POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CURADOR URBANO SEGUNDO – PASTO, NARIÑO

1. Introducción / Objetivo

El Curador Urbano Segundo de Pasto, Arquitecto Carlos Andrés Melo Guerrero, declara su compromiso con la protección, confidencialidad, integridad y disponibilidad de la información que gestiona, reconociendo que dicha información es un recurso estratégico para la entidad y un activo que debe preservarse frente a riesgos internos y externos.
El objetivo de esta política es establecer los principios, directrices y obligaciones mínimas que garanticen la gestión segura de los sistemas de información, procesos, datos y recursos asociados.

2. Alcance

Esta política aplica a:

- Todo el personal (funcionarios, contratistas, terceros) que acceda a sistemas, redes o información de este Despacho.
- Todos los activos de información (documentos físicos, digitales, bases de datos, servidores, computadoras, dispositivos móviles, redes).
- Todos los procesos, aplicaciones, servicios y contratos que gestionen, procesen o almacenen información de la entidad.

3. Principios de Seguridad

La política se fundamenta en los siguientes principios:

1. **Confidencialidad**: sólo las personas autorizadas pueden acceder a la información.
2. **Integridad**: la información debe mantenerse completa, exacta y sin modificaciones no autorizadas.
3. **Disponibilidad**: la información debe estar accesible para las personas autorizadas cuando lo requieran.
4. **Responsabilidad**: cada usuario es responsable del cumplimiento de las normas establecidas.
5. **Transparencia y trazabilidad**: las acciones sobre la información deben registrarse, ser auditables y justificables.
6. **Mejora continua**: la seguridad debe revisarse periódicamente y adaptarse frente a nuevos riesgos.

4. Directrices de seguridad

A continuación, las directrices principales que regirán la gestión de la seguridad de la información:

4.1 Control de acceso

- Cada usuario recibirá credenciales únicas (usuario + contraseña fuerte) y será sujeto a políticas de rotación de credenciales.
- El acceso remoto deberá realizarse mediante VPN segura o canales cifrados aprobados.
- Se definirá el principio de **mínimo privilegio**: cada usuario solo tendrá los accesos estrictamente necesarios.
- Los accesos serán monitoreados, auditados y revocados cuando ya no sean necesarios.

4.2 Seguridad operativa

- Todo software usado deberá contar con licencia válida o documentación que permita su uso legal, y debe ser validado por el área de sistemas.
- Se debe mantener respaldo periódico de la información crítica, con pruebas de recuperación.
- Actualizaciones y parches de seguridad deben aplicarse de forma oportuna.
- Control estricto sobre el uso de medios extraíbles (USB, discos externos), con escaneo antivirus u otras medidas de protección.

4.3 Seguridad física y del entorno

- Instalación de vigilancia (personal o servicio externo), control de accesos físicos a oficinas, salas de servidores, centros de datos.
- Monitoreo interno (cámaras, alarmas) y sistema eléctrico regulado con UPS, generadores o respaldo.
- Estaciones de trabajo ubicadas de forma que no queden expuestas a personas no autorizadas.
- Establecimiento de políticas de limpieza del escritorio ("clean desk") para evitar exposición no controlada de documentos.

4.4 Seguridad de las comunicaciones

- Toda comunicación de datos debe transitar por canales cifrados (TLS, VPN, etc.).
- Restricción del acceso a sitios no relacionados con funciones institucionales (redes sociales, tiendas online, etc.).
- Control de correo electrónico: políticas de adjuntos, bloqueo de dominios peligrosos, filtros antispam.
- Monitorizar tráfico de red para detectar comportamientos anómalos o amenazas.

4.5 Seguridad del recurso humano

- Realizar programas de formación, concienciación y sensibilización en seguridad de la información para todos los empleados.

- Incorporar cláusulas de confidencialidad en contratos, convenios y documentos de vinculación.
- Evaluaciones periódicas del desempeño en materia de buenas prácticas de seguridad.
- Sanciones o medidas correctivas en caso de incumplimiento.

4.6 Seguridad con proveedores / terceros

- Los contratos con proveedores que accedan o procesen información deben incluir cláusulas específicas de confidencialidad, niveles de servicio (SLA), auditoría y penalidades por incumplimiento.
- Realizar evaluaciones de seguridad a proveedores antes de contratarlos (due diligence).
- Control y monitoreo de accesos que los terceros tengan a los sistemas o instalaciones.

5. Roles y responsabilidades

Para que la política funcione, se deben asignar responsabilidades claras:

Rol	Responsabilidad principal
Curador Urbano Segundo	Aprobación de la política, liderazgo institucional y asignación de recursos.
Sistemas	Diseño, implementación y mantenimiento de controles técnicos, respaldo, monitoreo.
Comité de Seguridad	Evaluación de riesgos, auditorías, seguimiento de cumplimiento, mejoras.
Coordinadoras	Velar por cumplimiento de la política en su dependencia, reportar incidentes.
Usuarios finales / funcionarios / contratistas	Cumplir con las normas, participar en capacitaciones, reportar incidentes.

6. Gestión de incidentes y continuidad

- Definir un **Plan de Continuidad del Negocio (PCN)** y un **Plan de Recuperación ante Desastres (DRP).**
- Establecer procedimientos formales para reporte y manejo de incidentes de seguridad.
- Clasificación de incidentes por severidad (alto, medio, bajo) y acciones correspondientes.
- Realizar simulacros periódicos y pruebas del plan.

7. Monitoreo, auditoría y revisión

- Realizar auditorías internas y externas de seguridad de la información con frecuencia definida (al menos anual).
- Monitorear registros de accesos, logs, modificaciones a sistemas críticos.
- Revisar la política al menos cada año o cuando cambien los riesgos, tecnologías o estructura institucional.
- Llevar registro de hallazgos y acciones correctivas.

8. Comunicaciones y difusión

- Dar a conocer esta política a todos los empleados, contratistas, proveedores.
- Publicar la política de seguridad de la información en el portal institucional (versión pública).
- Incluirla en los documentos de inducción y formación de personal nuevo.

9. Sanciones y cumplimiento

- El incumplimiento de esta política podrá generar sanciones disciplinarias, acciones contractuales o legales, de acuerdo con la normativa vigente en Colombia.
- Los incidentes de seguridad serán investigados y se tomarán medidas correctivas de forma proporcional al impacto.

10. Vigencia y aprobación

Esta política entra en vigencia desde su fecha de aprobación y está vigente hasta que se modifique por orden de la autoridad competente.

Dada en Pasto, a los 02 días del mes de enero de 2025.

CARLOS ANDRÉS MELO GUERRERO
Curador Urbano Segundo de Pasto