RESUMEN – TRABAJO DE GRADO

AUTORES	**MONICA MARLEY VERGEL TRIGOS** **ANA DILIA SEPULVEDA ARENAS**
FACULTAD	**INGENIERÍAS**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**WILMAR ALIRIO GONZALEZ PEINADO**
TÍTULO DE LA TESIS	**DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMATIVA APLICANDO LA NORMA ISO 27002 PARA LA ALCALDIA DEL MUNICIPIO DE LA PLAYA DE BELEN, NORTE DE SANTANDER**

RESUMEN
(70 PALABRAS APROXIMADAMENTE)

LA SEGURIDAD INFORMÁTICA ES UN TEMA AMPLIO QUE SE ENFOCA EN PODER ENTENDER QUE UN RIESGO Y UNA VULNERABILIDAD SE PODRÍAN ENGLOBAR EN UNA DEFINICIÓN MÁS INFORMAL QUE DENOTA LA DIFERENCIA ENTRE RIESGO Y VULNERABILIDAD. A CONTINUACIÓN SE PROPONE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, PARA LA ALCALDÍA DE LA PLAYA DE BELÉN, TENIENDO EN CUENTA QUE EN LA ACTUALIDAD, NO SE TIENE CONTROL DE ACCESO A LA INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 155	PLANOS:	ILUSTRACIONES: 24	CD-ROM: 1

DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO 27002 PARA LA ALCALDÍA DEL MUNICIPIO DE LA PLAYA DE BELÉN, NORTE DE SANTANDER

MONICA MARLEY VERGEL TRIGOS
ANA DILIA SEPÚLVEDA ARENAS

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO 27002 PARA LA ALCALDÍA DEL MUNICIPIO DE LA PLAYA DE BELÉN, NORTE DE SANTANDER

MONICA MARLEY VERGEL TRIGOS
ANA DILIA SEPÚLVEDA ARENAS

Proyecto de grado presentado como requisito para optar al título de Ingeniero de Sistemas

Director
WILMAR ALIRIO GONZÁLEZ PEINADO
Magíster en Software Libre

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2015

CONTENIDO

LISTA DE GRÁFICAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El trabajo que se muestra a continuación, titulado: diseño de un manual de políticas de seguridad informática aplicando la norma ISO 27002 para la Alcaldía del municipio de La Playa de Belén, Norte de Santander, se encuentra dividido en seis capítulos, siendo el primero la propuesta del mismo, en el segundo se encuentran los marcos histórico, teórico, conceptual y legal. En el tercero se encuentra la metodología utilizada para el desarrollo del trabajo. El cuarto capítulo es el desarrollo de los objetivos, en donde encontramos los resultados arrojados por los mismos, siendo el tema principal el manual de políticas diseñado para la Alcaldía del municipio de La Playa de Belén. El quinto y sexto capítulo son las conclusiones y recomendaciones, respectivamente.

Los resultados obtenidos fueron satisfactorios, ya que se dio cumplimiento a los objetivos propuestos, realizando un reconocimiento de la Alcaldía Municipal de La Playa de Belén, las áreas que la conforman y los procesos informáticos que allí se manejan, conociéndose algunas falencias que se encuentran en su parte interna, lo cual arrojó una serie de factores de riesgos, para lo cual se realizó un informe de los hallazgos encontrados. Teniendo en cuenta todo esto, se vio la necesidad de la propuesta de un manual de políticas de seguridad de la información, el cual se diseñó dejándolo a consideración de la entidad para su implementación.

INTRODUCCIÓN

La propuesta de un manual de políticas de seguridad informática, para la Alcaldía del municipio de La Playa de Belén, basado en la ISO 27002; es el objetivo principal del presente trabajo, toda vez que, en la actualidad, la Alcaldía municipal de La Playa de Belén, no cuenta con políticas de seguridad informática, ya que el acceso a todas sus áreas físicas, lo puede realizar cualquier personal de la misma y en muchas de las ocasiones, personas particulares; ya que no cuenta con una herramienta que pueda controlar su ingreso o políticas de seguridad normadas que prohíba el acceso al departamento y a servidores de datos o información. Además, la Alcaldía, como toda institución maneja gran cantidad de información confidencial. En algunas oportunidades, no se tiene la certeza del grado de seguridad que manejan los sistemas informáticos, lo que puede generar una mala imagen institucional, dado al retraso que se presenta en los informes que deben presentarse al gobierno nacional, dejando en ocasiones paralizadas sus actividades. El personal que trabaja en el área de informática está consciente del riesgo que conlleva no tener políticas de seguridad, y han venido trabajando con una seguridad relativamente aprendida en sus estudios universitarios y del conocimiento aprendido de otras empresas por lo que es recomendable la aplicación de un manual de políticas de seguridad en la Alcaldía Municipal de La Playa de Belén.

Pero, ¿el diseño de un manual de políticas de seguridad informática de la Alcaldía del municipio de La Playa de Belén, constituirá un instrumento que le facilite a ésta, la protección, conservación y buen uso de la información y los recursos tecnológicos?

La seguridad de la información y el estudio de amenazas de riesgos de la información proporcionan ventajas para implantar procedimientos, métodos y controles con el objeto de administrar, proteger y salvaguardar uno de los activos más importantes, como es la información. También repercute en el uso de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir eficientemente con sus actividades. Una política de seguridad de la información es una forma de comunicarse con los usuarios, pues las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la Institución.

El trabajo brindará orientación y recomendaciones acerca de cómo mejorar los procesos para proteger la información. Dicha herramienta debe presentar la información de una manera sencilla y entendible para el usuario; además debe ser de fácil distribución, con el propósito de que llegue a más personas, pero principalmente a los alumnos interesados de la Facultad de Ingeniería de Sistemas de la Universidad Francisco de Paula Santander Ocaña, interesados en temas como la seguridad Informática.

1. DISEÑO DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO 27002 PARA LA ALCALDÍA DEL MUNICIPIO DE LA PLAYA DE BELÉN, NORTE DE SANTANDER

1.1 PLANTEAMIENTO DEL PROBLEMA

La seguridad informática es un tema muy amplio que se enfoca en poder entender que un riesgo y una vulnerabilidad se podrían englobar en una definición más informal que denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad a una Amenaza y el Riesgo a un Impacto. La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. Una persona no autorizada podría: Clasificar y desclasificar los datos, Filtrar información, Alterar la información, Borrar la información, Usurpar datos, Hojear información clasificada.[1]

Es por ello que la sociedad de la información es importante para todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablamos de empresas altamente automatizados por lo que su seguridad sigue siendo un punto pendiente en las empresas, basta con mirar sus actividades para darnos cuenta que la seguridad es el factor más determinante por el cual fracasan las organizaciones. Caso como éstos, es el de la Alcaldía de La Playa de Belén, la cual no ha tenido en cuenta la importancia de mantener segura la información en la entidad para prevenir el peligro de comprometer sus operaciones, las cuales son en una buena cantidad, ya que incluye lo que tiene que ver con su parte interna (empleados) y la externa (municipio); además de no analizar las vulnerabilidades a los que está expuesta la información y que afectan a su funcionamiento normal y el impacto que puede conllevar los incidentes de seguridad.

En la actualidad la Alcaldía municipal de La Playa de Belén, no cuenta con políticas de seguridad informática, ya que el acceso a todas sus áreas físicas, lo puede realizar cualquier personal de la misma y en muchas de las ocasiones, personas particulares; ya que no cuenta con una herramienta que pueda controlar su ingreso o políticas de seguridad normadas que prohíba el acceso al departamento y a servidores de datos o información. Además, la Alcaldía, como toda institución maneja gran cantidad de información confidencial. En algunas oportunidades, no se tiene la certeza del grado de seguridad que manejan los sistemas informáticos, lo que puede generar una mala imagen institucional, dado al retraso que se presenta en los informes que deben presentarse al gobierno nacional, dejando en ocasiones paralizadas sus actividades.

El personal que trabaja en el área de informática está consciente del riesgo que conlleva no tener políticas de seguridad, y han venido trabajando con una seguridad relativamente

[1] UNEMI. Seguridad informática (online). 1 ed. [Ecuador]: Repositorio, 2012 [citado 26 ago., 2014]. Disponible en: http://hdl.handle.net/123456789/1251

aprendida en sus estudios universitarios y del conocimiento aprendido de otras empresas por lo que es recomendable la aplicación de un manual de políticas de seguridad en la Alcaldía Municipal de La Playa de Belén.

1.2 FORMULACIÓN DEL PROBLEMA

¿El diseño de un manual de políticas de seguridad informática de la Alcaldía del municipio de La Playa de Belén, constituirá un instrumento que le facilite a ésta, la protección, conservación y buen uso de la información y los recursos tecnológicos?

1.3 OBJETIVOS

1.3.1 Objetivo general. Diseñar un manual de políticas de seguridad informática, aplicando la norma ISO 27002, para la Alcaldía del municipio de La Playa de Belén, Norte de Santander.

1.3.2 Objetivos específicos. Realizar un diagnóstico para conocer la situación actual relacionada con los distintos procesos informáticos realizados en la Alcaldía Municipal de La Playa de Belén.

Identificar los elementos de riesgos y fallas de seguridad informática, encontrados en la Alcaldía

Elaborar un informe de acuerdo a los hallazgos encontrados en la Alcaldía Municipal de La Playa de Belén, según la norma ISO 27002

Proponer un manual de políticas de seguridad informática para la Alcaldía municipal de La Playa de Belén

1.4 JUSTIFICACIÓN

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas informáticas disponibles, buscando proteger los datos, de la aparición de nuevas amenazas en los sistemas informáticos. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan.

La integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla en la integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.[2] De esta manera, las políticas de seguridad

[2] CUEVAS MARTINEZ, R. Puntos a cuidar en la información (online). 1 ed. [ ]: 2011. [citado 23 ago., 2014]. Disponible en: contenidosabiertos.academica.mx/jspui/.../puntos.a.cuidar.informacion.p...

informática surgen como una herramienta para concienciar, a la Alcaldía municipal de La Playa de Belén, sobre la importancia en aplicar controles de seguridad para proteger información sensible y/o servicios críticos, que permiten al municipio desarrollarse eficientemente en el sector de la educación, evitando de esta manera retrasos en los envíos de información a otras entidades públicas o privadas que lo requieran, a la vez de cumplir con las actividades sin tener inconvenientes que lleven a la paralización de las mismas. La ISO 27002 es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información.

Es por lo anterior que se plantea el diseño de las políticas de seguridad de la información basada en la ISO 27002, para la Alcaldía Municipal de La Playa de Belén, ya que la seguridad de la información y el estudio de amenazas de riesgos de la información proporcionan ventajas para implantar procedimientos, métodos y controles con el objeto de administrar, proteger y salvaguardar uno de los activos más importantes, como es la información. También repercute en el uso de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir eficientemente con sus actividades. Una política de seguridad de la información es una forma de comunicarse con los usuarios, pues las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la Institución.

1.5 DELIMITACIONES

1.5.1 Conceptual. La articulación del proyecto requiere de la aplicación teórica en aspectos relacionados con: Seguridad de la Información, políticas de seguridad, riesgos y amenazas en la información.

1.5.2 Operativa. El incumplimiento de los objetivos del presente trabajo, puede darse por factores ajenos a las autoras; sin embargo, en caso de presentarse inconvenientes, se buscará la asesoría a través del director del trabajo de grado.

1.5.3 Temporal. Se determina que el proyecto para su realización tenga una duración de ocho (8) semanas, de acuerdo con el cronograma de actividades que se incorpora al estudio.

1.5.4 Geográfica. La propuesta tendrá su desarrollo en el municipio de La Playa de Belén, Norte de Santander.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

2.1.1 Historia de las políticas de seguridad informática a nivel internacional. Sin dudas uno de los pioneros en el tema fue James P. Anderson, quien allá por 1980 y a pedido de un ente gubernamental produjo uno de los primeros escritos relacionados con el tema, Computer Security Threat Monitoring and Surveillance, describe ahí la importancia del comportamiento enfocado hacia la seguridad en materia de informática; y es allí donde se sientan también las bases de palabras que hoy suenan como naturales, pero que por aquella época parecían ciencia ficción.[3]

En ese documento se encuentran los primeros atisbos de definiciones casi proféticas:

Amenaza: la posibilidad de un intento deliberado y no autorizado de:

Acceder a información
Manipular información
Convertir un sistema en no-confiable o inutilizable

Riesgo: Exposición accidental e impredecible de información, o violación de la integridad de operaciones debido al malfuncionamiento de hardware o diseño incorrecto o incompleto de software.

Vulnerabilidad: una falla conocida o su sospecha tanto en hardware como en el diseño de software, o la operación de un sistema que se expone a la penetración de su información con exposición accidental.

Ataque: Una formulación especifica o ejecución de un plan para levar a cabo una amenaza.

Penetración: Un ataque exitoso; la habilidad de obtener acceso no-autorizado (indetectable) a archivos y programas o el control de un sistema computarizado."

Estas definiciones fueron vistas y planteadas en 1980.

La definición de Vulnerabilidad fue tan acertada por aquella época que hoy en día se derivan extensiones donde entre otras cosas se determina que una vulnerabilidad no conocida por nadie no tiene la entidad de tal ya que es inexplotable hasta tanto sea descubierta.

De lo que podemos inferir que el descubrimiento de la vulnerabilidad la convierte en tal.

[3] SEGURIDAD INFORMÁTICA. Historia de seguridad informática (online). 1 ed. [s.l.]: Informaticadomonline, 2012 [citado 20 ago., 2014]. Disponible en: http://informaticadomonline.designcloud24.com/seguridad-informatica/

James dejo el asunto difuso al incorporar la palabra "sospecha".[4]

Sin dudas este documento formara parte de la historia de la informática.

2.1.2 Historia del municipio de La Playa de Belén.[5] En el paraje de Llano Alto, donde construyó la primera casa doña María Claro de Sanguino, se inició en 1857 la fundación del municipio de La Playa de Belén. En este año, con motivo de la visita pastoral del obispo dominico Fray Bernabé Rojas al sitio de "Patatoque", los señores Jesús Rueda, Tiburcio Alvarez y Juan Esteban Vega, obtuvieron licencia del prelado para construir una capilla dedicada a San José.

No se ha establecido en qué época de aquel año pasó el obispo Rojas por Patatoque; su visita a la provincia de Ocaña, iniciada en el mes de enero, se prolongó hasta finales octubre. No puedo, entonces, hablar de una fecha exacta del nacimiento del terruño.

Debo agregar que 1857 fue un año de inestabilidad en la organización política territorial y que, por esta circunstancia, La Playa de Belén fue arrullada en sus primeros meses en las provincias de Ocaña y Mompox, y en el Estado de Santander.

El 4 de diciembre de 1862, el reverendo padre misionero Fray Milán bendijo la capilla, dedicada a San José. Don Justiniano J. Páez, en sus "Noticias históricas de la ciudad y provincia de Ocaña", dice que en este acto solemne se le dio al caserío el nombre de La Playa de Belén. El notable historiador, seguramente, acudió a la tradición porque no cita las fuentes de sus apuntes. Los playeros guardamos el mayor respeto por su versión y la hemos difundido.

La señora María Claro de Sanguino construyó la primera casa en 1857, razón por la cual se considera que ella y los señores Vega, Álvarez y Rueda fueron los primeros pobladores o fundadores.

Alrededor del modesto templo creció el pueblo, en el paraje conocido como Llano Alto, donde actualmente se encuentra la cabecera municipal.

En los archivos notariales se observa que la denominación, hasta 1913, fue La Playa. Registros históricos del señor Páez señalan que en 1818 el lugar se conocía como Playa, y en 1822 se denominaba La Playa.

El nombre actual se asignó al caserío por medio del Acuerdo No. 3, del 15 de septiembre de 1913, del Concejo de Aspasica, cuyo artículo primero dice: "Erígese en Corregimiento con

[4] Ibid., p.3.
[5] ALCALDIA LA PLAYA DE BELEN. Historia de la Playa de Belén (online). 2 rev. [La Playa-Colombia]: 2010 [citado 01 sep., 2014]. Disponible en: www.laplayadebelen-nortedesantander.gov.co/

el nombre de La Playa de Belén el territorio del caserío de La Playa de este Municipio".

Playa, La Playa o La Playa de Belén, son denominaciones ancestrales, por las características del suelo, similares a la ribera del mar o de río grande. En mi infancia acudíamos a los arenales de El Playón (la quebrada que serpentea de norte a sur, cuyo nombre es aumentativo de playa) y a otros lugares, aledaños a la cabecera, a jugar a los toros.[6]

2.2 MARCO TEÓRICO

Hablar de evolución de seguridad es complejo, desde el inicio de la vida en comunidad, existían acciones para evitar amenazas, proteger la vida y las posesiones, allí se usaban métodos defensivos y se manejaban conceptos de alertar, evitar, detectar, alarmar y reaccionar a los diferentes hechos que podían suceder.

La familia, posteriormente diseñó esquemas de protección y se crearon lugares para resguardarse.

Algunos descubrimientos arqueológicos denotan con evidencias la importancia de la seguridad para los antiguas generaciones, entre estos tenemos las pirámides egipcias, el palacio de Sargon, el Dios egipcio Anubis, los Sumaricos, el Código de Hammurabi, entre otros.

Hasta se dice que Julio César utilizaba esquemas de seguridad en época de guerra y en el gobierno.

La seguridad moderna se originó con la revolución industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero de la administración Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y traiciones por parte del personal, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio."[7]

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese los equipos, ni siquiera el empleado. Con la aparición de las computadoras, esta mentalidad se mantuvo, porque ¿Quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

---

[6] Ibid., p.3.

[7] ZAMORA, Franyeidis. Seguridad informática (online) 1 ed. [s.l.]: Acantelys, 2009 [citado 1 nov., 2014]. Disponible en: http://cip.org.pe/imagenes/temp/tesis/40342005.pdf

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera.

Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

La NTC-ISO/IEC 27002, proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios: Política de Seguridad de la Información, Organización de la Seguridad de la Información, Gestión de Activos de Información, Seguridad de los Recursos Humanos, Seguridad Física y Ambiental, Gestión de las Comunicaciones y Operaciones, Control de Accesos, Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, Gestión de Incidentes en la Seguridad de la Información, Gestión de Continuidad del Negocio y Cumplimiento.[8]

2.3 MARCO CONCEPTUAL

2.3.1 Seguridad informática. [9] Para llegar a una correcta definición de seguridad informática se debe conocer primero los conceptos de informática y seguridad respectivamente:

2.3.1.1 Definición de seguridad. La definición de seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, las sociedades actuales son sociedades de riesgo. El componente riesgo es permanente y da carácter propio de los estados y sociedades nacionales, como tal la seguridad no puede ser entendida como ausencia de amenazas.

2.3.1.2 Definición de informática. La informática surge en la preocupación del ser humano por encontrar maneras de realizar operaciones matemáticas de forma cada vez más rápida y fácilmente. Pronto se vio que con ayuda de aparatos y máquinas las operaciones podían realizarse de forma más eficiente, rápida y automática.

---

[8] ISO 27002.es. Norma ISO 27002 (online). [España]: UNAD, 2012 [citado 26 ago., 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf

[9] OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

Según la definición de la Real Academia Española, la palabra informática significa "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

2.3.1.3 Definición de seguridad informática. La definición de seguridad informática proviene entonces de los dos términos antes definidos.

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados.

Objetivo de la seguridad informática. La seguridad informática tiene como principal objetivo proteger el activo más importante que tiene la empresa que es su información de los riesgos a los que está expuesta.

Para que la información sea considerada confiable para la organización ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

Confidencialidad. Se define como la capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados.

Integridad. Se define como la capacidad de garantizar que una información o mensaje no han sido manipulados.

Disponibilidad. Se define como la capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial.[10]

2.3.2 Riesgos. Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños"

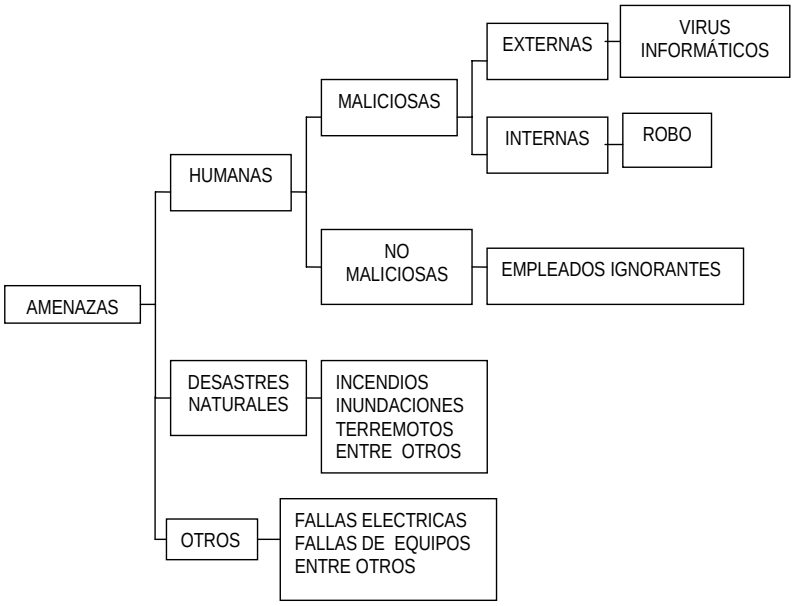
A raíz de esta definición podemos concluir que cualquier problema que afecte al total

[10] Ibid., p.3.

funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad.[11]

2.3.2.1 Tipos de amenazas a la seguridad. Ninguna empresa está exenta de sufrir amenazas a su seguridad, estas amenazas a las que son vulnerables las organizaciones son expuestas en la siguiente figura 1.

Figura 1. Tipos de Amenazas



Fuente: LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadoras, 2a Edición, Universidad de Jaen, Septiembre 1999. p.120.

Amenazas humanas. Las amenazas humanas como su nombre lo indica son aquellas acciones provocadas por el hombre y pueden ser de dos tipos maliciosas y no maliciosas

Maliciosas. Las amenazas maliciosas son aquellas que se llevan a efecto con el propósito de causar daño a la organización.

Las amenazas externas que pueden afectar al desarrollo y buen funcionamiento de las actividades de las empresas son frecuentemente originadas por el acceso a internet, ya que en esta red existen una serie de peligros como son los virus, hackers, entre otros que infiltrándose en la red interna de la organización provocando daños como mal funcionamiento de los sistemas y pérdida de información.

[11] LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadoras, 2a Edición, Universidad de Jaen, Septiembre 1999. p.120.

Las amenazas internas más frecuentes son las originadas por los propios funcionarios y ex - funcionarios de la organización motivados por la falta de dinero o represalia por algún tipo de enfrentamiento que hayan tenido con un superior.

No maliciosas. Este tipo de amenazas son producidas en la mayoría de los casos por errores ocasionados por empleados que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas.[12]
Amenazas por desastres naturales. Estas amenazas originadas por la naturaleza son las menos frecuentes en las organizaciones pero aún así no podemos dejar de considerarlas.

Otras amenazas son aquellas referentes a las que están fuera del alcance del hombre como son las interrupciones eléctricas, fallas de equipos originadas por los cortes de energía o no mantenerlos en el ambiente adecuado aunque esta es una responsabilidad más bien de carácter humano; entre otros.

¿Cómo enfrentar los riesgos? Los problemas de seguridad se multiplican con gran facilidad, por lo que las empresas deben perfeccionar los sistemas y los procesos para evitar amenazas o abordarlas cuando se produzcan. Para garantizar que la información de nuestra organización posea las características de seguridad ya mencionadas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad informática.[13]

2.3.3 Plan estratégico de seguridad informática. Un plan estratégico de seguridad informática está basado en un conjunto de políticas de seguridad elaboradas previo a una evaluación de los riesgos que indicará el nivel de seguridad en el que se encuentre la empresa. Estas políticas deben ser elaboradas considerando las características del negocio, la organización, su ubicación, sus activos y tecnología que posee la empresa.

2.3.4 Evaluación de los riesgos. La evaluación de los riesgos es el proceso por el cual se identifican las vulnerabilidades de la seguridad.

Por tanto el objetivo general de evaluar los riesgos será identificar las causas de los riesgos potenciales, en toda la organización, a parte de ella o a los sistemas de información individuales, a componentes específicos de sistemas o servicios donde sea factible y cuantificarlos para que la Gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos, en los diferentes puntos de análisis.[14]

Los pasos para realizar una valoración de riesgos se detallan a continuación:

---

[12] Ibid., p.132.
[13] Ibid., p.138.
[14] ECHENIQUE GARCÍA, José Antonio. Auditoria en Informática, 2a Edición. Mc Graw Hill. p.145.

Identificar los riesgos
Análisis de los riesgos

Identificar riesgos. En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático, existen formas de identificarlos como:

Cuestionarios de análisis de riesgos: La herramienta clave en la identificación de riesgos son los cuestionarios los mismos que están diseñados para guiar al administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en algunas instancias, este instrumento está diseñado para incluir riesgos asegurables e in-asegurables. El cuestionario de análisis de riesgos está diseñado para servir como un repositorio de la información acumulada de documentos, entrevistas e inspecciones. Su propósito es guiar a la persona que intenta identificar exposiciones a riesgo a través del proceso de la identificación en un modelo lógico y consistente.

Listas de chequeo de exposiciones a riesgo: Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.

Listas de chequeo de políticas de seguridad: Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar. El administrador de riesgos consulta las políticas recolectadas y aplicadas a la firma.

Sistemas expertos: Un sistema experto usado en la administración de riesgos incorpora los aspectos de las herramientas descritas anteriormente en una sola herramienta. La naturaleza integrada del programa permite al usuario generar propósitos escritos y prospectos.

Análisis de riesgos. Una vez se hayan identificado los riesgos, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

Ponderación de los Factores de riesgo. Ponderar el factor de riesgo es darle un valor de importancia en términos porcentuales al mismo bajo los criterios de especialistas en el área infor
mática que pueden identificar su impacto en la organización, teniendo en cuenta las posibilidades de que se puedan convertir en realidad.

