

A dark green rectangular banner with a light green shadow, tilted slightly to the right. It contains the title text in white.

MANUAL DE SEGURIDAD DIGITAL



CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 13/11/2025	GESTION TECNOLÓGICA		

1. Público objetivo

Dirigido a usuarios, funcionarios públicos, así como al personal técnico y administrativo del Instituto Municipal de Cultura y Turismo de Bucaramanga -IMCT, quienes intervienen directa o indirectamente en la aplicación y uso de este manual.

2. Introducción

Este manual tiene como objetivo establecer lineamientos claros para promover buenas prácticas de seguridad digital dentro del Instituto. Su alcance abarca a todos los funcionarios, incluyendo personal técnico, administrativo y usuarios en general. Está alineado con la normativa colombiana (Ley 1581 de 2012, Decreto 1377 de 2013) y estándares internacionales como ISO/IEC 27001.

3. Objetivo

El presente manual tiene como propósito establecer lineamientos, recomendaciones y buenas prácticas en materia de seguridad digital que permitan proteger la información, los sistemas tecnológicos y los recursos informáticos del Instituto. Busca fortalecer la cultura de ciberseguridad entre los funcionarios, contratistas y demás usuarios, minimizando riesgos asociados al uso indebido de tecnologías de la información, amenazas cibernéticas, accesos no autorizados, pérdida de datos, y ataques de ingeniería social.

4. Alcance

Este manual aplica a todos los procesos, sistemas, dispositivos, redes y recursos digitales utilizados dentro del entorno institucional, así como a todo el personal que interactúe con la infraestructura tecnológica de la entidad. Cubre actividades cotidianas como el uso de correo electrónico, navegación en internet, gestión de contraseñas, acceso remoto, copias de seguridad, instalación de software, y el manejo de incidentes de seguridad informática.

Incluye tanto dispositivos propiedad de la entidad como aquellos de uso personal cuando se conecten a la red institucional o accedan a información oficial.

5. Público objetivo

Este manual está dirigido a todos los actores que interactúan con los sistemas de información de la entidad pública, incluyendo, pero no limitándose a:

CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 ALCALDÍA DE BUCARAMANGA  Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 13/11/2025	GESTION TECNOLÓGICA	

- Funcionarios públicos: Personal de planta o de carrera administrativa que hace uso habitual de los sistemas institucionales.
- Personal técnico: Encargados de la administración, mantenimiento, desarrollo y soporte de infraestructura tecnológica y servicios informáticos.
- Personal administrativo y de apoyo: funcionarios o contratistas que gestionan información institucional en labores operativas.
- Contratistas y terceros: Que, por la naturaleza de sus funciones, requieran acceso a sistemas o datos institucionales.

6. Marco Normativo

Este manual se encuentra alineado con la normativa legal vigente en Colombia en materia de protección de datos, seguridad de la información y gobierno digital, así como con estándares internacionales reconocidos:

7. Normativa Colombiana

- ✓ Ley 1581 de 2012 – Ley de Protección de Datos Personales (Habeas Data).
- ✓ Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 en cuanto a tratamiento de datos.
- ✓ Ley 1266 de 2008 – Régimen general de habeas data financiero.
- ✓ Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC.
- ✓ Política de Gobierno Digital (CONPES 3975 de 2019) – Lineamientos de transformación digital en el sector público.
- ✓ Lineamientos de Seguridad y Privacidad de la Información del Ministerio TIC.

8. Estándares y Buenas Prácticas Internacionales

- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002 – Código de buenas prácticas para controles de seguridad de la información.
- NIST SP 800-53 / SP 800-61 – Controles de seguridad y manejo de incidentes.
- OWASP – Buenas prácticas para desarrollo seguro de aplicaciones web.
- Framework de Ciberseguridad del NIST – Identificar, proteger, detectar, responder y recuperar.

9. Principios de la Seguridad Digital

- ✓ Confidencialidad

CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 13/11/2025	GESTION TECNOLÓGICA	

- ✓ Garantiza que la información solo sea accesible a personas autorizadas.
- ✓ Integridad
- ✓ Asegura que la información no sea modificada de manera no autorizada.
- ✓ Disponibilidad
- ✓ La información debe estar disponible cuando sea requerida por los usuarios autorizados.
- ✓ Responsabilidad
- ✓ Cada funcionario debe asumir la responsabilidad por el uso correcto de los recursos digitales.

10. Políticas y Buenas Prácticas

10.1. Políticas de Contraseñas

Las contraseñas deben cumplir con requisitos mínimos para garantizar su seguridad. Se recomienda lo siguiente:

Requisito	Descripción
Longitud mínima	Al menos 12 caracteres.
Complejidad	Debe incluir letras mayúsculas, minúsculas, números y símbolos.
Frecuencia de cambio	Cada 90 días.
No reutilización	Evitar usar contraseñas anteriores.

10.2. Uso seguro del correo electrónico

Antes de abrir un correo electrónico o hacer clic en un enlace, verifique siempre la dirección del remitente, evite descargar archivos adjuntos sospechosos y reporte correos dudosos al área de sistemas.

10.3. Navegación segura en Internet

Evite ingresar a sitios web no oficiales, descargue software únicamente desde sitios verificados y no ingrese información personal en portales inseguros (sin HTTPS).

10.4. Manejo de incidentes de seguridad

Ante un incidente (pérdida de información, acceso no autorizado, virus, etc.), reporte de inmediato al área de sistemas siguiendo el protocolo establecido.

10.5. Copias de seguridad

CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 ALCALDÍA DE BUCARAMANGA	Instituto Municipal de Cultura y Turismo
VERSIÓN: 01			
FA: 13/11/2025	GESTION TECNOLÓGICA		

Realice respaldos periódicos de información crítica. Se recomienda mantener copias locales y en la nube, cifradas y actualizadas regularmente.

10.6. Actualizaciones de software

Mantener el software actualizado es vital para protegerse contra vulnerabilidades. Active las actualizaciones automáticas si es posible, y priorice sistemas operativos y antivirus.

10.7. Acceso remoto seguro

Utilice redes privadas virtuales (VPN) para acceder remotamente a los sistemas institucionales. Se debe implementar autenticación multifactor (MFA) para mayor seguridad.

10.8. Ingeniería social / Phishing

No comparta sus contraseñas. Sospeche de mensajes urgentes que piden hacer clic en enlaces o proporcionar datos. Siempre confirme a través de canales oficiales antes de actuar.

11. Recomendaciones Generales

- ✓ No deje su sesión abierta en equipos públicos.
- ✓ Evite usar redes Wi-Fi abiertas para trámites oficiales.
- ✓ No instale software sin autorización.
- ✓ Realice cursos periódicos de concientización en seguridad digital.

12. Glosario de Términos

- ✓ VPN: Red Privada Virtual que permite conexión segura.
- ✓ MFA: Autenticación multifactor.
- ✓ Phishing: Suplantación de identidad para obtener información.
- ✓ Malware: Software malicioso diseñado para dañar o explotar sistemas.

13. Anexos

- Plantilla de reporte de incidentes de seguridad.
- Formato de aceptación de políticas digitales.

CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 13/11/2025	GESTION TECNOLÓGICA	

REFERENCIA DE DOCUMENTOS CONSULTADOS

TABLA DE REFERENCIA DE DOCUMENTOS CONSULTADOS				
DOCUMENTOS DE REFERENCIA				
TIPO DE DOCUMENTO	TÍTULO DEL DOCUMENTO	CÓDIGO	ORIGEN	
			Externa	Interna
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements		X	
Documento técnico–normativo elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas		X	
ISO/IEC 18044:2004 TR	Information technology - Security techniques - Information security incident management		X	
Guía ISO/CEI 73 Gestión de riesgos – Terminología	Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas		X	

CÓDIGO: GT-M-02	MANUAL DE SEGURIDAD DIGITAL	 Instituto Municipal de Cultura y Turismo
VERSIÓN: 01		
FA: 13/11/2025	GESTION TECNOLÓGICA	

RELACIÓN DE VERSIONES

CAMBIOS DE VERSIONES								
ELABORACIÓN Y/O ACTUALIZACIÓN DEL DOCUMENTOS CONTROL DE CAMBIOS								
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO				
	DD	MM	AAAA					
01	13	11	2025	Elaboración inicial del documento				
ELABORÓ Y/O ACTUALIZÓ				PROCESO RESPONSABLE				
Gabriel Arguello Castro				Gestión Tecnológica				
Alid María Lindarte Rincón				Subdirectora Administrativa y Financiera				
REVISIÓN TECNICA SGC								
NOMBRES Y APELLIDOS				DEPENDENCIA RESPONSABLE				
Yeimis Vásquez Torres				Subdirección Técnica, Proceso de Gestión Integral				
APROBÓ (RESPONSABLE DEL PROCESO)								
NOMBRES Y APELLIDOS				CARGO		FECHA		
						DD	MM	AAAA
Alid María Lindarte Rincón				Subdirectora Administrativa y Financiera		10	08	2025
APROBÓ POR LA ALTA DIRECCIÓN- COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO “Si aplica”								
NÚMERO DE ACTA				N°.		FECHA		