CURADURÍA URBANA PRIMERA DE SINCELEJO

Sucre - Colombia

POLÍTICA DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

VIGENCIA 2025

Basado en el Modelo de Seguridad y Privacidad de la Información (MSPI)
Ministerio de Tecnologías de la Información y las Comunicaciones

Resolución MinTIC 1519 de 2020 - Anexo Técnico 3

www.curaduriaprimerasincelejo.com.co

Sincelejo, Enero 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La CURADURÍA URBANA PRIMERA DE SINCELEJO, en cumplimiento de sus funciones como particular que ejerce función pública para la verificación del cumplimiento de las normas urbanísticas, reconoce la importancia de proteger la información como uno de sus activos más valiosos.

La presente Política de Seguridad Digital y de la Información establece los lineamientos, principios y directrices que orientan la gestión de la seguridad de la información en la entidad, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Este documento se desarrolla en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones, y responde a los lineamientos establecidos en la Resolución 1519 de 2020 sobre estándares de publicación y divulgación de información.

2. OBJETIVO

2.1 Objetivo General

Establecer el marco de gestión de la seguridad de la información de la Curaduría Urbana Primera de Sincelejo, definiendo las políticas, lineamientos, roles, responsabilidades y controles necesarios para proteger los activos de información contra amenazas internas y externas, garantizando la continuidad del servicio y el cumplimiento de los requisitos legales aplicables.

2.2 Objetivos Específicos

1. Proteger la confidencialidad, integridad y disponibilidad de la información de la Curaduría.
2. Establecer controles para prevenir, detectar y responder a incidentes de seguridad.
3. Garantizar la continuidad de las operaciones ante eventos adversos.
4. Cumplir con los requisitos legales y regulatorios en materia de seguridad de la información.
5. Promover una cultura de seguridad de la información entre todos los colaboradores.
6. Proteger los datos personales de los ciudadanos conforme a la Ley 1581 de 2012.

3. ALCANCE

Esta política aplica a:

- Todos los funcionarios, contratistas y terceros que tengan acceso a los activos de información de la Curaduría.
- Todos los procesos, procedimientos y actividades relacionados con la gestión de la información.
- Todos los activos de información, incluyendo: datos, documentos, sistemas de información, equipos de cómputo, redes, software y aplicaciones.
- Las instalaciones físicas donde se procesa, almacena o transmite información.
- El sitio web institucional y los servicios digitales ofrecidos a la ciudadanía.

4. DEFINICIONES

TÉRMINO	DEFINICIÓN
Activo de Información	Cualquier elemento que tenga valor para la organización, incluyendo información, software, hardware, servicios e instalaciones.
Amenaza	Causa potencial de un incidente no deseado que puede resultar en daño a un sistema u organización.
Confidencialidad	Propiedad de que la información no esté disponible o sea divulgada a personas, entidades o procesos no autorizados.
Disponibilidad	Propiedad de estar accesible y utilizable bajo demanda por una entidad autorizada.
Incidente de Seguridad	Evento o serie de eventos de seguridad de la información no deseados que tienen una probabilidad significativa de comprometer las operaciones.
Integridad	Propiedad de exactitud y completitud de los activos de información.
MSPI	Modelo de Seguridad y Privacidad de la Información del MinTIC.
Riesgo	Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO

La presente política se fundamenta en las siguientes disposiciones normativas:

NORMA	CONTENIDO
Constitución Política	Art. 15 - Derecho a la intimidad y habeas data. Art. 20 - Derecho a la información.
Ley 527 de 1999	Comercio electrónico, firmas digitales y mensajes de datos.
Ley 1266 de 2008	Habeas data financiero.
Ley 1273 de 2009	Delitos informáticos.
Ley 1581 de 2012	Protección de datos personales.
Ley 1712 de 2014	Transparencia y acceso a la información pública.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC.
Decreto 1081 de 2015	Reglamentación transparencia y acceso a información.
Resolución 1519/2020	MinTIC - Lineamientos de publicación y estándares web.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
ISO/IEC 27001:2013	Sistemas de Gestión de Seguridad de la Información.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información en la Curaduría se rige por los siguientes principios:

6.1 Confidencialidad

La información debe ser accesible únicamente por las personas autorizadas. Se establecerán controles para prevenir la divulgación no autorizada de información sensible, clasificada o reservada.