Valoración del riesgo. La valoración del riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de las prioridades.[15]

[15] Ibid., p.146.

Cuadro 1. Valoración del riesgo

Cuadrante	Valoración del riesgo
Impacto significante y probabilidad Alta	Alto
Impacto significante y probabilidad Baja	Medio-alto
Impacto insignificante y probabilidad Al ta	Medio-bajo
Impacto insignificante y probabilidad B aja	Bajo

Fuente: ECHENIQUE GARCÍA, José Antonio. Auditoria en Informática, 2a Edición. Mc Graw Hill. p.148.

Una explicación más clara de la valoración es la siguiente:
Riesgo alto: Todos las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.

Riesgo medio: Son exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.

Riesgo bajo: Exposiciones a pérdidas que no causan un gran impacto financiero.[16]

2.3.5 Políticas de seguridad. Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Si bien existen algunos modelos o estructuras para su diseño, estás tienen que ser elaboradas de forma personalizada para cada empresa para así recoger las características propias que tiene la organización.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

Seguridad Física
Seguridad Lógica
Seguridad en redes
Seguridad en los recursos humanos
Seguridad en el Outsourcing
Planes de Contingencia

[16] ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. (online). 1 ed. [España]: Word Press, 2010 [citado 15 ago., 2014]. Disponible en: http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

2.3.5.1 Elementos de una política de seguridad. Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

Definición de violaciones y sanciones por no cumplir con las políticas.

Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer:

Explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.

Deberán establecer las expectativas de la organización, tales expectativas deben tener relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Las políticas deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.[17]

[17] Ibid., p.3.

2.3.6 Seguridad Física.[18] La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir el procesamiento de la información.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputo. Las principales amenazas que se prevén en la seguridad física son:

Desastres naturales, incendios accidentales tormentas e inundaciones.

Amenazas ocasionadas por el hombre.

Disturbios, sabotajes internos y externos deliberados.

Otras amenazas como las fallas de energía eléctrica o las fallas de los equipos.

Los recursos que se deben proteger físicamente van desde un simple teclado hasta un respaldo de toda la información que hay en el sistema, pasando por la propia máquina, igualmente se deben tener medidas de protección contra las condiciones climáticas y suministros de energía que pueden afectar la disponibilidad de los sistemas de información e interrumpir los procesos de la organización.

2.3.6.1 Seguridad de acceso físico. Se refiere a las medidas de seguridad para evitar el acceso de personas no autorizadas a los dispositivos de hardware y cualquier medio de salida de información como fax, copiadoras entre otros, ubicados tanto en el área de sistemas como en las áreas usuarias.

Organización. Para llevar un buen control de los accesos a la organización no sólo se requiere la capacidad de identificación, sino también negar asociarla a la apertura o cerramiento de puertas, permitir o negar accesos basados en restricciones de tiempo, área o sector de la empresa.

Existen varios métodos de control entre ellos están:

Guardias de seguridad
Detectores de Metales
Sistemas Biométricos
Seguridad con Animales
Protección Electrónica

[18] GAR FINKEL, Simson y GENE, Spafford. Seguridad Práctica en UNIX e Internet, 2ª Edición. Mc. Graw Hill, 1999. p.98.

Guardias de seguridad. La utilización de guardias de seguridad será con el fin de controlar el acceso de personas ajenas a la organización y del mismo personal que ahí trabaje; la guardianía debe ser durante las 24 horas del día y deben estar armados para lo cual el personal de seguridad debe poseer un permiso para el manejo de armas otorgado por la autoridad pertinente.

Algunas medidas de seguridad podrían ser:

Credenciales de identificación: Cualquier persona que ingrese a la organización deberá llevar una credencial.

Estás credenciales pueden clasificarse de la siguiente manera:

Normal o definitiva: para el personal permanente de planta.

Temporaria: para personal recién ingresado.

Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.

Visitas.

Bitácora de registro de accesos: Las personas ajenas a la organización deberán llenar este formulario que deberá contener el motivo de la visita, hora de ingreso, etc.

Control de Vehículos: Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

La utilización de guardias de seguridad también tiene su desventaja que es el soborno del guardia por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o salir de la empresa con equipos que no ha sido autorizado su salida. [19]

Área de sistemas. El área de sistemas es considerada como la más sensible a las amenazas debido a que en ella están ubicados los equipos que contienen toda la información que es procesada en las áreas usuarias y se le debe brindar un control adecuado y exclusivo.

Dentro de la organización lo más óptimo para mantener la seguridad y evitar accesos no

[19] Ibid., p.103

permitidos al área de sistemas es implementar como medio de protección los siguientes recursos:

Puerta con cerradura
Puerta de combinación
Puerta electrónica
Puertas sensoriales
Registros de entrada
Videocámaras

Escolta controladora para el acceso de visitantes

Puertas dobles

Alarmas

Seguridad en la ubicación y Dimensión del área de sistemas. Se refiere a las precauciones que se deben tomar en cuenta para la instalación física del área que servirá como eje central del procesamiento de la información de la empresa evitando de esta manera los accesos no permitidos, otras interrupciones y la falta de espacio físico para la adecuada operación del área.

Seguridad del equipamiento. La información vital de la organización es procesada en los equipos de computación los cuales deben recibir cuidados especiales para prevenir posibles fallas ocasionadas por la electricidad, temperatura o falta de mantenimiento del equipo que puedan provocar interrupciones mientras se estén procesando los datos.[20]

2.4 MARCO LEGAL

Leyes informáticas colombianas.[21] La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.

[20] Ibid., p.105.
[21] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico (online). 3 rev. [Bogotá]: UNAD, 2013. [citado 20 ago., 2014]. Disponible en: http://www.unad.edu.co/gidt/index.php/leyesinformaticas

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano:

Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.

Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Una norma posterior relacionada fue la Ley 679 de 2001, que estableció el Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en actitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones penales, sino administrativas (Artículo 10), pues siendo simple prohibición, deja un vacío que quita eficacia a la Ley, cuando se trata de verdaderos delitos informáticos.

Para subsanar lo anterior, el 21 de julio de 2009, se sancionó la Ley 1336, "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes". En forma específica, en su Capítulo VI, sanciona los "Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil" con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (SMLMV). [22]

[22] Ibid., p.5.

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones.

A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos", con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

Con los desarrollos jurídicos hasta ahora logrados acerca de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo (Davenport, 1999), de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral. [23]

Norma ISO 27002.[24] La ISO 27002 es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información. Funciona de la siguiente manera:

1. Las empresas que desean resguardar sus activos de información implementan la norma ISO 27001, la cual consiste en la creación de un Sistema de Gestión de la Seguridad de la

[23] Ibid., p.6.
[24] ISO 27002.es. Norma ISO 27002 (online). [España]: UNAD, 2012 [citado 26 ago., 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf

Información.

2. Para evaluar el desempeño del estándar anterior, se utiliza la ISO 27002 en la que están recopilados los controles que deben ser aplicados para evaluar el desempeño del estándar. Cabe destacar que la ISO 27001 también contiene un conjunto de controles; pero estos se refieren a los requisitos para la creación del SGSI y; por otra parte, los controles especificados en la ISO 27002 sirven para la evaluación de la misma. En este sentido, la ISO 27002 se utiliza como un documento de referencia y como tal, NO es certificable.

Contenido de la Norma. En total la norma contiene 39 objetivos de control y 133 controles los cuales están agrupados en 11 dominios. La siguiente figura muestra cada uno de los dominios de la norma.

1. Políticas de Seguridad. Consiste en los controles que se aplican a las políticas de seguridad de la información. Comprende tanto la elaboración del documento que recopile todas las políticas, como su revisión.

2. Organización de la Seguridad de la Información. Esta sección tiene dos objetivos de control que corresponden a la organización interna de la información y su trato con terceros.

3. Gestión de Activos. Este dominio posee dos activos que tratan la responsabilidad sobre los activos; es decir, quién es responsable de qué activo, y la clasificación de la información, que contiene una serie de directrices para clasificar la información y su posterior manipulación.

4. Seguridad de los Recursos Humanos. Comprende todos los controles que se deben implementar para evitar la fuga de información por parte del personal de la empresa. El dominio contiene tres controles que corresponden al ciclo de trabajo de una persona: antes del empleo, durante el empleo y el cese del empleo.

5. Seguridad física y del entorno. Para que los datos estén debidamente resguardados, es necesario que éstos se encuentren en una zona segura y con los equipos adecuados; debidamente preparados para ejecutar la tarea encomendada. Este dominio comprende los controles necesarios tanto para la preparación de áreas seguras, como para el emplazamiento y protección de equipos.

6. Gestión de Comunicaciones y Operaciones. Este dominio es el más largo de toda la norma y comprende diez objetivos de control que aseguran una comunicación efectiva entre los sistemas de información; así como asegura todas las operaciones que conlleven un intercambio de información, como: servicios de e-commerce, redes de datos, entre otros.[25]

[25] Ibid., p.7.

7. Control de Acceso. Es lógico pensar que; en una empresa, no todos los usuarios deben tener acceso a toda la información de la empresa; sino que cada usuario debe acceder únicamente a la información con la que trabaja. Para ello, se establecen 6 objetivos de control que definen la meta que se ha de alcanzar mediante la gestión de los accesos de usuario y la concesión de privilegios.

8. Adquisición, desarrollo y mantenimiento de sistemas de información. Para que la información de una empresa esté debidamente resguardada, es necesario que el sistema de seguridad que se ha implementado esté en una continua revisión. Para ello, se plantean 6 objetivos de control sobre los cuales ha de guiarse el tratamiento de los SI.

9. Gestión de Incidentes en la seguridad. Al implementar un sistema de gestión de la Seguridad de la Información, cualquier incidente implica un fallo en el mismo y ha de ser controlado correctamente para que no afecte otras áreas de la organización. Se plantean 2 objetivos: el primero está relacionado con la identificación de los puntos débiles del SGSI y el segundo con la gestión de incidentes y la implementación de mejoras al sistema.

10. Gestión de la continuidad del negocio. Este dominio tiene un solo objetivo y consiste en el alineamiento de los objetivos del SGSI con los objetivos de la compañía.

11. Cumplimiento. Este es el último dominio y se plantea como una evaluación. Se evalúan distintos factores: requisitos legales, normas de seguridad y cumplimiento técnico, y auditorías.

En conclusión la ISO 27002 sirve como un punto de información de la serie de normas 27000. Evalúa y rectifica su implementación mediante la aplicación de objetivos de control. Dichos objetivos han de ser cumplidos para garantizar la correcta implantación de las normas; así como el funcionamiento de la empresa en cuanto a la seguridad de la información.[26]

[26] Ibid., p.7.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACION

El tipo de investigación que se llevó a cabo en el desarrollo de este trabajo es: la investigación descriptiva, con un enfoque cuantitativo, ya que permite realizar observaciones objetivas y exactas del tema a realizar, para describir, analizar e interpretar los datos obtenidos, en términos claros y precisos, la investigación descriptiva son aquellas que describen de modo sistemático las características de una población, situación o área de interés. El proyecto se realizó teniendo en cuenta este tipo de investigación, ya que ayudó a facilitar el análisis de las ventajas y los beneficios que tiene el diseño de un manual de políticas de seguridad informática para la Alcaldía municipal de La Playa de Belén.

3.2 POBLACIÓN

La población objeto de estudio que se tuvo en cuenta en el proyecto, fue la conformada por los empleados de la Alcaldía Municipal de La Playa de Belén, la cual en su total es de 25 personas.

3.3 MUESTRA

La muestra es una parte del universo, que reúne todas las condiciones o características de la población objetivo, para determinar el direccionamiento estratégico de la Alcaldía. Para el caso se tomó como muestra el total de la población involucrada en el proceso, que equivale a los 25 funcionarios que laboran de forma permanente en la Alcaldía.

3.4 TÉCNICA E INSTRUMENTOS DE RECOLECCION DE LA INFORMACIÓN

Las técnicas e instrumentos de recolección empleadas para la obtención de la información necesaria para el desarrollo del proyecto, fueron la observación, encuesta y la revisión documental.

La observación directa permitió obtener información clara y precisa, a partir del detalle en tiempo real de los hechos y situaciones sociales, que se presentan y llevan a cabo normalmente.[27]

La encuesta, está compuesta de un cuestionario, que contiene una serie de preguntas enfocadas al manejo de la información, en cuya formulación se observa el problema estudiado. A través de ellas se especificaron los requerimientos para el presente proyecto y serán aplicadas a los funcionarios de la Alcaldía Municipal de La Playa de Belén (N.S.), con el propósito de hallar posibles soluciones.

[27] AZPEITIA FERNÁNDEZ, Almudena. Observación no-sistemática (online). 1 ed. [Madrid]: 2009 [citado 26 ago., 2014]. Disponible en: https://www.uam.es/personal_pdi/stmaria/jmurillo/Met_Inves_Avan/Presentaciones/Observacion_NoSistematica_(Trabajo).pdf

Con el apoyo de la revisión documental se consultaron textos e información en línea (consultas de sitios y páginas Web) con la finalidad de ampliar los conocimientos necesarios para alcanzar los objetivos propuestos y definir el marco teórico. Ver anexo.

3.5 ANALISIS DE LA INFORMACIÓN

Para la organización y tabulación de la información obtenida por la aplicación de la encuesta se analizó cuantitativamente mediante tablas y gráficas estadísticas que representadas adecuadamente dieron mayor claridad y elevaron el nivel de confianza a los interesados y encargados de la revisión y puesta en marcha del proyecto.

4. RESULTADOS

4.1 DIAGNÓSTICO PARA CONOCER LA SITUACIÓN ACTUAL EN LA ALCALDÍA MUNICIPAL DE LA PLAYA DE BELÉN

Con el fin de obtener un mejor conocimiento acerca de la Alcaldía municipal de La Playa de Belén, Norte de Santander, y hacer un diagnóstico, se realizó un sondeo de su organización administrativa, para así poder desarrollar el manual de funciones de acuerdo a lo que su administración proyecta en su mission, visión y objetivos.

4.1.1 Generalidades del municipio de La Playa de Belén.

4.1.1.1 Reseña histórica. En el paraje de Llano Alto, donde construyó la primera casa doña María Claro de Sanguino, se inició en 1857 la fundación del municipio de La Playa de Belén. En este año, con motivo de la visita pastoral del obispo dominico Fray Bernabé Rojas al sitio de "Patatoque", los señores Jesús Rueda, Tiburcio Alvarez y Juan Esteban Vega, obtuvieron licencia del prelado para construir una capilla dedicada a San José.

No se ha establecido en qué época de aquel año pasó el obispo Rojas por Patatoque; su visita a la provincia de Ocaña, iniciada en el mes de enero, se prolongó hasta finales octubre. No puedo, entonces, hablar de una fecha exacta del nacimiento del terruño. 1857 fue un año de inestabilidad en la organización política territorial y que, por esta circunstancia, La Playa de Belén fue arrullada en sus primeros meses en las provincias de Ocaña y Mompox, y en el Estado de Santander.

El 4 de diciembre de 1862, el reverendo padre misionero Fray Milán bendijo la capilla, dedicada a San José. Don Justiniano J. Páez, en sus "Noticias históricas de la ciudad y provincia de Ocaña", dice que en este acto solemne se le dio al caserío el nombre de La Playa de Belén. El notable historiador, seguramente, acudió a la tradición porque no cita las fuentes de sus apuntes. Los playeros guardamos el mayor respeto por su versión y la hemos difundido.

La señora María Claro de Sanguino construyó la primera casa en 1857, razón por la cual se considera que ella y los señores Vega, Álvarez y Rueda fueron los primeros pobladores o fundadores. Alrededor del modesto templo creció el pueblo, en el paraje conocido como Llano Alto, donde actualmente se encuentra la cabecera municipal.

En cuanto al origen del nombre, en los archivos notariales se observa que la denominación, hasta 1913, fue La Playa. Registros históricos del señor Páez señalan que en 1818 el lugar se conocía como Playa, y en 1822 se denominaba La Playa. El nombre actual se asignó al caserío por medio del Acuerdo No. 3, del 15 de septiembre de 1913, del Concejo de Aspasica, cuyo artículo primero dice: "Erígese en Corregimiento con el nombre de La Playa de Belén el territorio del caserío de La Playa de este Municipio".

Playa, La Playa o La Playa de Belén, son denominaciones ancestrales, por las

características del suelo, similares a la ribera del mar o de río grande. En mi infancia acudíamos a los arenales de El Playón (la quebrada que serpentea de norte a sur, cuyo nombre es aumentativo de playa) y a otros lugares, aledaños a la cabecera, a jugar a los toros.

4.1.1.2 Misión. Generar las condiciones necesarias para garantizar la prosperidad y competitividad de la población playera que contribuyan al logro de la visión 2015, con desarrollo y proyección en los diferentes niveles territoriales a través del turismo, en un escenario de equidad y respeto de los derechos de sus habitantes.

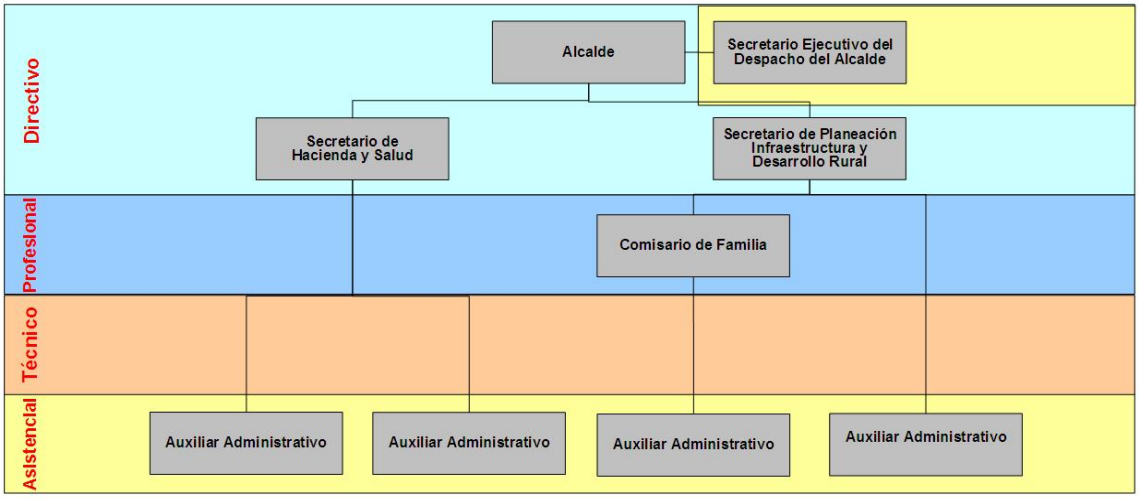
4.1.1.3 Visión. La Playa de Belén para el 2015 será un Municipio próspero, con competitividad, desarrollo social, cultural, educacional y proyección en lo regional, departamental y nacional a través del turismo; con políticas de equidad social respeto de los derechos de las personas, encaminadas a mejorar las condiciones de vida de sus habitantes.

4.1.1.4 Dependencias del Municipio. Las dependencias con las que cuenta en la actualidad la Alcaldía Municipal de La Playa de Belén, son:

Archivo y Almacén
Comisaria de Familia
Despacho del Alcalde
Secretaría de Hacienda y Salud
Secretaría de Planeación, Infraestructura y Desarrollo Rural
Secretaría Ejecutivo del Despacho del Alcalde
SISBEN

4.1.1.5 Estructura Organizacional.

Figura 2. Estructura organizacional



Fuente: Alcaldía Municipal de La Playa de Belén, 2015.

4.1.1.6 Objetivos de la Alcaldía municipal. Administrar los asuntos municipales y prestar los servicios públicos que determine la ley.

Interpretar la voluntad soberana de sus habitantes y en el marco de la Constitución, la ley y el Reglamento.

Ordenar el desarrollo de su territorio y construir las obras que demande el progreso municipal.

Planificar el desarrollo económico, social y ambiental de su territorio, de conformidad con la ley y en coordinación con otras entidades.

Promover el mejoramiento económico y social de sus habitantes.

Promover la participación comunitaria y el mejoramiento social y cultural.

Solucionar las necesidades insatisfechas de salud, educación, saneamiento ambiental, agua potable, servicios públicos, domiciliarios, vivienda, recreación y deporte, con especial énfasis en la niñez, la mujer, la tercera edad y los sectores discapacitados.

Velar por el adecuado manejo de los recursos naturales y del medio ambiente, de conformidad con la ley.

Velar por la preservación del territorio municipal y sus riquezas naturales, afín de que ellos sirvan y beneficien a los habitantes del Municipio, asegurando el progreso de la entidad territorial, sin perjuicio de las intervenciones que para efecto de su explotación, usos, distribución y consumo disponga la ley.

Ser el representante político, administrativo y legal del Municipio ante las diferentes instancias del orden nacional y departamental, dirigiendo sus actuaciones y las de la Administración Municipal en procura de lograr el bienestar y desarrollo de la comunidad.

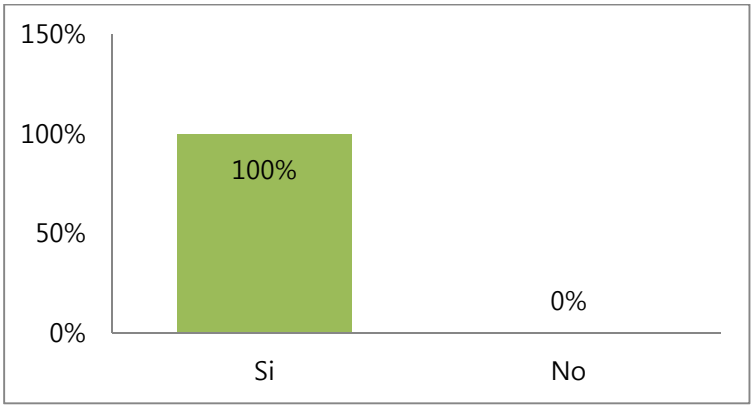
Las demás que le señalen la Constitución y la ley.

4.1.1.7 Infraestructura tecnológica. En cuanto a la infraestructura tecnológica, la Alcaldía Municipal de La Playa de Belén, N.S., cuenta con equipos de cómputo en las distintas áreas de trabajo ubicadas en su interior. En el anexo C, se encuentra una relación de los mismos con sus características.

4.1.1.8 Manual de funciones. El manual de funciones se encuentra en el anexo H.

4.1.2 Diagnóstico sobre los distintos procesos informáticos realizados en la Alcaldía Municipal de La Playa de Belén. De acuerdo a la encuesta realizada al personal encargado del area de Sistemas de la Alcaldía Municipal de La Playa de Belén, N.S., se tuvieron los siguientes resultados:

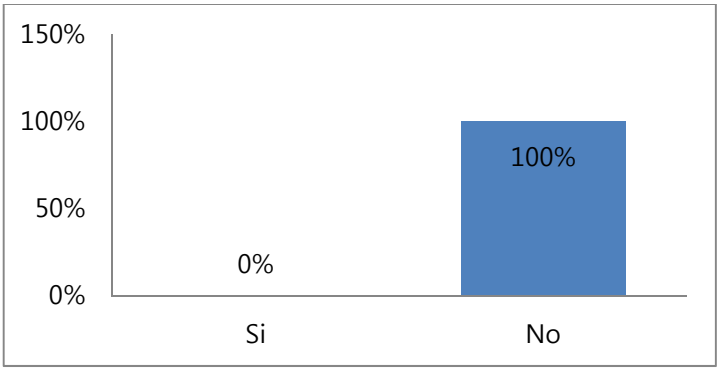
Gráfico 1. Conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información.



Fuente: Autores del proyecto.

El personal que se encuentra al frente de lo que a sistemas se refiere en la Alcaldía, teniendo en cuenta que la institución no cuenta con un area de sistemas definida; opinan que si tienen conocimiento de las responsabilidades y sanciones que puedan recibir frente a la seguridad de la información, toda vez que los dos funcionarios son ingenieros de sistemas y por ende, deben conocer acerca de dichas responsabilidades que deben manejar para poder ejercer un cargo concientemente.

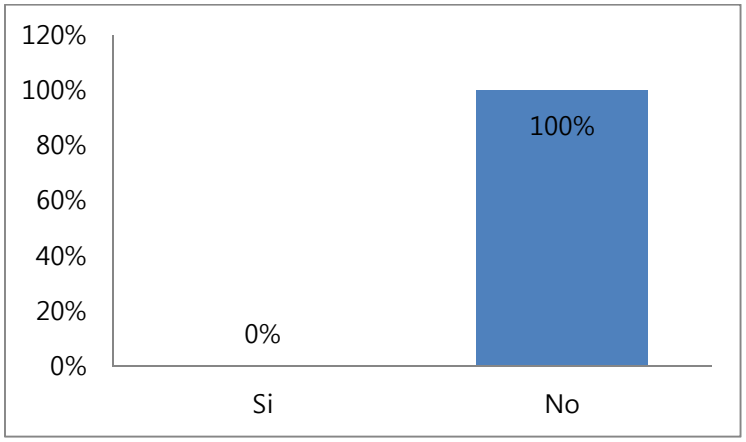
Gráfico 2. Acuerdo de confidencialidad de la información.



Fuente: Autores del proyecto.

En la Alcaldía y en el medio donde se encuentran estos funcionarios, no se cuenta con un acuerdo de confidencialidad de la información, lo que hace más riesgoso que se infiltre cualquier información ya sea de entrada o salida, no teniendo protección.

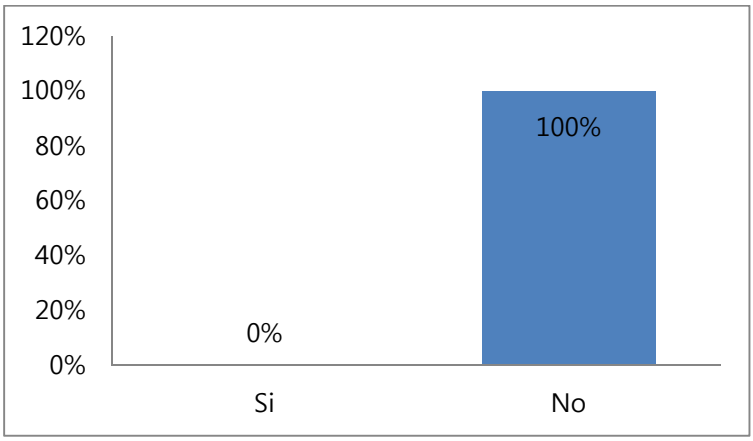
Gráfica 3. Identificación de las áreas de la Alcaldía.



Fuente: Autores del proyecto.

Las distintas áreas de la Alcaldía no cuentan con su debida identificación, haciendo falta una planeación estratégica en la misma, teniendo en cuenta que esto es de suma importancia tanto para el personal interno como para el usuario o quien visita las distintas dependencias, con el fin de evitar confusiones en las mismas.

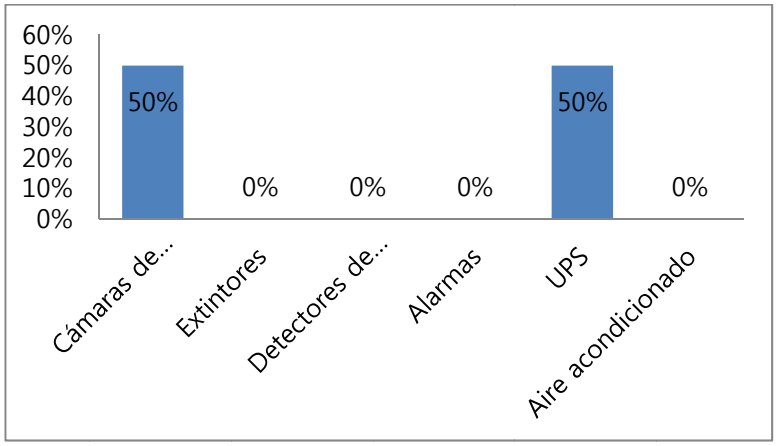
Gráfica 4. Control en el area para el ingreso del personal



Fuente: Autores del proyecto.

En cuanto a los controles en las distintas áreas a la hora de ingresar personal, no se tiene el mismo, por lo cual se genera desorden en la entrada del mismo y la falta de cumplimiento de normas y horarios.

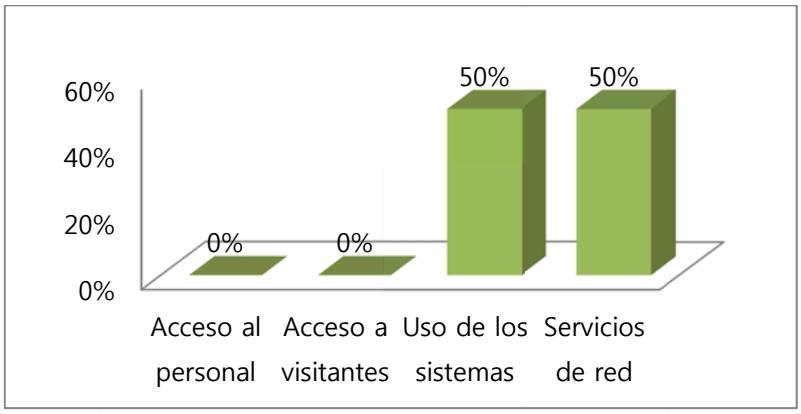
Gráfica 5. Elementos con los que cuenta el area.



Fuente: Autores del proyecto.

Según los encuestados, el area solo cuenta con cámaras de seguridad y una fuente de suministro eléctrico, conocida como UPS. El resto de elementos como extintores, detectores de humo, alarmas, aire acondicionado, no se cuentan en el area donde se labora, siendo éstos de mucha importancia para prestar un mejor servicio al usuario y poder laborar en mejores condiciones.

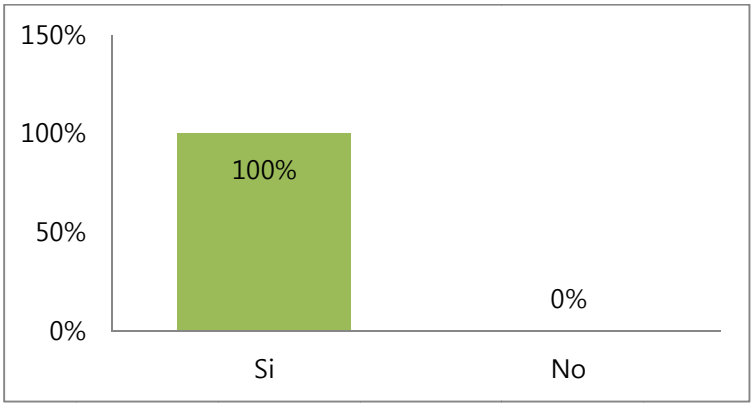
Gráfica 6. Registros con los que cuenta la Alcaldía.



Fuente: Autores del proyecto.

La Alcaldía solo cuenta con registros de uso de los sistemas y servicios de red. Cabe destacar que uno de los registros más importantes son los que en el momento no se encuentran en la institución, como son el de acceso al personal y acceso a visitantes; éstos deben ser de alguna manera establecidos, ya que en éstos es donde se puede buscar la manera de filtrar o infiltrar cualquier información, teniendo en cuenta que para muchos de ellos es importante poder adquirir la misma de esa institución.

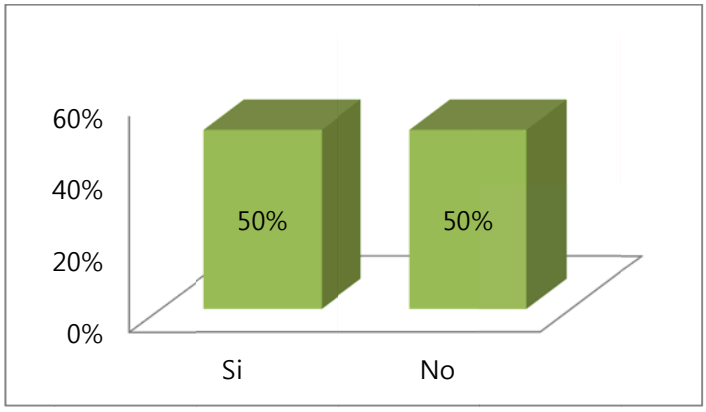
Gráfica 7. Se cuenta con mensajería electrónica interna para sus actividades.



Fuente: Autores del proyecto.

Uno de los servicios internos que se tienen, es el de mensajería electrónica interna para sus actividades. Con ésta se puede manejar datos, cualquier mensaje, correo, entre otros, desde las distintas áreas de la Alcaldía. Cabe destacar que para esta mensajería no existe ninguna protección ni seguridad que evite que un tercero pueda acceder a la misma.

Gráfica 8. Seguridad en el computador que utiliza



Fuente: Autores del proyecto.

La seguridad que sostiene cada computador utilizado no es la mejor, tan solo el 50% habla de una contraseña para permitir el acceso del usuario a los sistemas; pero el otro 50% dice no contar con ningún tipo de seguridad, por lo tanto, cualquier persona podrá acceder a estos equipos sin que nadie lo autorice y así obtener información de cualquier tipo sin restricción alguna.

Teniendo en cuenta todo lo anterior se tiene poco o nulo sistema de seguridad para la información en la Alcaldía municipal de La Playa de Belén, N.S.

De acuerdo a la siguiente tabla, se evaluará el impacto que tiene el riesgo en lo que respecta al área de sistemas de la Alcaldía Municipal de La Playa de Belén.

Cuadro 2. Impacto

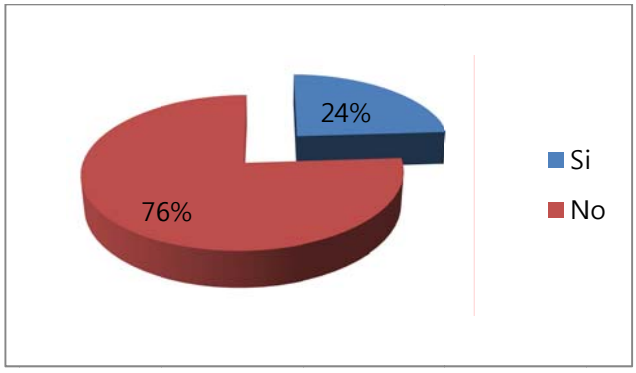
Muy Alto (MA)	0.8
Alto (A)	0.4
Moderado (M)	0.2
Bajo (B)	0.1
Muy bajo (MB)	0.05

Ítem	**Impacto del riesgo**				
	MA	A	M	B	MB
Conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información.					X
Acuerdo de confidencialidad de la información	X				
Identificación de las áreas de la Alcaldía		X			
Control en el area para el ingreso del personal	X				
Elementos con los que cuenta el area			X		
Registros con los que cuenta la Alcaldía	X				
Mensajería electrónica interna para sus actividades				X	
Seguridad en el computador que utiliza			X		

Fuente: Autores del proyecto.

4.1.2.1 Encuesta dirigida al personal de la Alcaldía municipal de La Playa de Belén. A continuación se muestran los resultados obtenidos luego de encuestar al personal de la Alcaldía de La Playa de Belén, con el fin de obtener información sobre los distintos movimientos informáticos realizados en la misma.

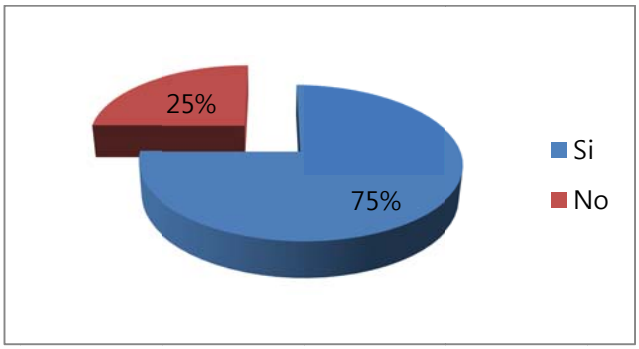
Gráfica 9. Mantenimiento periódico de hardware y software



Fuente: Autores del proyecto.

El 76% de los encuestados dicen que en la Alcaldía no se le realiza mantenimiento periódico de hardware y software a los equipos que allí se encuentran, obteniéndose con esto un riesgo en cuanto a los virus que puedan recoger los mismos. El 24% restante dice que si se le realiza dicho mantenimiento.

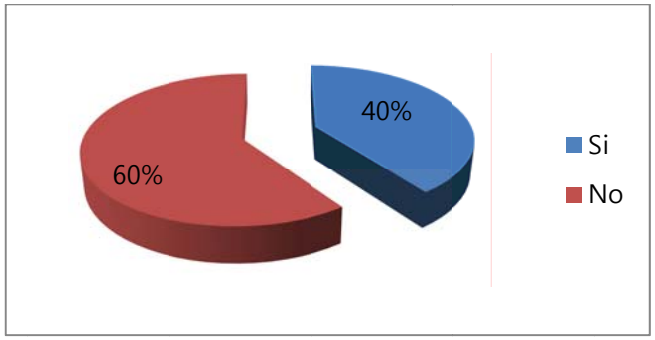
Gráfica 10. Controles contra software malicioso o espía (antivirus, antispyware, etc.)



Fuente: Autores del proyecto.

En cuanto a los controles contra software, de los encuestados el 75% dice que si existe en la Alcaldía este control, el cual en su mayoría se refiere al antivirus, ya que no se cuenta con más software espía que ayude a evitar cualquier daño por virus en los equipos de la entidad. El otro 25% dice que no existe.

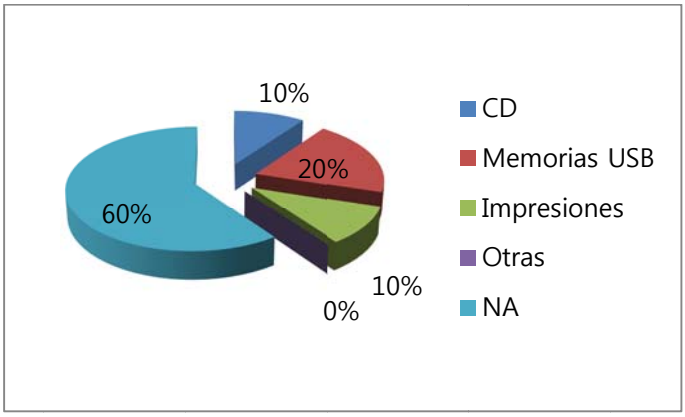
Gráfica 11. Realizan backup's (Copias de Seguridad de la Información)



Fuente: Autores del proyecto.

En lo que tiene que ver con copias de seguridad de la información, en la Alcaldía de La Playa de Belén, según el 60% de encuestados, no se tienen copias de seguridad de la información, arriesgando así que se pierda el 100% de la misma, en caso de llegar a fallar cualquier equipo que allí se utilice. El 40% dice si realizar copia de seguridad de la información que se maneja en su dependencia, por lo tanto se obtiene más confianza en la misma.

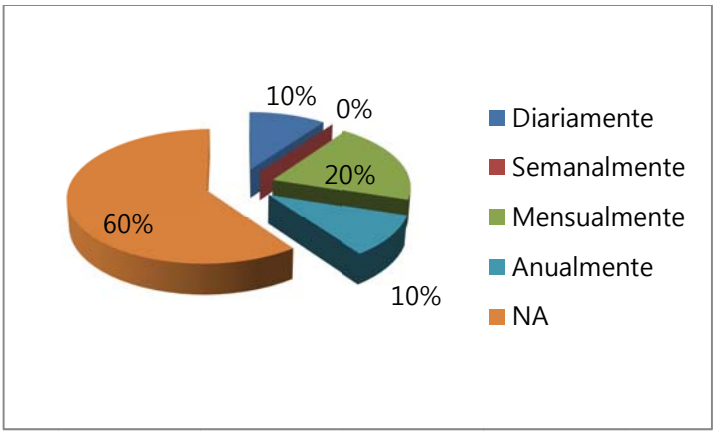
Gráfica 12. Medio de almacenamiento



Fuente: Autores del proyecto.

Como se registró en la gráfica 11, que no se obtiene backup´s en la información, el 60% en esta pregunta se abstiene de contestar, ya que al no realizar copia de seguridad de la información, no se almacena la misma. El otro 40% responde así: El 20% guarda la información en memorias USB, 10% en CD y el otro 10% realiza impresiones en papel y tinta, que son archivadas como copias de seguridad impresas.

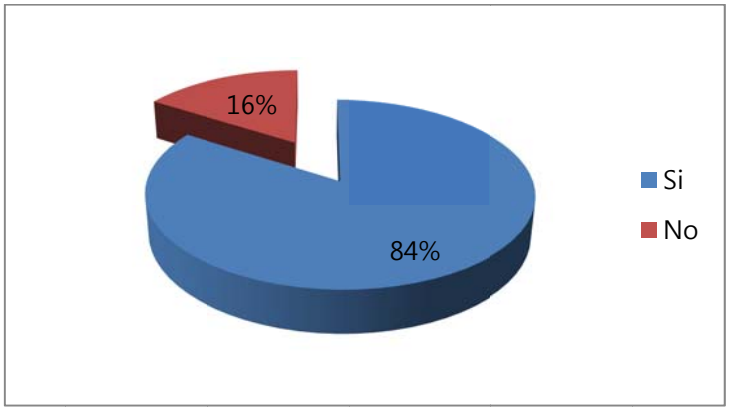
Gráfica 13. Periodicidad



Fuente: Autores del proyecto.

Las copias de seguridad de las que se habla en la gráfica 11, según el 20% de encuestados, se realiza de manera mensual, en un 10% se dice que diaria y anualmente, respectivamente. El 60%, es la cantidad de encuestados que dice no realizarse backup´s en la Alcaldía de la Playa de Belén.

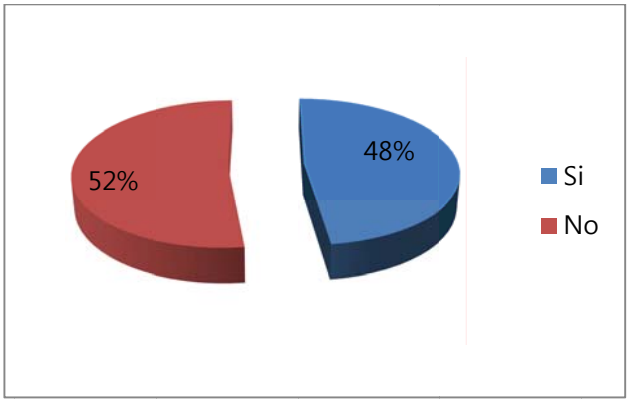
Gráfica 14. Mensajería electrónica interna



Fuente: Autores del proyecto.

La mensajería electronica es manejada de manera interna en la Alcaldía municipal de La Playa de Belén, dice el 84% de los encuestados, lo cual agiliza cualquier trámite que deba hacerse al interior de la institución. El otro 16% dicen que no se realiza ésta, lo cual genera algunas demoras en procedimientos informáticos que se realicen.

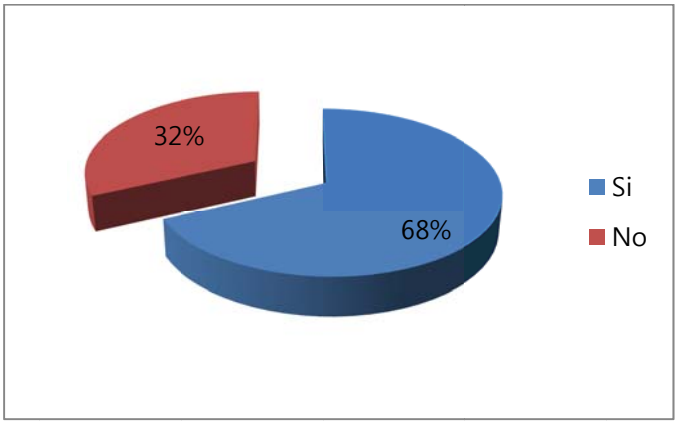
Gráfica 15. Seguridad en mensajería interna en la Alcaldía



Fuente: Autores del proyecto.

En lo que corresponde a la seguridad que se maneja en cuanto a la mensajería interna de la Alcaldía municipal de La Playa de Belén, el 52% no conoce algún sistema que sea utilizado para ello, mientras que el 48% restante dice que si se utiliza de algún modo algún tipo de seguridad para poder realizar este tipo de mensajería en red.

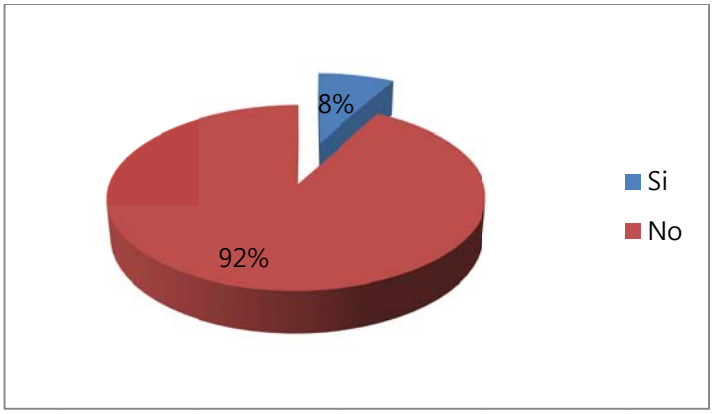
Gráfica 16. Contraseña en el computador para permitir el acceso del usuario a los sistemas



Fuente: Autores del proyecto.

El 68% del personal que labora en la Alcaldía de La Playa de Belén, dice que el computador que utiliza si cuenta con una contraseña para permitir el acceso del usuario a los sistemas, esto genera confianza y seguridad para la persona responsable del equipo. El otro 32% dice no contar con esta clase de seguridad, lo cual hace que cualquier persona pueda acceder a la información que sostenga el computador.

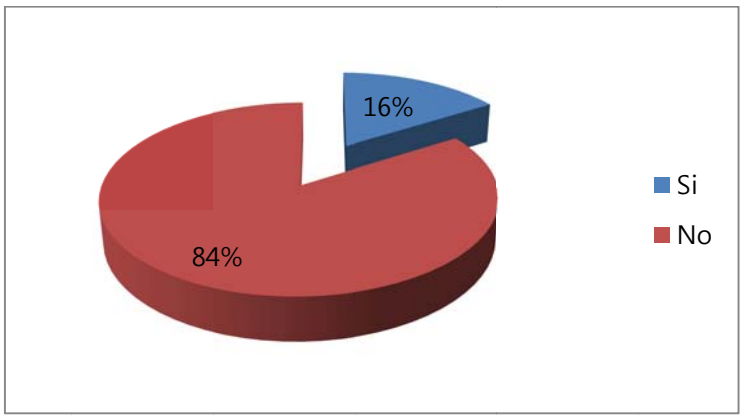
Gráfica 17. Programas para la encriptación



Fuente: Autores del proyecto.

Cuando nos referimos a programas para la encriptación, se refiere al camuflaje de la información a destinatarios no deseados. En el caso de la Alcaldía municipal de La Playa de Belén, se tiene que el 92% no conoce de esta clase de programas, por lo tanto dicen no contar con los mismos en la institución. Tan solo un 8% dice que si se cuenta con el mismo.

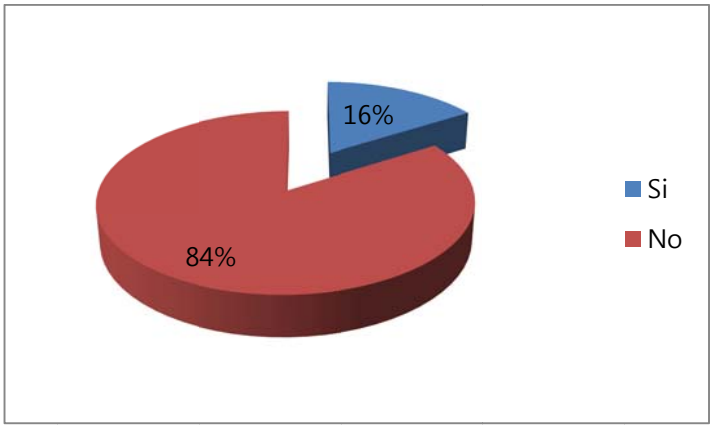
Gráfica 18. Procedimiento formal para reportes de incidentes



Fuente: Autores del proyecto.

La gran mayoría de los empleados de la Alcaldía de La Playa de Belén (84%), dicen que la institución no cuenta con un procedimiento formal para reportar cualquier incidente que se pueda presentar en la misma, como el robo de información, pérdida de datos, accesos no permitidos, entre otros. Estos hallazgos son preocupantes, debido a que todo esto es lo que genera el facilitamiento por parte de otras personas para ingresar a realizar cualquier robo de información sin problema, puesto que al no ser reportado no darán aviso y por tanto, no se corre ningún riesgo de señalamientos.

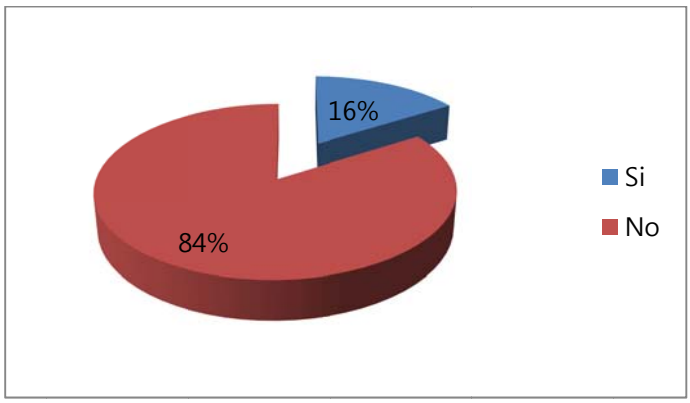
Gráfica 19. Plan de contingencia



Fuente: Autores del proyecto.

En cuanto a un plan de contingencia, tampoco es manejado en la Alcaldía de La Playa de Belén, comenta el 84% de encuestados de la misma. Por lo tanto, al presentarse cualquier incidente de seguridad en la institución, éste pasará por alto, resaltando que el 16% restante creen que sí existe dicho plan, pero no se le da el uso adecuado.

Gráfica 20. Recolección e investigación de evidencias sobre incidente de seguridad de la información



Fuente: Autores del proyecto.

Según el 84% de empleados de la Alcaldía de La Playa de Belén, no se realiza investigación y tampoco recolección de evidencias sobre el incidente de seguridad de la información, teniendo como base la gráfica 19, en la que se hace alusión a un plan de contingencia que no conocen, acá el mismo porcentaje de encuestados dice que tampoco se investiga acerca de cualquier incidente que acontezca.

Teniendo en cuenta que la Alcaldía solo cuenta con siete dependencias, aún así se necesita de un control al acceso de los equipos de cómputo y demás información, ya que no existe restricción para el ingreso de personal, tampoco existen registros de acceso y la seguridad de los computadores es media.

4.2 ELEMENTOS DE RIESGOS Y FALLAS DE SEGURIDAD INFORMÁTICA, ENCONTRADOS EN LA ALCALDÍA MUNICIPAL DE LA PLAYA DE BELÉN

La Alcaldía municipal de La Playa de Belén, como todo organismo, se encuentra expuesta a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

La Alcaldía deberá identificar los riesgos a los que se expone el Organismo en materia de seguridad de la información y generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

A continuación se hace relación a los riesgos y fallas de seguridad encontrados en la Alcaldía Municipal de La Playa de Belén:

En las distintas áreas de la Alcaldía se contratan, adquieren o desarrollan aplicaciones de software de manera independiente de acuerdo a sus necesidades. Para ello se deben adquirir

más softwares que agilicen procesos como es un sistema de Archivo y Gestión Documental aplicable.

A pesar de que se cuenta con un sistema Integral de comunicación interna entre algunas dependencias, se debe implementar uno que comunique todas las áreas de la Alcaldía de manera rápida, amigable y amena. Con ello se logrará integrar a las diferentes dependencias de manera confiable, que permita la toma de decisiones y conocer de manera inmediata y gratuita cualquier situación que facilitara la gestión integral en la administración.

El uso de medios de almacenamiento es escaso, para ello se deben utilizar medios de almacenamiento extraíbles USB, además del análisis de éstos con antivirus antes de ingresarlos a un PC, para la seguridad de los mismos, el uso de contraseñas para cada equipo y funcionario.

El proceso de soporte Técnico solo se hace cuando ya falla el equipo de cómputo. Factor éste que perjudica.

La Alcaldía municipal de La Playa de Belén, no cuenta con un plan de contingencia que ayude a la hora de presentarse cualquier incidente de seguridad informática.

No existe un plan de capacitación permanente y coordinado que responda a las necesidades de la Alcaldía Municipal de La Playa de Belén.

Con el fin de corregir estos riesgos, a continuación se expone un tratamiento que podrá ser tenido en cuenta con el fin de mitigar los mismos. Cabe destacar que antes de considerar el tratamiento de un riesgo, la Alcaldía deberá decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;

Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos de la Alcaldía;

Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;

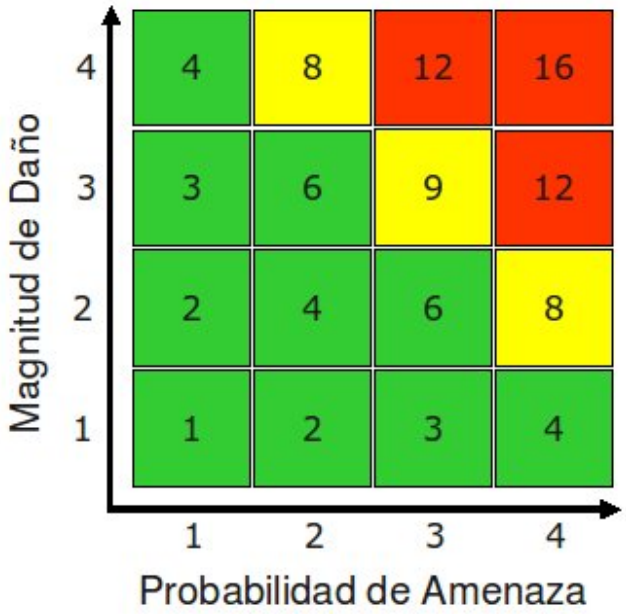
Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

4.2.1 Matriz de riesgo. A continuación se presenta una matriz de riesgo, basada en la clasificación, probabilidad de amenaza y magnitud de daño de los datos e información, así como de sistemas e infraestructura y del personal.

Los resultados de este estudio, se ven reflejando en las gráficas mediante un estándar de colores definido así:

Riesgo = Probabilidad de amenaza * Magnitud de Daño

Cuadro 3. Matriz de riesgo



Fuente: Autores del proyecto.

Cuadro 4. Datos e información

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
	Clasificación				Actos originados por la criminalidad común y motivación política													Sucesos de origen físico								
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato /	Costo de recuperación	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	3	4	2	4	2	2	3	4	2	3	3	3
Documentos institucionales (Proyectos,	x	x	x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Finanzas	x	x		4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Servicios bancarios	x	x		4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Directorio de Contactos	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Productos institucionales	x		x	3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Correo electrónico	x			3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Bases de datos internos	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Página Web externa	x	x		3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Respaldos	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Infraestructura (Planes, Documentación			x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Informatica (Planes, Documentación	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Base de datos de Contraseñas	x			3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Datos e información no institucionales			x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Navegación en Internet	x			3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Chat interno	x			4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Chat externo	x			4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Llamadas telefónicas internas	x			2	4	4	4	6	6	4	8	8	6	8	6	8	4	8	4	4	6	8	4	6	6	6
Llamadas telefónicas	x			4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12

Fuente: Autores del proyecto.

Cuadro 4. (continuación)

Matriz de Análisis de Riesgo																															
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																											
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato /	Costo de recuperación		Falta de inducción, capacitación y	Mal manejo de sistemas y	Utilización de programas no	Falta de pruebas de software nuevo	Perdida de datos	Infección de sistemas a través	Manejo inadecuado de	Unidades portables con	Transmisión no cifrada de datos	Manejo inadecuado de	Compartir contraseñas o	Transmisión de contraseñas por	Exposición o extravío de	Sobrepasar autoridades	Falta de definición de perfil,	Falta de mantenimiento	Falta de actualización de	Fallas en permisos de usuarios	Acceso electrónico no autorizado a	Acceso electrónico no autorizado a	Red cableada expuesta para el	Red inalámbrica expuesta al acceso	Dependencia a servicio técnico	Falta de normas y reglas claras (no	Falta de mecanismos de	Ausencia de documentación
	4	4	4		4	4	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	3	3	4	4	4	4	4	4
Documentos institucionales (Proyectos,	x	x	x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Finanzas	x	x		4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Servicios bancarios	x	x		4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Directorio de Contactos	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Productos institucionales	x		x	3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Correo electrónico	x			3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Bases de datos internos	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Página Web externa	x	x		3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Respaldos	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Infraestructura (Planes, Documentación			x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Informatica (Planes, Documentación	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Base de datos de Contraseñas	x			3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Datos e información no			x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Navegación en Internet	x			3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Chat interno	x			4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Chat externo	x			4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Llamadas telefónicas	x			2	8	8	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	6	6	8	8	8	8	8	8
Llamadas telefónicas	x			4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16

Fuente: Autores del proyecto.

Cuadro 5. Sistemas e Infraestructura

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
Sistemas e Infraestruct	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política													Sucesos de origen físico							
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	3	4	2	4	2	2	3	4	2	3	3	3
Equipos de la red cableada (router, switch, etc.)	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Equipos de la red inalámbrica (router punto	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Cortafuego			x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Servidores	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Computadoras		x	x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Portátiles		x	x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Programas de administración (contabilidad,	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Programas de manejo de proyectos	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Programas de comunicación (correo electrónico, chat,	x		x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Impresoras	x		x	3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Memorias portátiles			x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Celulares	x			2	4	4	4	6	6	4	8	8	6	8	6	8	4	8	4	4	6	8	4	6	6	6
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		x	x	4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Vehiculos	x		x	1	2	2	2	3	3	2	4	4	3	4	3	4	2	4	2	2	3	4	2	3	3	3

Fuente: Autores del proyecto.

Cuadro 5. (continuación)

Matriz de Análisis de Riesgo					Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																										
Sistemas e Infraestruct	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del	Falta de mantenimiento físico (proceso, repuestos e	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el	Falta de mecanismos de verificación de normas y reglas /	Ausencia de documentación
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,		4	4	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	3	3	4	4	4	4	4	4
Equipos de la red cableada (router, switch, etc.)	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Equipos de la red inalámbrica (router, punto	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Cortafuego			x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Servidores	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Computadoras		x	x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Portátiles		x	x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Programas de administración (contabilidad,	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Programas de manejo de proyectos	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Programas de comunicación (correo electrónico, chat,	x		x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Impresoras	x		x	3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Memorias portátiles			x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Celulares	x			2	8	8	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	6	6	8	8	8	8	8	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)		x	x	4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Vehículos	x		x	1	4	4	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	3	3	4	4	4	4	4	4

Fuente: Autores del proyecto.

Cuadro 6. Personal

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																				
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política												Sucesos de origen físico								
	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	2	2	3	3	2	4	4	3	4	3	4	2	4	2	2	3	4	2	3	3	3
Dirección / Coordinación	X			4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Administración	X	X		4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Personal técnico		X		3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Recepción		X		2	4	4	4	6	6	4	8	8	6	8	6	8	4	8	4	4	6	8	4	6	6	6
Piloto / conductor			X	1	2	2	2	3	3	2	4	4	3	4	3	4	2	4	2	2	3	4	2	3	3	3
Informática / Soporte técnico interno		X		4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12
Soporte técnico externo		X		3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Servicio de limpieza de planta		X	X	2	4	4	4	6	6	4	8	8	6	8	6	8	4	8	4	4	6	8	4	6	6	6
Servicio de mensajería de propio		X		3	6	6	6	9	9	6	12	12	9	12	9	12	6	12	6	6	9	12	6	9	9	9
Servicio de mensajería de externo		X		4	8	8	8	12	12	8	16	16	12	16	12	16	8	16	8	8	12	16	8	12	12	12

Fuente: Autores del proyecto.

Cuadro 6. (continuación)

Matriz de Análisis de Riesgo																																
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																												
	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento		Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado	Ausencia de documentación
					4	4	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	3	3	4	4	4	4	4	4
Dirección / Coordinación	X			4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Administración	X	X		4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Personal técnico		X		3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Recepción		X		2	8	8	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	6	6	8	8	8	8	8	8
Piloto / conductor			X	1	4	4	4	3	4	4	4	4	3	4	3	2	4	2	3	4	4	3	3	3	4	4	4	4	4	4
Informática / Soporte técnico interno		X		4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16
Soporte técnico externo		X		3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Servicio de limpieza de planta		X	X	2	8	8	8	6	8	8	8	8	6	8	6	4	8	4	6	8	8	6	6	6	8	8	8	8	8	8
Servicio de mensajería de propio		X		3	12	12	12	9	12	12	12	12	9	12	9	6	12	6	9	12	12	9	9	9	12	12	12	12	12	12
Servicio de mensajería de externo		X		4	16	16	16	12	16	16	16	16	12	16	12	8	16	8	12	16	16	12	12	12	16	16	16	16	16	16

Fuente: Autores del proyecto.

Figura 3. Análisis promedio de riesgo.

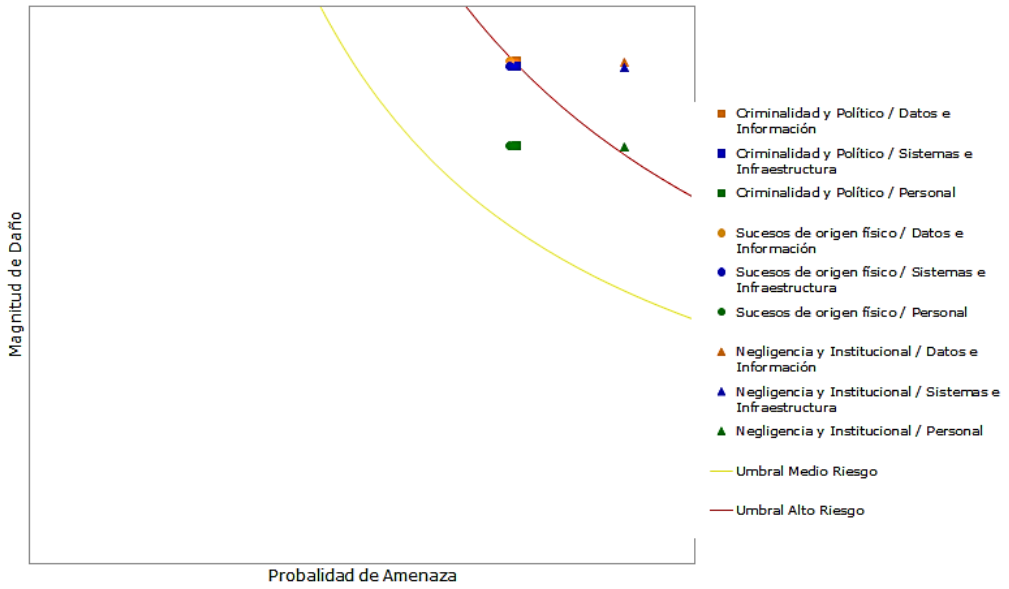
Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	**Sucesos de origen físico**	**Negligencia y Institucional**
Magnitud de Daño	**Datos e Información**	8.6	8.5	10.6
	Sistemas e Infraestructura	9.1	9.0	11.2
	Personal	7.3	7.2	8.9

Fuente: Autores del proyecto.

La probabilidad de que ocurran amenazas de tipo criminal, natural o por negligencia, se divide en tres (3) magnitudes de daño: baja, Mediana y Alta. La magnitud de daño baja se presenta cuando existen condiciones que hacen muy lejana la posibilidad de ataque. Mediana cuando existen condiciones que hacen poco probable un ataque en el corto plazo, pero que no son suficientes para evitarlo en el largo plazo, y Alta en casos donde el ataque es inminente, debido a que no existen condiciones internas y externas que impidan el desarrollo del ataque.

Figura 4. Análisis de factores de riesgo.



Fuente: Autores del proyecto.

La figura anterior, corresponde a los factores (actos criminales, sucesos físicos y negligencia) que originan o hacen efectiva la amenaza a los activos (Datos e información, sistemas e infraestructura y el personal) de la Alcaldía, evaluados en un umbral de riesgo.

Bajo: corresponde a una probabilidad de amenaza baja que origina una magnitud de riesgo igualmente baja, debido a que existen condiciones que hacen muy lejana la posibilidad de ataque, manteniendo un nivel aceptable de riesgo para los activos de la Alcaldía.

Medio: hace referencia a una probabilidad de amenaza mediana que origina una magnitud de riesgo igualmente mediana, debido a que existen condiciones que hacen poco probable un ataque en el corto plazo, pero no son suficientes para evitarlo en largo plazo, provocando una alerta de riesgo para los activos de la Alcaldía, la cual debe ser monitoreada y evaluada constantemente aplicando medidas correctivas que disminuyan la amenaza y la orienten a un nivel aceptable o nulo.

Alto: refleja una probabilidad de amenaza alta originando una magnitud de riesgo igualmente alta, donde el ataque es inminente, debido a que no existen condiciones internas y externas que impidan el desarrollo del ataque.

4.3 INFORME DE ACUERDO A LOS HALLAZGOS ENCONTRADOS EN LA ALCALDÍA MUNICIPAL DE LA PLAYA DE BELÉN, SEGÚN LA NORMA ISO 27002

Teniendo en cuenta la norma ISO 27002[28], la cual es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información, a continuación se dará un informe de los hallazgos encontrados en la Alcaldía Municipal de La Playa de Belén, asi:

Cuadro 7. Matríz de hallazgos, riesgos y controles.

Tema	Hallazgo	Riesgo	Nivel de ocurrencia	Área de impacto	Efecto	Responsable	Recomendaciones
1	La institución posee más de un sector responsable de los servicios de procesamiento de la información	-Dificultades para llevar a cabo estrategias y planes unificados relativos a la TI -Posible duplicación de esfuerzos y tareas	Ocasional	Toda la Alcaldía	Pérdida de dinero y atraso en la digitalización de la información.	Administración	Implementación del manual de políticas de seguridad en la información.
2	Las áreas informáticas identificadas dependen de una de las áreas usuarias	-Falta de independencia. -Incorrecta gestión de prioridades en la prestación de servicios	Ocasional	Toda la Alcaldía	Atraso en la digitalización de la información.	Área de informática	Implementación del manual de políticas de seguridad en la información.

[28] ISO 27002.es. Norma ISO 27002 (online). [España]: UNAD, 2012 [citado 26 ago., 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf

Cuadro 7. (continuación)

3	Las áreas informáticas identificadas carecen de estructura interna formalmente definida	-Falta de separación de funciones. -Desconocimiento, por parte del personal, de sus responsabilidades. -Dificultades ante eventuales necesidades de rendición de cuentas	Siempre	Toda la Alcaldía	Falta de organización estructural	Área de informática	Implementación del manual de políticas de seguridad en la información.
4	. Las áreas informáticas identificadas no disponen de planificación documentada y no dispone de planificación aprobada	-Falta de dirección y control de las actividades y proyectos informáticos encargados -Ineficiencia de los proyectos informáticos -"Malas" inversiones en TI -Disparidad entre los objetivos de la organización y de la TI	Siempre	Toda la Alcaldía	Protección deficient de la información	Área de informática	Implementación del manual de políticas de seguridad en la información.
5	Las áreas informáticas identificadas carece de procedimientos aprobados para el desarrollo y mantenimiento de sistemas	-Modificaciones no autorizadas sobre los Sistemas -Incorrecta administración de prioridades -Falta de aplicación de estándares de programación y documentación -Implementación de Sistemas no probados		Ocasional	Pérdida de la información Falta de orientación sobre las normas establecidas	Área de informática	Implementación del manual de políticas de seguridad en la información.
6	Las áreas informáticas identificadas carecen de procedimientos aprobados para la administración de la seguridad	-Accesos no autorizados a la información o los recursos de la Alcaldía -Inexactitud o falta de confiabilidad de los datos o Sistemas -Falta de disponibilidad de la información o recursos necesarios		Siempre	Falta de supervisión	Área de informática	Implementación del manual de políticas de seguridad en la información.
7	Las áreas informáticas identificadas carecen de plan de contingencias	-Interrupciones a la continuidad operativa del Organismo, con la consiguiente imagen negativa e incumplimiento de la misión asignada		Siempre	Pérdida de la información	Área de informática	Implementación del manual de políticas de seguridad en la información.

Cuadro 7. (continuación)

8	Las áreas informáticas identificadas carecen de procedimientos documentados de backup´s	-Pérdidas de información Interrupciones a la continuidad operativa del Organismo -Dependencia del personal que se encarga de la tarea		Ocasional	Pérdida de la información	Área de informática	Implementación del manual de políticas de seguridad en la información.
9	Las áreas informáticas identificadas carecen de procedimientos documentados para las actividades de soporte técnico. Asimismo carecen de procedimientos documentados para la gestión de licencias de software	Administración deficiente de prioridades, disconformidad de los usuarios, etc. Incumplimiento de la normativa aplicable.		Ocasional	Pérdida de dinero	Área de informática	Implementación del manual de políticas de seguridad en la información.
10	La institución no realiza auditorías internas de sistemas de información	Desequilibrio entre la informatización del organismo y la realización de auditorías.		Siempre	Pérdida de la información	Administración	Implementación del manual de políticas de seguridad en la información.

Fuente: Autores del proyecto.

4.4 PROPUESTA DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA ALCALDÍA MUNICIPAL DE LA PLAYA DE BELÉN

Las políticas de seguridad informática tienen como objetivo principal, establecer reglas sobre el uso de los sistemas informáticos y de comunicaciones de la Alcaldía municipal de La Playa de Belén, N.S., por parte de usuarios, administradores o terceros, proteger los recursos de información de la Entidad y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentals, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Basados en la norma ISO 27001, la cual describe cómo gestionar la seguridad de la información en una empresa o entidad, en este caso la Alcaldía municipal de La Playa de Belén. Dicha norma puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. Estas políticas buscan establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red y acceso físico; asegurar la implementación de las medidas de seguridad comprendidas en estas Políticas, identificando los recursos y las partidas presupuestarias correspondientes.

El diseño del manual de políticas de seguridad para la Alcaldía municipal de La Playa de Belén, se encuentra en el Anexo D.

4.4.1 Recomendaciones de políticas de seguridad de la información para la Alcaldía Municipal de La Playa de Belén. A continuación se presenta una serie de recomendaciones que podrán ser aplicadas cuando se aplique el manual de políticas de seguridad de la información en la Alcaldía Municipal de La Playa de Belén.

El Software utilizado es de uso interno y solo para ser utilizado en tareas de la prestación del servicio y procesos organizacionales.

No se debe entregar datos o reproducir total o parcialmente la información generada por la Entidad a personas ajenas o que no sean parte del proceso administrativo correspondiente.

El correo electrónico, internet e intranet son de uso exclusivo para realizar trabajos de la Entidad, se encuentra restringido el uso para otros fines.

Se prohíbe la descarga de archivos, transmisión o almacenamiento que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, etc. o que atente contra las buenas costumbres o principios, excepto que el trabajo lo amerite.

Cada funcionario será responsable por el mal uso del equipo de cómputo, incluyendo infecciones de virus.

Manejo apropiado de las impresiones:

Es muy importante tener presente las siguientes recomendaciones para el manejo de impresiones de documentos:

- Las impresoras sólo podrán ser utilizadas para imprimir documentos requeridos por la Entidad.

- Retirar los documentos que se envían a imprimir.

- Todo documento que quede en la impresora al final del día, debe ser eliminado.

- En caso del mal funcionamiento en una impresora, o que esté siendo mal utilizada, deberá informarse al área técnica.

- Cada área será la responsable de mantener los suministros correspondientes.

- El material impreso que contenga información sensible debe o No dejarlo descuidado en áreas abiertas o Ser removido de las impresoras sin demora
- Los impresos como cheques, certificados, contratos etc, deben ser almacenados en forma

segura y sólo proporcionados al personal autorizado.

Manejo apropiado de contraseña:

• Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.

• Las contraseñas se deben mantener confidenciales en todo momento.

• No compartir las contraseñas, con otros usuarios.

• Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.

• Selecciona contraseñas que no sean fáciles de adivinar.
• Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido.

• Cambia tus contraseñas regularmente.

• No utilizar la opción de almacenar contraseñas en Internet.

• No utilizar contraseña con números telefónicos, nombre de familia etc.

• No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

Crear una contraseña:

• Contraseñas fuertes contienen números y letras. Ver tabla adjunta.

• Utilizar contraseña que tengan por lo menos 8 caracteres

Manejo apropiado de control de Virus

La Alcaldía deberá definir un producto estándar licenciado en entorno de sus estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computo.

• El sistema de actualizaciones y detección diaria deberá estar automatizado a nivel central.

• Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus, al área de soporte.

• Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.
• Los dispositivos extraíbles, antes de ser usados deben ser escaneados con el antivirus.

Manejo de cuentas de sistemas

• Toda cuenta de acceso que se requiera modificar deberá ser solicitada a través de los administradores de los sistemas o en la opción de cambio de contraseña.

• El procedimiento de creación de cuentas, debe ser canalizado a través de los formularios correspondientes.

• Cuenta de red: Esta cuenta corresponde a la que utilizará cada usuario para conectarse a su equipo PC. Esta se solicitará al área encargada.

• Cuenta de Correo: Solicitarla formal al área encargada.

Manejo de acceso a internet

El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio. Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

• No navegar por sitios no confiables.

• Se prohíbe el uso de sitios de radios online.

• Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet.

• Se prohíbe el uso de sitios de chat (Messenger, chat, etc.).

• Se prohíbe el uso de internet para actividades ilícitas.

• Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.

• Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

• No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo)

• No permitir que el navegador de internet recuerde la contraseña automáticamente.

• Evitar participar en juegos de entretenimiento en línea.

• Si no está navegando por internet, cierre todas las ventanas abiertas.

• Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.

• Si requiere navegar en algún sitio bloqueado se deberá solicitar al área encargada.

Manejo de correo electrónico

• La Entidad en lo posible deberá contar con filtros para identificar y bloquear correos no deseados (Spam o Virus)

• El Correo electrónico institucional es de uso exclusivo para actividades relacionadas con la Entidad y queda restringido el uso para otros fines.

• Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

• La contraseña de correo debe ser cambiada periódicamente.

• No abrir link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).

• No completar datos personales en correos electrónicos sospechosos.

• Eliminar periódicamente los correos no deseados (spam o sospechoso).

Manejo de redes sociales

• En lo posible la Entidad deberá bloquear todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ellos, deberá enviar la solicitud formal al área correspondiente.

• Cabe destacar que cualquier foto subida o comentario en Facebook, twitter o en alguna red social es responsabilidad exclusiva del que la emite.

Manejo de software

• Se prohíbe la instalación que no cumpla con la las instrucciones del Área de Soporte y Operaciones.

• Los usuarios no deben instalar aplicaciones ni descargar aplicaciones que podrían provocar alguna vulnerabilidad o inestabilidad en los servicios.

• Toda solicitud debe ser canalizada por medio del área encargada de los sistemas de la Entidad.

Manejo de dispositivos móviles

Para garantizar la seguridad y estabilidad de la red y los dispositivos móviles, se describen algunos concejos y manejo adecuado, de los mismos:

- Los teléfonos móviles la Entidad se han adquirido específicamente para facilitar el desarrollo de actividades laborales relacionadas con la entidad y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales

- La instalación, configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área asignada para tal fin.
- Las actualizaciones de sistemas operativos de los dispositivos móviles, debe ser coordinado con el área encargada, que es la responsable de realizar las actualizaciones.

- Se debe mantener desactivada la red Wifi, Bluetooth, Infrarrojos, etc, en caso de que no esté siendo utilizada.

- Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el teléfono móvil. Si no está seguro del proceso debe comunicarse con el Área de Soporte.

- Es responsabilidad del funcionario reportar inmediatamente al Área de Soporte, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.

- Se debe solicitar al área de Soporte la configuración y acceso a los correos de la Entidad, a los teléfonos móviles donde exista servicio disponible y que pertenezcan a la institución.

- No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

- No acceder a los enlaces solicitados a través de SMS/MMS/Email podría ser código malicioso.

Manejo computadores portátiles

Para garantizar la seguridad y estabilidad de la red de la Entidad se describen algunos consejos y manejo adecuado.
- Todo computador portátil debe ser incorporado al dominio de la red de la Entidad, para esto sólo el área encargada.

- Los computadores portátiles de la Entidad se han adquirido específicamente para facilitar el desarrollo de actividades laborales. Su uso debe estar relacionado con las actividades del área a la cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales

• Los equipos portátiles deben permanecer en las instalaciones, durante los días y horarios hábiles de trabajo, pueden salir de las instalaciones, solo en el caso de utilizarlo en labores de la entidad.

• La instalación, configuración, modificación o eliminación de software sobre los equipos portátiles es responsabilidad exclusiva del área encargada.

• El área encargada tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado por la División Informática.

• La configuración, eliminación, modificación o cambio de sistema operativo es de responsabilidad del área encargada.

• La configuración e instalación de hardware de los equipos portátiles, es responsabilidad de área asignada para tal fin, según corresponda.

• Se debe mantener desactivada la red inalámbrica en caso de que no esté siendo utilizada.

• Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el equipo portátil. Si no está seguro del proceso debe comunicarse con el Área encargada.

• Es responsabilidad del funcionario reportar inmediatamente al Área encargada, cualquier daño o pérdida del equipo que le ha sido asignado.

• No insertar tarjetas de memoria sin haber comprobado previamente que están libres de vir us o de algún tipo de código malicioso.

5. CONCLUSIONES

Luego de realizado el proyecto y las actividades propuestas dentro de éste, se conocieron los distintos procesos informáticos realizados en las áreas pertenecientes a la Alcaldía Municipal de La Playa de Belén. Cabe resaltar que la Institución solo cuenta con siete dependencias, aún así se necesita de un control al acceso de los equipos de cómputo y demás información, ya que no existe restricción para el ingreso de personal, tampoco existen registros de acceso y la seguridad de los computadores es media.

Los datos obtenidos en este trabajo luego de realizada la encuesta, sirvieron para identificar algunos elementos de riesgos y fallas de seguridad informática, en la Alcaldía, dentro de los cuales se encontró que No existe un plan de capacitación permanente y coordinado que responda a las necesidades de la Alcaldía Municipal de La Playa de Belén, tampoco un plan de contingencia; el uso de medios de almacenamiento es escaso; y, el proceso de soporte técnico solo se hace cuando ya falla el equipo de cómputo.

Por medio de la presente investigación y de acuerdo a la norma ISO 27002, se pudieron evidenciar hallazgos en la Alcaldía Municipal de La Playa de Belén. De acuerdo a éstos, se formularon los riesgos que se corren, el nivel de ocurrencia en el que se encuentra el riesgo, el area de impacto, los efectos que producen y quién es el responsable de que ocurra o no ocurran los mismos. Al final se dio una recomendación general, la cual es la de implementar el manual de políticas de seguridad de la información, con el fin de corregir todos estos hallazgos y evitar correr riesgos en la información que se encuentra en la entidad.

Para la elaboración del diseño del manual de políticas de seguridad informática para la Alcaldía municipal de La Playa de Belén, se basó en la norma ISO 27001, la cual consiste en la creación de un Sistema de Gestión de la Seguridad de la Información. Esta norma debe ser aplicada en aquellas instituciones como la alcaldia, que desean resguardar sus activos de información. Se debe aclarar que la norma ISO 27002 es una guía de buenas prácticas que describe cuáles deben de ser los objetivos de control que se deben aplicar sobre la seguridad de la información. Por lo tanto, en el documento solo fue utilizada a la hora de evaluar los riesgos y hallazgos encontrados, mediante la aplicación de objetivos de control. Dichos objetivos han de ser cumplidos para garantizar la correcta implantación de las normas; así como el funcionamiento de la Alcaldía en cuanto a la seguridad de la información.

6. RECOMENDACIONES

Se requiere para mejorar el desempeño de la red de datos, la implementación de políticas de seguridad a los usuarios que acceden a la red de datos. Además de sistemas de seguridad informática que ayuden salvaguardar la integridad de la Red de datos de la Administración Municipal en cada uno de sus segmentos.

Es necesario realizar un informe de hallazgos, con el fin de que se identifiquen además los riesgos y las fallas de seguridad que se encuentren en la Alcaldía, para que se le de cumplimiento a los controles que se encuentran en el manual de seguridad de la información.

Presentar a la administración municipal encabezada por el alcalde, esta propuesta de Políticas de Seguridad de la Información para la Alcaldía Municipal de La Playa de Belén (N.S.), basada en la norma ISO/IEC 27002, para su respectiva aprobación e implementación.

BIBLIOGRAFÍA

ALCALDIA LA PLAYA DE BELEN. Historia de la Playa de Belén (online). 2 rev. [La Playa-Colombia]: 2010 [citado 01 sep., 2014]. Disponible en: www.laplayadebelen-nortedesantander.gov.co/

AZPEITIA FERNÁNDEZ, Almudena. Observación no-sistemática (online). 1 ed. [Madrid]: 2009 [citado 26 ago., 2014]. Disponible en: https://www.uam.es/personal_pdi/stmaria/jmurillo/Met_Inves_Avan/Presentaciones/Observacion_NoSistematica_(Trabajo).pdf

CUEVAS MARTINEZ, R. Puntos a cuidar en la información (online). 1 ed. [ ]: 2011. [citado 23 ago., 2014]. Disponible en: contenidosabiertos.academica.mx/jspui/.../puntos.a.cuidar.informacion.p...

ECHENIQUE GARCÍA, José Antonio. Auditoria en Informática, 2a Edición. Mc Graw Hill 225p.

ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. (online). 1 ed. [España]: Word Press, 2010 [citado 15 ago., 2014]. Disponible en: http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

GAR FINKEL, Simson y GENE, Spafford. Seguridad Práctica en UNIX e Internet, 2ª Edición. Mc. Graw Hill, 1999. 337p.

ISO 27002.es. Norma ISO 27002 (online). [España]: UNAD, 2012 [citado 26 ago., 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf

LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadoras, 2a Edición, Universidad de Jaen, Septiembre 1999. 323p.

MINISTERIO DE LA TIC. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

SEGURIDAD INFORMÁTICA. Historia de seguridad informática (online). 1 ed. [s.l.]: Informaticadomonline, 2012 [citado 20 ago., 2014]. Disponible en: http://informaticadomonline.designcloud24.com/seguridad-informatica/

UNEMI. Seguridad informática (online). 1 ed. [Ecuador]: Repositorio, 2012 [citado 26 ago., 2014]. Disponible en: http://hdl.handle.net/123456789/1251

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico (online). 3 rev. [Bogotá]: UNAD, 2013. [citado 20 ago., 2014]. Disponible en: http://www.unad.edu.co/gidt/index.php/leyesinformaticas

ZAMORA, Franyeidis. Seguridad informática (online) 1 ed. [s.l.]: Acantelys, 2009 [citado 1 nov., 2014]. Disponible en: http://cip.org.pe/imagenes/temp/tesis/40342005.pdf

ANEXOS

Anexo A. Encuesta dirigida al personal encargado del area de sistemas de la Alcaldía Municipal de La Playa de Belén, N.S.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
PLAN DE ESTUDIOS DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
ENCUESTA DIRIGIDA AL PERSONAL ENCARGADO DEL ÁREA DE SISTEMAS DE LA ALCALDIA MUNICIPAL DE LA PLAYA DE BELÉN, N.S.

Objetivo: Conocer la Seguridad de la Información en la Alcaldía municipal de La Playa de Belén.

(*Marque con una X su repuesta*)

1. ¿Tiene usted conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información? Sí __ No__

2. ¿Cuentan con un acuerdo de confidencialidad de la información? Sí__ No__

3. ¿Las áreas de la Alcaldía están debidamente identificadas o por lo menos el área donde usted labora? Sí__ No__

4. ¿Su área cuenta con controles de ingreso del personal? Sí__ No__

5. El área cuenta con:

Cámaras de Vigilancia	Sí __ No__
Extintores	Sí __ No__
Detectores de Humo	Sí __ No__
Alarmas	Sí __ No__
UPS (Fuente de Suministro Eléctrico)	Sí __ No__
Aire Acondicionado	Sí __ No__

6. Sabe usted si la Alcaldía cuenta con registros de:

Acceso al Personal	Sí __ No__
Acceso a Visitantes	Sí __ No__
Uso de los Sistemas	Sí __ No__
Servicios de Red	Sí __ No__

7. ¿Cuenta con mensajería electrónica interna para sus actividades? Sí __ No__

8. ¿El computador que usted utiliza cuenta con una contraseña para permitir el acceso del usuario a los sistemas? Sí __ No__

GRACIAS POR SU COLABORACIÓN !!!

Anexo B. Encuesta dirigida al personal de la Alcaldía Municipal de La Playa de Belén

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
PLAN DE ESTUDIOS DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
ENCUESTA DIRIGIDA AL PERSONAL DE LA ALCALDIA MUNICIPAL DE LA PLAYA DE BELÉN, N.S.

Objetivo: Conocer la Seguridad de la Información en la Alcaldía municipal de La Playa de Belén.

(*Marque con una X su repuesta*)

1. ¿Se realiza mantenimiento periódico de hardware y software? Sí __ No__

2. ¿La Alcaldía cuenta con controles contra software malicioso o espía (antivirus, antispyware, etc.)? Sí __ No__

3. ¿Realizan backup's (Copias de Seguridad de la Información)? Sí __ No__

4. ¿En qué medio se almacenan?
CD
Memorias USB
Impresiones
Otras _____

5. ¿Con que periodicidad se realizan?
Diariamente
Semanalmente
Mensualmente
Bimestralmente
Anualmente
Otras _____

6. ¿Cuenta con mensajería electrónica interna para sus actividades? Sí __ No__

7. ¿Sabe usted si la Alcaldía cuenta con seguridad en este tipo de mensajería? Sí __ No__

8. ¿El computador que usted utiliza cuenta con una contraseña para permitir el acceso del usuario a los sistemas? Sí __ No__

9. ¿Cuentan con programas para la encriptación (camuflar información a destinatarios no deseados) de datos? Sí __ No__

10. ¿La Alcaldía cuenta con un procedimiento formal para reportes de incidentes (robos de información, pérdida de datos, accesos no permitidos, etc.)? Sí __ No__

11. ¿Al presentarse un incidente de seguridad en la Alcaldía, se cuenta con un plan de contingencia? Sí __ No__

12. ¿Se investiga y recolectan evidencias sobre el incidente de seguridad de la información? Sí __ No__

GRACIAS POR SU COLABORACIÓN!!!

Anexo C. Infraestructura tecnología

Inventario de equipos de cómputo que se encuentran habilitados en la Alcaldía Municipal de La Playa de Belén

No	Nombre	DEPENDENCIA	Ubicación	Tipo	Marca	Modelo	Serie (S/N)	Estado
1	SAID ORTIZ ORTIZ	ARCHIVO Y ALMACÉN	ARCHIVO Y ALMACÉN	ESCRITORIO	QBEX	NO APLICA	NO TIENE	BUENO
2	PEDRO ANGARITA ALVAREZ	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	ARCHIVO Y ALMACÉN	PORTATIL	TOSHIBA	SATELLITE S55-A5279	6D100959M	BUENO
3	BERNARDO CLARO	SECRETRARÍA EJECUTIVA	SECRETRARÍA EJECUTIVA	ESCRITORIO	HP	COMPAQ 6000 PRO	MXJ01200TG	BUENO
4	RUBIELA CLARO	SECRETRARÍA EJECUTIVA	SECRETRARÍA EJECUTIVA	ESCRITORIO	COMPUMAX	NO APLICA	NO TIENE	REGULAR
5	HUMBERTO CLARO MANZANO	SISBEN	SISBEN	PORTATIL	TOSHIBA	SATELLITE S55-A5279	6D100685M	BUENO
6	HUMBERTO CLARO MANZANO	SISBEN	SISBEN	PORTATIL	ACER	ASPIRE 5735-6354	LXUA50X2819070512420 00	REGULAR
7	HUMBERTO CLARO MANZANO	SISBEN	SISBEN	ESCRITORIO	CLON	NO APLICA	NO TIENE	SIN USO
8	HUMBERTO CLARO MANZANO	SISBEN	SISBEN	ESCRITORIO	HURICANE	NO APLICA	SOEMWXPHSP1	SIN USO
9	MAYRA PEÑARANDA TORRES	FAMILIAS EN ACCION	FAMILIAS EN ACCION	ESCRITORIO	HP	COMPAQQ PRO 4300	MXL2291GG9	BUENO
10	MAYRA PEÑARANDA TORRES	FAMILIAS EN ACCION	FAMILIAS EN ACCION	PORTATIL	ACER	ASPIRE 5315-2142	LXALE0X0207470C71716 01	BUENO
11	STELLLA CLARO	FAMILIAS EN ACCION	FAMILIAS EN ACCION	ESCRITORIO	JANUS		140328251219	BUENO
12	MARIA ANGELICA LEON VELASQUEZ	SECRETARÍA DE HACIENDA Y SALUD	PREDIAL	ESCRITORIO	GLOGIC	NO APLICA	BTCR22200A19	BUENO
13	ANDREA PAOLA OVALLOS	SECRETARÍA DE HACIENDA Y SALUD	CONTABILIDAD	ESCRITORIO	COMPUMAX	NO APLICA	NO TIENE	BEUNO
14	ANDREA PAOLA OVALLOS	SECRETARÍA DE HACIENDA Y SALUD	SECRETARÍA DE HACIENDA Y SALUD	ESCRITORIO	QBEX	APOLO 4H00	B19111211277830	BUENO
15	ANDREA PAOLA OVALLOS	SECRETARÍA DE HACIENDA Y SALUD	SERVIDOR	ESCRITORIO	QBEX			BUENO
16	MARIA ANGELICA LEON VELASQUEZ	SECRETARÍA DE HACIENDA Y SALUD	SECRETARÍA DE HACIENDA Y SALUD	ESCRITORIO	HP	COMPAQ PRO 4300	MXL328159D	BUENO
17	LUISA FERNANDA GARCIA GARCIA	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	ESCRITORIO	HP	HP COMPAQ PRO 6300 SFF	MXL249177T	BUENO
18	EDWIN PEÑARANDA	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	ESCRITORIO	HP	COMPAQ PRO 4300	MXL2291GFS	BUENO
19	ALEXANDER ASCANIO BAYONA	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	ESCRITORIO	HP	COMPAQ PRO 4300	MXL2291GFV	BUENO
20	LEON ANGEL CLAROS EPULVEDA	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	ESCRITORIO	COMPAQ	COMPAQ PRO SG3313LA	CNX8202117	BUENO
21	YULIETH TARAZONA	COMISARIA DE FAMILIA	COMISARIA DE FAMILIA	ESCRITORIO	HP	HP COMPAQ dc5800	MXJ82200HQ	BUENO
22	MARCELA AREVALO SILVA	COMISARIA DE FAMILIA	COMISARIA DE FAMILIA	ESCRITORIO	HP	HP COMPAQ 6000 PRO	MXL01808LC	BUENO
23	GERSY ALONSO MONTAGUTH	COMISARIA DE FAMILIA	COMISARIA DE FAMILIA	ESCRITORIO	COMPUMAX	TODO EN UNO -UNNO MAX	HN87B00461000	BUENO
24	ANGELICA CLARO CLARO	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	CULTURA Y TURISMO	ESCRITORIO	GLOGIC	LOGIC 1320	AJ2002979000028	BUENO
25	LIGIA	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	BIBLIOTECA	ESCRITORIO	ACER	X6630G	PS00846267436002330100	BUENO
26	NATALIA BOBADILLA DURAN	SECRETARÍA DE PLANEACIÓN, INFRAESTRUCTURA Y DESARROLLO RURAL	PIT	ESCRITORIO	HP	COMPAQ PRO 4300	MXL32815BB	BUENO
27	LILIANA	SECRETARÍA DE HACIENDA Y SALUD	SALUD PUBLICA	ESCRITORIO	JANUS		140328251179	BUENO

PROCESADOR	R A M	Disco Du ro	Capac idad	Cantidad USB	SISTEMA OPERATIV O INSTALADO	OFFIMA TICA	ANTIVIR US	Marca	Model	Serie (S/N)	Estado
INTEL CORE I5	3GB	HITACH I	931 G B	6	Windows XP PROFESI ONAL	OFIFCE 2010	AVAST F REE	QBEX	NO APLICA	MF185BH0306110 1743	BUEN O
INTEL CORE I7	8GB	HITACH I GST	931 G B	3	WINDOWS 8	OFFICE 2010	AVAST F REE				
INTEL PENTIUM D UAL CORE	4GB	WDC	298 G B	10	WINDOWS 7 PROFESI ONAL	OFFICE 2007	AVAST F REE	HP	HP L1710	CNC746RNRN	BUEN O
INTEL CELERON 4 30	1GB	SAMSU NG	186 G B	8	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE	JANU S	1913LE	J1913LE12091902 242	BUEN O
INTEL CORE I7	8GB	HITACH I GST	931 G B	3	WINDOWS 7 ULTIMA TE	OFFICE 2010	AVAST F REE				
INTEL CORE 2 DU O	3GB	WDC	298 G B	3	WINDOWS XP PROFE SIONAL	OFFICE 2010	AVAST F REE				
INTEL CELERON	512 MB	MAXTO R	40 GB	4	WINDOWS XP PROFE SIONAL	OFFICE 2010	AVAST F REE	SAMS UNG	SYNCMAST ER 551	AN15HXBW53534 V	REGU LAR
INTEL PENTIUM 4	512 MB	MAXTO R	40 GB	4	WINDOWS XP PROFE SIONAL	OFFICE 2003	AVAST F REE				
INTEL CORE I5	4 G B	HITACH I	465 G B	8	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE	HP	HP LE2202X	3CQ2292G60	BUEN O
MOBILE INTEL CE LERON 540	2 G B	HITACH I	120 G B	3	WINDOWS VISTA UL TIMATE	OFFICE 2007	ESET SM ART 4				
INTEL CORE I7	4GB	TOSHIB A	1TB	8	WINDOWS 7 PROFESI ONAL	OFICCE 2010	AVG	JANU S	2015LE	J2015LE13112502 957	BUEN O
INTEL CORE I5	4 G B	SEATAG E	931 G B	7	WINDOWS 7 ULTIMA TE	OFFICE 2010	SIN ANTI VIRUS	SAMS UNG	S19B150N	HTJC700917	BUEN O
INTEL CORE 2 DU O	2 G B	SAMSU NG	298G B	6	WINDOWS XP PROFE SIONAL	OFFICE 2007	AVAST F REE	SAMS UNG	SYNCMAST ER	H9LQ614049	BUEN O
INTEL CORE I5	3GB	HITACH I	931 G B	6	WINDOWS XP PROFE SIONAL	OFFICE 2010	AVAST F REE	QBEX	MF185BH	MF185BH0306110 2097	BUEN O
INTEL CORE I5	3GB				Windows XP PROFESI ONAL	OFFICE 2007		QBEX		R1C65A001435	BUEN O
INTEL CORE I5	4 G B	HITACH I	465 G B	8	WINDOWS 7 PROFESI ONAL	OFICCE 2010	AVAST F REE		HP LV2011	CNC313PZJH	BUEN O
INTEL CORE I 7	4 G B	TOSHIB A	931 G B	8	WINDOWS 7 ULTIMA TE	OFFICE 2010	AVAST F REE	HP	HP LA2205	3CQ2280PJM	BUEN O
INTEL CORE I5	4 G B	HITACH I	465 G B	8	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE	HP	HP LV2202X	3CQ2292G3V	BUEN O
INTEL CORE I5	4GB	HITACH I	465 G B	8	WINDOWS 7 PROFESI ONAL	OFFICE 2010	SIN ANTI VIRUS	HP	HP	3CQ2292G51	BUEN O
DUAL CORE INTE L PENTIUM	2 G B	SAMSU NG	232 G B	4	WINDOWS 7 PROFESI ONAL	OFICCE 2010	AVAST F REE	COMP AQ	W17Q	CNC820RY9P	BUEN O
INTEL CORE 2 DU O	2 G B	SEATAG E	160 G B	8	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE	HP	HP COMPAQ LE1711	CNC005QJ3M	BUEN O
INTEL PENTIUM D UALCORE	4 G B	SEATAG E	298 G B	10	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE	ACER	AL1706	L460C1484001	BUEN O
INTEL PENTIUM R 2,7 GHZ	4 G B	Western Digital	465 G B	5	WINDOWS 7 PROFESI ONAL	OFFICE 2010	AVAST F REE				
INTEL CORE I5 3G HZ	4GB	SEATAG E	931 G B	6	WINDOWS 7 STARTE R	OFFICE 2010	AVAST F REE	SAMS UNG	S19B150	HTJC804001	BUEN O
INTEL CORE I7	4GB				WINDOWS 8	OFFICE 2013		ACER	Pantalla antire flejo 21,5	MMLXLAA00641 70724B4212	BUEN O
INTEL CORE I5	4GB		465G B		WINDOWS 7 PROFESI ONAL	OFFICE 2013	AVG	HP	LV2011	CNC313PY8L	BUEN O
INTEL CORE I7	4GB	TOSHIB A	1TB					JANU S	2015LE	52015LE13112500 581	BUEN O

Fuente: Autores del proyecto.

Marca	Serial	Estado	Marca	Serial	Estado	Marca	Serial	Estado	MARCA	SERIAL	ESTADO
QBEX	11090205919	BUENO	QBEX	1E56170	REGULAR	EPSON L210	S25K322377	BUENO	STARTEC	721107300097	
COMPAQ	FF8180088Y	BUENO	HP	417441002		EPSON L210	S25K031010	BUENO	STARTEC	521402301085	
HP	BAUDU0JVBYD27L	BUENO	COMPUMAX	72101905NF	BUNEO	EPSON L210	S25K164377	BUENO			
						EPSON L210	S25K322414	BUENO			
DELUX	NZ8DLFAK900	BUENO	GENIUS	X3C8295890072							
HP	BAUDU0OGA2U0LI	BUENO	HP	537748001	BUENO	HP OFFICEJET 4500	CN15EF31M9	BUENO	STARTEC	521402300985	BUENO
JANUS	JSKBMSCOMBO1266346	BUENO	JANUS	JSKBMSCOMBO1266346	BUENO	HP LASERJET M1212 nf mfp	CN69C9N097	BUENO	STARTEC	721107300103	BUENO
GENIUS	XEC207035940	BUENO	GENIUS	XEC207035940	BUENO	EPSON FX-2190	FCTY122722	BUENO	STARTEC	721107300100	BUENO
GENIUS	ZM7902139967	BUENO	GENIUS	151322402728	BUENO	SAMSUNG ML-2240	1467BKDQ610013X	BUENO	UNITEC	NO TIENE	BUENO
QBEX	1E56170	BUENO	QBEX	NO TIENE	BUENO	EPSON L210	S25K149794	BUENO	STARTEC	721107300117	BUENO
DELUX	NZ8DLFAK900	BUENO	QBEX	IE56170					STARTEC	521402301084	
HP	BDAEV0Q5Y4OAB4	BUENO	HP	600553002	BUENO	HP LASERJET P6006dn	VND3C50067	BUENO	STARTEC	541402301104	BUENO
HP	BDAEV0QVB3N91Y	BUENO	HP	FCGLH0D9W3KA0A	BUENO	XEROX PHASER 3117	L92391538	BUENO	STARTEC	521207300815	DAÑADA
HP	BAUDU0OGA2U0LH	BUENO	HP	FCGLH0DDR2UTIG	BUENO	EPSON L210 - SAMSUNG ML 2160	S25K064986 - 27BMB8GC3F0040B	BUENO - TONER DAÑADO	ESTABILIZADOR VOLTRONIC	NO TIENE	BUENO
GENIUS	XP11AS815678	BUENO	HP	FCGLH0D9W2QFLZ	BUENO	SAMSUN ML 2165W	Z7C2B8GC3B00FPZ	BUENO	NO TIENE		
HP	BAUDU0OGA2U74G	BUENO	COMPAQ	FF0817000B30	BUENO	SAMSUNG ML 2160	Z7BMB8GC8A0086Z	BUENO	ESTABILIZADOR VOLTRONIC	NO TIENE	BUENO
HP	BAUDU0JVBYGEOG	BUENO	HP	FATSQ0B9WYPKH9	BUENO	ML-2165W	Z7C2B8GC3B00L4D		ESTABILIZADOR-PROELECTRONIC	NO TIENE	BUENO
GENIUS	ZM8702210726	BUENO	GENIUS	151226601181					YPCOM	507140300450	BUENO
COMPUMAX	01405314NF	BUENO	COMPUMAX	01405314NF	BUENO	EPSON L210	S25K022136	BUENO DONACION IFINORTE	YPCOM	84103310	MALO
GENIUS	XEC207036031	BUENO	GENIUS	XEC207036031	BUENO				STARTEC	521207301091	BUENO
ACER	DKUSB1P03K4120068DK701	BUENO	ACER	DC1121100742016238K701	BUENO	HP DESKJET D1400	VN82D3201W	BUENO	ESTABILIZADOR-MICROMAR	770324073126	BUENO
HP	BDADEV0Q5Y407VO	BUENO	HP	600553-002	BUENO						
JANUS	7709990622256	BUENO	JANUS	7709990622256	BUENO	HP DESKJET D1460	VN82C32057	BUENO	ARTELECTRO	NO TIENE	BUENO

Fuente: Autores del proyecto.

Host Name	Direccion IP	Direccion MAC	TECNICO	FECHA
ALMACEN PC6	DINAMICA	00-30-67-C6-1C-18		19-feb-14
TOSHIBAS55	DINAMICA	7C-05-07-D3-39-24		19-feb-14
ALCALDIA-PC	DINAMICA	00-0F-FE-F6-02-58		19-feb-14
SECALCALDIA2-PC	DINAMICA	00-1E-90-90-72-13		19-feb-14
Sisben-PC	DINAMICA	7C-05-07-D3-38-61		19-feb-14
sisben	DINAMICA	00-21-6B-11-39-5A		19-feb-14
SISBEN2		00-13-8F-1D-AD-20		19-feb-14
		00-0A-E6-D2-3C-D4		19-feb-14
FAMILIAENACCION	DINAMICA	75-E3-B5-AF-78-13		19-feb-14
USER-PC	DINAMICA	00-1B-38-6F-11-23		19-feb-14
FamiliasEnAccio	DINAMICA	74-D4-35-4C-92-18		19-ene-15
Predial-PC	DINAMICA	00-1E-8C-F5-57-12		20-feb-14
PC4	DINAMICA	00-21-97-DB-76-25		20-feb-14
	DINAMICA	00-30-67-C6-10-2A		20-feb-14
sec-HP	DINAMICA	78-E3-B5-C0-F9-36		21-feb-14
Planeacion-PC	DINAMICA	10-60-4B-5D-26-E9		24-feb-14
MAQ02	DINAMICA	78-E3-B5-AF-76-A0		24-feb-14
MAQ03	DINAMICA	78-E3-B5-AF-77-4A		25-feb-14
Planeacion1	DINAMICA	00-1C-25-84-90-07		25-feb-14
InspeccionPlic	DINAMICA	00-1F-29-D3-5C-AC		25-feb-14
COMISARIADEFAMI	DINAMICA	78-E7-D1-86-E6-8C		25-feb-14
ComisariaFamilia	DINAMICA	50-E5-49-6D-51-17		27-feb-14
USUARIO-PC	DINAMICA	90-2B-34-B3-19-84		04-mar-14
	DINAMICA	30-0E-D5-BD-CA-5C		19-ene-15
	DINAMICA	78-E3-B5-C0-EE-81		19-ene-15

Fuente: Autores del proyecto.

Anexo D. Manual de políticas de seguridad informática
La Playa de Belén, N.S.

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

ALCALDIA MUNICIPAL LA PLAYA DE BELÉN

2015

CONTENIDO

ANEXOS

FORMATOS

1. INTRODUCCIÓN

La Alcaldía municipal de La Playa de Belén, Norte de Santander identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, razón por la cual es necesario que la entidad establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por la Alcaldía**.** Para la elaboración del mismo, se toman como base la norma ISO 27001:2005 y las recomendaciones del estándar ISO 27002:2005.

Las políticas incluidas en este documento se constituyen como parte fundamental de la seguridad informática de la Alcaldía de La Playa y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La Seguridad de la Información es una prioridad para la Alcaldía y por tanto es res ponsabilidad de todos velar porque no se realicen actividades que contradigan la e sencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas de Seguridad Informática de la Alcaldía de La Playa de Belén, N.S., con el fin de regular la gestión de la seguridad de la información al interior de la Entidad.

3. ALCANCE

Las políticas de Seguridad de la Información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la Alcaldía de La Playa de Belén, N.S., para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. RESPONSABILIDAD Y AUTORIDAD

El Alcalde, asigna las funciones relativas a la Seguridad Informática de la Alcaldía de La Playa de Belén, al jefe del área de informática (en su defecto a quien él proponga y tenga las capacidades para tal tarea), en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en las presentes Políticas.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan del presente manual.

Todo el personal, sea cual fuere su nivel jerárquico, es responsable de la implementación de estas Políticas de Seguridad de la Información dentro de sus dependencias, así como del cumplimiento de dichas Políticas por parte de su equipo de trabajo.

Las máximas autoridades de la Alcaldía municipal de La Playa de Belén, deben aprobar estas políticas y son responsables de sus modificaciones.

5. POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

En la Alcaldía municipal de La Playa de Belén la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, la Alcaldía municipal implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en la alcaldía municipal; este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información.

La alcaldía municipal se compromete a implementar y mantener como parte del desarrollo de su modelo de gestión, programas y planes de capacitación, entrenamiento y concientización en toda la entidad sobre Seguridad de la Información, de manera que se minimice la ocurrencia y el impacto de incidentes de seguridad de la información.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

5.1. Compromiso de la Dirección

El Alcalde municipal aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Entidad.

El Alcalde municipal y el cuerpo directivo de la Entidad demostrará su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este documento a todos los funcionarios de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las Políticas de Seguridad de la Información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

5.2. Regulación

Las políticas contenidas en este documento deberán ser conocidas, aceptadas y cumplidas por todos los funcionarios y contratistas de la Alcaldía municipal. El incumplimiento de las mismas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario interno para los funcionarios y se convertirá en una causa válida de terminación del contrato con los contratistas, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

5.3. Políticas generales de seguridad de la información

La Alcaldía municipal ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1. El Comité Directivo del Sistema Integrado de Gestión será el responsable del mantenimiento, revisión y mejora de las políticas, normas y acciones de Seguridad de la Información en la entidad.
2. Los activos de información de la entidad serán identificados y clasificados para establecer los mecanismos de protección necesarios.
3. La entidad definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.
4. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de la entidad.
6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la entidad.
7. Es responsabilidad de todos los funcionarios y contratistas de la entidad reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.
9. La entidad contará con un Plan de Contingencia que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

Adicionalmente la entidad cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

6. ORGANIZACIÓN DE LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN
REF.: ISO/IEC 27001:2005 A.6

6.1. Coordinación de la función de Seguridad de la Información

[ISO/IEC 27001:2005 A.6.1.2; A.6.1.3]

La Alcaldía municipal establece un Comité de Seguridad de la Información (Comité Directivo del SIG), conformado por un grupo interdisciplinario de directivos (Secretarios de Despacho), responsable del análisis, revisión y centralización de todas las acciones referidas a la gestión de Seguridad de la Información de la Institución y de mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos del negocio.

Sus funciones y responsabilidades son descritas en el Anexo 1.

6.2. Autorización para el uso de infraestructura de información

[ISO/IEC 27001:2005 A.6.1.4]

La Alcaldía municipal establece que la adquisición de infraestructura nueva para el procesamiento de información (equipos, software, aplicaciones e instalaciones físicas) debe ser analizada y revisada por el Comité de Seguridad y el Secretario de Despacho del área directamente afectada. Esta autorización será de acuerdo a los procedimientos respectivos y asegurará que las políticas de seguridad sean cumplidas en su totalidad.

6.3. Acuerdos de confidencialidad

[ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de la entidad y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la entidad a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

6.4. Contacto con las autoridades y con grupos de interés especiales

[ISO/IEC 27001:2005 A.6.1.6; A.6.1.7]

La entidad debe establecer y mantener una relación cercana con autoridades relevantes (policía, bomberos, defensa civil), así como con grupos de interés o foros de especialistas en seguridad, para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información.

6.5. Auditorías internas

[ISO/IEC 27001:2005 A.6.1.8]

La Alcaldía municipal realizará revisiones internas a su Modelo de Gestión de Seguridad de la Información con el fin de determinar si las políticas, actividades, procedimientos y controles establecidos dentro del sistema están conformes con los requerimientos institucionales, requerimientos de seguridad, regulaciones aplicables, y si éstos se encuentran implementados y mantenidos eficazmente. Estas auditorías se ejecutan según lo establecido en el programa de auditorías definido por la Oficina de Control Interno y en caso de ser necesario se pueden programar revisiones parciales o totales sobre un proceso, área, etc. con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

Las auditorias del Modelo de Gestión de Seguridad de la Información de la entidad serán desarrolladas por el Jefe de Control Interno manteniendo un criterio de revisión independiente.

6.6. Riesgos relacionados con terceros

[ISO/IEC 27001:2005 A.6.2.2]

La entidad identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

7. GESTIÓN DE ACTIVOS DE INFORMACIÓN

REF.: ISO/IEC 27001:2005 A.7

7.1. Inventario de activos de información

[ISO/IEC 27001:2005 A.7.1.1; A.7.1.2]

Las diferentes dependencias con el fin de garantizar la administración y control sobre los activos de la Entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del Modelo de Gestión de Seguridad de la Información, de acuerdo con lo establecido en los "*Lineamientos de Inventario y Clasificación de Activos de Información***"**. Anexo 2.

En este inventario se debe identificar el propietario del activo, quien debe asegurar que la información y los activos asociados con su procesamiento están clasificados de manera apropiada, así como de establecer los controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

7.2. Uso adecuado de los activos

[ISO/IEC 27001:2005 A.7.1.3] [Acuerdos 047 y 056 de 2000 Archivo General de la Nación]

La información, archivos físicos, los sistemas, los servicios, y los equipos (ej. PCs, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la Alcaldía, son activos de la entidad y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio.

Así mismo, la Alcaldía podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este documento y en cualquier proceso legal que se requiera.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Secretarios de Despacho o Jefes de Dependencia.

La consulta de expedientes o documentos que reposan en las oficinas y/o dependencias de la Alcaldía se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable y/o custodio de aquellos.

El funcionario y/o contratista se compromete a cumplir con los procedimientos establecidos para el servicio y consulta de documentos físicos (Gestión Documental).

Los funcionarios y terceros tienen derecho a que se le expidan copias de los documentos que reposan en los archivos, siempre y cuando la reproducción no afecte al documento original. En todo caso el solicitante pagará los costos de reproducción de acuerdo a las tarifas señaladas por la entidad.

Las restricciones y reserva de los documentos físicos estarán determinadas por la importancia de los mismos y por el daño o alteración de tipo biológico, químico y físico que pudieran tener los documentos que impida el préstamo de los mismos.

El Secretario de Despacho o el Técnico de Archivo serán quienes determinen el carácter de reserva o restricción de los documentos físicos.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "*Acuerdo de Confidencialidad de la Información*" (anexo 3), donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos en el presente documento para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad" y se procederá de acuerdo con el "Procedimiento investigación de Incidentes de Seguridad" del parágrafo 8.5 del presente documento.

7.2.1. Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de la Alcaldía municipal, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Alcaldía municipal.

- El intercambio no autorizado de información de propiedad de la Alcaldía municipal, de sus clientes y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y Comité Directivo del SIG, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) La Alcaldía municipal debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los funcionarios y terceros, al igual que los contratistas, no pueden asumir en nombre de la Alcaldía municipal, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la entidad.

7.2.2. Correo electrónico

Los funcionarios y terceros autorizados a quienes la entidad les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la entidad, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de la entidad y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por el Responsable de la Estrategia GELT en la entidad, de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el Responsable de la Estrategia GELT en la entidad.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la entidad, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de la entidad como punto de contacto en comunidades interactivas de contacto social, tales como *facebook* y/o *myspace*, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el Jefe de Dependencia y el Responsable de la Estrategia GELT en la entidad.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que la alcaldía proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del Responsable de la Estrategia GELT en la entidad. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a

nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

h) Toda información de la entidad generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas de PDF. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la entidad y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

7.2.3. Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por la Alcaldía municipal a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la Alcaldía es responsabilidad de la Secretaría de Planeación y Obras, y por tanto son los únicos autorizados para realizar esta labor directamente o a través de un contratista. Así mismo, los medios de instalación de software deben ser los proporcionados por la Alcaldía a través de esta dependencia.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo (PCs) relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Secretaría de Planeación y Obras en coordinación con la Oficina de Control Interno.

c) La Oficina de Control Interno debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios.

   Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los funcionarios y terceros autorizados por la Oficina de Control Interno, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica de la entidad.

e) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la Alcaldía; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Oficina de Control Interno.

f) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Oficina de Control Interno y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

7.3. Clasificación de la información

[ISO/IEC 27001:2005 A.7.2]

La Alcaldía municipal con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o clientes, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Toda la información de la entidad debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el Comité Directivo del SIG.

Los niveles de clasificación de la información definidos en la Alcaldía son:

- Pública
- Confidencial
- Restringida

Los criterios, niveles de clasificación y aplicación se encuentran detallados en los "*Lineamientos de Inventario y Clasificación de Activos de Información*" Anexo 2 y estos son revisados y aprobados de manera periódica por el Comité Directivo del SIG.

Los propietarios de los activos de información son los responsables de identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación.

8. SEGURIDAD EN EL RECURSO HUMANO

REF.: ISO/IEC 27001:2005 A.8

8.1. Responsabilidades del personal

[ISO/IEC 27001:2005 A.8.1.1]

Todos los funcionarios de la Alcaldía municipal de La Playa de Belén y terceros que tengan la posibilidad de acceder a la información de la entidad y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información de la Alcaldía municipal. De igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

Todos los funcionarios de la Alcaldía municipal de La Playa de Belén deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la entidad.

8.2. Selección de personal

[ISO/IEC 27001:2005 A.8.1.2]

Toda vinculación laboral realizada por de la Alcaldía municipal de La Playa de Belén se rige por las leyes de la República de Colombia y por lo dispuesto en el Código Sustantivo del Trabajo.

Todo funcionario contratado por de la Alcaldía municipal de La Playa de Belén es seleccionado adecuadamente, de acuerdo con los requerimientos de cada cargo y siguiendo las tareas descritas en el *Procedimiento de Gestión del Talento Humano*. Sin importar el método de contratación, todo funcionario recibe y acepta las políticas de seguridad de la entidad.

La Alcaldía municipal de La Playa de Belén verifica la información brindada durante el proceso de vinculación de los funcionarios; de igual forma, debe realizar estudio de seguridad a todos los candidatos a cargos de la entidad.

8.3. Términos y condiciones de empleo

[ISO/IEC 27001:2005 A.8.1.3]

Todos los funcionarios y aquellos terceros definidos por la Alcaldía municipal de La Playa de Belén, deben acoger las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son entregados, previo a la entrega de éstos y teniendo en cuenta que estos términos y responsabilidades son extensibles fuera de la entidad.

Todos los funcionarios y aquellos terceros que tengan acceso a información sensible de la entidad o a la infraestructura tecnológica que contenga este tipo de información, deben firmar, previamente a la entrega del acceso, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual se debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requerimiento.

Adicionalmente, con funcionarios y terceros deben quedar establecidos acuerdos en aspectos como propiedad intelectual, protección de la información y leyes aplicables.

8.4. Capacitación y entrenamiento en seguridad de la información

[ISO/IEC 27001:2005 A.8.2.2]

La Alcaldía municipal de La Playa de Belén debe asegurar que todos los funcionarios que tengan definidas responsabilidades en el Modelo de Gestión de Seguridad de la Información, son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.

De igual forma, todos los funcionarios y, cuando sea relevante, los terceros, tendrán un proceso formal de concientización, mediante el cual se capacitará sobre las políticas de seguridad de la entidad y los riesgos conocidos a los que se puede ver expuesta, en caso que estas no se cumplan.

Los programas de concientización, educación y entrenamiento se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

8.5. Procesos disciplinarios

[ISO/IEC 27001:2005 A.8.2.3]

En el caso de identificarse un incidente de seguridad, este será registrado e investigado con el fin de determinar las causas y responsables de acuerdo con el "*Lineamientos de investigación de Incidentes de Seguridad*" Anexo 4; posteriormente, la Alcaldía municipal de La Playa de Belén tomará las acciones pertinentes para el funcionario y/o tercero vinculados con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la entidad dicho incidente.

8.6. Finalización de vinculación laboral o cambio de rol

[ISO/IEC 27001:2005 A.8.3]

El Secretario de Gobierno, en conjunto con el jefe directo del funcionario y/o responsable del tercero (supervisor contractual), son los encargados del proceso de terminación de labores y aseguran que todos los activos propios de la organización sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de "Retiro".

En caso que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su nuevo rol.

El Secretario de Gobierno, adicionalmente, se encarga de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos de personal.

9. SEGURIDAD FÍSICA Y AMBIENTAL

REF.: ISO/IEC 27001:2005 A.9

9.1. Control de acceso físico

[ISO/IEC 27001:2005 A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Las áreas de carga, descarga, entrega de suministros y demás puntos de acceso a las instalaciones de la Alcaldía municipal de La Playa de Belén, deben ser controladas y en lo posible separadas de las áreas seguras para evitar el acceso no autorizado a estas últimas.

Los funcionarios y terceros de la Alcaldía municipal de La Playa de Belén, así como los visitantes, deben portar su identificación de manera visible durante el tiempo que permanezca dentro de las instalaciones de la entidad.

Los privilegios de acceso a las áreas seguras y restringidas de la Alcaldía municipal de La Playa de Belén deben ser periódicamente revisados, actualizados y monitoreados.

9.2. Protección y ubicación de los equipos

[ISO/IEC 27001:2005 A.9.2]

Los equipos que hacen parte de la infraestructura tecnológica de la Alcaldía municipal de La Playa de Belén tales como, servidores, routers, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, plantas telefónicas, así como estaciones de trabajo y

dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de la Alcaldía municipal de La Playa de Belén no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

La Alcaldía municipal de La Playa de Belén mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

La Alcaldía municipal de La Playa de Belén debe proveer suministros y equipamiento de soporte como electricidad, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual manera, la Alcaldía municipal de La Playa de Belén debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a esta infraestructura tecnológica.

9.3. Retiro y seguridad de equipos y medios de información fuera de las instalaciones

[ISO/IEC 27001:2005 A.9.2.5; A.9.2.7]

Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos de la Alcaldía municipal de La Playa de Belén que se encuentren fuera de las instalaciones de la organización, siguiendo las siguientes directrices:

- Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
- Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- Los equipos de la Alcaldía municipal de La Playa de Belén deberán contar con un seguro (póliza) que los proteja de robo.
- En caso de pérdida o robo de un equipo de la Alcaldía municipal de La Playa de Belén, se deberá informar inmediatamente superior inmediato para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

El retiro de equipos de cómputo, periféricos, dispositivos de almacenamiento, software e información considerada crítica propiedad de la Alcaldía municipal de La Playa de Belén, fuera de las instalaciones de la entidad debe seguir los procedimientos establecidos por la Secretaría de Gobierno, la Secretaría de Planeación y Obras y la Oficina de Archivo y Almacén.

9.4. Eliminación o reutilización segura de equipos y medios

[ISO/IEC 27001:2005 A.9.2.6]

La Alcaldía municipal de La Playa de Belén debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

Cuando un equipo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información de la Alcaldía municipal de La Playa de Belén que allí se encuentre almacenada. Luego el equipo deberá ser sometido a un proceso de eliminación segura de la información sensible almacenada y del software instalado, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

REF.: ISO/IEC 27001:2005 A.10

10.1. Documentación de procedimientos operativos

[ISO/IEC 27001:2005 A.10.1.1]

Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica de la Alcaldía municipal de La Playa de Belén. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

10.2. Control de cambios

[ISO/IEC 27001:2005 A.10.1.2]

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar riesgos asociados que pueden afectar la operación de la entidad.

Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de Seguridad (Comité de Coordinación del SIG), el cual debe establecer los requerimientos de seguridad necesarios conforme a las políticas establecidas por la Alcaldía municipal de La Playa de Belén, que tengan como fin evitar un impacto adverso en las operaciones de la entidad.

10.3. Segregación de funciones

[ISO/IEC 27001:2005 A.10.1.3]

Toda tarea en la cual sus funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

- Todos los sistemas de disponibilidad crítica o media de la entidad, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.
- Los módulos ejecutables de software (cuando se adquiera) nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.
- El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.
- Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

10.4. Separación de los ambientes de desarrollo, prueba y producción

[ISO/IEC 27001:2005 A.10.1.4]

La Alcaldía municipal de La Playa de Belén ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

Dado lo anterior, los ambientes establecidos por la Alcaldía municipal de La Playa de Belén se definen así:

- *Ambiente de Desarrollo*: Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.
- *Ambiente de Pruebas*: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos y realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de la Alcaldía municipal de La Playa de Belén.

- *Ambiente de Producción*: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios

para la ejecución de las operaciones de la Alcaldía municipal de La Playa de Belén. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.

A través de las políticas de control de acceso físico y lógico definidas por la entidad, se controla el acceso a cada uno de los ambientes. Adicionalmente, los ambientes de desarrollo, pruebas y producción deben estar totalmente separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

La entidad debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados.

La entidad debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

10.5. Gestión de la capacidad

[ISO/IEC 27001:2005 A.10.3.1]

La Alcaldía municipal de La Playa de Belén mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

Los resultados de dichas mediciones serán analizados y presentados al Comité de Seguridad (Comité Directivo del SIG) y en caso de ser necesario la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos.

10.6. Aceptación de sistemas

[ISO/IEC 27001:2005 A.10.3.2]

La Alcaldía municipal de La Playa de Belén debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software son clara y adecuadamente definidos, documentados, y aprobados acordes a las necesidades de la entidad. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y funcionales establecidas por la entidad.

10.7. Protección contra software malicioso

[ISO/IEC 27001:2005 A.10.4]

La Alcaldía municipal de La Playa de Belén establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del Comité de Seguridad de la información autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente. La Oficina de Control Interno auditará el cumplimiento en el uso de las herramientas de seguridad.

Así mismo, La Alcaldía municipal de La Playa de Belén define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la Alcaldía municipal de La Playa de Belén.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Este sólo podrá ser utilizado, si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por el Comité de Seguridad de Información.

10.8. Copias de respaldo

[ISO/IEC 27001:2005 A.10.5]

La Alcaldía municipal de La Playa de Belén debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el Comité de Seguridad de Información y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la entidad, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La Alcaldía municipal de La Playa de Belén establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

10.9. Gestión de medios removibles

[ISO/IEC 27001:2005 A.10.7]

El uso de medios de almacenamiento removibles (ejemplo: CD, Dvd, USB, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la Alcaldía municipal de La Playa de Belén, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

El Comité de Seguridad de Información es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de la Alcaldía municipal de La Playa de Belén sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la Alcaldía municipal de La Playa de Belén que este contiene.

El almacenamiento, etiquetado y eliminación de cualquiera de estos medios de almacenamiento, debe estar de acuerdo con el esquema de clasificación y seguir los *"Lineamientos de Inventario y Clasificación de Activos de Información"* Anexo 2.

10.10. Intercambio de información

[ISO/IEC 27001:2005 A.10.8]

La Alcaldía municipal de La Playa de Belén firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de la Alcaldía municipal de La Playa de Belén es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada, cuyo uso aceptable se especifica en la política "7.2 Uso adecuado de los activos".

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

Los medios transportados fuera de las instalaciones de la Alcaldía municipal de La Playa de Belén, deberán cumplir con los controles establecidos en los *"Lineamientos de Gestión de Medios e Información en Tránsito"* Anexo 4.

10.11. Comercio y transacciones electrónicas

[ISO/IEC 27001:2005 A.10.9]

La Alcaldía municipal de La Playa de Belén, para el desarrollo de sus actividades de comercio y transacciones electrónicas, cuando se implementen, debe definir y establecer mecanismos para generar conexiones y transferencias de información seguras, de acuerdo con la legislación nacional y las demás regulaciones aplicables.

Los servicios de comercio electrónico deben establecer los requerimientos necesarios para proporcionar a los usuarios la información pertinente sobre las transacciones en línea, tal como las condiciones y costos de la transacción, así como las medidas de seguridad pertinentes.

Se debe expedir un soporte, en papel o por medios electrónicos, al momento de la realización de cada transacción. Dicho soporte deberá contener al menos la siguiente información:

- Fecha, hora (hora y minuto).
- Código del equipo (para operaciones por Internet: la dirección IP desde la cual se hizo la misma. para operaciones con dispositivos móviles: el número desde el cual se hizo la conexión).
- Número de la transacción.
- Costo de la operación para el cliente o usuario.
- Tipo de operación.
- Entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan la operación.

Con el fin de proteger la información disponible públicamente, se deben implementar mecanismos que permitan verificar constantemente que no sean modificados los enlaces (links) del sitio Web, ni suplantados los certificados digitales, ni modificada indebidamente la resolución de sus DNS.

10.12. Monitoreo del uso de los sistemas

[ISO/IEC 27001:2005 A.10.10]

La Alcaldía municipal de La Playa de Belén, con el fin de garantizar la seguridad de su información, debe brindar los mecanismos y controles adecuados para detectar las actividades de procesamiento de información no autorizadas.

Las aplicaciones que hacen parte de la infraestructura para el procesamiento de información, comunicaciones y seguridad de la Alcaldía municipal de La Playa

de Belén deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

La Alcaldía municipal de La Playa de Belén, mediante la metodología de análisis de riesgos establecida para la seguridad de la información, debe identificar el nivel de monitoreo requerido para las aplicaciones y dispositivos tecnológicos y establecer los controles necesarios para la mitigación de dichos riesgos.

Si en el proceso de la revisión de los archivos de registro de eventos (logs) se llegase a evidenciar la ocurrencia de un incidente de seguridad, se determinará el nivel de criticidad del incidente y se seguirán las disposiciones definidas en los *“Lineamientos investigación de Incidentes de seguridad” Anexo 4.*

A través de la definición de perfiles de acceso, todos los registros de auditoría generados por los sistemas de información de la Alcaldía municipal de La Playa de Belén son protegidos de accesos y modificaciones no autorizadas, razón por la cual todos los registros sólo mantienen privilegios de lectura.

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, todos los relojes de los sistemas informáticos de la Alcaldía municipal de La Playa de Belén deben estar sincronizados.

11. CONTROL DE ACCESO

REF.: ISO/IEC 27001:2005 A.11

11.1. Control de acceso lógico

[ISO/IEC 27001:2005 A.11.1]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de la Alcaldía municipal de La Playa de Belén debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y que se definan por las diferentes dependencias de la entidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de la Alcaldía municipal de La Playa de Belén asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización, los cuales deben ser revisados de manera periódica por la Oficina de Control Interno de la Alcaldía.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros e implementada por el Comité de Seguridad de la Información.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de la Alcaldía municipal de La Playa de Belén, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

11.2. Gestión de contraseñas de usuario

[ISO/IEC 27001:2005 A.11.2.3]

Todos los recursos de información críticos de la Alcaldía municipal de La Playa de Belén tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por el Comité de Seguridad de la Información.

La creación, modificación y eliminación de usuarios y contraseñas en la infraestructura de procesamiento de Información es responsabilidad del Comité de Seguridad de la información, o a quien este delegue a través de documento escrito y explícito del alcance de la gestión delegada.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información de la Alcaldía municipal de La Playa de Belén debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la entidad. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

11.3. Escritorio y pantalla limpia

[ISO/IEC 27001:2005 A.11.2.4]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de la Alcaldía municipal de La Playa de Belén deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CD, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

11.4. Segregación de redes

[ISO/IEC 27001:2005 A.11.4.5]

La plataforma tecnológica de la Alcaldía municipal de La Playa de Belén que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El Comité de Seguridad de la información es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Alcaldía municipal de La Playa de Belén debe establecer mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la entidad.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

11.5. Computación móvil

[ISO/IEC 27001:2005 A.11.7.1]

El uso de los equipos portátiles fuera de las instalaciones de la Alcaldía municipal de La Playa de Belén únicamente se permitirá a usuarios autorizados por el Comité de Seguridad de la Información, previa solicitud de la dependencia respectiva, y estos se protegerán mediante el uso de los siguientes controles tecnológicos:

- Antivirus.
- Cifrado de datos.
- Restricción en la ejecución de aplicaciones.
- Restricción de conexión de dispositivos USB.
- Protección física mediante la guaya de seguridad.

La sincronización de dispositivos móviles con cualquier sistema de información de Alcaldía municipal de La Playa de Belén, sólo estará permitido para personal autorizado por el Comité de Seguridad de la información y la dependencia respectiva.

11.6. Teletrabajo

[ISO/IEC 27001:2005 A.11.7.2]

Cualquier funcionario de Alcaldía municipal de La Playa de Belén, autorizado por el Comité de Seguridad de la información, que requiera tener acceso a la información de la entidad desde redes externas, podrá acceder remotamente mediante un proceso de autenticación, mediante el uso de conexiones seguras y asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA

REF.: ISO/IEC 27001:2005 A.12

12.1. Identificación de requerimientos de seguridad

[ISO/IEC 27001:2005 A.12.1.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en la Alcaldía municipal de La Playa de Belén, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del Comité de Seguridad de la información y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre Alcaldía municipal de La Playa de Belén y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad del Comité de Seguridad de la Información garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Secretaría de Gobierno establecer estos aspectos con las obligaciones contractuales específicas.

12.2. Controles criptográficos

[ISO/IEC 27001:2005 A.12.3.1]

Con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información, la Alcaldía municipal de La Playa de Belén debe establecer el uso de protocolos y controles criptográficos para el uso en aplicativos, transferencia de información, enlaces de comunicaciones, protección de medios, acceso remoto, sobres digitales y firmas digitales, y no se permite el uso de herramientas o mecanismos de encripción de información diferentes a las autorizadas por el Comité de Seguridad de la Información.

La administración de claves criptográficas y certificados digitales estará a cargo del Comité de Seguridad de la Información.

12.3. Seguridad de los sistemas

[ISO/IEC 27001:2005 A.12.4]

La Alcaldía municipal de La Playa de Belén con el fin de minimizar el riesgo de corrupción de los sistemas de información que se encuentran en producción, no permite la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción.

Las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a los mismos que soporten sistemas de información, deben solamente ser implementados en el ambiente de producción, después de un protocolo de pruebas adecuado que involucre aspectos funcionales, de seguridad, de compatibilidad con otros sistemas de información y facilidad de uso.

Los administradores de las plataformas de producción son los responsables de controlar el acceso y uso de los programas fuente de los archivos de los sistemas y/o de las aplicaciones que operan en ellas, así como de coordinar y/o ejecutar las actualizaciones programadas. El acceso de los proveedores a los sistemas de producción solo es permitido para realizar labores de soporte o mantenimiento, previa autorización del administrador de la plataforma con el respectivo monitoreo de las actividades realizadas.

Los proveedores de desarrollo de software no deben tener interacción directa con los sistemas de información de la Alcaldía municipal de La Playa de Belén en el momento de hacer el paso a producción, siendo esta actividad responsabilidad del administrador de la plataforma respectiva.

No se permite la copia de información *Confidencial* o *Restringida* desde el ambiente de producción al ambiente de pruebas. En caso de requerirse, se debe garantizar que los datos reales son mezclados de manera aleatoria (data scramble o data masking) sin afectar la estructura funcional de la solución.

No se permite el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes. El uso de versiones de prueba que no hayan sido liberadas al mercado (Beta), deben ser autorizadas por el Comité de Seguridad de la Información, quienes deben mantener actualizado el inventario de software autorizado en la entidad.

12.4. Gestión de vulnerabilidades técnicas

[ISO/IEC 27001:2005 A.12.6]

El Comité de Seguridad de la Información es responsable de identificar las vulnerabilidades técnicas del conjunto de plataformas tecnológicas, de comunicaciones y seguridad que soporten sistemas de información críticos de la Alcaldía municipal de La Playa de Belén.

El personal que administra la plataforma tecnológica es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la entidad.

Se debe generar por lo menos una vez al año por parte del comité de seguridad de la información el programa de pruebas de vulnerabilidades para las plataformas críticas del negocio cuya viabilidad técnica y de administración lo permita. Dichas pruebas deben ser realizadas por lo menos una vez al año por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad del personal que administre la infraestructura tecnológica, de comunicaciones y seguridad.

La Oficina de Control Interno realizará el seguimiento y verificación de los procesos de identificación de las causas que generaron las vulnerabilidades y la generación de las acciones de corrección a las que haya lugar.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD

REF.: ISO/IEC 27001:2005 A.13

13.1. Comunicación de incidentes y eventos de seguridad de la información

[ISO/IEC 27001:2005 A.13.1]

Se considera un evento de seguridad la ocurrencia de una situación que indica una posible violación a las políticas de seguridad de la información, o fallas en los controles que no genere un impacto en el desarrollo de las operaciones de la organización y que puede ser controlado rápidamente.

Se considera un incidente de Seguridad de la información, la ocurrencia de un acto intencional o no intencional que tiene una alta probabilidad de afectar el buen funcionamiento de los sistemas de información, que a causa de este acto se vea afectada la operación de la entidad y que por lo tanto amenaza la seguridad de la información.

Todo funcionario y/o tercero de la Alcaldía municipal de La Playa de Belén debe reportar mediante el formato de "*Reporte de Incidentes de Seguridad Informática*" (Formato 2) al líder del proceso, cualquier situación que se pueda considerar como un evento de seguridad y que comprometa la preservación de la confidencialidad, disponibilidad y/o integridad de la información.

Es responsabilidad del Comité de Seguridad de la Información determinar si la situación reportada corresponde a un evento o a un incidente de seguridad y ejecutar las acciones necesarias según el caso.

El Grupo de Atención a Incidentes debe ser multidisciplinario dentro de las diferentes áreas de la entidad y no será mayor a 5 personas y será liderado por el Coordinador del Comité de Seguridad de la Información.

El Alcalde municipal o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas. Si alguien no autorizado lleva a cabo tareas relacionadas con esta actividad, será interpretado como incumplimiento de las políticas establecidas.

13.2. Manejo de incidentes de seguridad

[ISO/IEC 27001:2005 A.13.2]

El Comité de Seguridad de la Información es el único ente autorizado o a quién este designe para evaluar las debilidades o incidentes de seguridad reportados. Por lo tanto, el Comité de Seguridad de la Información debe asignar un responsable o un grupo de personas responsables de realizar la investigación, seguimiento a los eventos de seguridad reportados e informar al Comité los resultados, actividades para las cuales puede requerir del apoyo de otras áreas de la entidad o de entidades externas. Este grupo será llamado Grupo de Atención de Incidentes.

El Comité de Seguridad de la Información debe mantener registro de aquellas anomalías o debilidades que le sean reportadas y que amenacen la seguridad de la información de la Alcaldía municipal de La Playa de Belén y debe asegurar el registro de los incidentes ocurridos teniendo en cuenta las causas, el impacto ocasionado, su frecuencia y forma de resolución, con el objeto de tener estadísticas anuales de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y las políticas cuando sea necesario. Es responsabilidad de todos los funcionarios y/o terceros involucrados preservar la confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes de seguridad de la información. Dicho registro se realizará mediante el Formato de "*Reporte de Incidentes de Seguridad Informática*". (Formato 2).

La Alcaldía municipal de La Playa de Belén debe establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de acciones maliciosas en contra de la información crítica de la entidad y que deba ser sancionada disciplinariamente. Aquellas actividades que generen sospecha de mal uso de la información de Alcaldía municipal de La Playa de Belén, deben ser registradas de forma que pueda ser usada como evidencia en la aplicación de sanciones acordes al impacto causado.

14. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

REF.: ISO/IEC 27001:2005 A.14

14.1. Seguridad de la información en la continuidad del negocio

[ISO/IEC 27001:2005 A.14.1.1]

Para la Alcaldía municipal de La Playa de Belén la seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

Alcaldía municipal de La Playa de Belén debe contar con un plan documentado, probado y actualizado que asegure la continuidad de las operaciones de sus procesos críticos, ante la ocurrencia de eventos no previstos o desastres naturales. Las directrices y lineamientos mínimos requeridos para recuperar y restablecer las operaciones de los servicios de tecnología, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan.

14.2. Análisis de riesgo e impacto del negocio

[ISO/IEC 27001:2005 A.14.1.2]

La Alcaldía municipal de La Playa de Belén debe realizar análisis de riesgos y análisis de impacto en el negocio, de acuerdo a las mejores prácticas, con el fin de definir el "*Plan de Contingencia de Sistemas de Información*" adecuado para la entidad. Dichas actividades deberán ser ejecutadas al menos una (1) vez al año o cada vez que se presente un cambio importante en la Entidad.

14.3. Declaración de desastre y activación de los planes de continuidad del negocio

[ISO/IEC 27001:2005 A.14.1.3]

La declaración de desastre es la notificación formal de desastre a los líderes de todos los equipos de recuperación. Esta notificación implica la iniciación de las actividades descritas en el "*Plan de Contingencia de Sistemas de información*" para cada uno de los equipos de recuperación.

La Alcaldía de La Playa de Belén definirá los responsables de declarar un desastre, así como, los voceros autorizados para definir el inicio de una

contingencia dentro de la Institución. Una vez se haya dado esta autorización de inicio, comenzarán a ejecutarse cada una de las actividades definidas dentro del "*Plan de Contingencia de Sistemas de Información*".

14.4. Entrenamiento y capacitación

[ISO/IEC 27001:2005 A.14.1.4]

Todos los funcionarios, así como los terceros involucrados, deben ser entrenados y concientizados de sus roles y responsabilidades asignados dentro del "*Plan de Contingencia de Sistemas de Información*" de la entidad.

14.5. Pruebas y mantenimiento del plan de continuidad

[ISO/IEC 27001:2005 A.14.1.5]

La Alcaldía de La Playa de Belén definirá un área responsable de coordinar en forma periódica las pruebas del "*Plan de Contingencia de Sistemas de Información*" y de mantenerlo actualizado, de acuerdo con las necesidades y requerimientos de la entidad.

15. CUMPLIMIENTO DE REQUERIMIENTOS

REF.: ISO/IEC 27001:2005 A.15

15.1. Cumplimiento de requerimientos

[ISO/IEC 27001:2005 A.15.1.1]

La Alcaldía de La Playa de Belén debe cumplir con la legislación aplicable propia de las leyes colombianas, las regulaciones dadas por entes de control, gubernamentales o nacionales que apliquen, y las obligaciones contractuales con terceros. En consistencia, se deben documentar dichos requerimientos para cada sistema de información.

En la Alcaldía de La Playa de Belén, el Asesor Jurídico, es el responsable de asesorar a la entidad sobre los requisitos normativos y regulatorios dados por entes de control, así como de las obligaciones con terceros y funcionarios, siempre enmarcados dentro del cumplimiento de la legislación colombiana vigente.

15.2. Derechos de propiedad intelectual

[ISO/IEC 27001:2005 A.15.1.2]

La Alcaldía de La Playa de Belén cumplirá con la reglamentación de propiedad intelectual vigente en el país y ejecutará revisiones periódicas para asegurar que se estén respetando los derechos de propiedad intelectual.

Los derechos de propiedad intelectual incluyen licencias de códigos fuente que hagan parte de desarrollos internos de software, documentos generados como parte del conocimiento de las actividades de la Alcaldía de La Playa de Belén, propuestas comerciales, patentes, información publicitaria y comercial que involucre la imagen corporativa de la entidad.

El Comité de Seguridad de la Información es el responsable por mantener y administrar el inventario y control de todas las licencias de software, hardware y aplicaciones utilizadas en la Alcaldía de La Playa de Belén, así como los medios y contratos que se relacionan con la actividad comercial de compra de software y hardware para la entidad. Está prohibido el uso de software ilegal o no licenciado. Los funcionarios son responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas que soportan los sistemas de información de la entidad.

Deben existir acuerdos contractuales claramente definidos entre la Alcaldía de La Playa de Belén y cualquier proveedor que realice actividades de desarrollo de software, en los cuales se especifiquen los compromisos de preservación de los derechos de propiedad intelectual. Todos los programas de software usados para el desarrollo de las operaciones de la entidad, deben incluir los avisos de información de derechos de autor correspondiente y estos deben aparecer cuando el usuario inicie la aplicación.

Se permite el uso de documentos, cifras y/o textos de carácter público o de cualquier otra índole, siempre y cuando estos cumplan con las reglamentaciones nacionales vigentes para la preservación de los derechos morales e intelectuales de las obras o referencias citadas.

15.3. Protección de registros

[ISO/IEC 27001:2005 A.15.1.3]

La Alcaldía de La Playa de Belén se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requerimientos normativos, legales o regulatorios de pérdida, destrucción o falsificación. Es por ello que los registros están identificados en el "*Listado Maestro de Registros*", y son protegidos de acuerdo a su nivel de clasificación según lo establecido en el "*Lineamientos de Inventario y Clasificación de Activos de Información*" Anexo 2.

De igual forma, y cumpliendo la legislación colombiana vigente, la Alcaldía de La Playa de Belén establece que la información personal de los funcionarios y/o contratistas es de carácter confidencial, por lo cual se implementarán los controles necesarios para su protección y en ningún momento puede ser divulgada a terceras partes a menos que cuente con la autorización formal del funcionario y/o contratista o en los casos en que la normatividad lo permita.

ANEXOS

Anexo 1. Funciones y responsabilidades del Comité de Seguridad.

EL Comité de Seguridad de la Información es un cuerpo integrado por representantes de todas las áreas de la Alcaldía Municipal, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

El Comité de Seguridad de la Información se crea con los siguientes objetivos:

1) Revisar y proponer al Alcalde municipal para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para esta Universidad.
2) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información del ente territorial frente a posibles amenazas, sean internas o externas.
3) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Alcaldía municipal.
4) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información
5) Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los sistemas o servicios de la entidad, sean preexistente o nuevos.
6) Promover la difusión y apoyo a la seguridad de la información dentro de la Universidad, como así, coordinar el proceso de administración de la continuidad de las actividades.

Las funciones del Comité de Seguridad de Información – CSI, de la Alcaldía municipal de La Playa de Belén, son las siguientes:

- Dentro del flujo de aprobación de las Políticas de Seguridad de la Información, el CSI es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de éstas.
- El CSI aprueba normas y procedimientos de seguridad de la Información.
- Revisa y valida normas y procedimientos en general, a fin de verificar que se estén cumpliendo los aspectos de seguridad dentro de los procesos.
- Por medio del CSI se supervisa y controla el Plan de Seguridad de la Información para analizar temas tales como:
  - Revisar el avance del plan y dar directrices en caso de atrasos.
  - Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades.

  - Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la organización.
  - Definir proyectos de tecnología que impliquen la aplicación de Seguridad de la Información en el contexto del negocio (Servicio, Producto e Información).
  - Generar resúmenes de actividades englobadas en el marco de la Seguridad de la Información para ser presentadas ante las máximas autoridades de la organización.
  - Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Organización frente a posibles amenazas, sean internas o externas.
  - Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Organización.
- Por medio del CSI se instruirá al Responsable de Seguridad de la Información (Secretario de Planeación Municipal) el inicio del proceso de revisión anual de las políticas vigentes. Dicha instrucción se dará en la sesión de Diciembre de cada año.
- Aprobar las principales iniciativas para incrementar la Seguridad de la Información de acuerdo a las competencias y responsabilidades asignadas a cada Dependencia, así como acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.
- Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios de la Organización, sean preexistente o nuevos.
- Promover la difusión y apoyo a la Seguridad de la Información dentro de la Organización, así como también, coordinar el proceso de administración de la continuidad de las actividades.

Anexo 2. Lineamientos de Inventario y Clasificación de Activos de Información.

Este documento establece los criterios y mecanismos que deberán ser utilizados por los usuarios internos de la Alcaldía de La Playa de Belén, para clasificar y manejar la información que generen, posean o utilicen, llevando a cabo las actividades que bajo su responsabilidad tendrán como usuarios, propietarios o custodios técnicos de los activos de información de la entidad.

1. Inventario de activos de información

Mediante la definición de un inventario la Alcaldía municipal especifica y reconoce cuales son los activos de información más importantes del negocio y define clasificar mínimo los activos de información que se encuentran consignados en el inventario.

El inventario permite identificar los activos de información a los que se les debe brindar mayor protección y que se puede requerir para servir a otros propósitos del negocio como por ejemplo: controles de seguridad física, estudioso financieros o de cálculos de primas de seguros (gestión de activos), entre otros.

Para elaborar el inventario se deben realizar las siguientes actividades:

1.1. Definición de activos

Esta actividad consiste en reconocer y determinar que activos de información van a hacer parte de la matriz de inventario y clasificación de activos y definir para estos las propiedades y la información que permite identificar a los activos de información en la entidad, para obtener su valor para el negocio.

La definición se lleva a cabo de la siguiente manera:

- Cada dependencia deberá realizar un levantamiento de los activos de información que están bajo su custodia en el Formato de "*Inventario de Activos de Información*" (Formato 1), reportando los activos de información más importantes, identificándolos y valorándolos.
- El Comité de Seguridad de la Información será el encargado de revisar la actividad de Definición y aprobar la información consignada.

A continuación se define el significado de cada campo presente en la tabla de inventario:

Tipo de Activo		
CODIGO	**TIPO ACTIVO**	**DESCRIPCION**
SI	Sistema de Información	ERP, Aplicativos, Sistemas de Información
D	Documentos	Proyectos, Planes, Manuales, Presupuestos en físico
P	Recurso Humano	Personal: empleados, proveedores, practicantes, etc.
HW	Hardware	PC's, Servidores, Switches, Routers, Backup, PDA
SW	Software	Sw de Ofimática, Sw de Base, Base de Datos, Herramientas TI
ID	Información Digital	Información en Servidor Archivos, USB, CD's, DVD's, etc.
STR	Servicios de Terceros	Internet, Telefonía, Energía, Agua, Vigilancia, etc.
L	Sitio	Centro de Datos, Archivo Central, Oficina, Sede Principal, Bóveda
COM	Red de Comunicaciones	Red Lan, Red Wan, Red VPN, Acceso Remoto VPN
S	Servicios	Soporte Técnico, Gestión de Servicios TI, etc.

Clasificación Información		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION**
C	Confidencial	Restringida a un conjunto de personas de la Alcaldía
I	Uso Interno	Sólo personal de la Alcaldía o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	**INTEGRIDAD**	**DESCRIPCION**
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	**DISPONIBILIDAD**	**DESCRIPCION**
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Valor del Activo		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION (Clasificación Información)**
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta, Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja, Baja

Frecuencia de Uso		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION**
A	Alta	Información utilizada en forma diaria o semanal
M	Media	Información utilizada en forma mensual o semestral
B	Baja	Información utilizada en forma anual

1.2. Revisión de activos

La actividad de Revisión se refiere a la verificación que se puede llevar a cabo para determinar si un activo de información continúa o no siendo parte del inventario, si los valores asignados a los activos de información en los campos de la matriz de inventario y clasificación deben ser actualizados.

La Revisión se puede realizar semestral y será supervisada por el Comité de Seguridad de la Información. Las razones para realizar una Revisión son:

- Actualización de procesos que desarrolla la dependencia.
- Inclusión de nuevas actividades en los procesos que desarrolla la dependencia.
- Inclusión de un nuevo activo importante.
- Desaparición de una oficina, dependencia, proceso o cargo (propietario o custodio del activo) en la entidad.
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de información.

1.3. Actualización de activos

Una vez realizada la Revisión de Activos de Información, con los resultados obtenidos se procede a actualizar la matriz de inventario y clasificación de activos. Esta actividad la realiza el jefe de la dependencia con su equipo de trabajo y es supervisada por el Comité de Seguridad de la información.

1.4. Publicación

El inventario de activos de información se debe publicar impreso a cada uno de los responsables de la información (propietarios y custodios técnicos), y su actualización será controlada por los jefes de las dependencias, quienes mantendrán una copia magnética del formato de inventario para utilizarse en los eventos que se requiera de modificaciones a la información allí consignada.

La publicación oficial es la impresa y esta lleva las firmas de aprobación de los responsables, el archivo magnético no es oficial pues solo se utiliza para fines de actualización.

2. Clasificación de activos de información

La Clasificación de Activos de Información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados. La información con base en su valor y de acuerdo a los requisitos de confidencialidad tiene diferentes grados de protección o manejo especial que se definen en la clasificación de activos de información.

El esquema de clasificación estipula los niveles de protección para cada activo de información y señala las consideraciones especiales de manejo, restricciones, distribución, almacenamiento y destrucción de la información.

Los jefes de dependencia que definieron el activo de información en el inventario deben revisar y confirmar el nivel de clasificación asignado al activo, y confirmar si el activo está clasificado adecuadamente.

La clasificación de los activos de información se basa en la información consignada en el inventario, cumpliendo con los siguientes componentes:

2.1. Niveles de clasificación y confidencialidad

- Niveles de acceso
- Métodos de distribución
- Restricciones en la distribución electrónica
- Almacenamiento y archivado

- Destrucción
- Penalizaciones por revelación deliberada de la información.

Cada activo de información tendrá asociado un único nivel de clasificación y un único nivel de confidencialidad. Cada nivel de confidencialidad posee características propias de protección, manejo y tratamiento del activo en cuanto a Niveles de acceso, Métodos de distribución, Restricciones en la distribución electrónica, Almacenamiento, Archivado, Disposición y Destrucción.

Una vez que a un activo de información se le asigna un nivel de confidencialidad este adquiere las características específicas anteriormente mencionadas para el nivel confidencialidad asignado. Adicionalmente para cada activo de información se definen unos atributos de de clasificación, estos indican propiedades adicionales y específicas que cada activo de información posee y las cuales permiten identificar el nivel de riesgo base inherente a cada activo de información con respecto a la preservación del nivel de confidencialidad asignado.

2.1.1. Niveles de clasificación

- **Pública:** La información pública de la Alcaldía municipal de La Playa de Belén es la información que ha sido declarada de conocimiento público de acuerdo a alguna norma jurídica o por parte del Alcalde municipal. Esta información puede ser entregada o publicada sin restricciones a los funcionarios de la entidad o a cualquier persona sin que esto implique daños a terceros ni a las actividades y procesos de la Alcaldía municipal.

- **Confidencial:** La información confidencial de la alcaldía es toda aquella información que no es pública y que además no ha sido aún clasificada. A la información confidencial solo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados, tal como aparece consignado en el inventario de activos de información.

  Los Secretarios de Despacho definirán en sus dependencias cual información es Reservada o Confidencial.

2.1.2. Niveles de confidencialidad

La información confidencial debe ser entendida como: La existencia de información más crítica a nivel de pérdida de su confidencialidad que otra y que por ende debe tener una mayor protección.

La información que es confidencial hoy puede llegar a ser pública en un momento posterior, de conocimiento público para un conjunto de personas y parte de ella es pública para la comunidad en general en algunos casos.

Para saber cuándo se puede permitir el acceso y uso de la información a personas distintas a las responsables de la misma y para poder establecer el grado de protección que se le debe aplicar a la información de la entidad, es necesario clasificarla totalmente en términos de su confidencialidad.

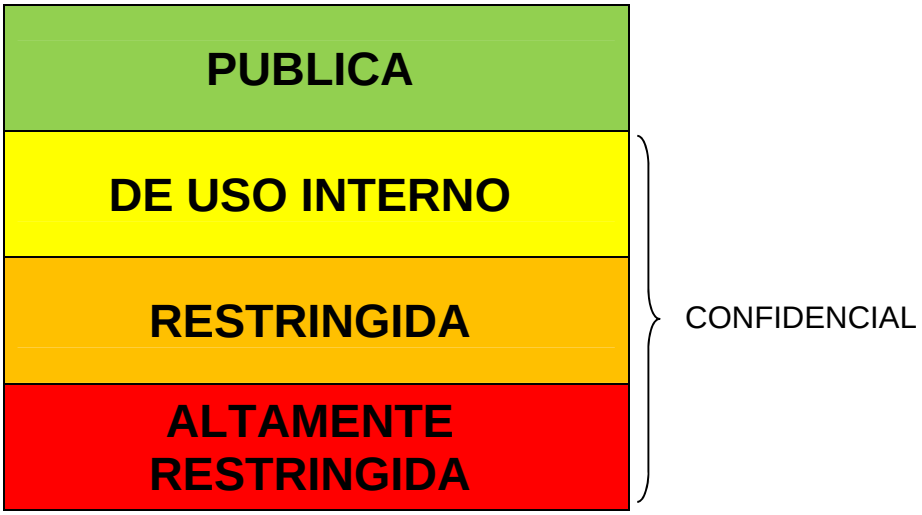
Para realizar una clasificación más precisa y fácil de manejar se definen tres grados de confidencialidad de la información de la Alcaldía municipal de La Playa de Belén: de uso interno, restringida y altamente restringida. A continuación se define cada una de ellas.

- **Uso interno:** Es toda información consignada en el inventario de activos de información que es utilizado por el personal de la Administración municipal para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma leve a terceros o a los sistemas y/o procesos de la Alcaldía municipal.

- **Restringida:** Información que es utilizada por solo un grupo de empleados para realizar sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la institución.

- Altamente restringida: Información que es utilizada solo por un grupo de empleados para realizar sus labores y que no puede ser conocida por otros empleados o terceros sin autorización especial del Alcalde. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas, a la dependencia responsable, a la Alcaldía o al municipio como entidad territorial.

Para la Alcaldía municipal de La Playa, la relación que se establece entre los niveles de Clasificación y los niveles de Confidencialidad es como se muestra a continuación:



Los diferentes niveles de clasificación tienen características y recomendaciones de manejo:

CRITERIO	NIVEL DE CLASIFICACION			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Definición	Es la información que ha sido declarada de conocimiento público de acuerdo a alguna norma jurídica o por parte de la persona o grupo de personas de la Alcaldía con autoridad para hacerlo. Esta información puede ser entregada o publicada sin restricciones a los empleados o a cualquier persona, sin que esto implique daños a terceros ni a las actividades y procesos de la alcaldía.	Es toda información consignada en el inventario de activos de información que es utilizada por el personal de la ALCALDÍA para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma leve a terceros o a los sistemas y/o procesos de la ALCALDÍA.	Información que es utilizada por solo un grupo de empleados para realizar sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la entidad.	Información que es utilizada por solo un grupo de empleados para realizar sus labores y que no puede ser conocida por otros empleados o terceros sin autorización especial de la Gerencia. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas, a la dependencia responsable, a la alcaldía o al municipio como entidad territorial.
Criterio de definición de confidencialidad	Muy baja (MB):"El conocimiento o divulgación no autorizada de este activo de información no tiene ningún impacto negativo en el proceso." Atributos: A2: "No está restringida a un número limitado de empleados". A3: "No restringida a personas externas". A7: "Declarado de conocimiento público".	Baja (B): "El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera leve al proceso." Media (M): "El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera importante al proceso." Atributos: A3: "Restringida a personas externas"	Alta (A): " El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a la Institución o sus negocios". Atributos: A2: "Restringido a un número determinado de empleados".	Muy Alta (MA): " El conocimiento o divulgación no autorizada de este activo de información impacta negativamente al Distrito". Atributos A8 (G): El impacto para la organización es "Grave" en caso de ser conocida, modificada o no tener disponibilidad.

CRITERIO	NIVEL DE CLASIFICACION			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Acceso permitido	Todos (Cualquier persona Interna o Externa)	Todos los Empleados de la Alcaldía de La Playa de Belén y contratistas con un compromiso firmado de confidencialidad y con autorización del propietario para su uso.	Solo los Usuarios expresamente autorizados en el Inventario de activos y contratistas con un compromiso firmado confidencialidad y con autorización del propietario para su uso.	Empleados de la Alcaldía con un compromiso firmado de confidencialidad de información y con autorización formal del Alcalde para acceder a esta información.
Etiquetado: - Documentos en papel	No es requerido	No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse, si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.	SI, es obligatorio por parte del Propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.	SI, es obligatorio por parte del Propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.
Etiquetado: - Archivos Electrónicos (Texto, Word, Excel, dibujos, planos, etc.)	No es requerido	No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse los documentos o información que estén en archivos electrónicos se les deben agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.	SI, es obligatorio por parte del Propietario de la información. Los documentos o información que estén en archivos electrónicos se les deben agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.	SI, es obligatorio por parte del Propietario de la información. Los documentos o información que estén en archivos electrónicos se les debe agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.
Etiquetado: - Aplicaciones	No es requerido	No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse, las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.	SI, es obligatorio por parte del Propietario de la información. Las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.	SI, es obligatorio por parte del Propietario de la información. Las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.
Etiquetado: - Carpeta en sistemas	No es requerido	No es requerido, queda a discreción del propietario de la información. En caso	SI, es obligatorio por parte del Propietario de la información. Las carpetas en	SI, es obligatorio por parte del Propietario de la información. Las carpetas en

		de etiquetarse, las carpetas en servidores de archivos o en PCS se les deben colocar un nombre o identificador distintivo (icono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.	servidores de archivos o en PCS se les deben colocar un nombre o identificador distintivo (ícono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.	servidores de archivos o en PCS se les deben colocar un nombre o identificador distintivo (ícono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.
CRITERIO	**NIVEL DE CLASIFICACION**			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Método de distribución recomendado: - Internamente	Ninguno. Esta información puede distribuirse en cualquier medio al público en general, incluso a cualquier ente o persona por fuera de la organización.	Electrónica: Mediante el sistema de correo electrónico de la Alcaldía y a través de las redes de datos y sistemas únicamente. Se debe evitar en lo posible manejar esta información en dispositivos de almacenamiento externo (Diskets, CDS, DVD's, memorias USB, SD, etc.) que no sean autorizados por la Alcaldía. Física: Actividad de manejo de correspondencia interno.	Electrónica: Mediante el sistema de correo electrónico de la Alcaldía y a través de las redes de datos y sistemas de la únicamente. Se debe evitar en lo posible manejar esta información en dispositivos de almacenamiento externo (Diskets, CDS, DVD's, memorias USB, SD, etc.) que no sean autorizados por la Alcaldía. Física: Proceso de manejo de correspondencia interno, verificando que el destinatario si es un usuario autorizado en el inventario de activos de información, de otra forma se requiere de autorización por parte del propietario de la información.	Electrónico: Solo en la red de la Alcaldía cuando se instale y los archivos deberán estar cifrados, la entrega se hace solo a un destinatario legítimo del inventario de activos de información. (Se recomienda el uso de certificado digital en el correo electrónico) Física: Entrega directa, firma de recepción personal requerida no transferible, entregada por el propietario de la información directamente.
Método de distribución recomendado: - Hacia terceros	Ninguno. Esta información puede distribuirse en cualquier medio al público en general, incluso a cualquier ente o persona por fuera de la organización.	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónica: Si se entrega en medio electrónico en lo posible se debe tener los archivos y/o datos de acceso de solo lectura. Se puede entregar la información vía e-mail a destinatarios con cuentas ajenas a	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónica: Si se entrega en medio electrónico en lo posible se debe tener los archivos y/o datos de acceso de solo lectura. No se puede entregar la información vía e-mail a destinatarios con cuentas ajenas a la	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónico: Siempre se debe entregar esta información de manera cifrada al destinatario legítimo directamente. (Se debe utilizar certificado digital si se requiere obligatoriamente transmitir por correo

		la Alcaldía. Se debe evitar utilizar listas de distribución al momento de enviar este tipo de información. Física: Si es posible se debería entregar solo en medio físico (Papel), el menor número de copias posible, y solo al receptor autorizado, firmando una carta de recibido.	Alcaldía, si la información no posee clave. Se debe evitar utilizar listas de distribución al momento de enviar este tipo de información. Física: Si es posible se debería entregar solo en medio físico (Papel), el menor número de copias posible, y solo al receptor autorizado, firmando una carta de recibido, mediante la empresa de mensajería de la Alcaldía o directamente por parte del propietario de la información.	electrónico) Físico: En este caso debe utilizarse una empresa de transporte de valores con un proceso formal de verificación del destinatario y entrega directa.

CRITERIO	**NIVEL DE CLASIFICACION**			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Almacenamiento y archivado: - Información impresa	No requiere precauciones especiales.	Se debe establecer una política de escritorio limpio, asegurar el acompañamiento y seguimiento de las acciones de personas externas en las instalaciones.	Se debe archivar en áreas seguras bajo llave (Cajones, Cuarto de archivo, estantes, etc.)	Se debe archivar en áreas seguras bajo llave (Cajones, Cuarto de archivo, estantes, etc.). Se recomienda guardar este tipo de información en caja fuerte si es posible. Cada vez que se archive asegúrese de que sea por fuera de la vista de otras personas.
Almacenamiento y archivado: - Información electrónica	No requiere precauciones especiales.	Se puede almacenar en cualquier sistema o repositorio siempre y cuando se asegure que no es accesible a personas por fuera de las redes y sistemas de información de la Alcaldía (i.e. desde Internet, servicios FTP, Web, etc.). Debe existir copia de la información solamente en los medios, sistemas de información o recursos indicados en el campo ubicación del inventario de activos de información.	Se debe almacenar en sistemas o repositorios centralizados, bien administrados desde donde se comparta la información, está prohibido dejar sin protección de autenticación de usuario/password esta información y con los privilegios indicados en el inventario de activos de información y los asignados por el propietario a los usuarios autorizados. Debe evitarse almacenar este tipo de información en PCS que no tengan administración formal de seguridad. Debe existir copia de la información solamente en los medios, sistemas de	Los controles individuales mínimos sugeridos para la información digital son: la autenticación con usuario y contraseña al sistema donde reposa la información y adicionalmente usuario y contraseña para el archivo (si es posible se debe cifrar la información). Si esta información se encuentra en un PC o portátil, al equipo deben tener acceso solo las personas autorizadas, preferiblemente utilizando autenticación fuerte de mínimo dos factores. Debe existir copia de la información solamente en los medios, sistemas de información o recursos

			información o recursos indicados en el campo ubicación del inventario de activos de información.	indicados en el campo ubicación del inventario de activos de información.
Almacenamiento y archivado: - Correo electrónico	No requiere precauciones especiales.	Se debe asegurar que esta información no se envíe a terceros no autorizados para recibirla por este medio.	Asegúrese de que la información no queda en los elementos enviados y adicionalmente asegúrese de que el backup del correo electrónico se realiza de manera segura (protegido con usuario y contraseña).	Se debe evitar en lo posible el uso de este medio, en caso de que sea necesario debe manejarse a través de certificados digitales.
Destrucción: - Información impresa	No requiere precauciones especiales.	No requiere precauciones especiales.	Se deben utilizar máquinas destructoras de papel.	Debe utilizarse una destructora de papel pero preferiblemente debe incinerarse y esta acción debe ser llevada a cabo por el propietario del activo.
Destrucción: - Reciclaje de papel	Es permitido sin restricciones	Es permitido solo para uso interno	No es permitido	No es permitido
Destrucción: - Medios de almacenamiento	No requiere precauciones especiales.	Borrado seguro de información, destrucción física de medios que vayan a desecharse.	Borrado seguro de información, destrucción física de medios que vayan a desecharse.	Borrado seguro de información, destrucción física de medios que vayan a desecharse.

CRITERIO	**NIVEL DE CLASIFICACION**			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Transmisión oral: - Conversaciones y reuniones	No requiere precauciones especiales.	Se debe evitar referenciar esta información por fuera de las instalaciones de la Alcaldía, cuando se lleven a cabo deben ser en conversaciones privadas y en voz baja, evitando en lo posible zonas públicas, tales como pasillos, corredores, balcones, etc.	Se debe evitar referenciar esta información por fuera de las instalaciones de la Alcaldía al menos que sea una reunión formal por fuera de las mismas. Evite reunirse en salas que no sean cerradas y que no permitan aislar el ruido. Si la información fue anotada en papelógrafos o tableros, o documentos no formales (trozos de papel, libretas o agendas personales, etc.), esta debe ser borrada o destruida inmediatamente se abandone el sitio o se transfiera a un medio formal dispuesto por la Alcaldía (Archivo de Acta, archivo formal de notas, etc.).	Se debe evitar referenciar esta información por fuera de las instalaciones de la Alcaldía al menos que sea una reunión formal por fuera de las mismas. Evite reunirse en salas que no sean cerradas y que no permitan aislar el ruido. En lo posible asegúrese que esta información solo es transmitida solo a las mínimas personas necesarias. Si la información fue anotada en papelógrafos o tableros, o documentos no formales (trozos de papel, libretas o agendas personales, etc.), esta debe ser borrada o destruida inmediatamente se abandone el sitio o se transfiera a un medio formal dispuesto por la Alcaldía (Archivo de Acta, archivo formal de notas, etc.).
Transmisión oral:	No requiere precauciones	No se debería entregar información	Evite en lo posible establecer	Evite en lo posible establecer conversaciones

- Telefónica	especiales.	de uso interno a personas no autorizadas por este medio.	conversaciones telefónicas en donde se maneje este tipo de información, más aun si hay posibles escuchas no autorizados cerca del sitio en donde se encuentra. Si se requiere haga uso de un teléfono en una zona segura o aislada (Sala de Reuniones, teleconferencia)	telefónicas en donde se maneje este tipo de información, más aun si hay posibles escuchas no autorizados cerca del sitio en donde se encuentra. Si se requiere haga uso de un teléfono en una zona segura o aislada (Sala de Reuniones, teleconferencia)
Transmisión oral: - Voice Mail o máquina de grabación automática de mensajes	No requiere precauciones especiales.	No se debería entregar información de uso interno a personas no autorizadas por este medio.	No se deberían dejar mensajes con este tipo de información	No se deberían dejar mensajes con este tipo de información
Transmisión por fax: - Uso de cubierta de fax	Si se requiere cubierta, debe identificar a la alcaldía.	Si se requiere cubierta, debe identificar a la alcaldía.	Si se requiere cubierta, debe identificar a la alcaldía y debe estar etiquetado como confidencial.	Se debe evitar la transmisión por FAX, solo con autorización del Alcalde se debe llevar a cabo. En tal caso se debe etiquetar como altamente confidencial.
Transmisión por fax: - Uso de cubierta de fax	Si se requiere cubierta, debe identificar a la alcaldía.	Si se requiere cubierta, debe identificar a la alcaldía.	Si se requiere cubierta, debe identificar a la alcaldía y debe estar etiquetado como confidencial.	Se debe evitar la transmisión por FAX, solo con autorización del Alcalde se debe llevar a cabo. En tal caso se debe etiquetar como altamente confidencial.

CRITERIO	**NIVEL DE CLASIFICACION**			
	PUBLICA	**USO INTERNO**	**RESTRINGIDA**	**ALTAMENTE RESTRINGIDA**
Transmisión por fax: - Cuidados en la transmisión	No se requiere precauciones especiales	No se debería entregar información de uso interno a personas no autorizadas por este medio.	No se debería entregar información de uso interno a personas no autorizadas por este medio.	No se deberían dejar mensajes con este tipo de información
Seguridad física: - Estaciones de trabajo	Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo por fuera de	Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible. Se debe tener un estricto control de vigilancia para el retiro de	Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible. Se debe tener un estricto control de vigilancia para el retiro de	Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo

	las instalaciones.	estaciones de trabajo por fuera de las instalaciones.	estaciones de trabajo por fuera de las instalaciones.	por fuera de las instalaciones. Conecte lo menos posible la estación a Internet.
Seguridad física: - In formación impresa en zona de impresión	No requiere precauciones especiales.	Se debe tener las impresoras por fuera del alcance del público en general y se debe buscar la impresión inmediatamente.	Se debe tener las impresoras por fuera del alcance del público en general y se debe buscar la impresión inmediatamente.	Se debe tener una persona atendiendo todo el proceso de impresión en la zona de impresoras desde el inicio, esta debe estar autorizada a ver la información.
Seguridad física: - Portátiles, Tablets, Smartphones.	No requiere precauciones especiales.	No descuide el equipo en zonas que no posean vigilancia o control de salida de equipos.	Nunca debe dejar solo el equipo y siempre debe utilizar cable de aseguramiento (lockdown cable), y si no es posible se debe dejar bajo vigilancia y cuando se salga de la oficina se debe dejar este bajo llave.	Nunca debe dejar solo el equipo y siempre debe utilizar cable de aseguramiento (lockdown cable), y si no es posible se debe dejar bajo vigilancia y cuando se salga de la oficina se debe dejar este bajo llave. Se debe procurar tener la información cifrada.
Seguridad física: - Acceso a oficina.	No requiere precauciones especiales.	No requiere precauciones especiales.	El acceso a las áreas que poseen información confidencial debe tener algún tipo de restricción física de acceso (Puerta con llave, tarjeta, vigilancia), este control debe ser aplicado cuando la oficina este desatendida.	El acceso a las áreas que poseen información confidencial debe tener algún tipo de restricción física de acceso (Puerta con llave, tarjeta, vigilancia), este control debe ser aplicado cuando la oficina este desatendida.
Fotocopiado de información: - Tipo de copias permitidas	No requiere precauciones especiales.	No requiere precauciones especiales.	Solo cuando sea necesario	Debe ser autorizado por el propietario de la información.

Anexo 3. Acuerdo de confidencialidad de la Información.

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

En _____ (ciudad) a ____ de _____ de 20__.

De un lado, _____ (nombre y apellidos del DIVULGANTE), en su propio nombre y derecho / en nombre y representación de _____ (nombre de la entidad), con domicilio a efectos del presente Acuerdo en _____ (calle, número, planta, letra; en principio, el domicilio social o de la sede principal de la entidad) de _____ (ciudad y departamento), en adelante “EL DIVULGANTE”.

Y de otro, _____ (nombre y apellidos del posible INVERSOR), en su propio nombre y derecho / en nombre y representación de _____ (nombre de la entidad), con domicilio a efectos del presente Acuerdo en _____ (calle, número, planta, letra) de _____ (ciudad y departamento), en adelante “EL INVERSOR”.

Ambas partes se reconocen recíprocamente con capacidad para obligarse y, al efecto, suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información en base a las siguientes ESTIPULACIONES:

PRIMERA.- Objeto. El presente Acuerdo se refiere a la información que EL DIVULGANTE proporcione al INVERSOR, ya sea de forma oral, gráfica o escrita y, en estos dos últimos casos, ya esté contenida en el “Plan Estratégico General” o en cualquier otro tipo de documento (planes sectoriales, planes de acción, manuales, procedimientos, etc.), con ocasión de las negociaciones que se están desarrollando / que se van a desarrollar a fin de _____.

SEGUNDA.- 1. EL INVERSOR únicamente utilizará la información facilitada por EL DIVULGANTE para el fin mencionado en la Estipulación anterior, comprometiéndose EL INVERSOR a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus empleados, asociados y a cualquier persona que, por su relación con EL INVERSOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del INVERSOR para con EL DIVULGANTE.

2. EL INVERSOR o las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización escrita y expresa del DIVULGANTE.

3. De igual forma, EL INVERSOR adoptará respecto de la información objeto de este Acuerdo, las mismas medidas de seguridad que adoptaría normalmente

respecto a la información confidencial de su propia Empresa, evitando en la medida de lo posible su pérdida, robo o sustracción.

TERCERA.- Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

Cuando la información se encontrara en el dominio público en el momento de su suministro al INVERSOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

Cuando la información ya estuviera en el conocimiento del INVERSOR con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL INVERSOR notificará al DIVULGANTE tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

En caso de que EL INVERSOR pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL DIVULGANTE.

CUARTA.- Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al DIVULGANTE y el hecho de revelarla al INVERSOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.

En caso de que la información resulte revelada o divulgada o utilizada por EL INVERSOR de cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al DIVULGANTE los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último *(si se quiere, se puede fijar aquí mismo una cantidad determinada como indemnización).*

QUINTA.- Las partes se obligan a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo.

SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de _____ después de finalizada la relación entre las partes o, en su caso, la

prestación del servicio.

SÉPTIMA.- En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Tribunales de _____, con renuncia a su fuero propio, aplicándose la legislación _____ (del país donde estén situados los Juzgados y Tribunales indicados) vigente.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha al comienzo indicados.

POR EL INVERSOR, POR EL DIVULGANTE,

Fdo.: _____ Fdo.: _____

Anexo 4. Lineamientos de investigación de Incidentes de Seguridad.

El personal encargado de la administración de seguridad debe ser plenamente identificado por todos los empleados de la Alcaldía (servidores públicos y contratistas).

Si un empleado de la Alcaldía detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de seguridad informática. Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar el equipo de la red de datos, notificar al área de seguridad informática quien trabajará en coordinación con el área de soporte técnico, para la eliminación del virus antes de restablecer la conexión a la red de datos. Es responsabilidad del usuario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.

Si un empleado detecta una vulnerabilidad en la seguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

El área de seguridad informática debe documentar todos los reportes de incidentes de seguridad. Cualquier error o falla en los sistemas debe ser notificado a soporte técnico, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad.

Las acciones disciplinarias tomadas contra empleados o contratistas y proveedores por la ocurrencia de una violación de seguridad, deben ser consistentes con la magnitud de la falta, ellas deben ser coordinadas con el área de Recursos Humanos (Secretaría de Gobierno).

1. Registro de fallas

El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:

- Nombre de la persona que reporta la falla
- Hora y fecha de ocurrencia de la falla
- Descripción del error o problema
- Responsable de solucionar el problema
- Descripción de la respuesta inicial ante el problema
- Descripción de la solución al problema
- Hora y fecha en la que se solucionó el problema

Los registros de fallas deben ser revisados semanalmente. Los registros de

errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

2. Intercambios de información y correo electrónico

Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros de la Alcaldía y están sujetos a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente:

- Enviar cadenas de mensajes
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la administración de la seguridad de la información.
- Enviar propaganda de candidatos políticos
- Actividades ilegales, no éticas o impropias
- Actividades no relacionadas con la misión y los fines del municipio como entidad territorial
- Diseminar direcciones de correo electrónico a listas públicas

No deben utilizarse reglas de reenvío automático a direcciones que no pertenecen a la entidad. No existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la Alcaldía.

Deben establecerse controles sobre el intercambio de información de la Alcaldía con terceros para asegurar la confidencialidad e integridad de la información, y que se respete la propiedad intelectual de la misma. Debe tomarse en consideración:

- Acuerdos para el intercambio de software
- Seguridad de media en tránsito
- Controles sobre la transmisión mediante redes

Debe establecerse un proceso formal para aprobar la publicación de información de la Alcaldía. La información contenida en sistemas públicos no debe contener información restringida, confidencial o de uso interno. De igual manera, los equipos que brindan servicios Web, correo electrónico, u otros servicios públicos no deben almacenar información restringida, confidencial o de uso interno. Antes que un empleado de la Alcaldía libere información que no sea de uso general debe verificarse la identidad del individuo u organización recipiente utilizando firmas digitales, referencias de terceros, conversaciones telefónicas u otros mecanismos similares.

Debe establecerse controles sobre equipos de oficina como teléfonos, faxes e impresoras que procesan información sensible de la Alcaldía. Información

restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea.

3. Administración de incidentes de seguridad

Luego de reportado el incidente de seguridad, éste debe ser investigado por el área de seguridad informática (Comité de Seguridad). Se debe identificar la severidad del incidente para la toma de medidas correctivas.

El personal encargado de la administración de la seguridad debe realizar la investigación de los incidentes de forma rápida y confidencial.

Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en la Alcaldía.

Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales en caso de ser necesario.

Anexo 5. Lineamientos de Gestión de Medios e Información en Tránsito.

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiable, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

La información a ser transferida en media digital o impresa debe ser etiquetada con la clasificación de información respectiva y detallando claramente el remitente y recipiente del mismo.

La información enviada por servicios postales debe ser protegida de accesos no autorizados mediante la utilización de:

- Paquetes sellados o lacrados.
- Entrega en persona.
- Firmado y sellado de un cargo.

Inventario de Activos de Información.
Formato 1.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	Clasificación	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
					Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno

UBICACION FISICA	UBICACION LOGICA	FRECUENCIA DE USO	FECHA ACTUALIZACION

Instrucciones de diligenciamiento:

Tipo de Activo		
CODIGO	**TIPO ACTIVO**	**DESCRIPCION**
SI	Sistema de Información	ERP, Aplicativos, Sistemas de Información
D	Documentos	Proyectos, Planes, Manuales, Presupuestos en físico
P	Recurso Humano	Personal: empleados, proveedores, practicantes, etc.
HW	Hardware	PC's, Servidores, Switches, Routers, Backup, PDA
SW	Software	Sw de Ofimática, Sw de Base, Base de Datos, Herramientas TI
ID	Información Digital	Información en Servidor Archivos, USB, CD's, DVD's, etc.
STR	Servicios de Terceros	Internet, Telefonía, Energía, Agua, Vigilancia, etc.
L	Sitio	Centro de Datos, Archivo Central, Oficina, Sede Principal, Bóveda
COM	Red de Comunicaciones	Red Lan, Red Wan, Red VPN, Acceso Remoto VPN
S	Servicios	Soporte Técnico, Gestión de Servicios TI, etc.

Clasificación Información		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION**
C	Confidencial	Restringida a un conjunto de personas del Banco
I	Uso Interno	Sólo personal del Banco o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	**INTEGRIDAD**	**DESCRIPCION**
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	**DISPONIBILIDAD**	**DESCRIPCION**
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Valor del Activo		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION (Clasificación Información)**
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta, Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja, Baja

Frecuencia de Uso		
CODIGO	**CONFIDENCIALIDAD**	**DESCRIPCION**
A	Alta	Información utilizada en forma diaria o semanal
M	Media	Información utilizada en forma mensual o semestral
B	Baja	Información utilizada en forma anual

Formato 2. Reporte de Incidentes de Seguridad.

Fecha y hora del llenado del reporte: _____

Datos personales

Llene esta parte con los datos personales de la persona que está llenando el reporte.

Nombre completo:	
Cargo:	Oficina:
Dependencia:	Correo electrónico:
Teléfono móvil:	Teléfono fijo:

Información sobre el incidente

La información que usted proporcione acerca del incidente ayudará a dar solución de una mejor y más rápida forma.

Fecha y hora en que se suscito el incidente: _____

Uso indebido de información.		Cambio en la configuración en equipo.
Uso inadecuado de recursos informáticos.		Ataque o infección de malware, o código malicioso (virus, gusanos, troyanos, etc.)
Divulgación no autorizada de información personal.		Acceso o intento de acceso a un sistema informático.
Acceso o intrusión física.		Pérdida o destrucción no autorizada de información.
Ingeniería social.		Interrupción en los servicios de red.
Uso indebido de correo electrónico institucional.		Anomalía o vulnerabilidad técnica del software.
Modificación de información de un sitio o página.		Robo o pérdida de equipo.
Robo o pérdida de información.		Amenaza o acoso por medio electrónico
Modificación, instalación o eliminación de software.		Otro no contenido:

Descripción del incidente

Brevemente describa y proporcione información acerca del incidente				
Detección del incidente				
Describa brevemente como se detecto el incidente				
El incidente aun esta en progreso	Sí		No	
Tiempo aproximado de duración del incidente:				

Información sobre el activo o bien afectado

Si conoce la información, llene los campos acerca de la información concerniente al bien afectado.

Código del activo o del bien				
Descripción del activo o bien:				
Localización física:				
Descripción breve de la información en cuestión:				
¿Existe una copia o respaldo de la información?	Sí		No	
¿El recurso afectado tiene conexión con la organización?	Sí		No	
¿El recurso afectado tiene conexión a internet?	Sí		No	
Sistema operativo:				

En caso de intrusión llene esta parte.

Nombre(s) de la maquina(s) comprometida(s).		
Sistema operativo indicando versiones:		
Indique las acciones que se tomaron antes o después de la intrusión:		
Usuarios comprometidos:		
Existen otras máquinas afectadas por la intrusión. Especifique.		
¿Se ha contactado a otras organizaciones? Especifique.		
Se autoriza o no al para suministrar información a otras organizaciones que colaboren para la solución e investigación del incidente.	Sí	No
Nombre completo y firma del responsable que autoriza.		

Otros contactos

Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente:

Nombre:	
Correo electrónico:	Teléfono:
Nombre:	
Correo electrónico:	Teléfono: