2012

PLAN DE CONTINGENCIA INFORMATICO

Personería Municipal de Yumbo

Tabla de Contenido

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

CAPITULO I: ANALISIS DE LA SITUACION ACTUAL INFORMATICA EN LA PERSONERÍA MUNICIPAL

1.1. Introducción.

Todos los Sistemas de Redes de Computadoras siempre van a estar expuestos a diferentes factores de riesgo y problemas, dichos agentes pueden llegar a ser tanto humanos como físicos. Frente a cualquier adversidad, la velocidad con que se determine la gravedad del problema depende de la capacidad y el plan a seguir para determinar con exactitud, las características principales de cada contrariedad.

A partir de diferentes fallas en componentes específicos pueden originarse pérdidas fatales, ya sea por desastres naturales o humanos que traerían consigo daños irreparables.

Este tipo de planes permiten reducir las consecuencias que se generan a partir de estos fallos y errores, y en su mayor posibilidad evitar dichos problemas, también garantizar la seguridad física de un sistema de información de datos. También se tendrán un análisis de los riesgos, respaldo de la información y como se decía anteriormente, recuperación de los datos.

Permite realizar un Análisis de Riesgos, Respaldo de la información y su posterior Recuperación de los datos.

1.2. Objetivos e Importancia del Plan de Contingencia.

Garantizar la continuidad de la operatividad en los diferentes procesos, de los elementos considerados críticos que componen los Sistemas de Información.

Definir actividades y procedimientos a ejecutar en caso de fallas o desastres de los elementos que componen un Sistema de Información.

Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes y durante la emergencia.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

1.3. Sistema de Red de Computadoras en la Personería Municipal.

La Red de la Personería Municipal de Yumbo, no cuenta con una estructura determinada basándose en Tecnologías de la información (TI), se tiene una serie de computadores conectados entre sí con la ayuda de switches. Un sistema de comunicación interno, dos sistemas de información principales que son; IntraFile que maneja la gestión documental, y el ASCII; que se utiliza para llevar toda la contabilidad de la entidad.

No se cuenta con equipos que administren la Red (Servidor), hay un equipo que cumple con esa función pero no está acondicionado estrictamente para esta tarea, porque además cumple con funciones adicionales.

1.4. Sistemas de Información de la Personería Municipal.

La Personería Municipal del municipio de Yumbo cuenta con dos (02) Software de Aplicación que son básicamente los que manejan la parte documental de la entidad y la parte contable.

Se incluyen documentos electrónicos, información histórica de la entidad en medios magnéticos e impresos en papeles, documentación y manuales.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

CAPITULO II: PLAN DE REDUCCIÓN DE RIESGOS

Se busca tener un amplio análisis de todas esas posibles causas por las cuales pueden estar expuestos los equipos de computo conectados a la Red de la Personería Municipal, igualmente como todos los datos que se encuentran almacenados en los diferentes medio magnéticos de la entidad.

Se realizara un detallado Análisis de Riesgos para poder tener claridad del proceder en los diferentes casos.

2.1. Análisis De Riesgos

Mediante este análisis se pretende desglosar de una manera amplia los posibles riesgos que puedan afectar tanto los equipos como la información que a diario se procesa en la entidad.

Bienes susceptibles a un daño	**Daño**	**Fuentes de Daño**
Personal	Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas	Acceso no autorizado
Hardware		Ruptura de las claves de acceso a los sistema computacionales

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Software y utilitarios	Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.	Desastres Naturales: a) Movimientos telúricos b) Inundaciones c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario)
Datos e información	Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia	Fallas de Personal Clave: por los siguientes inconvenientes: a) Enfermedad b) Accidentes c) Renuncias d) Abandono de sus puestos de trabajo e) Otros
Documentación		
Suministro de energía eléctrica		Fallas de Hardware: a) Falla en el Servidor Despacho (Hw) b) Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall)
Suministro de telecomunicaciones		Incendios

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

2.1.1. Valoración de los Riesgos

En la entidad se tendrá una valoración de cada riesgo (alto, mediano, bajo y muy bajo) y se identificaran las aplicaciones que representen mayor riesgo de la siguiente manera:

El objetivo de este ítem es determinar hasta qué grado es factible combatir los riesgos encontrados. Los riesgos que no queremos o podemos combatir se llaman riesgos restantes y no hay otra solución que aceptarlos.

Los riesgos serán medidos bajo la siguiente nomenclatura:

Alto

Mediano

Bajo

Muy bajo

2.1.2. Riesgos

Para que un sistema se pueda definir como seguro, debe cumplir 3 características fundamentales:

- ✓ Integridad: La información solo puede ser modificada por quien está autorizado.
- ✓ Confidencialidad: la información solo debe ser legible para los autorizados.
- ✓ Disponibilidad: debe estar disponible cuando se necesita.

Son muchas las soluciones que se han desarrollado para contrarrestar el problemas de disminución de los riesgos en los sistemas de información, pero

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

en general se puede concluir que el problema de la inseguridad no ha sido resuelto, y la perspectiva que se tiene es que, es muy difícil hallar una salida debido a que las amenazas son evolutivas, a medida que crecen los métodos de contingencia, crecen y se crean nuevos mecanismos para hacer daño.

En la Personería Municipal de Yumbo se han identificado una serie de riesgos, que podrían llegar a causar detrimentos graves, tanto en los archivos como en los equipos informáticos de la entidad, dichos riesgos son:

Robo Común de Hardware e Información:

Se considera como un factor de frecuencia moderada pero de un impacto grave, con una probabilidad de ocurrencia aleatoria, y al mismo tiempo con unas consecuencias altamente desastrosas.

Situación actual en la entidad:

La entidad cuenta con vigilancia permanente de cámaras de seguridad, no se cuenta con personal de vigilancia.

La salida de los equipos informáticos es registrada por el personal de la Oficina de Despacho.

A pesar de estas medidas de seguridad, en el mes de diciembre del año 2.011, se reporto un caso en el que fueron hurtados unos discos duros donde se encontraban los videos de seguridad, los cuales reportaban sobre un robo en una de las oficinas, igualmente parte de la información almacenada por el sistema Intrafile.

Vandalismo:

Se considera como un factor de frecuencia muy bajo pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Situación actual en la entidad:

En la entidad actualmente este es un riesgo que no se considera que se pueda presentar, pero si ha pasado, ya que se cuenta con un personal muy bien nombrado y en su mayoría profesional.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

No se corre un peligro alto de que los equipos sean dañados con intensión, ni que la información se pierda.

Fallas en los Equipos:

Situación actual en la entidad:

En la entidad se considera como un factor de frecuencia alto y con un impacto grave, con una probabilidad de ocurrencia muy considerable, y con unas consecuencias altamente desastrosas.

La Personería Municipal no cuenta con un servidor que controle la red de computadores, no se cuenta con un sistema de Backup, los equipos informáticos no tienen UPS, y además se tienen muchos fallos en la Red Eléctrica ya que no existe un adecuado cableado eléctrico, debido a que las instalaciones de la Personería Municipal de Yumbo son antiguas.

Existe Mantenimiento tanto preventivo como correctivo de los equipos de cómputo, pero en su mayoría son dispositivos obsoletos que ya casi cumplen su ciclo de vida.

Virus Informáticos:

Para este tipo de riesgo se considera como un factor continuo de frecuencia, con un impacto grave.

Situación actual en la entidad:

La entidad no cuenta con un Software Antivirus corporativo, la aplicación que se utiliza es gratuita por lo tanto la seguridad no es de alta confianza. Se debería obtener un Antivirus corporativo, y tratar de que las licencias no se expiren y sus actualizaciones sean constantes.

Todos los programas y aplicativos que se instalan son manejados estrictamente por el personal encargado de Informática los cuales son instalados con su respectiva licencia.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Equivocaciones:

La equivocaciones casi siempre son de manera involuntaria por tal razón se considera como un factor de frecuencia moderada y de probabilidad de ocurrencia moderado.

Situación actual en la entidad:

Se debe tener en consideración que al personal nuevo se debe Capacitar inicialmente para que conozca su ambiente de trabajo y dejar claro sus funciones con ayuda del Manual de Procedimiento.

Se deben convocar reuniones de capacitación, ante nuevas opciones en los sistemas o algún cambio de aplicación o al ingreso del personal nuevo.

Accesos no Autorizados:

Se considera como un factor de frecuencia aleatoria pero de un impacto grave.

Todos los usuarios deben tener un "login" o un nombre de cuenta de usuario y una clave de acceso a los equipos, esto conlleva a tener un mayor control en la información.

Situación actual en la entidad:

Algunos equipos cuentan con usuarios administrativos e invitados, pero no todos tienen esta restricción.

Cuando existe el sistema de usuarios con sus respectivos permisos, la contraseña es compartida con todos los compañeros de oficina y/o dependencia.

No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves.

Fraude:

Se considera como un factor de media frecuencia pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Situación actual en la entidad:

Por ser una entidad pública como su nombre lo indica la información es pública, pero puede ser utilizada para uso mal intencionados, ya que no se cuenta con restricciones en la información y cualquier funcionario o contratista tiene acceso a ella.

Fuego:

Se considera como un factor de baja frecuencia pero de un impacto grave, con una probabilidad de ocurrencia muy casual.

Situación actual en la entidad:

La Personería de Yumbo cuenta con un sistema sencillo de prevención de incendios, basado en extintores, los cuales están ubicados estratégicamente en los pasillos de la entidad.

Se han ejecutado programas de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que ayuda a enfrentar este tipo de situaciones y sus efectos.

Fenómenos Naturales:

Como los fenómenos naturales son eventos impredecibles, su frecuencia es aleatoria pero el impacto es muy alto dependiendo del tipo de fenómeno.

Por la zona geográfica en que se encuentra la entidad, solo podemos asociar como riesgo propenso a ocurrir, el terremoto.

Las inundaciones por causa de la lluvia no se contemplan para esta entidad ya que las instalaciones aunque no son excelentes, se cuenta con una estructura en buen estado.

Estos riesgos explicados anteriormente los podemos clasificar según su probabilidad de ocurrencia, de la siguiente manera:

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Tipo de Riesgo	Probabilidad de Ocurrencia	Causa Controlable	Intensidad del Daño (1-10)
Robo de hardware e información	Alto	Si	5
Vandalismo	Mediano	Si	10
Fallas en los equipos	Mediano	No	8
Virus Informáticos	Alta	Si	8
Equivocaciones	Mediano	Si	5
Accesos no autorizados	Alta	Si	5
Fraude	Bajo	Si	3
Fuego	Muy Bajo	Si	10
Fenómenos Naturales	Muy Bajo	No	10

2.2. Análisis de Fallas en la Seguridad

El estudio que se ha realizado sobre las posibles fallas en la seguridad de la información implican muchos factores en la entidad, principalmente de que en la planta de cargos de la entidad no existe un ingeniero de sistemas o una persona con conocimientos de informática, igualmente no se tiene un departamento o proceso de Sistemas, razón por la cual no se cuenta con un área especializada o responsable para que maneje y lidere todo lo relacionado con información que se encuentra digitalmente y con la parte física de los equipos de computo.

Se maneja un inventario de Hardware y Software, por lo cual se tiene un conocimiento muy preciso de lo que posee la entidad en cuanto a equipos y programas de cómputo que necesitan licencia.

La Seguridad de la Información en la Personería Municipal de Yumbo se ve fácilmente vulnerada puesto que no existe una red bien establecida, tampoco

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

hay un servidor, y los equipos cuentan con un sistema de antivirus gratuito, que no brinda las condiciones mínimas de seguridad y prevención de antivirus.

No se tiene un sistema de Backup sistemático, por consiguiente nunca se realizan copias de seguridad de la información de los equipos.

2.3. Protecciones Actuales

En la Personería Municipal del Municipio de Yumbo se realizan las siguientes protecciones:

Al Robo de Información: Algunos equipos cuentan con claves de usuario, se mantienen cerradas las puertas de las oficinas si no hay nadie en el momento. Algunos escritorios cuentan con llave de seguridad, el cuarto de Archivo Central permanece bajo llave.

Al Vandalismo: Se mantienen vigilancia por parte de un policía bachiller en la entrada de la entidad, las oficinas nunca permanecen solas.

A la Protección de la Información y Equipos: Por el momento en los equipos se cuenta con protección de antivirus gratuito, y se le realiza mantenimiento preventivo. Se vacunan los dispositivos de almacenamiento que se utilizan en los equipos. Cuando se requiere personal contratista se intenta conseguir a empleados debidamente preparados.

Fuego: se tienen instalados extintores, en sitios estratégicos y se ha brindado entrenamiento en el manejo de los extintores al personal.

2.3.1. Seguridad de información

Para todas las empresas la información es uno de los bienes más preciados con que se cuenta, por esta razón muchas de estas no se miden en gastos en cuanto a Seguridad de la información y de los equipos informáticos, ya que este es un tema que puede llegar a afectar la imagen de cualquier institución, inclusive la vida privada de las personas.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

La mejor manera de protección contra la pérdida o la modificación no autorizada de los datos de la entidad es realizar copias de seguridad (Backup), y almacenar dichas copias en un lugar seguro.

Para realizar estos Backups, de debe tener un estudio previo, que me permita definir, que sistema de Backup se va a utilizar, si es necesario utilizar algún dispositivo electrónico especializado para realizar estas copias de seguridad, con qué frecuencia se va a realizar y sobre todo cuales son los archivos a los cuales se les hará la respectiva copia, también donde se almacenaran estas copias.

La implementación de un Sistema de Backup debe ir acompañado de ciertas directrices que deben seguirse paso a paso para que su objetivo final tenga un buen resultado. Crear una política de seguridad donde se incluya la realización del Backup en el tiempo establecido y de manera obligatoria.

2.3.2. Prevención de Contingencias

En este ítem se tendrá un análisis mas especifico de las tareas que se tienen que realizar para poder prevenir el impacto de los riesgos en caso de que alguno de estos suceda. Adicionalmente, permitirá llevar un mayor control sobre el desarrollo de las tareas de respaldo tanto de Hardware y Software en caso tal de que no se estén llevando a cabo, a fin de estar preparados cuando surja alguna eventualidad.

Tipo de Riesgo	Medida a Tomar
Robo de hardware e información	Control del personal y personas visitantes en la entidad por medio de las cámaras de seguridad. Implementar el sistema de Backup por medio de una aplicación informática.
Vandalismo	Capacitación y Evaluación al personal contratante.
Fallas en los equipos	Realizar mantenimiento preventivo, se debe realizar reposición por tiempo de vida útil, y mantenimiento preventivo en la red eléctrica. Adquirir antivirus y

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

	firewall corporativos.
Virus Informáticos	Adquirir antivirus y firewall corporativos, y actualizados.
Equivocaciones	Capacitación y Evaluación al personal, tanto como contratista como de planta.
Accesos no autorizados	En el caso de los accesos Físicos No Autorizados se deben tener letreros de advertencia, orientación al personal de visita y de planta. En el caso de accesos Lógicos No Autorizados se deben de realizar cambios de Claves de acceso periódicamente.
Fraude	Control y Evaluación del personal a cargo de la jefatura de cada proceso.
Fuego	Se eliminaran todo tipo de material inflamable dentro de las oficinas, se debe tener una ventilación adecuada, capacitación al personal y mantenimiento preventivo a la red eléctrica para evitar cortos eléctricos.
Fenómenos Naturales	Capacitación al personal a cargo de los entes especializados en dichos casos (Bomberos, Defensa Civil, etc.) con el fin de disminuir perdidas humanas en el momento de ocurrir estos tipos de casos.

CAPITULO III: PLAN DE RESPALDO DE LA INFORMACIÓN

3.1. Actividades Previas al Desastre

Vamos a definir todas las actividades de planeación, preparación, entrenamiento y ejecución de las acciones de resguardo de la información.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

PLAN DE ACCION

Sistemas de Información en la entidad:

A continuación se determinan los sistemas de información utilizados en la Personería Municipal de Yumbo, los cuales son primordiales para el correcto desarrollo de las operaciones diarias.

Nombre del Sistema	***Procesos que Utilizan el Sistema***
ASCII	Contabilidad Tesorería
INTRAFILE	Despacho Personería Contabilidad Tesorería Gestión Documental Asesoría y Control PVCO Derechos Humanos Asuntos Judiciales Victimas
EXTRANET	Gestión Documental

Actividades a Realizar para recuperar la información:

Esta es la principal razón para que la implementación de un sistema de Backup sea una realidad, porque la primera herramienta que se utiliza recuperar información es mediante la copia de seguridad que se hace en su debido tiempo periódico.

Por lo regular el Backup es almacenado en la oficina de sistemas, o en el despacho en este caso. Estas copias de seguridad deben estar debidamente clasificadas para poder tener una rápida identificación de la información que se necesita.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Almacenamiento y Respaldos de la Información:

Se deben crear unas Políticas de Seguridad, que incluyan la forma de almacenar la información en el equipo de informática, la manera de realizar una copia de seguridad, etc.

Se debe implementar de manera urgente un sistema de Backup el cual me permita de manera organizada y bien estructurada identificar la información requerida.

Prácticas Habituales:

Dentro de las Políticas de Seguridad se tienen que incorporar recomendaciones sobre el cuidado y el aseo de los equipos de cómputo.

Y se debe poner en práctica la reposición de equipos, básicamente este proceso se lleva a cabo en tres situaciones muy particulares:

- ✓ Cuando cumple su Ciclo de Vida.
- ✓ Cuando falla el Hardware.
- ✓ Cuando exista una perdida.

3.2 ACTIVIDADES DURANTE EL DESASTRE

En este caso se debe primero que todo identificar una persona, la cual es la encargada de coordinar y evaluar la posibilidad de salvar recursos informáticos (Hardware e Información), sin arriesgar la vida.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

Si no existe la posibilidad de salvar algún equipo informático, esta persona deberá ponerse a disposición de cualquier equipo de personas para combatir el siniestro.

La persona que será delegada para esta actividad, deberá tener un conocimiento amplio en informática, condiciones físicas apropiadas para realizar transporte físico de equipos, responsabilidad, etc.

Si es necesario, dependiendo del siniestro que suceda, se debe contar con un directorio telefónico de fácil acceso con los principales números de los organismos directamente relacionados (Bomberos, Defensa Civil, Policía, etc.)

3.3 ACTIVIDADES DESPUES DEL DESASTRE

Cuando un siniestro sucede se deben seguir ciertas medidas debidamente listadas y ordenas por el personal a cargo, dichas actividades son clasificadas de la siguiente manera:

Tipo de Riesgo	Medida a Tomar
Robo de hardware e información	Diagnostico y su respectivo informe al Despacho de la Personería, si es el caso informar a la Policía.
Vandalismo	Evaluación del daño y restauración de los archivos con las copias de seguridad. Se comunicara con el Despacho de Personería, y si el caso lo amerita le hará el respectivo llamado a la Policía.
Fallas en los equipos	Se realiza el diagnostico y se procede al mantenimiento correctivo o ver las políticas de reposición del equipo.
Virus Informáticos	Desinfección o eliminación con el

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

	antivirus corporativo actualizado.
Equivocaciones	Diagnostico, si es el caso se restauran los archivos con las copias de seguridad, también se solicitan al encargado de sistemas restaurar las contraseñas de ingreso.
Accesos no autorizados	Bloqueos de las contraseñas de acceso, y evaluación del proceso a cargo para realizar las respectivas acciones.
Fraude	Diagnostico y su respectivo informe al Despacho de la Personería, si es el caso informar a la Policía.
Fuego	Como primera medida utilizar los extintores, seguido de una llamada a los Bomberos Voluntarios de Yumbo. Cortar el fluido eléctrico. Y si el siniestro incluye heridos se llamara al Hospital La Buena Esperanza de Yumbo.
Fenómenos Naturales	Coordinar con las entidades directamente implicadas. (Bomberos, Defensa Civil, Policía, Hospital, etc.)

Se debe realizar un diagnostico de los daños para así poder definir desde el Despacho de la Personería, cuales serian los puntos que hay que recuperar.

En este nivel del Plan de Contingencia Informático se deben tomar decisiones importantes como definir roles del personal según la emergencia, cambiar la priorización de algunas actividades, etc.

La persona encargada de coordinar la ejecución del Plan de Contingencia Informático deberá establecer las diferentes etapas en que se desarrollen las actividades ya mencionadas en documento.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co

También se deberá llevar un registro documental de cada vez que ocurra un siniestro, para poder tener un archivo de ejecución del Plan de Contingencia, el cual me permita hacer un análisis mas profundo de los riesgos y así poder realizar una retroalimentación al Plan.

El Plan de Contingencia Informático debe tener un constante chequeo por parte de los directos implicados en el tema, en colaboración con los altos directivos. La optimización de este también debe ser una actividad fundamental después de ocurrida alguna contingencia o por algún cambio tecnológico, para así poder tener un verdadero mejoramiento de las actividades del plan y un refuerzo de los mecanismos que tuvieron un correcto funcionamiento.

Carrera 4 No 4 - 26 B/Belalcazar Yumbo - Valle Tel: (57 2) 669 3686
E-mail: ministeriopublico@personeriayumbo.gov.co