6.2 Integridad

La información debe ser exacta, completa y no modificada sin autorización. Se implementarán controles para detectar y prevenir alteraciones no autorizadas en los datos.

6.3 Disponibilidad

La información y los sistemas deben estar disponibles cuando se requieran. Se establecerán mecanismos de respaldo, recuperación y continuidad para garantizar el acceso oportuno.

6.4 Autenticidad

Se debe garantizar la identidad de los usuarios y la autenticidad de la información. Los sistemas deben verificar que los usuarios son quienes dicen ser.

6.5 No Repudio

Se deben mantener registros que permitan demostrar las acciones realizadas por los usuarios, de manera que no puedan negar haber realizado dichas acciones.

6.6 Responsabilidad

Todas las personas que tengan acceso a la información de la Curaduría son responsables de su protección. Las acciones de cada usuario deben ser trazables e identificables.

7. ROLES Y RESPONSABILIDADES

7.1 Curador Urbano (Alta Dirección)

- Aprobar y respaldar la política de seguridad de la información.
- Asignar recursos para la implementación de controles de seguridad.
- Revisar periódicamente el estado de la seguridad de la información.
- Promover la cultura de seguridad en la organización.

7.2 Responsable de Seguridad de la Información

- Coordinar la implementación de la política de seguridad.
- Gestionar los incidentes de seguridad de la información.
- Realizar evaluaciones de riesgos y proponer controles.
- Supervisar el cumplimiento de las políticas de seguridad.
- Coordinar las capacitaciones en seguridad de la información.

7.3 Propietarios de Activos de Información

- Clasificar la información bajo su responsabilidad.
- Definir los niveles de acceso autorizados.
- Revisar periódicamente los permisos de acceso.

7.4 Todos los Colaboradores

- Cumplir con las políticas y procedimientos de seguridad.
- Reportar incidentes de seguridad de manera oportuna.
- Proteger la información a la que tienen acceso.
- Participar en las capacitaciones de seguridad.

8. POLÍTICAS DE SEGURIDAD

8.1 Política de Uso Aceptable

1. Los recursos tecnológicos de la Curaduría deben usarse exclusivamente para fines laborales.
2. Está prohibido instalar software no autorizado en los equipos de la entidad.
3. No se permite el acceso a sitios web de contenido inapropiado, ilegal o peligroso.
4. El correo institucional debe usarse de manera profesional y responsable.
5. La información confidencial no debe compartirse por canales no seguros.

8.2 Política de Contraseñas

1. Las contraseñas deben tener mínimo 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
2. Las contraseñas deben cambiarse cada 90 días como máximo.
3. No se permite compartir contraseñas ni escribirlas en lugares visibles.
4. No se deben reutilizar las últimas 5 contraseñas.
5. Las cuentas se bloquearán después de 5 intentos fallidos de autenticación.

8.3 Política de Respaldo de Información

1. Se realizarán copias de seguridad diarias de la información crítica.
2. Las copias de seguridad se almacenarán en ubicación diferente a la sede principal.
3. Se realizarán pruebas de restauración trimestralmente.
4. Los respaldos deben estar cifrados y protegidos.
5. Se mantendrá un registro de las copias de seguridad realizadas.

8.4 Política de Seguridad del Sitio Web

1. El sitio web debe contar con certificado SSL/TLS (HTTPS) vigente.
2. Se realizarán análisis de vulnerabilidades periódicamente.
3. El CMS y sus componentes deben mantenerse actualizados.
4. Se implementarán controles contra ataques comunes (SQL Injection, XSS, CSRF).
5. Los formularios deben contar con protección CAPTCHA.

9. GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.1 Inventario de Activos

La Curaduría mantendrá un inventario actualizado de todos los activos de información, que incluya: identificación del activo, propietario, ubicación, clasificación y controles aplicados. El inventario se revisará anualmente.

9.2 Clasificación de la Información

La información se clasificará en los siguientes niveles:

NIVEL	DESCRIPCIÓN	CONTROLES
PÚBLICA	Información que puede ser conocida por cualquier persona	Sin restricciones de acceso. Publicada en sitio web.
CLASIFICADA	Información que puede causar daño a derechos de personas (Art. 18 Ley 1712)	Acceso restringido. Control de acceso por roles. Cifrado en tránsito.
RESERVADA	Información que puede causar daño a intereses públicos (Art. 19 Ley 1712)	Acceso muy restringido. Cifrado en reposo y tránsito. Registro de accesos.

10. CONTROL DE ACCESO

10.1 Gestión de Usuarios

- Cada usuario tendrá credenciales únicas e intransferibles.
- Los accesos se otorgarán según el principio de mínimo privilegio.
- Se realizará revisión trimestral de los permisos de acceso.
- Las cuentas de usuarios que dejen la entidad serán deshabilitadas inmediatamente.

10.2 Control de Acceso Físico

- El acceso a las áreas donde se procesa información sensible estará controlado.
- Se mantendrá un registro de visitantes.
- Los equipos de cómputo deben bloquearse cuando no estén en uso.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

- Las instalaciones contarán con sistemas de control de acceso.
- Se implementarán controles ambientales (temperatura, humedad, protección contra incendios).
- Los equipos críticos contarán con UPS y protección contra sobretensiones.
- Se mantendrá la política de escritorio limpio y pantalla limpia.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD

12.1 Reporte de Incidentes

Todos los colaboradores deben reportar inmediatamente cualquier incidente o sospecha de incidente de seguridad al Responsable de Seguridad de la Información, incluyendo pero no limitado a:

- Accesos no autorizados o intentos de acceso.
- Pérdida o robo de equipos o información.
- Infección por malware o virus.
- Correos de phishing o ingeniería social.
- Fallas en los sistemas de información.

12.2 Procedimiento de Respuesta

El procedimiento de respuesta a incidentes incluye las siguientes fases:

- Identificación: Detectar y confirmar el incidente.
- Contención: Limitar el impacto del incidente.
- Erradicación: Eliminar la causa del incidente.
- Recuperación: Restaurar los sistemas a su operación normal.
- Lecciones aprendidas: Documentar y mejorar los controles.

13. PLAN DE CONTINUIDAD DEL NEGOCIO

La Curaduría establecerá un Plan de Continuidad del Negocio que garantice la prestación de los servicios esenciales ante eventos adversos. El plan incluirá:

- Análisis de impacto en el negocio (BIA).
- Estrategias de recuperación.
- Procedimientos de respaldo y restauración.
- Sitios alternos de operación.
- Pruebas periódicas del plan.

14. CUMPLIMIENTO Y AUDITORÍA

14.1 Cumplimiento Legal

La Curaduría garantizará el cumplimiento de toda la normatividad aplicable en materia de seguridad de la información, protección de datos personales, transparencia y acceso a la información pública.

14.2 Auditorías Internas

Se realizarán auditorías internas de seguridad de la información al menos una vez al año, que incluirán la revisión de políticas, controles implementados y cumplimiento de procedimientos.

14.3 Sanciones

El incumplimiento de las políticas de seguridad de la información podrá dar lugar a acciones disciplinarias, sin perjuicio de las responsabilidades civiles o penales que correspondan.

15. VIGENCIA Y ACTUALIZACIÓN

La presente política entrará en vigencia a partir de su aprobación por el Curador Urbano y será revisada y actualizada al menos una vez al año, o cuando se presenten cambios significativos en la normatividad, la tecnología o los riesgos identificados.

Las actualizaciones serán comunicadas a todos los colaboradores y publicadas en el sitio web institucional.

_____

[NOMBRE DEL CURADOR URBANO]

Curador Urbano Primero de Sincelejo

Fecha de Aprobación: _____

URL de Publicación: https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital