Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÒN

I. INTRODUCCIÒN

Este instrumento refiere a la Política de Seguridad de la Información de la Personería Distrital de Buenaventura, para su elaboración se posesiona como base los registros y requisitos referidos en el estándar ISO/IEC 27001. Las políticas incluidas en este manual se instituyen como parte primordial del Modelo de Gestión de Seguridad de la Información de la Entidad y se convierten en el asiento para la organización de los controles, procedimientos y estándares.

Si bien es cierto la seguridad informática se localiza en un momento de gran incremento, en ocasión a los variables escenarios y nuevas tarimas de computación valederas. El suceso de interconectarse a través de puntos de redes, apertura a nuevas perspectivas para sondear más allá de los términos, argumento que ha llevado a la visión de nuevos riesgos en los sistemas de información, como son el hurto, virus, perdida de información entre otras situaciones circunstanciales. Esto nos acarrea a desplegar documentos que sitúen la inercia adecuada. Esta política es prioridad para la entidad y por tanto es responsabilidad de todos los funcionarios velar por el imperecedero cumplimiento de las políticas determinadas en el vigente documento.

II. OBJETIVOS Y ALCANCE

a. Objetivo General.

Instaurar y difundir los criterios y conductas que corresponden a todos los funcionarios, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la Personería Distrital de Buenaventura o que tenga acceso a los activos de información, con la intención de salvaguardar la Confidencialidad, Disponibilidad e Integridad de la información a fin de fortificar la prolongación de las prontitudes administrativas, y operativas de la Entidad, preservando convenientemente la información,

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

subyugando los riesgos y perfeccionando la transformación en tecnologías de información. Por lo cual, se producirá en concordancia con las disposiciones legales actualizadas.

b. Objetivos Específicos:

- Sensibilizar a los funcionarios y contratistas sobre la estimación de realizar un uso apropiado de los bienes y servicios informáticos que ofrece este ente.

- Adecuar el progreso continuo en los términos informáticos que acarree la entidad.

- Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

c. ALCANCE:

Con el presente, se puntualizan las políticas y pautas informáticas para todos los beneficiarios que asumen a su cargo peculios informáticos; dirigirlos a merecer los productos institucionales y anunciarles las políticas que conviene utilizar para el buen uso de los equipos de cómputo, aplicaciones y restantes productos informáticos. La capacidad concreta y sus posteriores actualizaciones emplean a cada uno de los activos y recurso de la información de este Ente.

Las Políticas y Normas de Seguridad de la información son aplicables a la administración de:

- **La información:** Conjunto organizado de datos procesados almacenados en cualquier medio magnético y/o físico.
- **Las Personas:** Beneficiarios y Administradores de la información, bien sean los empleados, contratistas y terceros que prestan servicios a la entidad.
- **El hardware**: Dispositivos de computación, telecomunicaciones y redes.
- **El software**: Sistemas estratégicos, esquemas, productos y aplicaciones.
- **Procesos:** Establece las Políticas y Normas de Seguridad de la información, resguardan cada una de las operaciones y funciones que se apoyen en sistemas de información

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

III. MARCO CONCEPTUAL :

La seguridad de Información puntualiza a la entidad las medidas estructurales, metódicas y sociales, indispensable para salvaguardar los activos de información: hacking informático, divulgación, duplicación, intercepción, destrucción, pérdida, daños, deterioros, robo, mal uso, interrupción de sistemas, entre otros; que se pueda ocasionar de forma premeditada o accidental.

IV. NORMATIVIDAD

El marco que regula la seguridad de la información está conformado Norma Internacional ISO 27000 y 27001, con sus respectivas actualizaciones liberadas, que se ha configurado como un estándar de facto a la hora de auditar los aspectos relacionados con la seguridad de la información en las organizaciones.

BENEFICIOS DE LA NORMA ISO 27001

Los trances riesgos de seguridad de la información constituyen una amenaza desmedida para las empresas debido a la posibilidad de pérdida financiera o daño, la pérdida de los servicios esenciales de red, o de la reputación y confianza por los usuarios.

V. NECESIDAD DEL SISTEMA DE SEGURIDAD INFORMATICA

La creación de Políticas de Seguridad Informática en la Personería de Buenaventura, es de vital necesidad y de urgencia evidente, donde se asume la intervención total de la información, instalación, desinstalación y ejecución de Software por parte de los Administradores del Sistema, y con ello inspeccionar el acceso a dichas aplicaciones.

Las normas y políticas expuestas en este pliego nos sirven de reseña, sin la intención de posicionarla como norma absoluta, puesto que esta se encuentra sujeta a constantes cambios, de acuerdo a las necesidades circunstanciales siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios prestados por la red a los usuarios finales.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

Todo responsable en el manejo de equipos tecnológicos y programas informáticos pertenecientes a la Personería de Buenaventura, deber conocer y acatar el presente reglamento, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier casualidad que implique la seguridad de la información o de la red institucional.

VI. TERMINOLOGÍA Y DEFINICIONES DE CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Activo de información**: Esta situación hace referencia al recurso perceptible o intangible que sea de valor e importancia para la organización.
- **Integridad:** Consiste en salvaguardar que el activo de información describa las propiedades de: exactitud, precisión, consistencia, confiablidad y totalidad.
- **Confidencialidad:** Reside en garantizar que el activo de información no sea divulgado por personas, entidades o procesos NO autorizados.
- **Disponibilidad:** Trata en garantizar que el activo de información sea posible y disponible en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.
- **Trazabilidad:** Asegurar que en todo momento se podrá determinar quién accedió a qué activo de información (servicio, datos, etc.), qué hizo y en qué momento lo hizo.
- **Autorización:** Refiere al otorgamiento a una persona, entidad o proceso, para acceder a un activo de información.
- **Confiabilidad:** La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.
- **Eficiencia:** Criterio de calidad en que el procesamiento y suministro de la información, que debe contar con la capacidad de lograr ese efecto con el mínimo de recursos posibles o en el menor tiempo posible.
- **Archivos:** es la agrupación de datos que se acopian en el Disco Duro y/o cualquier otro medio de almacenamiento.
- **Autorización:** Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información o activos físicos.
- **Backup:** Copiar y resguarda la información para protegerla de posibles riesgos.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

- **Contraseña:** Clave para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc. Esta clave debe ser personal e intransferible y no se debe anotar en documentos físicos de fácil acceso.
- **Cuenta de Usuario:** Es el identificador que utiliza un Sistema de Información en la autenticación de un usuario.
- **Cuenta de Correo:** Prestación en línea que abastece un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en Internet.
- **Equipos de cómputo**: Dispositivo electrónico que se emplea para procesar datos. También pueden ser considerados como equipos de cómputo los equipos que prestan servicios de almacenamiento y procesamiento desde la nube.
- **Hardware**: Partes físicas de un sistema de procesamiento de datos,
- **Información:** Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Medios de almacenamiento externo:** Medio utilizado para el almacenamiento de información, que puede conectarse o introducirse y retirarse del Hardware por varias interfaces como puertos USB, unidad de cinta, unidades de disco, etc.
- **Recursos informáticos:** Software y hardware.
- **Red:** Nombre dado al conjunto de equipos de cómputo y de telecomunicaciones, interconectados entre sí al interior de la organización, para permitir a los usuarios acceso a los recursos tecnológicos.
- **Software**: Es el conjunto de instrucciones mediante las cuales el Hardware puede realizarlas tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.
- **Software ilegal:** Es el Software que se adquiere y se instala sin el consentimiento de la empresa que lo desarrolla o sin licencia de uso.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

VII. POBLACIPÒN DESTINATARIA.

Existen diferentes grupos de personas que se relacionan con el sistema de información, los cuales por sus funciones dentro de la Personería de Buenaventura tienen diferentes acciones y autorizaciones frente al sistema. Estas personas se pueden diferenciar en Practicantes o Judicantes, Usuarios, Líderes de Procesos y Administradores del sistema de información.

VIII. OBLIGACIONES DE LOS FUNCIONARIOS Y CONTRATISTAS EN RELACIÓN CON LA INFORMACIÓN

Funcionarios, contratistas y terceros

- Acatar las políticas de Seguridad de la Información, contempladas en el presente escrito.
- Recurrir únicamente a software y demás recursos tecnológicos autorizados.
- Custodiar por el desempeño de las políticas de Seguridad de la Información dentro de su ambiente laboral.
- Recurrir a los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.

Los objetivos que se pretenden alcanzar con el cumplimiento de los deberes:

- Cerciorar que los funcionarios puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos por el procedimiento elegido.
- Certificar que la información entregada sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

- Organizar a cada uno de los funcionarios por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

LAS SITUACIONES QUE SE PUEDEN PRESENTAR POR EL NO CUMPLIMENTO DE LOS DEBERES ANTES DESCRIPTOS.

- **Phishing (Pesca).-** Es el acto de pescar usuarios mediante señuelos y de este modo obtener información financiera y contraseñas para intentar adquirir información confidencial de forma fraudulenta.
- **Spoofing (suplantación de identidad)**.- Es una técnica que consiste en hacer creer al receptor de un mensaje de correo electrónico, que quien remite el mensaje es alguien de confianza. El verdadero emisor queda suplantado por una dirección real, que ofrece garantías al receptor, que abrirá ingenuamente el mensaje sin conocer los verdaderos motivos (ocultos).
- **Hoax (correos falsos).-** Es un mensaje de correo electrónico con contenido falso o engañoso. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante, a que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.
- **Spammers.-** Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido; habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.
- **Crimeware.-** Es un software diseñado específicamente para cometer delitos financieros en entornos en línea, técnicas mediante la ingeniería social u otras técnicas genéricas de fraude en línea. El objetivo es robar identidades en línea para acceder a los datos financieros de un usuario, con el fin de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.
- **Malware (Software malicioso)**.- Es un tipo de software que tiene como objetivo infiltrarse o dañar un Pc sin el consentimiento de su dueño.
- **Virus.** Es un software que se copia por sí mismo, infecta un Pc, se propaga dentro de todo los archivos, luego se copia de Pc a Pc; estos virus se adhieren en archivos

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

específicos (de arranque, script, macros o ejecutables); el fin de este software es alterar o corromper el funcionamiento normal de un Pc.

- **Spyware.** Es un software cuyo objetivo es mandar información a un tercero de toda las páginas visitadas; el fin es espiar y recabar información de las páginas a las cuales fueron visitadas (incluyen claves de cuenta, correos, etc.) para luego en lo posterior, enviar o saturar de publicidades. La recolección de esta información es mediante un canal falso, produciendo un consumo de ancho de banda de internet y a su vez poniendo lento el computador.
- **Gusano.** Es un software cuyo único cometido radica en pasar de Pc en Pc a través de redes informáticas en forma automática sin la intervención de ningún usuario; estos normalmente buscan traspasar los agujeros de seguridad para infectar toda la red a su alcance.
- **Adware**.- Se trata de un software que permite publicidad no deseada vía Internet y que generalmente se instala sin nuestro consentimiento.
- **Scareware (Software de miedo).-** Es un software que engaña a un usuario para descargar un programa haciendo creer que está infectado de virus; es un método de estafa para hacer comprar un software utilizando prácticas comerciales poco éticas.
- **Rogue software.** Software que hace creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso; esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.
- **Hijacking.** Es una técnica ilegal que tiene por objetivo el adueñarse o robar (TCP/IP, página web, dominio, navegadores, módems, temas de foros, sesiones de terminal, servicios etc.) mediante una conexión de red.
- **Defacement.** Hace referencia a la deformación o cambio de manera intencionada a una página web, ya sea por venganza, diversión o burla; esto se debe a algún error de programación de la página por algún bug en el propio servidor o por una mala administración de este.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

- **Hacker.** Persona que es capaz de eludir los sistemas de seguridad de un computador para acceder a la información que contiene ya sea con fines maléficos o benéficos.
- **Rootkit.** Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

IX. RAZON DEL MÉTODO DE INFORMACIÒN

Actividades convidadas por el sistema.

La finalidad del Sistema de Información es brindar productos viables a los usuarios, en cada uno de los sistemas que prestar el servicio, donde puede incurrir en acercarse a un riesgo informático que deben ser estudiados y analizados diligentemente, como fragmento de un esclarecimiento profundo de políticas de seguridad, y rezagado en un plan de casualidades que nos consienta restablecer la metodología complementaria, o parte de él, en caso de una situación calamitosa, por circunstancias inherentes y no viciadas , o hechos vandálicos o fortuito, cualquiera de ella puede afligir el hardware, el software o la biósfera física del sistema de información.

Productos que crean diferentes exigencias para permitir a ellos, para ello realizare una descripción puntual y clara de cada uno.

- **Comedimientos de software**

El software es una técnica de disposición rápidos facilita también la reinstalación en caso de contingencia Instalar en el aparato exclusivo del software ineludible la reducción de riesgos. De esta forma tener registrado el software asegura la calidad de la procedencia del mismo. En todo caso un catálogo del software provee una técnica correcta de testificar la reinstauración en caso de pérdida.

- **Centralización en la red.**

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

Los usuarios de la Personería Distrital de Buenaventura están acreditados para depositar información en la red, debidamente se causa por procesos, donde se concurre en zonas en la red plenamente particulares y/o restringidas para cierto grupo de usuarios, y otros públicos que pueden ser consentidos por muchas personas e incluso por todas las que tienen acceso a la red.

Correo Electrónicos.

Como instrumento institucional está capacitado para que los usuarios de la entidad se permitan la interrelacionarnos cerca y externa, así mismo el correo puede ser asentido internamente, o a exterior de la entidad, vía internet.

Acceso a Internet.

La vía a Internet consiente en que los usuarios internos de la red puedan acceder a todos los servicios que Internet provee y solo se podrá consultar información de carácter institucional.

Reservas de una red

Los accesos en la red son específicamente el correo, las páginas web y la entrada de archivadores de los discos.

Impresión en red

Ciertos beneficiarios tienen impresoras particulares en sus equipos, y otro grupo de usuarios recubran su información en impresoras de red.

- **Las amenazas:**

Cuando la categorización y funcionamiento de un conector de almacenamiento de la información se creen convincentes, se deben seguir considerando las circunstancias “amenazables” que pueden afectar datos informáticos, los cuales son casi inevitables, de modo que la forma más viable de defensa en la copia (en el caso de los datos) y la separación –en cuanto a la estructura de redes.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

Estos fenómenos pueden ser causados por las circunstancias mencionadas en el acápite VIII.

X. IMPACTO INSTITUCIONAL

Generalmente el recorrido de una política de seguridad se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y elementos de identificación. Estos mecanismos permiten que los funcionarios de la Personería de Buenaventura tienen sólo los permisos que se les dio.

La seguridad informática debe ser aprendida para que no impida el trabajo de los funcionarios haciéndolos necesarios que puedan utilizar el sistema informático con toda facilidad. Por eso en lo referido a obtener una política de seguridad, conviene:

- Ocasionar medidas y ordenamientos para cada servicio de la entidad sin que el compromiso de los funcionarios corra riesgos o se perciba ostentoso.
- Sensibilizar a los funcionarios con los problemas ligados con la seguridad de los sistemas informáticos.

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

Información: Es el objeto de mayor valor para la entidad, el objetivo es salvaguardar la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Equipos que la soportan: Software, hardware y organización.

Usuarios: los determinados así, a los sujetos que manipulan la organización tecnológica y de comunicaciones que manejan la información.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

XI. DEFINICION DE LAS ACTIVIDADES A CONCRETAR:

Recursos informáticos

- El funcionamiento de los peculios informáticos, estarán administrados por el cumplimiento de las "Políticas, Normas y Procedimientos de seguridad", y deber ser acatada por todos los usuarios de la entidad.
- El peculio informático disponible para cada usuario serán para rutina única de actividades de la Personería de Buenaventura.
- Los administradores del sistema de información son los responsables de mantener el hardware, software y entorno físico del centro de cómputo.
- La manipulación física y lógica de la estructura de la red de datos de la Personería es responsabilidad exclusiva de los administradores del sistema, y ninguna persona por fuera de este grupo está autorizada para manipular ninguno de los enlaces de la red de datos sin la previa autorización de la dependencia de Informática.

Acceso a Internet

- La Personería definirá a que usuarios les autoriza el acceso a Internet, según la necesidad de sus diligencias
- Se les suspenderá el servicio de Internet a los usuarios que tengan un reporte de navegación alto y que las páginas visitadas no sean de carácter institucional.
- La Personería restringe a los usuarios descargar archivos que pongan en riesgo las seguridades de la red de datos y el desempeño del canal de comunicaciones con Internet.
- El acceso es descalificado mostrando que por política institucional el acceso está priorizado.
- Cuando sea necesario la descarga de un programa de tipo particular con restricción, se debe solicitar a la dependencia de Informática, el cual analizara la viabilidad del producto.

Instalación de Software

- Todo el software que se instale en los equipos de la Personería de Buenaventura o en equipos que sean propiedad de terceros que funcionen dentro de las instalaciones de la entidad, debe estar legalmente licenciado.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

- Los productos de software y/o hardware que se instalen en los equipos de cómputo de la Personería debe ser autorizada y realizada o supervisada por usuario de la oficina de sistema.
- Las aplicaciones que se instalen en los equipos de cómputos deben causar reconocimiento, que verifique las actividades ejecutadas por los usuarios sobre los datos o la información.
- La instalación de software en forma ilegal será catalogada como una falta grave al reglamento interno de trabajo.

Instalación de equipos

- Los equipos que se conectan a la red de datos debe tener instalados programas Antivirus debidamente licenciados y actualizados. El programa debe residir en memoria, en los casos que el usuario inhabilite esta funcionalidad será responsable por los daños causados.
- La instalación de equipos de cómputo en la Personería de Buenaventura deber ser autorizada y/o supervisada por dependencia de informática.

Correo electrónico

- El correo electrónico debe manejarse de modo responsable; su fin es servir como instrumento para apresurar las líneas oficiales que afirmen la gestión institucional. Se debe utilizar la administración, operación y uso del correo electrónico como un instrumento de comunicación organizacional para facilitar el intercambio de información de los funcionarios.
- Con el propósito de minimizar los riesgos de virus, no existirán correos de destinatarios desconocidos y/o que no hacen referencia al asunto.
- No está autorizado devolver correos basuras o SPAM, estos correos son simplemente identificables ya que provocan al usuario a enviar cientos de correos a diferentes destinatarios, con la promesa de que esto les mejorará la vida.
- Los correos que entran y salen por Internet, no pueden exceder del tamaño definido en los lineamientos de la oficina de informática, para evitar que el desempeño del conducto de conexión a Internet se vea ostentoso.
- La información contenida en el correo electrónico debe ser depurada periódicamente, solo se debe almacenar información de carácter institucional.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

- El uso del correo electrónico es autorizado siempre y cuando se haga de modo responsable y no ocasione problemas legales a la entidad; no atente contra la imagen de la entidad; y no interfiera con el trabajo de los funcionarios.
- Como norma general está prohibido enviar mensajes de manera masiva, con contenido de cadenas a falsos virus etc., excepto si los mensajes contienen información de interés institucional,
- Los usuarios que no hagan parte de la familia institucional, se desactivarán y eliminarán después de veinte (30) días de su desvinculación, previa comunicación.

Régimen de seguridad.

- Se carga un detallado método de contingencias que cobije cada uno de los viables asuntos fatales que puedan perturbar al sistema de información. el compromiso y responsabilidad es del líder de cada diligencia y debe ser generosamente divulgado entre todo el personal involucrado en el proceso.

Metodologías de protección del sistema

- Legalizar la información: esta técnica nos minimiza riesgos, al adaptar contraseñas dificultosas de curiosear a partir de datos personales del individuo.
- Atención detenida y constante a la red.
- Programas tecnológicos protectores, manteniendo los sistemas de información con las actualizaciones que más impacten en la seguridad.

Afirmación común que nos acerca a un riesgo de la seguridad, el cual debemos evitar

- **Asegurar la protección porque no abro archivos desconocidos.** Es una acción errada, pues se vitalizan distintas formas de contaminación, puesto que el software ejecuta actividades sin la intervención del usuario, colocando en riesgo los sistemas.

  Aun así contando con programas de antivirus, ellos en general no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los computadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamiento de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

Buenaventura, Calle 2 Edificio CAD, piso 10. Teléfono 2978928
E-mail: personería.distrital@personeriabuenaventura.gov.co
www.personeriabuenaventura.gov.co
NIT.835 000010-3

XII. RECURSOS HUMANOS DISPONIBLES.

XIII. OBLIGATORIEDAD

El Manual de Políticas de Seguridad de la Información es de obligatorio acatamiento para todos los funcionarios, contratistas, o terceras personas que obtengan acceso a los activos de información de la Personería Distrital de Buenaventura. Cada uno de los usuarios, bien sean funcionarios, contratistas o terceros de la entidad, se encuentran obligados a cumplir con la protección en la información y las políticas de seguridad de la información después de terminar su relación con la Entidad. Cuando el usuario violenta las disposiciones de las políticas de seguridad de la información, ya sea por negligencia o dolo, la Personería en uso de las normas aplicara medidas pertinentes. Pudiendo solicitar la apertura de proceso disciplinario al funcionario o funcionarios que hayan violado las políticas y procedimientos de seguridad de la información.