PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CONCEJO MUNICIPAL DE PASTO

PRESENTACIÓN

El Plan de Seguridad Informática es fundamental en una corporación como el Concejo Municipal de Pasto, debido a la posible pérdida, destrucción, daño de equipos, robo, entre otras amenazas a las que se encuentra cualquier institución o corporación, teniendo en cuenta que en un sistema de red, donde todos los días se hace uso de computadoras, periféricos y otros dispositivos como celulares, la información se puede ver expuesta a diferentes riesgos y puede ser causal de distintos problemas internos.

En nuestro entorno de trabajo, las distintas dependencias hacen uso de equipos (Hardware) y programas (Software) los cuales están expuestos a múltiples factores de riesgos de tipo social, natural o físicos.

Por esta razón es importante que en el Concejo Municipal de Pasto, exista un plan de seguridad y privacidad de la información, el cual será realizado bajo las indicaciones del modelo de seguridad y privacidad de la información (MSPI), plan que hace parte integral de la Estrategia de Gobierno Digital de tal forma que ayude a mejorar el control que se le debe dar a la información y no presentar problemas futuros en la eficacia laboral en la corporación.

1. OBJETIVOS

1.1. Objetivo General

El objetivo principal de la seguridad y privacidad de la información es mantener un ambiente moderadamente seguro, alineado a la misión del Concejo Municipal de Pasto, y que permita proteger los activos de información de la misma, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad de la Corporación.

1.2. Objetivos Específicos

- Proteger los activos de información del Concejo Municipal de Pasto, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar y capacitar a los servidores públicos, funcionarios, contratistas y partes interesadas acerca del Sistema de Gestión de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante revisiones por parte de la alta dirección y auditorías internas planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión del Modelo de Seguridad y Privacidad de la Información.

2. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del Concejo Municipal de Pasto.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades públicas y la empresa privada sean confiables.

FASE DE DIAGNÓSTICO

- Estado actual de la entidad.
- Identificación el nivel de madurez.
- Levantamiento de información.

FASE DE PLANIFICACIÓN

- Contexto de la entidad
    - Entender la entidad.
    - Necesidades y expectativas de las partes interesadas.
- Liderazgo
    - Determinar alcance del MSPI.
    - Liderazgo y compromiso de la alta dirección.
    - Política de seguridad.
    - Roles de la identidad, responsabilidades y autoridad.
- Planeación
    - Acciones para abordar los riesgos y oportunidades.

- Objetivos y planes para lograrlos.

- Soporte

  - Recursos.
  - Competencias.
  - Sensibilización.
  - Comunicación.
  - Documentación.

FASE DE IMPLEMENTACIÓN

- Control y planeación operacional.
- Plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Definición de indicadores de gestión.

FASE DE EVALUACIÓN Y DESEMPEÑO

- Monitoreo, medición, análisis y evaluación.
- Auditoria interna.
- Revisión por la alta dirección.

FASE DE MEJORA CONTINUA

- Acciones correctivas.
- Mejora continua.

a) Protección de la información y de los bienes informáticos

El usuario o funcionario deberán reportar de forma inmediata al responsable del área de sistemas, cuando detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

El usuario o funcionario tiene la obligación de proteger las unidades de almacenamiento que se encuentre bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

b) Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones del Concejo Municipal de Pasto, deberá registrar al momento de su entrada, el equipo de cómputo y equipos audiovisuales en el área de recepción. Los

computadores de escritorio, portátiles y cualquier activo de tecnología de información podrán ser retirados de las instalaciones del Concejo Municipal de Pasto únicamente con la autorización de salida del área de recursos físicos, siguiendo el debido proceso.

c) Protección y ubicación de los equipos

Los usuarios de los equipos tendrán en cuenta para la protección de los equipos lo siguiente:

- Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos, sin autorización del encargado del área de sistemas, en caso de requerir este servicio deberá solicitarlo de forma escrita.
- El funcionario encargado de recursos físicos, será la persona encargada de hacer la entrega formal de los activos informáticos de la Corporación y la instalación y ubicación autorizada será potestad del encargado del área de sistemas.
- El equipo de cómputo asignado, deberá ser de uso exclusivo de las funciones de los funcionarios o servidores del Concejo Municipal de Pasto.
- Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente a la destinada para archivos de programa y sistemas operativos, o unidades de almacenamiento externas.
- Mientras se opere el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos. Se debe evitar colocar objetos encima del equipo de cómputo u obstruir las salidas de ventilación del monitor o de la CPU.
- Se debe mantener el equipo de cómputo en un lugar limpio sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar la reubicación de los cables al encargado del área de sistemas.
- Se prohíbe rigurosamente al usuario o funcionario distinto al personal dela oficina de sistemas abrir o destapar los equipos de cómputo.

d) Mantenimiento de equipos

Únicamente el personal autorizado por el área de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático. Los usuarios deberán asegurarse de respaldar en copias de seguridad la información que consideren relevante cuando el equipo sea enviado a reparación, y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información derivada del proceso de reparación.

El mantenimiento preventivo de los equipos de cómputo de la corporación (Planta telefónica, servidores, computadores de escritorio, computadores portátiles, computadores todo en uno, impresoras, escáner, circuito cerrado de televisión (DVR y Cámaras), se hará según el cronograma.

e) Perdida de equipo

El funcionario que tenga bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia, en consecuencia responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El servidor o funcionario deberá dar aviso inmediato al funcionario administrativo de almacén de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad, a su vez en caso de robo deberá dar entrega del oficio de denuncia por parte de la Policía Nacional.

3. IDENTIFICACION DE PROCESOS Y SERVICIOS

A continuación se relaciona los principales procesos de software identificados en el Concejo Municipal de Pasto:

COMPUCONTA SOFTWARE

El software principalmente permite automatizar las áreas financieras, administrativas y de control de la entidad.

Los módulos adquiridos por el software COMPUCONTA funcionan en:

- Contabilidad
- Presupuesto
- Almacén
- Nomina
- Contratación

La garantía, el mantenimiento y la supervisión del software son realizados por los desarrolladores del mismo.

4. RESPALDO DE LA INFORMACION

Las copias de seguridad que están disponibles en la Corporación son las siguientes:

MEMORIAS USB: Son aquellos dispositivos de almacenamiento asignados al funcionario o servidor público, este Backup lo hará manualmente el usuario cada vez que crea necesario y reposará bajo su custodia, allí el usuario almacenará la información que considere vital.

DISCO DURO: Se destina 1 disco duro en el área de sistemas, para que regularmente se haga una copia desde los computadores que manejen la información con mayor prioridad, este disco duro estará bajo la custodia únicamente del Ingeniero de Sistemas.

5. ACTIVOS SUSCEPTIBLES DE DAÑO

Para realizar un análisis de todos los elementos de riesgos a los cuales están expuesto los equipos informáticos y la información procesada del Concejo Municipal de Pasto, se iniciara describiendo los activos que se pueden encontrar dentro de las tecnologías de información y la comunicación de la Corporación: El personal, hardware, software, periféricos, datos, información, documentación física y magnética, suministro de energía eléctrica y suministro de telecomunicaciones.

A continuación se explica detalladamente cuales pueden ser los posibles daños y cuáles pueden ser las potenciales fuentes de los daños.

- Posibles daños

  - ✓ Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones.
  - ✓ 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.
  - ✓ Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante robo o infidencia.

- Fuentes de daño

  - ✓ Acceso no autorizado.
  - ✓ Ruptura de las claves de acceso al sistema informático.
  - ✓ Desastres naturales (Movimientos telúricos, inundaciones, fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario).
  - ✓ Fallas de Personal (Enfermedad, accidentes, renuncias, abandono de su puesto de trabajo).
  - ✓ Fallas de Hardware (Falla en los servidores o falla en el hardware de red)
  - ✓ Cableado de la Red, Router, FireWaall.
  - ✓ Falla en el servicio del proveedor de internet.

- Clases de riesgos

  - ✓ Incendios.
  - ✓ Robo de equipos y archivos.
  - ✓ Falla en los equipos.
  - ✓ Acción de virus informático.
  - ✓ Fenómenos naturales.
  - ✓ Accesos no autorizados.

6. IDENTIFICAR Y MINIMIZAR DE LOS RIESGOS

Corresponde al Plan de Seguridad y Privacidad informático minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno de los equipos de cómputo.

Para la identificación de los riesgos informáticos del Concejo Municipal de Pasto, se han considerado tres criterios:

- Grado del daño: El grado del daño causado puede ser (Leve, Moderado, Grave y Muy Grave).
- Frecuencia del evento: Puede ser (Nunca, Casi nunca, Casi siempre o Siempre).
- Impacto: El impacto de un evento puede ser (Leve, Moderado, Grave y Muy Grave).

El Plan de Seguridad y Privacidad informático es un procedimiento que define como una entidad continuará o recuperará sus funciones en caso de una complicación no planeada.

Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- Leves (Caídas de energía de corta duración, fallas en disco duro, equivocaciones, daño de archivos, acceso no autorizado)
- Muy Grave (Destrucción de equipos, incendios, inundaciones, daño de equipo, robos)

En el Concejo Municipal de Pasto, existen diferentes tipos de riesgos a los que está expuesto un bien o un activo, ante un posible perjuicio o daño. Existen diferentes tipos de riesgos:

- Riesgos Naturales (Mal tiempo, terremoto, inundaciones, entre otros.)
- Riesgos tecnológicos (Incendios eléctricos, fallas de energía, entre otros).
- Riesgos sociales (Actos terroristas, desordenes, entre otros).

A continuación vamos a describir algunos de los riesgos a los que se encuentra expuesta la entidad y como minimizar su impacto.

1. **Incendio o fuego en la instalación.**

Grado del daño: Muy grave
Frecuencia del evento: Casi Nunca
Grado de impacto: Grave
Responsable: Ingeniero de Sistemas

Objetivo	Actividad	Indicador
Verificar que en las oficinas donde están ubicados los	Verificación de la ubicación de extintores.	Numero de extintores verificados * 100 / Número

servidores y ordenadores cuenten con un extintor cargado.	Verificación de fechas de recarga y fechas de vencimiento.	total de extintores de la Entidad
Capacitar a los servidores públicos del Concejo Municipal de Pasto, sobre el uso de elementos de seguridad y primeros auxilios, para eventos de contingencia.	Coordinar con la oficina de SGSST, capacitaciones para atender eventos que comprometan la seguridad del personal y de los elementos físicos de la Entidad	Numero de capacitaciones realizadas * 100 / Número total de capacitaciones programadas por la Entidad

2. Robo de equipos y archivos digitales.

Grado del daño: Grave
Frecuencia del evento: Casi Nunca
Grado de impacto: Muy Grave
Responsable: Almacenista

Objetivo	Actividad	Indicador
Prevenir la perdida y/o daño de equipos y/o información del Concejo Municipal de Pasto.	Entregar mediante acta, por parte de la oficina de Almacén a cada servidor, los elementos de trabajo, de los cuales se hará responsable de su buen uso y cuidado.	Numero de actas de entrega * 100 / Número total de equipos activos que posee la Entidad
Controlar la salida de la Entidad de equipos de cómputo, eléctricos y electrónicos.	La autorización para la salida de los Equipos, debe ser por escrito y firmada por el responsable de la oficina de Almacén del Concejo Municipal de Pasto.	Numero de actas de salida de equipos debidamente firmadas * 100 / Número total de actas de salida de equipos.
Coordinar con la Policía Nacional, acciones tendientes a la recuperación de equipos que hayan sido sustraídos violentamente de la Entidad.	Informar a los entes competentes, sobre el hurto a mano armada de los equipos asignados a cada servidor del Concejo Municipal de Pasto.	Número de denuncias sobre hurto de equipos realizadas * 100 / Número total de equipos hurtados en la entidad.

En el Concejo Municipal de Pasto, no se han presentado casos en los cuales haya existido manipulación y reubicación de los equipos sin el debido conocimiento y autorización del responsable de cada activo tecnológico y el jefe de sistemas, comprobando que los equipos están protegidos por cada funcionario autorizado.

Tampoco se ha reportado algún tipo de robo, sin embargo se recomienda estar siempre alerta.

3. Falla en los equipos.

Grado del daño: Grave
Frecuencia del evento: Casi Nunca
Grado de impacto: Muy Grave
Responsable: Ingeniero de Sistemas - Almacenista

Objetivo	Actividad	Indicador
Adelantar acciones tendientes a la prevención de falla en los equipos por falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.	Número de mantenimientos de equipos realizados * 100 / Número total de equipos de la entidad.
Reemplazar el hardware de los equipos, que así lo requieran de forma inmediata.	Reportar a la oficina de Almacén los requerimientos de Hardware, para ser incluidos en el plan de compras de la Entidad.	Número total de solicitudes de hardware reportadas * 100 / Número total de solicitudes de hardware tramitadas para reposición.
Prevenir los daños en los equipos de cómputo, eléctricos y electrónicos, por fallas de energía eléctrica.	Realizar un diagnóstico para colocar UPS´s de energía de respaldo en cada dependencia del Concejo Municipal de Pasto, preferiblemente cada ordenador con su UPS.	Diagnostico realizado y entregado a Almacén para ser incorporado en el Plan de Compras de la Entidad.

Una vez analizado el riesgo de la falla de los equipos de cómputo, se establecerán y se ejecutaran jornadas de mantenimiento preventivo de los mismos, se implementarán estabilizadores (UPS) en cada uno de los equipos para que en caso de una falla eléctrica los dispositivos se apaguen de manera correcta.

4. Acción de virus informático.

Grado del daño: Grave
Frecuencia del evento: Casi Siempre
Grado de impacto: Grave
Responsable: Ingeniero de Sistemas – Almacenista

Objetivo	Actividad	Indicador
Prevenir los daños a la información, por software malicioso o dañino.	Solicitar la adquisición de un antivirus con sus respectivas licencias y así mismo evitar que las licencias expiren. Únicamente el área de sistemas es la encargada de realizar la	Solicitud realizada y entregada a Almacén para ser incorporado en el Plan de Compras de la Entidad.

	instalación de software en cada uno de los equipos de acuerdo con su necesidad. Cada computador que se encuentre en el Concejo Municipal de Pasto, deben tener únicamente los programas instalados por el personal de sistemas.	Reportes a la Secretaria General, sobre equipos que tengan software no instalado por el área de sistemas.

Se recomienda adquirir un antivirus eficiente y apropiado, instalarlo y mantenerlo actualizado en cada uno de los equipos de cómputo del Concejo Municipal de Pasto, para prevenir daños por causa de virus informáticos.

A todos los funcionarios se les recomienda no ingresar a páginas inseguras, para evitar daños, y tener un control de sus memorias USB, discos duros externos y tarjetas de memoria ratificando que no contengan ningún tipo de virus.

5. Terremoto.

Grado del daño: Muy Grave
Frecuencia del evento: Casi Nunca
Grado de impacto: Muy Grave
Responsable: Ingeniero de Sistemas

Objetivo	Actividad	Indicador
Prevenir la pedida de la información ocasionada por sismo o terremoto.	Cuando la información no presente ningún tipo de pérdida o los daños sean mínimos y el acontecimiento únicamente haya afectado parte de la infraestructura de la entidad y no se vean afectos los datos, pero se hace necesario evacuar las instalaciones trasladando al personal a zonas seguras, haciendo que el trabajo se vea interrumpido durante algunas horas o días, dependiendo del grado de daño ocasionado, mientras se adecua	Número total de evacuaciones por sismo realizadas en el año. Información misional actualizada y publicada en la página web de la Corporación.

	nuevamente el establecimiento. Cuando el sismo, ocasione pérdidas totales en las instalaciones, esto afectaría gravemente a las operaciones del Concejo Municipal de Pasto y la información física y digital puede verse perjudicadas seriamente. Para, evitar la pérdida de la información misional, esta debe reposar en la página web de la Corporación.	

En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

6. Sabotaje Informático.

Grado del daño: Grave
Frecuencia del evento: Casi Nunca
Grado de impacto: Moderado
Responsable: Ingeniero de Sistemas

Objetivo	Actividad	Indicador
Prevenir el sabotaje informático.	Que ingrese solo el personal autorizado a las instalaciones. Buena seguridad física donde se encuentran los principales equipos de cómputo. Cada dependencia o modulo en la institución este bajo vigilancia. Contraseñas de ingreso en cada computador. Buenos controles administrativos. Asignar a cada persona la responsabilidad de la protección de la información y los equipos en cada área.	Número total de casos de sabotaje informático presentados en un año.

	Ubicar los equipos que tienen información confidencial en lugares seguros y de extrema vigilancia. Aparte de la vigilancia que tiene el Concejo Municipal de Pasto, tanto como cámaras de seguridad y personal con esta función, se requiere tener una lista de números telefónicos de las diferentes dependencias policiales y lugares donde se pueda hacer un llamado de emergencia. Tener en cuenta las políticas internas de seguridad, además, es importante mantener la medida de ingreso de personas debidamente identificadas, así como la marcación de zonas de acceso restringido. Mantener adecuados archivos de reserva. (Backup) Identificar y establecer operaciones criticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.	

7. Póliza de Aseguramiento.

Grado del daño: Grave
Frecuencia del evento: Anual
Grado de impacto: Grave
Responsable: Secretaría General

Objetivo	Actividad	Indicador
Mantener protegidos los equipos de cómputo, eléctricos	Adquirir una póliza que respalde los equipos, electrónicos, eléctricos y de computo, contra riesgos como	Póliza vigente adquirida

y electrónicos a través de una póliza de seguro de PYME.	Incendio, Terremoto, AMIT, Hurto calificado, etc.	

7. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

Se debe considerar la planeación de actividades previas ante alguna catástrofe, como programas de resguardo de la información que busquen realizar un proceso de recuperación de datos, evitándole tiempo y recursos monetarios al Concejo Municipal.

Se realizarán procedimientos respectivos a:

- Sistemas de información: La entidad cuenta con un software contable para respaldar la información y los cambios realizados por los funcionarios, se realizarán Backups semanalmente, para las dependencias que a diario ingresan información nueva y se efectuarán copias de seguridad frecuentemente,
- Equipos de cómputo: Se debe tener en cuenta todos los elementos de hardware, impresoras, scanners, módems.

Se recomienda emplear los siguientes criterios sobre la identificación y protección de equipos:

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.
- Mantenimiento actualizado del inventario de los equipos de cómputo.

Ante una falla en la red de internet y telefonía, se optará por la telefonía móvil, por lo cual se informará a las entidades del gobierno y a la comunidad en general un número con el cual mayormente se tiene contacto, esta línea la tendría disponible el secretario general.

Para soportar una falla en las comunicaciones, el Concejo Municipal de Pasto puede realizar las siguientes actividades:

- Tener mínimo 2 proveedores del servicio de internet.
- Contar con un dispositivo digital (celular) con plan móvil permanente en la recepción o secretaria general.
- Capacitar al recepcionista para que pueda brindar la información adecuada ante estos casos.

8. RECOMENDACIONES GENERALES

8.1. Relacionadas con los equipos de cómputo

- Poner especial atención a las actualizaciones del navegador web, el sistema operativo como Windows es propenso a fallos, riesgo que puede ser aprovechado por delincuentes informáticos, frecuentemente se liberan actualizaciones que solucionan dichos fallos.
- Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, nos ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por las personas encargadas del área de sistemas.
- Tener el antivirus actualizado con frecuencia. Escanear con el antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados por internet.
- Estar pendiente de la fecha de caducidad dela licencia con el fin de renovarla inmediatamente tan pronto esta se cumpla.
- Es recomendable tener instalado en los equipos algún tipo de software anti-spyware para evitar que se introduzcan en el equipo programas espías destinados a recopilar información confidencial sobre el usuario.
- Para prevenir infecciones por virus informático, los usuarios del Concejo Municipal de Pasto no deben hacer uso de software que no haya sido proporcionado y validado por el área de sistemas.
- Los usuarios del Concejo Municipal de Pasto deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado antes de ejecutarse.
- Ningún usuario, funcionario, empleado o personal externo, podrá descargar software, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del área de sistemas.

8.2. Relacionados con la navegación en internet y la utilización de correo electrónico.

- Navegue por páginas web seguras y de confianza, para identificarlas verifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad, extreme la precaución si va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:

    - Empezar por https

- En la barra del navegador deben aparecer el icono de candado cerrado. A través de este icono se puede acceder a un certificado que confirma la autenticidad de la página.

- Utilizar contraseñas seguras, es decir aquellas compuestas por ocho caracteres, como mínimo y que combinen letras, números y símbolos. Es conveniente además que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia a este desde equipos públicos.
- Sea cuidadoso al utilizar programas de acceso remoto. A través de internet y mediante estos programas (AnyDesk), es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.
- Ponga especial atención en el tratamiento de su correo electrónico, ya que este se ha convertido en una de las formas más utilizadas para introducir código malicioso, llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:

    - No abra mensajes de correo de remitentes desconocidos.
    - Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
    - No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc.
    - Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

8.3. Relacionada con el uso de dispositivos extraíbles.

El funcionario o usuario que tenga asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

La persona encargada de administrar cada equipo deberá velar por el uso adecuado de dispositivos de almacenamiento externo, USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

Cada vez que se inserte un dispositivo externo a la red de la corporación, deberá ser analizado con el software del antivirus.

8.4. Relacionada con conexiones remotas

En el Concejo Municipal de Pasto solo está disponibles 1 forma de conexiones remota:

- AnyDesk

La conexión remota se deberá hacer bajo la supervisión de un funcionario y con la debida autorización del encargado del área de sistemas.

8.5. Relacionada con el personal

El Área de Sistemas del Concejo Municipal de Pasto, realizará una socialización del presente Plan con los servidores públicos de la Corporación, con el fin de dar buen uso a los equipos, el manejo y salvaguarda de los mismos y su información. De igual manera, se realizarán evaluaciones periódicas sobre el cumplimiento de lo expuesto anteriormente.

Elaborado por:	**Revisado por:**	**Aprobado por:**
VICTOR HUGO RIVERA ACHICANOY Ingeniero de Sistemas	SILVIO ROLANDO BRAVO PANTOJA Secretario General SANDRA ARGOTE Oficina de Control Interno	GUSTAVO ALONSO NUÑEZ Presidente