MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DIGITAL E INFORMÁTICA (Borrador)

CONTRALORÍA GENERAL DEL DEPARTAMENTO DE SUCRE

RESOLUCIÓN No. _____ DE 2026

"Por medio de la cual se adopta la Política Institucional y el Manual de Estándares de Seguridad Digital y Privacidad de la Información en la Contraloría General del Departamento de Sucre"

El Contralor General del Departamento de Sucre, en ejercicio de sus atribuciones constitucionales y legales, en especial las conferidas por el artículo 272 de la Constitución Política de Colombia, la Ley 87 de 1993, la Ley 1581 de 2012, la Ley 1712 de 2014, el Decreto 1083 de 2015, el Decreto 767 de 2022 y la Resolución 1519 de 2020 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y

CONSIDERANDO

Que el artículo 272 de la Constitución Política asigna a las contralorías departamentales la vigilancia de la gestión fiscal en sus respectivas jurisdicciones territoriales, exigiendo altos estándares de transparencia, eficiencia e integridad institucional.

Que la Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional) establece la obligación de divulgar información proactiva y de calidad, requiriendo canales digitales íntegros y seguros.

Que el Anexo Técnico 3 de la Resolución 1519 de 2020 del MinTIC exige de forma perentoria la adopción, publicación e implementación de un Modelo de Seguridad y Privacidad de la Información (MSPI) que proteja los activos digitales frente a incidentes cibernéticos.

RESUELVE

ARTÍCULO PRIMERO. ADOPCIÓN: Adoptar el presente Manual de Políticas y Estándares de Seguridad Digital e Informática para la Contraloría General del

Departamento de Sucre, de obligatorio cumplimiento para todos los funcionarios, contratistas, pasantes y terceros con acceso a la infraestructura tecnológica del ente de control.

---

1. INTRODUCCIÓN Y MARCO LEGAL

La Contraloría General del Departamento de Sucre, consciente de la importancia estratégica de la información en el ejercicio del control fiscal, establece este manual para mitigar riesgos, proteger los datos institucionales y cumplir de forma rigurosa con los lineamientos del Gobierno Digital en Colombia. Este documento constituye el pilar fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), integrando las directrices de ciberseguridad con la rendición de cuentas pública.

Marco Legal Vigente

Norma	Descripción y Aplicabilidad Técnico-Jurídica
Constitución Política (Art. 272)	Competencias de control fiscal territorial y autonomía administrativa de la Contraloría de Sucre.
Ley 1712 de 2014	Ley de Transparencia y Acceso a la Información Pública. Obliga a garantizar la integridad y disponibilidad web.
Ley 1581 de 2012	Régimen General de Protección de Datos Personales. Principio de seguridad en el tratamiento de datos de la ciudadanía.
Decreto 767 de 2022	Lineamientos de la Política de Gobierno Digital y de Seguridad de la Información para entidades públicas.
Resolución MinTIC 1519 de 2020	Define los estándares, directrices y condiciones mínimas de seguridad digital web en su Anexo Técnico 3.

2. OBJETIVOS Y ALCANCE

Objetivo General

Establecer las directrices, estándares y lineamientos de seguridad digital orientados a preservar la confidencialidad, integridad y disponibilidad de los activos de información y la infraestructura tecnológica de la Contraloría General del Departamento de Sucre.

Alcance

Las políticas contenidas en este manual se aplican a la totalidad de las dependencias, procesos, plataformas digitales, servidores públicos, contratistas de prestación de servicios, pasantes y cualquier tercero que interactúe con los sistemas informáticos o la información oficial de la Contraloría de Sucre.

3. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD

Para garantizar la efectividad del MSPI, se define la siguiente línea de gobierno institucional:

- **Alta Dirección (Contralor Departamental):** Instancia máxima responsable de respaldar institucionalmente y aprobar las directrices y recursos para la seguridad digital.
- **Comité Institucional de Gestión y Desempeño:** Organismo encargado de evaluar los riesgos de seguridad digital periódicamente y articular las políticas con el Modelo Integrado de Planeación y Gestión (MIPG).
- **Responsable de Seguridad de la Información (Líder de TI / CISO):** funcionario técnico encargado de supervisar el cumplimiento operativo de este manual, gestionar las defensas técnicas, auditar el acceso lógico y coordinar la respuesta ante incidentes cibernéticos.

4. DESARROLLO DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD

4.1. DESARROLLO GENERAL

Las políticas y estándares de seguridad digital e informática de la **Contraloría General del Departamento de Sucre** tienen por objeto establecer las medidas, directrices y patrones técnicos de administración, uso y organización de las Tecnologías de la Información y las Comunicaciones (TIC). Estas regulaciones son de obligatorio cumplimiento para todo el personal (servidores públicos, contratistas, pasantes y terceros) comprometido en el uso y explotación de los servicios informáticos y plataformas tecnológicas proporcionados por el proceso de **Gestión de Tecnologías de la Información y las Comunicaciones (o el proceso homólogo encargado del recurso tecnológico)** de la entidad.

El presente manual se constituye como la herramienta oficial de difusión, apropiación y cultura sobre las políticas de seguridad digital a nivel institucional. Su implementación está orientada a asegurar y facilitar los principios de integridad, confidencialidad, disponibilidad y confiabilidad de la información generada, procesada y custodiada por todas las dependencias de la entidad, con especial énfasis en el manejo de los datos misionales del control fiscal, el uso correcto de los bienes informáticos (tanto de *hardware* como de *software* disponible) y la infraestructura de red. Todo esto con el propósito fundamental de mitigar y minimizar los riesgos tecnológicos, las amenazas cibernéticas y las vulnerabilidades en el uso de las tecnologías de la información, garantizando la continuidad del negocio y el cumplimiento de los mandatos legales de transparencia.

4.2. SEGURIDAD INSTITUCIONAL

La seguridad institucional de la información en la **Contraloría General del Departamento de Sucre** se concibe como un proceso transversal que involucra la cultura organizacional, la gestión del riesgo y el compromiso de todas las dependencias. La entidad fundamenta su estrategia de protección en la mitigación de brechas digitales y en la correcta asignación de responsabilidades sobre los activos informáticos.

Para garantizar este estándar, se establecen las siguientes directrices institucionales de

obligatorio cumplimiento:

- **4.2.1. Cultura y Sensibilización en Seguridad Digital:** El área encargada de las Tecnologías de la Información y las Comunicaciones (TIC), en coordinación con el proceso de Gestión del Talento Humano, diseñará y ejecutará estrategias para fomentar la *Concientización en Seguridad de la Información y Privacidad*, orientadas a identificar técnicas de ingeniería social (como *phishing*, *vishing* y *smishing*), uso seguro de contraseñas y reporte oportuno de incidentes tecnológicos.
- **4.2.2. Inventario de Activos físicos y de Información:** Cada dependencia o proceso de la Contraloría General del Departamento de Sucre es corresponsable de la custodia y administración de la información que genera, así como del uso correcto de los equipos de cómputo asignados. Por su parte, el Área de TI será la encargada de consolidar, actualizar y mantener el inventario técnico de dichos activos físicos y de información a nivel institucional.
- **4.2.3. Uso de Recursos Tecnológicos Institucionales:** Los equipos de cómputo, redes de conectividad, plataformas de almacenamiento y cuentas de correo electrónico asignados por la Contraloría General del Departamento de Sucre son propiedad exclusiva de la entidad y deben ser utilizados única y exclusivamente para el cumplimiento de las funciones misionales y obligaciones contractuales.
- **4.2.4. Seguridad en la Gestión del Talento Humano (Ingreso, Retiro y Traslado):** Todo proceso de vinculación o contratación de personal debe incluir la suscripción formal de los compromisos de seguridad. Asimismo, al momento del retiro, desvinculación o traslado de un funcionario o contratista, el jefe inmediato notificará de inmediato al Área de TI para proceder con la revocatoria inmediata de todas las credenciales de acceso lógico, entrega de equipos asignados y eliminación de permisos en los sistemas de información institucionales, evitando la existencia de cuentas huérfanas o accesos residuales.

4.3. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Con el fin de mitigar riesgos operativos, salvaguardar la infraestructura crítica y garantizar la integridad de los recursos tecnológicos de la entidad, se establecen las siguientes directrices para todo el personal:

4.3.1. Gestión y Reporte de Riesgos Físicos: El usuario o funcionario deberá reportar de forma inmediata al Área de Tecnologías de la Información (o la dependencia que haga sus veces) cualquier riesgo real o potencial detectado sobre los equipos de cómputo o de comunicaciones, tales como filtraciones o caídas de agua, fluctuaciones o choques eléctricos, caídas, golpes o peligro inminente de incendio. Asimismo, es responsabilidad exclusiva del usuario asegurar, custodiar y evitar en todo momento la pérdida, alteración o fuga de información institucional almacenada en las estaciones de trabajo, equipos personales asignados o unidades de almacenamiento (discos duros externos, memorias USB), incluso cuando estos medios no se encuentren en uso o contengan información bajo reserva legal.

4.3.2. Controles Ambientales de Infraestructura: Los centros de cableado, cuartos de racks y servidores principales de la entidad deben contar de manera obligatoria con sistemas de aire acondicionado regulado y de operación permanente, extintores de incendios de agente limpio (CO2) adecuados para equipos electrónicos, y sistemas de alimentación ininterrumpida (UPS) con la capacidad técnica requerida para mitigar fallas, sobretensiones o cortes en el fluido eléctrico, garantizando la continuidad de los servicios digitales institucionales.

4.3.3. Controles de Acceso Físico

- **4.3.3.1. Registro de Equipos Externos:** Las personas que tengan acceso a las instalaciones de la **Contraloría General del Departamento de Sucre** deberán registrar al momento de su entrada cualquier equipo de cómputo,

equipo de comunicaciones, medios de almacenamiento o herramientas técnicas que no sean propiedad de la entidad. Este registro se realizará en el área de recepción o portería, y los elementos podrán ser retirados el mismo día. En caso de requerir que el equipo permanezca en la entidad, se deberá tramitar la autorización correspondiente.

- **4.3.3.2. Retiro de Activos Tecnológicos Institucionales:** Las computadoras portátiles y cualquier activo de tecnología de la información propiedad de la entidad podrán ser retirados de las instalaciones de la **Contraloría General del Departamento de Sucre** únicamente con la autorización explícita del proceso o área que lo tenga a su cargo según el inventario oficial y con el respectivo aval del Contralor. Para ello, se deberá anexar el formato o comunicado de autorización debidamente firmado por el responsable de cada macroproceso o proceso; en ausencia de estos, la autorización final deberá ser emitida por el funcionario responsable de la dependencia o quien haga sus veces.

4.3.4. Seguridad en Áreas de Trabajo

- **4.3.4.1. Restricción a Infraestructura Crítica:** El Área de Tecnologías de la Información y las Comunicaciones (o la oficina de sistemas) de la **Contraloría General del Departamento de Sucre**, así como los cuartos de servidores y racks, son considerados áreas de acceso restringido. Por motivos de seguridad institucional y protección de datos, solo el personal técnico explícitamente autorizado podrá acceder a estas instalaciones.

4.3.5. Protección y Ubicación de los Equipos

- **4.3.5.1. Modificación y Reubicación de Equipos:** Los usuarios no deben mover, reubicar ni trasladar los equipos de cómputo o de comunicaciones asignados, así como tampoco instalar o desinstalar dispositivos periféricos internos, ni retirar los sellos de seguridad de los mismos sin la previa autorización y acompañamiento técnico del Área de TIC. En caso de requerir una modificación física, ésta deberá ser solicitada formalmente.
- **4.3.5.2. Exclusividad del Recurso Tecnológico:** El equipo de cómputo,

conectividad y software asignado a cada puesto de trabajo deberá ser de uso exclusivo para el cumplimiento de las funciones misionales y las obligaciones contractuales de los servidores públicos y contratistas de la **Contraloría General del Departamento de Sucre**.

- **4.3.5.3. Responsabilidad en el Uso de Herramientas Informáticas y Recursos Estatales:** De conformidad con los deberes consagrados en la Ley 1952 de 2019 (Código General Disciplinario), es obligación imperativa de cada servidor público y contratista actuar con la máxima diligencia, responsabilidad y cuidado en el manejo de las herramientas informáticas, sistemas de información y aplicativos instalados en los equipos asignados. El usuario responderá por el uso correcto de estos recursos, debiendo garantizar que su operación se ciña estrictamente a los fines institucionales y de control fiscal, evitando cualquier acción u omisión por impericia o negligencia que ponga en riesgo la infraestructura tecnológica, la seguridad digital o la confidencialidad de la información de la Contraloría General del Departamento de Sucre. Queda terminantemente prohibido que un usuario o funcionario distinto al personal encargado de las TIC, abra o destape los equipos de cómputo.

- **4.3.5.4 Directrices para el Mantenimiento Preventivo y Reparación de Equipos Informáticos**

  Todo procedimiento de mantenimiento técnico, ya sea preventivo o correctivo, ejecutado sobre los activos tecnológicos de la Contraloría General del Departamento de Sucre (CGS), debe ceñirse estrictamente a los siguientes protocolos de seguridad de la información:

  - **Copia de Respaldo Obligatoria:** Antes de entregar cualquier equipo informático al personal de soporte técnico (interno o externo), el usuario custodio, con el apoyo del Área de TIC, deberá realizar una copia de seguridad (backup) completa de la información misional u oficial almacenada localmente. La entidad no se hace responsable por la pérdida de datos no respaldados durante procedimientos técnicos.
  - **Borrado Seguro y Control de Datos Sensibles:** Si el mantenimiento requiere el traslado del equipo fuera de las instalaciones de la entidad

o exige la intervención de un tercero externo, se deberán aplicar técnicas de borrado seguro o extraer las unidades de almacenamiento que contengan información clasificada, reservada o sujeta a la Ley de Protección de Datos Personales (Ley 1581 de 2012).

- **Supervisión y Registro:** Toda intervención técnica debe quedar registrada en la Hoja de Vida de Equipos Informáticos, detallando la fecha, el nombre del técnico responsable, las piezas reemplazadas y la firma de conformidad del funcionario usuario del equipo.

- **4.3.5.5 Protocolos ante la Pérdida, Extravío o Préstamo de Equipos Informáticos**

La protección de los activos de información móviles y de escritorio exige una cadena de custodia formal y un régimen de responsabilidades perfectamente definido:

- **Autorización Formal de Préstamos:** Ningún equipo de cómputo, periférico o dispositivo de conectividad propiedad de la CGS podrá ser retirado de las sedes físicas institucionales sin la respectiva autorización firmada por la Secretaría General y validada técnicamente por el Área de TIC. Se expedirá un acta de asignación temporal en la que el funcionario asume la custodia total del activo.
- **Protocolo Inmediato ante Pérdida o Hurto:** En caso de robo, hurto o extravío de un equipo informático institucional, el funcionario responsable deberá instaurar de manera inmediata (dentro de las 24 horas siguientes al hecho) la denuncia penal correspondiente ante la Fiscalía General de la Nación.
- **Notificación Técnica:** Simultáneamente, el hecho deberá ser reportado al Área de TIC adjuntando copia de la denuncia, con el fin de proceder de forma remota al bloqueo de cuentas institucionales, revocación de credenciales de acceso a la red de la Contraloría y el borrado remoto de datos si el dispositivo cuenta con dicha tecnología.
- **Responsabilidad Fiscal y Administrativa:** Cualquier pérdida, sustracción o deterioro material o lógico de un activo tecnológico, derivado de dolo o negligencia, activará los procesos de investigación administrativa y disciplinaria correspondientes. Dicha actuación estará sujeta al análisis y juicio

de valor previo por parte del Comité de Gestión (o el comité competente), y obligará al funcionario o contratista responsable a asumir la reposición del bien. Así mismo las conductas que vulneren la confidencialidad, integridad y disponibilidad de la información de la CGS serán tipificadas como faltas de conformidad con el Código General Disciplinario, sin perjuicio de las acciones penales a que haya lugar bajo la Ley 1273 de 2009 (Ley de Delitos Informáticos).

- **4.3.5.6 Política de Control, Registro y Uso de Dispositivos de Almacenamiento Extraíbles**
  Con el objetivo de mitigar los riesgos de fuga de información institucional e infección por código malicioso (malware), se dictan las siguientes directrices:

- **Restricción de Uso:** Queda prohibida la conexión de memorias USB, discos duros externos, tarjetas de memoria o cualquier otro medio de almacenamiento extraíble que no esté debidamente registrado y autorizado por el Área de TIC.
- **Cifrado Obligatorio:** Los dispositivos extraíbles que se autoricen para el traslado de información institucional deberán contar con mecanismos de seguridad definidos por el Área de TIC, garantizando que, ante una eventual pérdida del medio físico, la información permanezca inaccesible para terceros.
- **Escaneo de Seguridad:** Todo medio extraíble autorizado deberá ser sometido a un escaneo antivirus obligatorio automatizado al momento de ser conectado a cualquier estación de trabajo enlazada a la red de la CGS.

4.4. ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO

Las operaciones técnicas e informáticas internas se ejecutarán siguiendo protocolos estandarizados:

- **Gestión de Backups:** Implementación de un cronograma institucional de respaldos lógicos a cargo del Área de TIC para mitigar riesgos de pérdida de datos. En casos pertinentes y contando con los recursos tecnológicos necesarios, se realizará la activación obligatoria del registro técnico de eventos en la infraestructura perimetral y de servidores para auditorías informáticas forenses o

detección de intrusos.

- **Gestión de Vulnerabilidades (Parches):** Despliegue de ventanas de mantenimiento preventivo para la actualización de plataformas ciudadanas. Cuando el servicio dependa de un tercero, el contratista estará obligado a cumplir con los niveles de seguridad digital exigidos en el marco del MSPI.

4.5. ACCESO LÓGICO, CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Como respuesta directa al plan de mejoramiento derivado de la auditoría del Índice de Transparencia (ITA), el control de acceso lógico se endurecerá bajo el principio de menor privilegio:

- **Autenticación Robusta:** Las contraseñas de red, computadores institucionales y correos electrónicos deberán tener una longitud mínima de ocho(8) caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales, con cambio obligatorio periodico. Contando con los recursos tecnológicos necesarios, se implementará de forma progresiva el Doble Factor de Autenticación (2FA).
- **Uso Exclusivo del Correo Institucional:** Está terminantemente prohibido tramitar, enviar o recibir información oficial, informes de control fiscal o datos de procesos de la Contraloría a través de correos personales (Gmail, Outlook, Yahoo, etc.). Toda comunicación oficial se realiza desde el dominio oficial corporativo.
- **Control de Privilegios:** Los usuarios finales no tendrán permisos de Administrador local en sus estaciones de trabajo, impidiendo la instalación no autorizada de software ajeno a la misión institucional.

4.6. CLÁUSULAS DE CUMPLIMIENTO

Toda orden de compra, contrato de prestación de servicios jurídicos, técnicos, de apoyo o de auditoría, así como los convenios interadministrativos suscritos por la Contraloría General del Departamento de Sucre, deberán incluir de forma obligatoria cláusulas contractuales específicas donde los contratistas se comprometan a acatar las directrices del presente Manual de Políticas de Seguridad, la Ley 1581 de 2012 y el secreto profesional sobre los expedientes en custodia.

4.7. VIOLACIONES DE SEGURIDAD INFORMÁTICA

Cualquier comportamiento que vulnere la confidencialidad, disponibilidad o integridad de los sistemas de la Contraloría se considerará un incidente grave. Esto incluye, pero no se limita a: compartir credenciales de acceso, utilizar software espía o malicioso, evadir los firewalls institucionales o extraer bases de datos oficiales sin autorización. Los incidentes serán reportados formalmente ante la Oficina de Control Interno Disciplinario de la entidad y, de configurarse delitos informáticos, ante la Fiscalía General de la Nación bajo el marco de la Ley 1273 de 2009.

4.8. ACUERDO DE CONFIDENCIALIDAD

Todo funcionario público al momento de su posesión, y todo contratista al momento de la firma de su acta de inicio, deberá suscribir de forma anexa el **Acuerdo de Confidencialidad y No Divulgación de Información**. Este documento mantendrá sus efectos legales y vinculantes incluso después de finalizado el vínculo laboral o contractual con la Contraloría General del Departamento de Sucre, respondiendo patrimonial y legalmente por cualquier filtración de datos bajo reserva legal.

Dada en Sincelejo, Sucre, a los ___ días del mes de _____ de 2026.

_____

CONTRALOR GENERAL DEL DEPARTAMENTO DE SUCRE