
Manual de políticas de seguridad y privacidad de la información

Contenido

1. OBJETIVO.

El MPSPI proporciona un marco robusto y estructurado que facilita la adopción de medidas de seguridad adaptables a los constantes cambios tecnológicos y normativos. Esto garantiza que la gestión de la información se realice con eficiencia y eficacia, minimizando los riesgos y asegurando la continuidad operativa de los procesos críticos.

El presente manual tiene como propósito establecer las directrices, lineamientos y controles necesarios para la implementación, gestión y mejora continua de la seguridad y privacidad de la información, en alineación con el Modelo de Seguridad y Privacidad de la Información (MPSPI). Este manual busca garantizar que los activos de información de la Alcaldía de Popayán sean protegidos conforme a los principios de confidencialidad, integridad y disponibilidad, con un enfoque en la identificación, evaluación y mitigación de riesgos asociados a la información.

Además, el manual promueve una cultura organizacional de seguridad mediante la concienciación, la formación continua y el cumplimiento normativo, asegurando que todos los actores involucrados comprendan y cumplan sus responsabilidades. Este documento refuerza la alineación con estándares internacionales, como la ISO 27001, y las regulaciones locales aplicables.

2. RESPONSABLE.

Es responsabilidad del jefe de sistemas de la entidad velar por el cumplimiento de estas políticas. Asimismo, los servidores públicos, contratistas y terceros vinculados a la Alcaldía de Popayán tienen la responsabilidad de cumplir con la ejecución de las políticas contempladas en este manual, incluyendo sus objetivos, manuales, procedimientos y documentos complementarios. Su aplicación es de carácter obligatorio para toda la entidad.

3. ALCANCE.

El presente manual es aplicable a todas las actividades, procesos, sistemas y recursos tecnológicos relacionados con la gestión de la información en la Alcaldía de Popayán. Su alcance incluye, pero no se limita a:

- **Funcionarios y contratistas:** Todo el personal de la entidad, independientemente de su nivel jerárquico y tipo de vinculación, deberá cumplir con las disposiciones establecidas.

- **Terceros y proveedores:** Cualquier entidad externa que interactúe con los sistemas de información o tenga acceso a datos gestionados por la entidad deberá cumplir con los acuerdos de confidencialidad y las políticas de seguridad aquí descritas.
- **Activos de información:** Incluye todos los datos físicos y digitales, sistemas de software, hardware, redes y documentación relevante para la entidad.
- **Procesos críticos:** Aquellas actividades esenciales para la continuidad operativa y los servicios prestados a los ciudadanos.

4. TERMINOS Y DEFINICIONES.

Para garantizar un comprensión clara y uniforme, se amplían los siguientes términos clave relacionados con la seguridad y privacidad de la información:

- **Activo de información:** Cualquier recurso que posea valor para la organización en términos de información, como bases de datos, documentos físicos, sistemas de comunicación, personas, o infraestructura tecnológica.
- **Amenaza:** Cualquier evento o circunstancia que pueda impactar negativamente la seguridad de la información, comprometiendo su confidencialidad, integridad o disponibilidad.
- **Vulnerabilidad:** Debilidad inherente a un activo o control que puede ser explotada por una amenaza para causar daño o interrupción.
- **Riesgo:** La combinación de la probabilidad de que una amenaza se materialice y el impacto resultante sobre los activos de información.
- **Confidencialidad:** Propiedad de la información que asegura que solo sea accesible por personas, entidades o procesos autorizados.
- **Integridad:** Garantía de que la información se mantenga completa y sin alteraciones no autorizadas durante su almacenamiento, procesamiento o transmisión.
- **Disponibilidad:** Aseguramiento de que la información esté accesible y utilizable cuando sea requerida por usuarios autorizados.
- **Gestión de incidentes de seguridad:** Conjunto de procedimientos y controles destinados a identificar, analizar y mitigar eventos que comprometan la seguridad de la información.

- **Clasificación de información:** Proceso de categorización de datos en función de su nivel de sensibilidad y el impacto potencial de su divulgación, pérdida o alteración.
- **Auditoría de seguridad:** Evaluación sistemática y documentada de los sistemas y procesos para verificar el cumplimiento de las políticas y normativas de seguridad establecidas.

- **Sistemas de Gestión de Seguridad de la Información – (SGSI):** Conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información es fundamental para la Alcaldía de Popayán, dado que protege los datos críticos que respaldan los servicios a la comunidad. Este apartado del manual establece las políticas esenciales para asegurar que la gestión de información sea coherente, efectiva y alineada con el MPSPI. Las políticas cubren aspectos clave como organización interna, seguridad de dispositivos móviles, teletrabajo y la relación con proveedores.

5.1 POLÍTICA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.

5.1.1 ORGANIZACIÓN INTERNA.

Para garantizar una gestión eficaz de la seguridad de la información, la Alcaldía de Popayán ha definido roles y responsabilidades de la seguridad de la información, que se detalla en el documento “Política General de Seguridad y Privacidad de la Información”, garantizando una distribución adecuada de las tareas y responsabilidades.

5.1.2 DISPOSITIVOS MÓVILES.

La alcaldía de Popayán establece los siguientes lineamientos:

a. Control de dispositivos.

- Todos los dispositivos móviles institucionales usados para acceder, procesar o almacenar información de la Alcaldía de Popayán deben estar registrados y protegidos con contraseñas robustas.
- Los dispositivos móviles institucionales deben contar con sistemas de protección actualizados.

- Todo dispositivo móvil institucional debe estar registrado ante el Grupo interno de trabajo de Tecnologías TIC.
- No se debe almacenar información confidencial o sensible en los dispositivos móviles institucionales sin las debidas medidas de cifrado aprobadas.
- Los dispositivos móviles proporcionados por la Alcaldía de Popayán deben usarse exclusivamente para el desarrollo de actividades institucionales.
- Cuando los usuarios utilizan dispositivos personales para el desarrollo de sus funciones o actividades, deben mantener una separación entre el uso personal y el uso institucional de los dispositivos.

b. Medidas de seguridad.

- Los dispositivos personales se recomiendan configurarse con bloqueo automático y contraseñas robustas. Para dispositivos institucionales la medida es obligatoria.
- Se prohíbe la instalación de software en los dispositivos institucionales sin previa autorización.
- Los sistemas operativos y aplicaciones de los dispositivos móviles deberían mantenerse actualizados con los últimos parches de seguridad.
- Los dispositivos institucionales deben estar protegidos contra software malicioso.
- La configuración de seguridad de los dispositivos institucionales no puede ser modificada por los usuarios no autorizados.

c. Conexiones de red.

- Evitar la conexión a redes wifi públicas para acceder a recursos institucionales.
- El acceso remoto debe realizarse exclusivamente mediante VPN institucional.
- Las conexiones bluetooth deberían desactivarse cuando no se utilicen.

d. Gestión de incidente y responsabilidades.

- Los encargados de las distintas dependencias de la Alcaldía de Popayán deberán comunicar las responsabilidades de los usuarios internos en el manejo de la información almacenada en los dispositivos móviles.
- No se permite compartir la información institucional a usuarios no autorizados, recordando que toda información relacionada a la Alcaldía de Popayán es propiedad exclusiva de la entidad.

5.1.3 TELETRABAJO.

La Alcaldía de Popayán establece las siguientes directrices para garantizar la seguridad de la información en modalidad de teletrabajo:

a. Control de dispositivos y sistemas.

- Todos los dispositivos utilizados para el teletrabajo que pertenezcan a la Alcaldía de Popayán deben cumplir con las políticas de seguridad establecidas por la entidad.
- La instalación y actualización del software antivirus institucional es obligatoria. En caso del desarrollo de funciones o actividades en equipos personales, este deberá contar con un software antivirus gratuito como mínimo.
- El medio de almacenamiento de datos de los equipos institucionales usados para teletrabajo debería estar cifrado. Si se utiliza un equipo personal para el teletrabajo, se debería crear una carpeta o ruta de trabajo en la que se almacenará toda la información relacionada con la entidad, y esta carpeta debería estar cifrada.
- Los equipos institucionales asignados deben ser usados exclusivamente con propósitos institucionales, evitando su uso para fines personales.

b. Medidas de seguridad y acceso.

- Los usuarios deben seguir las mismas políticas y procedimientos de seguridad de la información que se aplican al entorno de trabajo presencial.
- Se debe mantener la protección de datos confidenciales y el cumplimiento de las normativas de la entidad.
- Los usuarios deben evitar el uso de redes Wi-Fi públicas para acceder a los sistemas y datos de la entidad.
- El usuario deberá bloquear (Windows+L) o apagar los dispositivos cuando no se encuentre en su puesto de teletrabajo.

c. Gestión de acuerdos y autorizaciones.

- Los usuarios deben firmar un acuerdo de teletrabajo que incluya las políticas de seguridad de la información.
- El acuerdo debe especificar el compromiso de proteger la información de la entidad.
- Se debe establecer el uso responsable de los recursos tecnológicos institucionales asignados.

d. Gestión de incidentes y finalización.

- Todos los incidentes de seguridad relacionados con teletrabajo deben ser reportados de inmediato al Grupo interno de trabajo de Tecnologías TIC para su gestión.
- Al finalizar el vínculo laboral con la entidad, el funcionario o contratista debe hacer entrega de los dispositivos brindados por la entidad para el teletrabajo en buenas condiciones, salvo el desgaste natural.

5.2 POLÍTICAS DE GESTIÓN DE ACTIVOS.

La Alcaldía de Popayán establece las siguientes directrices para la gestión de los activos de información:

5.2.1 INVENTARIO DE ACTIVOS.

- El Grupo interno de trabajo de Tecnologías TIC realizará un control centralizado del inventario, para garantizar que todos los activos de información sean debidamente registrados, clasificados y monitoreados.
- El Grupo interno de trabajo de Tecnologías TIC realizará un instructivo para la identificación y clasificación de los activos, incluyendo información, software, hardware, servicios y componentes de red.
- El Grupo interno de trabajo de Tecnologías TIC, clasificara y gestionara su inventario de activos conforme a los procedimientos de Gestión de Activos formalizados.
- Se realizará actualización del inventario de activos de información de forma frecuente, con el apoyo de los responsables de cada dependencia.
- El inventario de activos deberá ser revisado y aprobado por el encargado del Grupo interno de trabajo de Tecnologías TIC.
- Se debe mantener un registro actualizado del ciclo de vida completo del activo, desde su adquisición hasta su desecho.

5.2.2 PROPIEDAD DE LOS ACTIVOS.

- Los activos de información mantenidos en el inventario deberán ser asignados a un usuario responsable en cada dependencia.
- Todo encargado de dependencia debe asegurarse de la asignación oportuna de la propiedad de los activos.
- Los responsables deben garantizar que los activos estén debidamente inventariados, clasificados, protegidos y dentro del dominio de la entidad.

- Los usuarios asignados responderán por la custodia, protección y preservación tanto del hardware como del software.
- En caso de daño de los activos asignados, los usuarios deberán informar de manera inmediata y detallada al Grupo interno de trabajo de Tecnologías TIC.

5.2.3 CONTROL DE MOVIMIENTOS DE ACTIVOS.

- Los activos no deberán salir de las instalaciones del edificio CAM de la Alcaldía de Popayán sin autorización.
- En casos extraordinarios, se deberá solicitar y diligenciar una orden de salida, la cual será emitida y autorizada exclusivamente por la dependencia de bienes inmuebles.
- Cuando un usuario con relación de prestación de servicios requiera de un activo de información para el desarrollo de sus actividades, el responsable será el encargado de la respectiva dependencia.
- Se debe mantener registro de todos los movimientos y traslados de activos de información.
- Los activos prestados o asignados temporalmente deben ser monitoreados y controlados.

5.2.4 CLASIFICACIÓN DE LA INFORMACIÓN.

- Toda información debe ser clasificada de acuerdo con su confidencialidad, integridad y disponibilidad, según las categorías:
    - **Pública:** información disponible sin restricciones.
    - **Confidencial:** información sensible accesible solo por personal autorizado.
    - **Restringida:** información crítica cuya divulgación podría generar daños significativos.
- Los usuarios que generen la información son responsables de asignar y revisar periódicamente su clasificación.
- La información clasificada debe ser claramente etiquetada según su categoría de seguridad.
- El acceso a información clasificada debe estar restringido al personal autorizado.
- La información que ha cumplido su ciclo de vida útil debe ser desclasificada y destruida de forma segura según los procedimientos establecidos.

5.2.5 GESTIÓN DE MEDIOS REMOVIBLES.

- Los puertos USB y lectores de CD/DVD deberán permanecer bloqueados por defecto.
- La habilitación de puertos se realizará bajo solicitud justificada vía correo electrónico, según el procedimiento establecido.
- Se debe mantener un registro de las autorizaciones otorgadas.
- El uso de medios removibles debe cumplir con las políticas de clasificación de activos.

5.3 POLÍTICAS DE CONTROL DE ACCESO.

La Alcaldía de Popayán establece las siguientes directrices para el control de acceso a la información, sistemas y recursos tecnológicos.

5.3.1 CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA.

- Todos los sistemas de información y recursos tecnológicos de la Alcaldía de Popayán deberán estar protegidos mediante mecanismos de autenticación que incluyan el uso de un nombre de usuario y una contraseña.
- Se deberá incorporar autenticación de dos factores (2FA) para accesos a sistemas críticos.
- Los usuarios son responsables de la seguridad de sus credenciales de acceso y no deben compartir sus contraseñas con terceros bajo ninguna circunstancia.
- Cualquier intento de compartir o divulgar contraseñas será considerado una violación grave a las políticas de seguridad de la información.
- En caso de sospecha de que una contraseña ha sido vulnerada, el usuario deberá notificar de manera inmediata al Grupo interno de trabajo de Tecnologías TIC.

5.3.2 SUMINISTRO DE CONTROL DE ACCESO.

- El Grupo interno de trabajo de Tecnologías TIC será el responsable de gestionar y administrar el suministro de controles de acceso a los sistemas y recursos tecnológicos de la entidad.
- Todo control de acceso debe garantizar que solo el personal autorizado tenga acceso a la información según su rol y necesidad.
- El Grupo interno de trabajo de Tecnologías TIC es el responsable exclusivo de la creación, modificación, suspensión y asignación de usuarios y contraseñas.

- El responsable de cada dependencia será el responsable de solicitar usuario y contraseña para los colaboradores del área mediante correo electrónico institucional según el procedimiento establecido.
- Las cuentas de usuario no deberían ser utilizadas por más de una persona bajo ninguna circunstancia.
- La desactivación de acceso para usuarios que ya no estén autorizados debe realizarse de manera inmediata.
- Se debe mantener un registro actualizado de todos los accesos otorgados y revocados.

5.3.3 GESTIÓN DE CONTRASEÑAS.

- Las contraseñas son personales e intransferibles, y se prohíbe su uso y divulgación a terceros.
- Es responsabilidad de los usuarios el correcto uso de las contraseñas asignadas para el acceso a los sistemas y aplicativos.
- El acceso a los sistemas tiene un tiempo determinado según el tipo de contratación o relación con la Alcaldía.
- Las contraseñas deben cumplir los siguientes requisitos:
    - Longitud mínima de 8 caracteres.
    - Inclusión de letras mayúsculas, minúsculas, números y caracteres especiales.
    - No relacionarse con información personal u obvia.
    - Ser diferente a la última contraseña utilizada.
- Las contraseñas deberán actualizarse como mínimo cada 2 meses.
- Se debe validar que la contraseña realmente se actualice y no se repita.
- El sistema debe forzar el cambio de contraseñas temporales en el primer inicio de sesión.
- Los procedimientos de recuperación de contraseñas deben incluir verificación de identidad.

5.3.4 PERÍMETROS DE SEGURIDAD.

- Los lugares de alta confidencialidad que contengan información sensible deben contar con autorización específica para su acceso.
- Las áreas son delimitadas como de acceso restringido según su nivel de seguridad.

- El acceso a los centros de cómputo requiere previa autorización y acompañamiento de un usuario adscrito al Grupo interno de trabajo de Tecnologías TIC
- Se debe llevar registro de las autorizaciones otorgadas para el acceso a los centros de cómputo.
- El acceso y manipulación física o lógica de los dispositivos de red, centros de datos y equipos de cómputo está restringido a usuarios adscritos al Grupo interno de trabajo de Tecnologías TIC.
- Se debe mantener un registro de todos los accesos a áreas restringidas.
- Se deben implementar controles biométricos o de tarjetas de acceso para áreas críticas.

5.3.5 MANEJO DE COPIAS DE SEGURIDAD.

- El Grupo interno de trabajo de Tecnologías TIC debe asegurar que todas las copias de seguridad de los sistemas y datos críticos se realicen de manera regular, para garantizar la protección de la información frente a perdidas, daños o incidentes de seguridad.
- Se prohíbe incluir en las copias información personal, archivos de música, videos o documentos transitorios.
- Se debe implementar un sistema automatizado para la realización de copias de seguridad, minimizando la intervención manual y reduciendo el riesgo de errores humanos.
- Los medios de respaldo deben almacenarse en ubicaciones seguras y controladas.
- Solo el personal autorizado por el Grupo interno de trabajo de Tecnologías TIC ,debe tener acceso a los medios de respaldo.
- Las copias de seguridad automáticas deben almacenarse en el servidor dispuesto y debería tener un espejo en la nube.
- Se deben realizar auditorías periódicas del proceso de copias de seguridad.
- Se debe mantener documentación actualizada de los procedimientos de respaldo y restauración.

5.4 POLÍTICAS DE CRIPTOGRAFÍA.

La Alcaldía de Popayán establece las siguientes directrices para la implementación y gestión de controles criptográficos:

5.4.1 APLICACIÓN DE CONTROLES CRIPTOGRÁFICOS.

- Los controles criptográficos son aplicables a copias de seguridad y equipos portátiles según su nivel de criticidad y si cuenta con los recursos hardware requeridos.
- El Grupo interno de trabajo de Tecnologías TIC es responsable de implementar los controles criptográficos necesarios para proteger la información que:
    - Viaja a través de redes públicas.
    - Se guarda en dispositivos de almacenamiento.
    - Requiere garantías de confidencialidad, integridad y no repudio.

5.4.2 Los medios de almacenamiento removibles y que contengan información sensible deben estar cifrados usando métodos aprobados por el Grupo interno de trabajo de Tecnologías TIC.

5.4.3 CERTIFICADOS Y PROTOCOLOS DE SEGURIDAD.

- Todos los servicios web expuestos por la Alcaldía deben contar con certificados SSL/TLS vigentes.
- Los certificados SSL/TLS deben ser emitidos por una autoridad certificadora reconocida.
- La gestión de los certificados incluye:
    - Una clave privada instalada en el servidor que nunca debe ser compartida.
    - Una clave pública incorporada en el certificado SSL/TLS.
- El correo electrónico institucional debe utilizar el protocolo TLS para proteger la privacidad de las comunicaciones.
- El dominio de correo electrónico debe estar protegido con un certificado adecuado para garantizar su autenticidad y prevenir intentos de suplantación de identidad.
- Las redes inalámbricas institucionales deben implementar como mínimo el protocolo WPA2.

5.4.4 CIFRADO DE INFORMACIÓN.

- Las copias de seguridad que contengan información sensible deben estar cifradas.
- El cifrado de discos duros institucionales se realizará según el procedimiento establecido por el Grupo interno de trabajo de Tecnologías TIC.
- Todo desarrollo o adquisición de aplicaciones debe incluir métodos criptográficos para el tratamiento de información sensible.
- Los mecanismos de cifrado deben utilizar algoritmos estándar reconocidos internacionalmente.

5.4.5 RESPONSABILIDADES Y GESTIÓN.

- El Grupo interno de trabajo de Tecnologías TIC es responsable de:
  - Adquirir y gestionar los certificados SSL/TLS.
  - Administrar los mecanismos de cifrado en medios almacenamiento.
  - Gestionar las solicitudes de cifrado de equipos.
- Los usuarios pueden solicitar el cifrado de equipos, carpetas o medios asignados a través de la mesa de ayuda.

5.5 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO.

La Alcaldía de Popayán establece las siguientes directrices para garantizar la seguridad física y del entorno de sus activos de información:

5.5.1 PERÍMETRO DE SEGURIDAD FÍSICA.

- Las áreas que contengan información sensible o crítica deben estar protegidas mediante controles de acceso físico apropiados.
- Los perímetros de seguridad deben estar claramente definidos y su nivel de protección debe corresponder a los activos que contienen.
- Las entradas a áreas seguras deben estar protegidas con controles de acceso como tarjetas, controles biométricos o recepcionistas.
- Los visitantes deben ser registrados y acompañados en todo momento dentro de áreas restringidas.
- Las instalaciones deben contar con sistemas de vigilancia CCTV y monitoreo permanente.
- Se debe mantener un registro detallado de todos los accesos a áreas restringidas.
- El horario autorizado para recibir visitantes es de lunes a viernes de 8:00 a.m. a 12:00 p.m. y de 2:00 p.m. a 5:00 p.m.

5.5.2 SEGURIDAD EN OFICINAS, RECINTOS E INSTALACIONES.

- Las ventanas, puertas y otras posibles entradas deben estar debidamente aseguradas cuando no haya personal presente.
- Los activos tecnológicos no podrán trasladarse fuera de sus oficinas sin autorización y acompañamiento del personal del Grupo interno de trabajo de Tecnologías TIC.
- Las oficinas deben ser revisadas regularmente para identificar posibles vulnerabilidades físicas.
- Los documentos confidenciales deben guardarse bajo llave cuando no estén en uso.
- Se debe implementar una política de escritorio y pantalla limpia.

