el uso del código móvil, la configuración debe asegurar que el código móvil autorizado opera de acuerdo con una política de seguridad claramente definida, y se debe evitar la ejecución del código móvil no-autorizado.

1.15 Respaldo o Back-Up

Objetivo: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Control

Se deben hacer copias de respaldo de la información y software y se deben probar regularmente en concordancia con la política de copias de respaldo acordada.

1.16 Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

1.16.1 Controles de redes

Control

Las redes deben ser adecuadamente manejadas y controladas para poder proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

1.16.2 Seguridad de los servicios de la red

Control

En todo contrato de redes se deben identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

1.17 Gestión de medios

Objetivo: Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

1.17.1 Gestión de medios removibles

Deben existir procedimientos para la gestión de los medios removibles.

1.17.2 Procedimientos para el manejo de información

Control

Se deben establecer los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso.

1.17.3 Seguridad de la documentación del sistema

Control

Se debe proteger la documentación del sistema con accesos no-autorizados.

1.18 Intercambio de información

Objetivo: Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

1.18.1 Políticas y procedimientos de intercambio de información

Control

Se deben establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

1.18.2 Acuerdos de intercambio

Control

El acuerdo de intercambio debe considerar las siguientes condiciones de seguridad:

a) Manejo de las responsabilidades para el control y notificación de la transmisión, despacho y recepción.

b) Procedimientos para notificar al remitente de la transmisión, despacho y recepción.

c) Procedimientos para asegurar el rastreo y no-repudio.

1.18.3 Medios físicos en tránsito

Control

Los medios que contienen información deben ser protegidos contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.

1.18.4 Mensajes electrónicos

Control

Se debe proteger adecuadamente la información involucrada en mensajes electrónicos.

1.18.5 Sistemas de información comercial

Control

Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.

1.19 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

1.19.1 Comercio electrónico

Control

La información involucrada en el comercio electrónico que pasa a través de redes públicas debe protegerse de la actividad fraudulenta, disputas de contratos, divulgación no autorizada y modificación.

1.19.2 Transacciones en-línea

Control

Se debe proteger la información involucrada en las transacciones en-línea para evitar una transmisión incompleta, routing equivocado, alteración, divulgación, duplicación o repetición no-autorizada del mensaje.

1.19.3 Información públicamente disponible

Control

Se debe proteger la integridad de la información puesta a disposición en un sistema públicamente disponible para evitar una modificación no-autorizada.

1.20 Monitoreo

Objetivo: Detectar las actividades de procesamiento de información no autorizadas.

1.20.1 Registro de auditoría

Control

Se deben producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

1.20.2 Uso del sistema de monitoreo

Control

Se deben establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se deben revisar regularmente los resultados de las actividades de monitoreo.

1.20.3 Protección del registro de información

Control

Se deben proteger los medios de registro y la información del registro para evitar la alteración y el acceso no autorizado.

1.20.4 Registros del administrador y operador

Control

Se deben registrar las actividades del administrador del sistema y el operador del sistema.

1.20.5 Registro de fallas

Control

Se deben registrar y analizar las fallas, y se deben tomar las acciones necesarias.

1.20.6 Sincronización de relojes

Control

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se deben sincronizar con una fuente que proporcione la hora exacta acordada.

10.2 CONTROL DEL ACCESO

1.21 Requerimiento del negocio para el control del acceso

Objetivo: Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

1.21.1 Política de control del acceso

Control

Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

1.22 Gestión de acceso del usuario

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

1.22.1 Registro del usuario

Control

Debe existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.

1.22.2 Gestión de privilegios

Control

Se debe restringir y controlar la asignación y uso de privilegios.

1.22.3 Gestión de las claves secretas de los usuarios

Control

La asignación de claves secretas se debe controlar a través de un proceso de gestión formal.

1.22.4 Revisión de los derechos de acceso del usuario

Control

La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

1.23 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información, evitar el robo de información de los medios de procesamiento de la información. La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

1.23.1 Uso de claves secretas

Control

Se debe requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de claves secretas.

1.23.2 Equipo del usuario desatendido

Control

Los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada.

1.23.3 Política de escritorio y pantalla limpios

Control

Se debe adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

1.24 Control de acceso a la red

Objetivo: Evitar el acceso no autorizado a los servicios de la red. Se debe controlar el acceso a los servicios de redes internas y externas.

1.24.1 Política sobre el uso de los servicios de la red

Control

Los usuarios sólo deben tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

1.24.2 Autentificación del usuario para las conexiones externas

Control

Se deben utilizar métodos de autentificación apropiados para controlar el acceso de usuarios remotos.

1.24.3 Identificación del equipo en las redes

Control

La identificación automática del equipo se debe considerar como un medio para autenticarlas conexiones de ubicaciones y equipos específicos.

1.24.4 Protección del puerto de diagnóstico y configuración remoto

Control

Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

1.24.5 Segregación en redes

Control

Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.

1.24.6 Control de conexión a la red

Control

Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales.

1.24.7 Control de routing de la red

Control

Se deben implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales.

1.25 Control del acceso al sistema operativo

Objetivo: Evitar el acceso no autorizado a los sistemas operativos.

1.25.1 Procedimientos para un registro seguro

Control

El acceso a los sistemas operativos debe ser controlado mediante un procedimiento de registro seguro.

1.25.2 Identificación y autentificación del usuario

Control

Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debe escoger una técnica de autentificación adecuada para sustanciar la identidad de un usuario.

1.25.3 Sistema de gestión de claves secretas

Control

Los sistemas para el manejo de claves secretas deben ser interactivos y deben asegurar claves secretas adecuadas.

1.25.4 Uso de las utilidades del sistema

Control

Se debe restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.

1.25.5 Cierre de una sesión por inactividad

Control

Las sesiones inactivas deben ser cerradas después de un período de inactividad definido.

1.25.6 Limitación del tiempo de conexión

Control

Se deben utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo.

1.26 Control de acceso a la aplicación y la información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

1.26.1 Restricción del acceso a la información

Control

El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de control de acceso definida.

1.26.2 Aislar el sistema confidencial

Control

Los sistemas confidenciales deben tener un ambiente de cómputo dedicado (aislado).

1.27 Computación y tele-trabajo móvil

Objetivo: Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.

1.27.1 Computación y comunicaciones móviles

Control

Se debe establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.

1.27.2 Tele-trabajo

Control

Se debe desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de tele-trabajo.

10.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1.28 Requerimientos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.

1.28.1 Análisis y especificación de los requerimientos de seguridad

Control

Los enunciados de los requerimientos comerciales para los sistemas de información nuevos, o las mejoras a los sistemas de información existentes, deben especificar los requerimientos de los controles de seguridad.

1.29 Procesamiento correcto en las aplicaciones

Objetivo: Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

1.29.1 Validación de la input data

Control

Se debe validar la input data de las aplicaciones para asegurar que esta data sea correcta y apropiada.

1.29.2 Control del procesamiento interno

Control

Los chequeos de validación se deben incorporar en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

1.29.3 Integridad del mensaje

Control

Se debe identificar los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.

1.29.4 Validación de la output data

Control

Se debe validar la output data de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.

1.30 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.

1.30.1 Política sobre el uso de controles criptográficos

Control

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

1.30.2 Gestión de claves

Control

Se debe establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

1.31 Seguridad de los archivos del sistema

Objetivo: Garantizar la seguridad de los archivos del sistema.

1.31.1 Control del software operacional

Control

Se deben establecer procedimientos para el control de la instalación del software en los sistemas operacionales.

1.31.2 Protección de la data del sistema

Control

La data de prueba se debe seleccionar cuidadosamente, y se debe proteger y controlar.

1.31.3 Control de acceso al código fuente del programa

Control

Se debe restringir el acceso al código fuente del programa.

1.32 Seguridad en los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.

1.32.1 Procedimientos del control del cambio

Control

Se debe controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio.

1.32.2 Revisión técnica de la aplicación después de cambios en el sistema

Control

Cuando se cambian los sistemas de operación, se deben revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad.

1.32.3 Restricciones sobre los cambios en los paquetes de software

Control

No se deben fomentar modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser estrictamente controlados.

1.32.4 Filtración de información

Control

Se deben evitar las oportunidades para la filtración de información.

1.32.5 Desarrollo de software abastecido externamente

Control

El desarrollo del software abastecido externamente debe ser supervisado y monitoreado por la organización.

1.33 Gestión de la Vulnerabilidad Técnica

Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

1.33.1 Control de las vulnerabilidades técnicas

Control

Se debe obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados.

10.4 GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN

1.34 Reporte de los eventos y debilidades de la seguridad de la información

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

1.34.1 Reporte de eventos en la seguridad de la información

Control

Los eventos de seguridad de la información deben ser reportados a través de los canales gerenciales apropiados lo más rápidamente posible.

1.34.2 Reporte de las debilidades en la seguridad

Control

Se debe requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

1.35 Gestión de los incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

1.35.1 Responsabilidades y procedimientos

Control

Se deben establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.

1.35.2 Aprender de los incidentes en la seguridad de la información

Control

Se deben establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

1.35.3 Recolección de evidencia

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal); se debe recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

10.5 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1.36 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Objetivo: Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

1.36.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio

Control

Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

1.36.2 Continuidad del negocio y evaluación del riesgo

Control

Se deben identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

1.36.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

Control

Se deben desarrollar e implementar planes para mantener, restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos.

1.36.4 Marco Referencial de la planeación de la continuidad del negocio

Control

Se debe mantener un solo marco referencial de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, tratar consistentemente los requerimientos de seguridad de la información e identificar las prioridades para la prueba y el mantenimiento.

1.36.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio deben ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.

10.6 CUMPLIMIENTO

1.37 Cumplimiento de los requerimientos legales

Objetivo: Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

1.37.1 Identificación de la legislación aplicable

Control

Se debe definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

1.37.2 Derechos de propiedad intelectual (IPR)

Control

Se debieran implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

1.37.3 Protección de registros organizacionales

Control

Se debieran proteger los registros importantes de pérdida, destrucción, falsificación; en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

1.37.4 Protección de la data y privacidad de la información personal

Control

Se debiera asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

1.37.5 Prevención del mal uso de los medios de procesamiento de la información

Control

Se debiera disuadir a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

1.37.6 Regulación de controles criptográficos

Control

Los controles criptográficos se debieran utilizar en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes.

1.38 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

1.38.1 Cumplimiento con las políticas y estándares de seguridad

Control

Los gerentes debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

1.38.2 Chequeo del cumplimiento técnico

Control

Los sistemas de información debieran chequearse regularmente para ver el cumplimiento de los estándares de implementación de la seguridad.

1.39 Consideraciones de auditoría de los sistemas de información

Objetivo: Maximizar la efectividad y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

1.39.1 Controles de auditoría de los sistemas de información

Control

Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales debieran ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.

1.39.2 Protección de las herramientas de auditoría de los sistemas de información

Control

Se debiera proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o trasgresión posible.

11. ANEXO 2

11.1. TABLA DE CARACTERÍSTICAS Y/O RESPONSABLE POR ACTIVOS

- **DomainController**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Sist. Carlos Manosalvas
		Cargo:	Jefe de Ingeniería de Sistemas
Descripción:			
Es un servidor que se encarga de la seguridad de un dominio, es decir, administra toda la información correspondiente a usuarios y recursos de su dominio. Sirve para tareas tales como resolver las direcciones DNS, almacenar las carpetas de los usuarios, hacer copias de seguridad, almacenar software de uso común, etc.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-1: Características y/o Responsable del activo DomainController

- **Active Directory**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. César Martínez Yagual
		Cargo:	Jefe de Seguridad Informática
Descripción:			
Es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y administrar centralizadamente el acceso a los recursos de la red. Este proporciona la capacidad de establecer un único inicio de sesión y un repositorio central de información para toda su infraestructura.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-2: Características y/o Responsable del activo Active Directory

- **Exchange Server**

Ubicación:	Dpto. de Informática	**Responsable:**	Sr. Enrique Navas
		Cargo:	Asist. Ingeniería en Sistemas
Descripción:			
Servidor que permite crear un entorno más seguro, estable, escalable y con mayor capacidad de gestión. Permite el manejo de un buzón de usuario, accedido desde el Microsoft Office Outlook.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-3: Características y/o Responsable del activo Exchange Server

- **SMS**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. César Martínez Yagual
		Cargo:	Jefe de Seguridad Informática
Descripción:			
Este software instalado en un servidor es el que permite distribuir de forma fiable las actualizaciones, tanto de Microsoft como de aplicaciones de terceros.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-4: Características y/o Responsable del activo SMS

- **Dataprotector**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Máximo Andramuño
		Cargo:	Jefe de Producción
Descripción:			
Es un software de gestión de backups que soporta copias de seguridad tanto a disco como a cinta. Está diseñado para simplificar las tareas de backups y recuperación de datos reduciendo los tiempos de realización a la menor ventana posible.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5" TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5" TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5.			

Tabla 11-5: Características y/o Responsable del activo Dataprotector

- **Isa Server**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Juan Carlos Vizñhay
		Cargo:	Supervisor de Desarrollo
Descripción:			
Es el Gateway integrado de seguridad perimetral que permite proteger su entorno de Tecnologías Informática (TI) frente a las amenazas de Internet, además de proporcionar a los usuarios un acceso remoto seguro a las aplicaciones y datos corporativos.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-6: Características y/o Responsable del activo Isa Server

- **HelpDesk**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Néstor Macías
		Cargo:	Jefe de Soporte
Descripción:			
Este software se adapta a las necesidades de la entidad, y permite resolver cualquier tipo de problema de forma ordenada, rápida y eficiente, además ayuda a organizar y controlar los activos logrando una mayor productividad corporativa con la consecuente reducción de costos de soporte. Permite a los usuarios internos (empleados) y externos (clientes) ser los beneficiarios de la aplicación al conseguir una eficaz solución real de los problemas a tiempo, llevando registros, reasignaciones y seguimientos del usuario reportado hasta la satisfactoria solución del problema.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 4 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO			

Tabla 11-7: Características y/o Responsable del activo HelpDesk

- **Sharepoint**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Diana Pisco
		Cargo:	Asist. de Ingeniería en Sistemas
Descripción:			
Es la plataforma de colaboración empresarial que le permite incrementar la productividad y administrar los contenidos a través de la conocida interfaz de Office. Conecta perfectamente usuarios, equipos y conocimiento para que las personas puedan aprovechar la ventaja de compartir información relevante que les permita trabajar de una forma más eficiente a través de los procesos empresariales.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-8: Características y/o Responsable del activo SharePoint

- **Ultimus – Desarrollo**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Diana Pisco
		Cargo:	Asist. de Ingeniería en Sistemas
Descripción:			
Es una aplicación de software empresarial completa diseñada para crear un ambiente operacional que ayuda a las personas de una organización a manejar la automatización y el mejoramiento de sus procesos y supervisa la ejecución de los mismos.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO			

Tabla 11-9: Características y/o Responsable del activo Ultimus-Desarrollo

- **Ultimus – Producción**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Diana Pisco
		Cargo:	Asist. de Ingeniería en Sistemas
Descripción:			
Es una aplicación de software empresarial completa diseñada para crear un ambiente operacional que ayuda a las personas de una organización a manejar la automatización y el mejoramiento de sus procesos y supervisa la ejecución de los mismos.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5.			

Tabla 11-10: Características y/o Responsable del activo Ultimus-Producción

- **ON – BASE**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Bernardo Íñiguez
		Cargo:	Administrador de Base de Datos
Descripción:			
Es una solución de administración de contenido ECM (Gestión de contenido empresarial) que combina el gerenciamiento integrado de documentos, la automatización de procesos empresariales y el registro de acciones en una sola aplicación. Permite automatizar procesos de negocios, reducir el tiempo y el costo de efectuar funciones de negocios importantes y mejorar la eficiencia organizacional. Una de las grandes ventajas es que facilita el intercambio de documentos e información en una interface intuitiva y simple con empleados, socios de negocio y clientes.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO			

Tabla 11-11: Características y/o Responsable del activo Ultimus-Producción

- **Aplicaciones – Desarrollo – Visual.Net**

Ubicación:	Dpto. de Informática	**Responsable:**	Lsi. Elena Hurtado
		Cargo:	Jefe de Desarrollo
Descripción:			
Sistema en etapa de desarrollo a cargo del departamento de Informática.			
Características			
▪ PROCESADOR DE 600 MHZ ▪ MEMORIA RAM 256 MB ▪ SISTEMA OPERATIVO WINDOWS 7 o SISTEMA OPERATIVO WINDOWS XP PROFESSIONAL ▪ DISCO DURO DE 1TB			

Tabla 11-12: Características y/o Responsable Aplicaciones – Desarrollo - Visual .Net

- **Aplicaciones – Testing – Visual.Net**

Ubicación:	Dpto. de Informática	**Responsable:**	Lsi. Alicia Rosero
		Cargo:	Supervisora de Desarrollo
Descripción:			
Sistema implementado en el nivel de Testing de la M.I. Municipalidad de Guayaquil.			
Características			
▪ PROCESADOR DE 600 MHZ ▪ MEMORIA RAM 256 MB ▪ SISTEMA OPERATIVO WINDOWS 7 o SISTEMA OPERATIVO WINDOWS XP PROFESSIONAL ▪ DISCO DURO DE 1TB			

Tabla 11-13: Características y/o Responsable Aplicaciones-Testing-Visual.Net

- **Aplicaciones – Producción – Visual.Net**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. César Martínez Yagual
		Cargo:	Jefe de Seguridad Informática
Descripción:			
Sistema implementado en el nivel de producción del la M.I. Municipalidad de Guayaquil.			
Características			
▪ PROCESADOR DE 600 MHZ ▪ MEMORIA RAM 256 MB ▪ SISTEMA OPERATIVO WINDOWS 7 o SISTEMA OPERATIVO WINDOWS XP PROFESSIONAL ▪ DISCO DURO DE 1TB			

Tabla 11-14: Características y/o Responsable Aplicaciones-Producción-Visual.Net

- **Base de Datos – Desarrollo – SQL**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Bernardo Iñiguez
		Cargo:	Administrador de Base de Datos
Descripción:			
Conjunto de datos utilizado en el ambiente de desarrollo de la M.I. Municipalidad de Guayaquil.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5.			

Tabla 11-15: Características y/o Responsable Base de Datos-Desarrollo-SQL

- **Base de Datos – Testing**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Henry Hernández
		Cargo:	Supervisor de Desarrollo
Descripción:			
Datos utilizados para el testing de los sistemas de la M.I. Municipalidad de Guayaquil.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5.			

Tabla 11-16: Características y/o Responsable Base de Datos-Testing

- **Base de Datos – Producción – SQL**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. César Martínez Yagual
		Cargo:	Jefe de Seguridad Informática
Descripción:			
Conjunto de datos SQL SEVER utilizado en el nivel de producción de la M.I. Municipalidad de Guayaquil			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-17: Características y/o Responsable Base de Datos-Producción-SQL

- **Base de Datos – Oracle – Desarrollo**

Ubicación:	Dpto. de Informática	**Responsable:**	Lsi. Elena Hurtado
		Cargo:	Jefe de Desarrollo
Descripción:			
Conjunto de datos utilizado en el ambiente de desarrollo de la M.I. Municipalidad de Guayaquil.			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-18: Características y/o Responsable Base de Datos-Oracle-Desarrollo

- **Base de Datos – Producción**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Bernardo Iñiguez
		Cargo:	Administrador de Base de Datos
Descripción:			
Conjunto de datos correspondiente a la producción de la M.I. Municipalidad de Guayaquil			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-19: Características y/o Responsable Base de Datos- Producción

- **Base de Datos – Terminal de Transferencia de Víveres**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. Bernardo Iñiguez
		Cargo:	Administrador de Base de Datos
Descripción:			
Conjunto de datos correspondiente a la terminal de Transferencia de Víveres			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 8GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB ▪ UNIDAD DE DVD-ROM ▪ CONTROLADOR INTELIGENTE PARA ARREGLO DE DISCOS QUE PERMITA MÍNIMO RAID0, RAID1 Y RAID5 ▪ CAPACIDAD MÍNIMA EN DISCOS DUROS: 8 DISCOS ▪ 2 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 72GB 15000RPM CADA UNO CONFIGURADOS EN RAID1, PARA INSTALACIÓN DE SISTEMA OPERATIVO ▪ 6 DISCOS DUROS 2.5” TIPO HOT PLUG TECNOLOGÍA SAS DE 146GB 10000RPM CADA UNO CONFIGURADOS EN RAID5. ▪ 2 TARJETAS DE RED GIGABIT ETHERNET ▪ VENTILADORES Y FUENTE DE PODER REDUNDANTES			

Tabla 11-20: Características y/o Responsable Base de Datos-Terminal de Transferencia de Víveres

- **Claves de usuarios**

Ubicación:	Dpto. de Informática	**Responsable:**	Ing. César Martínez Yagual
		Cargo:	Jefe de Seguridad Informática
Descripción:			
La clave de acceso es la contraseña que un usuario emplea para acceder a un servicio, sistema o programa			
Características			
▪ PROCESADOR INTEL XEON QUAD CORE E5440 DE 2.83GHz ▪ FSB DE 1333MHz ▪ MEMORIA CACHÉ L2 2x6MB ▪ MEMORIA RAM 4GB, DIMM PC2-5300, EXPANDIBLE HASTA 64GB			

Tabla 11-21: Características y/o Responsable del Activo Clave de Usuarios

12. ANEXO 3

12.1. REGLAMENTO DE SEGURIDAD INFORMÁTICA DE LA DIRECCIÓN DE INFORMÁTICA

CAPÍTULO I
GENERALIDADES

Art. 1. **Ámbito de Aplicación**.- La aplicación del presente reglamento lo efectuará todo el personal de la Dirección de Informática de la Muy Ilustre Municipalidad de Guayaquil.

Art. 2. **Alcance.**- Regular el control de acceso a la Dirección de Informática, el manejo y mantenimiento de equipos de computación; así como, preservar la información de la Muy Ilustre Municipalidad de Guayaquil.

Se considerará "equipos de computación" a los computadores (servidores), microcomputadores independientes (stand alone) y, o conectados a otros equipos vía red.

Art. 3. **Actualización.**- Es responsabilidad de la Dirección de Informática revisar y sugerir la actualización del presente reglamento, según las necesidades que se presenten a futuro, para lo cual contará con el apoyo de la Dirección de Organización y Métodos.

CAPÍTULO II
DE LAS SEGURIDADES FÍSICAS

Art. 4. **De los accesos permitidos a la Dirección de Informática**.- El guardia de seguridad que se encuentra en la puerta de acceso de la Dirección de Informática, anotará el nombre de la persona y unidad administrativa o empresa a la que pertenece, en una bitácora indicando fecha, hora de entrada y salida de la Dirección y las novedades si las hubiere.

Para efectuar la limpieza d las instalaciones de la Dirección, deberá encontrarse al momento de realizar esta actividad, una persona que será designada por el Director de Informática, quien de existir cualquier novedad la reportará en forma inmediata.

El acceso a la Dirección de Informática estará vigilado las 24 horas del día, por medio de la instalación de un circuito cerrado de televisión que permita controlar el ingreso y desplazamientos internos de las personas que se encuentren en la Dirección.

El acceso a la Dirección de Informática antes de las 8h30 y luego de las 16h30, así como los días sábados, domingos y días feriados, será totalmente restringido, exceptuándose el ingreso de personal que por efecto de su horario rotativo, deba cumplir funciones normales de labor o aquellas que cuenten con la autorización del Director o su delegado, siempre que en dicha autorización se indique con claridad las actividades extraordinarias a ejecutar.

Art. 5. **Del control en el acceso a las instalaciones del Centro de Cómputo**.- Se restringe el acceso a la sala donde se encuentran los servidores que manejan o administran los sistemas automatizados; únicamente podrá ingresar el personal que cuente con la autorización del Director de Informática.

Art. 6**. De las normas de seguridad que deben existir en el Centro de Cómputo**.- El Director de Informática, el Jefe de Seguridad e Higiene Industrial y un delegado de Auditoría Interna coordinarán acciones para mantener actualizada y en aplicación las normas física, tanto de equipo como de personal.

Art. 7. **De la entrega – recepción de bienes y correspondencia**.- La recepción de correspondencia y de bienes se la realizará en el hall de ingreso de la Dirección de Informática, para lo cual el guardia de seguridad deberá tomar las previsiones del caso.

Art. 8. **De las prohibiciones**.- Será responsabilidad de cada uno de los funcionarios de la Dirección de Informática, no permitir que personal ajeno haga uso de sus estaciones de trabajo sin la debida autorización del Director del área, excepto cuando se realicen operativos en conjunto.

Art. 9. **De la permanencia en las instalaciones en días no laborables, fines de semana y noches.-** La permanencia del personal en las instalaciones de la Dirección de Informática será con la debida autorización del Director del Área.

CAPÍTULO III
SEGURIDAD LÓGICA

Art. 10. **Del control de herramientas lógicas de transferencia de archivos.-** A fin de evitar que personal no autorizado transfiera archivos de datos desde los computadores centrales, el Jefe de Seguridad Informática restringirá el uso de las herramientas de transferencias de datos que se encuentran en el sistema operativo.

Art. 11. **De la seguridad de información en ambiente de red.-** Toda la información interna de vital importancia procesada en los computadores que administran los sistemas automatizados, que estén respaldados en medios magnéticos (tapebackup), debe guardárselo bajo llave en cajas de seguridad o bóveda dentro de la Dirección de Informática, misma que estará bajo la custodia del Jefe de Seguridad.

La información almacenada en los servidores del Centro de Cómputo se deberá respaldar diariamente en las instalaciones municipales, y cada semana se guardará un respaldo en una bóveda habilitada para este efecto la cual estará fuera de las instalaciones municipales.

Art. 12. **Del acceso a servidores de Producción.-** Cuando el personal del Departamento de Desarrollo necesite acceder al servidor de Producción se deberá solicitar autorización al Director o su delegado, la misma que será realizada a través del sistema automatizado con el que se cuenta para tal efecto o del formulario correspondiente.

El Operador Stand By (de guardia) tendrá opción de utilizar las claves Stand By y Emergencia según la gravedad y/o prioridad del requerimiento, el cual deberá ser debidamente justificado.

Art. 13. **De la periodicidad de los respaldos.-** Los respaldos serán:

a. Diarios
b. Semanales
c. Mensuales

a.- Respaldos Diarios.- Se deberá respaldar diariamente toda la base de datos y aplicaciones necesarias para la recuperación en caso de fallas o pérdida de datos, para lo cual se utilizarán cintas magnéticas, las mismas que serán reusables (máximo 26 veces) y registradas en la hoja de registro de las cintas de respaldo.

b.- Respaldos Semanales.- Se deberá respaldar semanalmente la base de datos, aplicaciones y archivos log's necesarios para la recuperación en caso de fallas o pérdidas de datos, para lo cual se deberá utilizar cintas magnéticas nuevas no reusables, debidamente etiquetadas, y registradas en la hoja de registro de las cintas de respaldo.

c.- Respaldos Mensuales.- Se deberá respaldar mensualmente la base de datos, aplicaciones y archivos log's para la recuperación en caso de fallas o pérdida de datos, para lo cual se deberá utilizar cintas magnéticas nuevas no reusables, estableciéndose la generación de dos (2) copias por cada respaldo magnético de información efectuado, para una mayor seguridad, debidamente etiquetadas y registradas en la hoja de registro de las cintas de respaldo.

Dicha labor será responsabilidad del Operador y del Supervisor de Producción, además se utilizarán las cintas magnéticas hasta que exista un medio de mayor capacidad y seguridad, el cual remplazará al mismo.

Art. 14. **De las revisiones periódicas de información contenida en las cintas de respaldo.** Las revisiones deben hacerse durante la semana siguiente del respaldo semanal y el responsable será el Supervisor de Producción.

Art. 15. **De la baja a las cintas archivadas y cintas defectuosas.-** Se dará de baja en forma inmediata tanto a las cintas defectuosas como aquellas que tengan más de cinco años archivadas , dicha actividad será solicitada por el Jefe de Seguridad Informática y realizada bajo la supervisión de la Dirección de Auditoría Interna.

Art. 16.- **De la custodia de las cintas de respaldos.-** Las cintas que contienen la información respaldada por más de un año, deberán ser retiradas por el Supervisor de Producción de la bóveda habilitada para este efecto, la cual estará fuera de las instalaciones municipales y trasladadas a la Dirección de Informática para ser entregadas a través del acta respectiva al Jefe de Seguridad Informática para ser su custodio.

Art. 17. **Del Plan de Contingencia para recuperación de Información**. En caso de que sea necesario recuperar información de los respaldos, esta se tomará del último respaldo, utilizando para ellos los ARCHIVE LOG, EXPORT FILES, BASES DE DATOS, PROGRAMAS Y ARCHIVOS DEL SISTEMA OPERATIVO, los mismos que poseen información/datos momentos antes de producirse cualquier situación.

Art. 18. **De las modificaciones a los programas.-** Las modificaciones a los programas de un sistema automatizado que no signifiquen desarrollo de nuevos sistemas o subsistemas, pero que impliquen cambios a los procedimientos deberán ser comunicados de manera paralela al desarrollo de los mismos, a la Dirección de Organización y Métodos, por el Director de Informática para la actualización de éstos.

Art. 19. **Del Plan de Contingencia.-** La Dirección de Informática formulará un plan de contingencia que prevea las acciones a tomar de suspensión en el procesamiento automático de los datos por problemas con los equipos, programas o con el personal.

Art. 20. **Del registro de programas.-** Es responsabilidad del Jefe de Desarrollo de Sistemas llevar y actualizar el registro de los programas que constituyen propiedad de la Municipalidad, así como de sus modificaciones sustanciales y documentación de éstos.

Art. 21. **Del procesamiento de información en lugares remotos.-** Es responsabilidad de la Dirección de Informática diseñar e implementar un método que permita establecer un control al acceso de los datos que se procesa en lugares remotos, evitándose de esta manera que usuarios no autorizados modifiquen los datos que se almacenan en las bases de datos.

DISPOSICIÓN TRANSITORIA.- En relación al Art. 14, se deberá efectuar un Inventario físico general a fin de establecer el real estado de las cintas tanto las defectuosas como aquellas que tengan más de 5 años archivadas.