5.5.3 CONTROLES DE ACCESO FÍSICO.

- Las áreas seguras como centros de datos, centros de cableado y áreas de archivo deben contar con controles de acceso físico.
- En áreas seguras está prohibido fumar, comer o beber.
- Las actividades de limpieza en áreas seguras deben ser supervisadas.
- Se prohíbe el ingreso de maletas, bolsos u objetos no relacionados con las labores de mantenimiento.

5.5.4 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS.

- La plataforma tecnológica debe contar con protección física y eléctrica contra daños, fraudes o accesos no autorizados.
- Los centros de datos deben contar con sistemas de protección eléctrica y UPS.
- Todos los equipos deben de realizársele mantenimiento preventivo y/o correctivo dentro de la entidad. En caso de no poder dar solución internamente, se deberá remitir la situación a un externo con contrato vigente.
- Los visitantes a áreas de procesamiento de información requieren acompañamiento permanente.
- Las áreas de carga y descarga deben estar separadas de las áreas de procesamiento de información.

5.5.5 MANTENIMIENTO DE EQUIPOS.

- Los equipos deben recibir mantenimiento preventivo con determinada frecuencia.
- Los mantenimientos deben realizarse fuera de horas pico de trabajo.

- Se debe notificar a los usuarios con anticipación.
- Solo personal autorizado puede realizar mantenimientos.
- Se debe mantener registro de todos los mantenimientos realizados.
- Los equipos deben ser revisados después del mantenimiento para verificar su funcionamiento.
- Se deberá revisar periódicamente la eficacia de los procedimientos de mantenimiento.

5.5.6 RETIRO DE EQUIPOS DE ACTIVOS.

- Se debe asegurar el respaldo de datos antes del retiro de equipos.
- El Grupo interno de trabajo de Tecnologías TIC debe verificar el respaldo de la información.
- Los equipos retirados deben pasar por proceso de borrado seguro.
- Los equipos funcionales pueden ser reasignados previa evaluación.
- Se debe documentar el motivo del retiro y el diagnóstico realizado.
- El inventario debe actualizarse inmediatamente después del retiro.

5.5.7 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS.

- Todo equipo debe pasar por el proceso de borrado seguro antes de su reutilización.
- Se debe realizar respaldo de información relevante antes de la reutilización.
- Los medios de almacenamiento deben destruirse de forma segura cuando sea necesario.
- Se debe mantener registro de la disposición final de equipos.

5.5.8 ESCRITORIO Y PANTALLA LIMPIOS.

- Los documentos confidenciales deben mantenerse fuera de la vista cuando no se usen.
- Los documentos impresos deben retirarse inmediatamente de las impresoras.
- Los dispositivos de almacenamiento removibles deben guardarse bajo llave.
- Los escritorios deben quedar libres de documentos al finalizar la jornada.
- Las pantallas deben bloquearse (Win + L) al ausentarse del puesto de trabajo.

- Los nombres de usuario y/o contraseñas no deben escribirse en notas adhesivas ni dejarse visibles.
- Los documentos confidenciales no deben desecharse en papeleras comunes.

5.6 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES.

La Alcaldía de Popayán establece las siguientes directrices para garantizar la operación correcta y segura de los servicios de procesamiento de información, asegurando la integridad y disponibilidad de sus sistemas:

5.6.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS.

- El Grupo interno de trabajo de Tecnologías TIC ha establecido los siguientes procedimientos de operación documentados, que son de obligatorio cumplimiento para todo el personal autorizado:
  - Manuales e instructivos detallados para la instalación, configuración y mantenimiento de sistemas, garantizando la uniformidad en las operaciones.
  - Procedimientos e instructivos específicos para establecer la gestión de las copias de respaldo.
  - Formato detallado para definir los requisitos de desarrollo de software, que contempla las interdependencias con otros sistemas, estándares de codificación y requisitos de seguridad.

5.6.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO.

La alcaldía de Popayán establece los siguientes controles obligatorios para la protección contra código malicioso:

- **Controles preventivos:**
  - Implementación de software antivirus actualizado en todos los equipos.
  - Restricción de privilegios de administrador.
  - Capacitación regular a usuarios sobre amenazas de seguridad.

- **Controles de detección**
  - Escaneos programados para todos los sistemas.
  - Monitoreo en tiempo real de actividades sospechosas.
  - Análisis de logs y alertas de seguridad.
  - Verificación de integridad de archivos críticos.

- **Controles de respuesta**
  - Procedimientos documentados de respuesta a incidentes.
  - Aislamiento inmediato de sistemas comprometidos.
  - Análisis forense de incidentes.
  - Proceso de recuperación y restauración.

5.6.3 RESPALDO DE INFORMACIÓN.

La Alcaldía de Popayán implementa una estrategia integral de respaldo de información que incluye:

- Política de copias de seguridad:
  - Establecimiento de frecuencias de respaldo de la información.
  - Procedimientos detallados de respaldo y restauración de la información.
- Gestión de medios de respaldo:
  - Almacenamiento en ubicaciones seguras y controladas.
  - Protección física y ambiental de medios de respaldo.
  - Control de acceso a medios de respaldo.
- Verificación y pruebas:
  - Pruebas regulares de restauración.
  - Verificación de integridad de respaldos.
  - Simulacros de recuperación.

5.6.4 SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.

La Alcaldía de Popayán establece las siguientes directrices para garantizar la separación efectiva de ambientes:

- **Separación de ambientes:**
  - El ambiente de desarrollo debe ser utilizado exclusivamente para la creación y modificación de código fuente.
  - El ambiente de pruebas debe usarse exclusivamente para probar y validar cambios en el código fuente.
  - El ambiente de producción debe ser utilizado exclusivamente para la ejecución de aplicaciones en producción.
  - Se prohíbe realizar cambios directos en el código fuente en el ambiente de producción.

- **Control de accesos:**
  - El acceso al ambiente de desarrollo debe estar restringido a los desarrolladores autorizados.
  - El acceso al ambiente de pruebas debe limitarse a testers y desarrolladores autorizados.
  - El acceso al ambiente de operación debe restringirse a los administradores de sistemas y operadores autorizados.
  - Se deben utilizar credenciales diferentes para cada ambiente.
  - Los usuarios deben tener el nivel mínimo de privilegios necesario para su rol en cada ambiente.
- **Gestión de datos:**
  - No se deben almacenar datos de producción en el ambiente de desarrollo.
  - Los datos de prueba deben ser ficticios o anonimizados.
  - Se debe mantener un control estricto sobre sobre la copia de datos productivos a otros ambientes.
  - La información sensible debe ser enmascarada o eliminada en ambientes no productivos.
- **Proceso de promoción:**
  - Los cambios deben seguir un flujo formal desde desarrollo hasta producción.
  - Cada promoción entre ambientes debe ser documentada y aprobada.
  - Se deben realizar pruebas exhaustivas antes de promover a producción.
- **Controles adicionales:**
  - Las herramientas de desarrollo no deben estar disponibles en ambiente de producción.
  - Los compiladores, editores y herramientas de desarrollo deben restringirse a los ambientes correspondientes.
  - Se deben mantener registros de todas las promociones entre ambientes.
  - Las configuraciones de seguridad deben ser apropiadas para cada ambiente.

- Se deben realizar auditorías periódicas para verificar la separación efectiva de ambientes.

5.6.5 SINCRONIZACIÓN DE RELOJES.

La Alcaldía de Popayán implementa las siguientes medidas para la sincronización de tiempo:

- **Gestión de tiempo:**
  - Establecimiento de una fuente única de tiempo autorizada.
  - Sincronización automática de todos los sistemas.
- **Controles de sincronización:**
  - Uso de protocolos seguros de sincronización como NTP.
  - Mantenimiento de configuraciones de zona horaria.

5.6.6 CONTROL DE SOFTWARE OPERACIONAL.

La Alcaldía de Popayán establece los siguientes controles para la gestión del software operacional:

- La instalación de software debe ser autorizada formalmente.
- La instalación de software debe ser realizada por personal autorizado del Grupo interno de trabajo de Tecnologías TIC.
- Se debe mantener inventario del software autorizado.
- La documentación debe mantenerse actualizada.

5.6.7 GESTIÓN DE VULNERABILIDADES TÉCNICAS.

La Alcaldía de Popayán implementa las siguientes medidas para la gestión de vulnerabilidades técnicas:

- **Identificación y evaluación:**
  - Monitoreo continuo de nuevas vulnerabilidades.
  - Evaluación de impacto potencial.
  - Seguimiento de vulnerabilidades identificadas.
- **Gestión de parches:**
  - Implementación programada de parches.
  - Verificación post-implementación.
- **Medidas de mitigación:**
  - Restricción de acceso a sistemas vulnerables.
  - Monitoreo aumentado en sistemas afectados.

5.7 SEGURIDAD DE LAS COMUNICACIONES.

- Las redes de la entidad deben estar protegidas mediante controles de seguridad apropiados.
- Se debe implementar segmentación de redes según su criticidad y propósito.
- El acceso a la red debe estar controlado y monitoreado.
- Se debe cifrar la información sensible durante su transmisión.
- Se deben implementar mecanismos de detección y prevención de intrusiones.

5.8 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

5.8.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS

- Todo nuevo sistema o modificación debe incluir requisitos de seguridad desde su fase inicial.
- Se debe realizar un análisis de riesgos para identificar los controles necesarios.
- Se debe verificar que los controles implementados cumplan con los requisitos establecidos.

5.8.2 DESARROLLO SEGURO.

- se debe implementar una metodología de desarrollo seguro de software.
- Todo código debe ser revisado en búsqueda de vulnerabilidades antes de su implementación.
- se deben realizar pruebas de seguridad en todas las etapas del desarrollo.
- Los ambientes de desarrollo, pruebas y producción deben estar separados.

5.9 POLÍTICAS DE CUMPLIMIENTO.

5.9.1 IDENTIFICACIÓN DE REQUISITOS.

- Todos los requisitos legales, normativos y contractuales aplicables deben ser identificados, documentados y revisados periódicamente para garantizar su vigencia.
- Las violaciones de cumplimiento deben ser reportadas de manera inmediata al responsable designado, y gestionadas conforme a los procedimientos establecidos, incluyendo la implementación de medidas correctivas.

5.9.2 REVISIONES DE SEGURIDAD.

- Se deben realizar auditorías internas y externas periódicas para evaluar el cumplimiento de los requisitos legales, normativos y de las políticas internas de la organización.
- Los resultados de las auditorías deben ser documentados en informes oficiales que incluyan hallazgos, análisis de riesgos y recomendaciones específicas.
- Las recomendaciones derivadas de las auditorías deben ser evaluadas e implementadas de acuerdo con un plan de acción con plazo definidos y responsables asignados.

6 SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Se debe desarrollar un programa continuo de sensibilización en seguridad de la información, diseñado para fomentar una cultura organizacional de protección y cumplimiento. Las capacitaciones deben ser personalizadas según los diferentes roles y responsabilidades dentro de la organización, asegurando que cada participante reciba información relevante y adecuada a sus funciones. Además, la efectividad de los programas de sensibilización debe ser evaluada regularmente mediante métricas específicas y retroalimentación. Es fundamental mantener registros detallados de todas las actividades de sensibilización realizadas, incluyendo asistentes, contenidos impartidos y resultados obtenidos.

7 APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS.

Las políticas deben ser revisadas con frecuencia para garantizar su vigencia y adecuación a los requisitos legales, normativos y operativos. Cualquier cambio realizado debe ser aprobado por la alta dirección antes de su implementación. Además, se debe mantener un registro actualizado de todas las revisiones y modificaciones realizadas, incluyendo la fecha y el detalle de los ajustes. Por último, las actualizaciones deben ser comunicadas de manera clara y oportuna a todos los usuarios involucrados, asegurando su conocimiento y comprensión.

8 SANCIONES.

El incumplimiento de estas políticas será sujeto a sanciones que se aplicarán en función de la gravedad de la infracción. Todas las sanciones deberán seguir el debido proceso disciplinario establecido por la organización, garantizando transparencia y equidad. Así mismo, se debe mantener un registro detallado de todas las sanciones aplicadas, incluyendo su naturaleza y los motivos correspondientes.

9 CONTROL DE CAMBIOS.

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
01	24/12/2024	Se elabora y aprueba el documento por primera vez para s u incorporación al S.I.G.MECI CALIDAD.
02	24/11/2025	Mediante la presente actualización se adiciona como responsable al jefe de sistemas, asignándole el cumplimiento de lo establecido en este manual.

Elaborado por:	Revisado por:	Aprobado por:
Nombre: Andrés Felipe Hoyos Mosquera 	**Nombre:** Carlos Andrés Muñoz Calambás**.** 	**Nombre:** Andrés Fernando Piamba Caicedo 
Cargo: Contratista TIC	**Cargo:** Profesional Universitario SIG MECI – Calidad	**Cargo:** Jefe Oficina Asesora TIC
Fecha: 24/12/2024	**Fecha: 24/12/2024**	**Fecha: 24/12/2024**