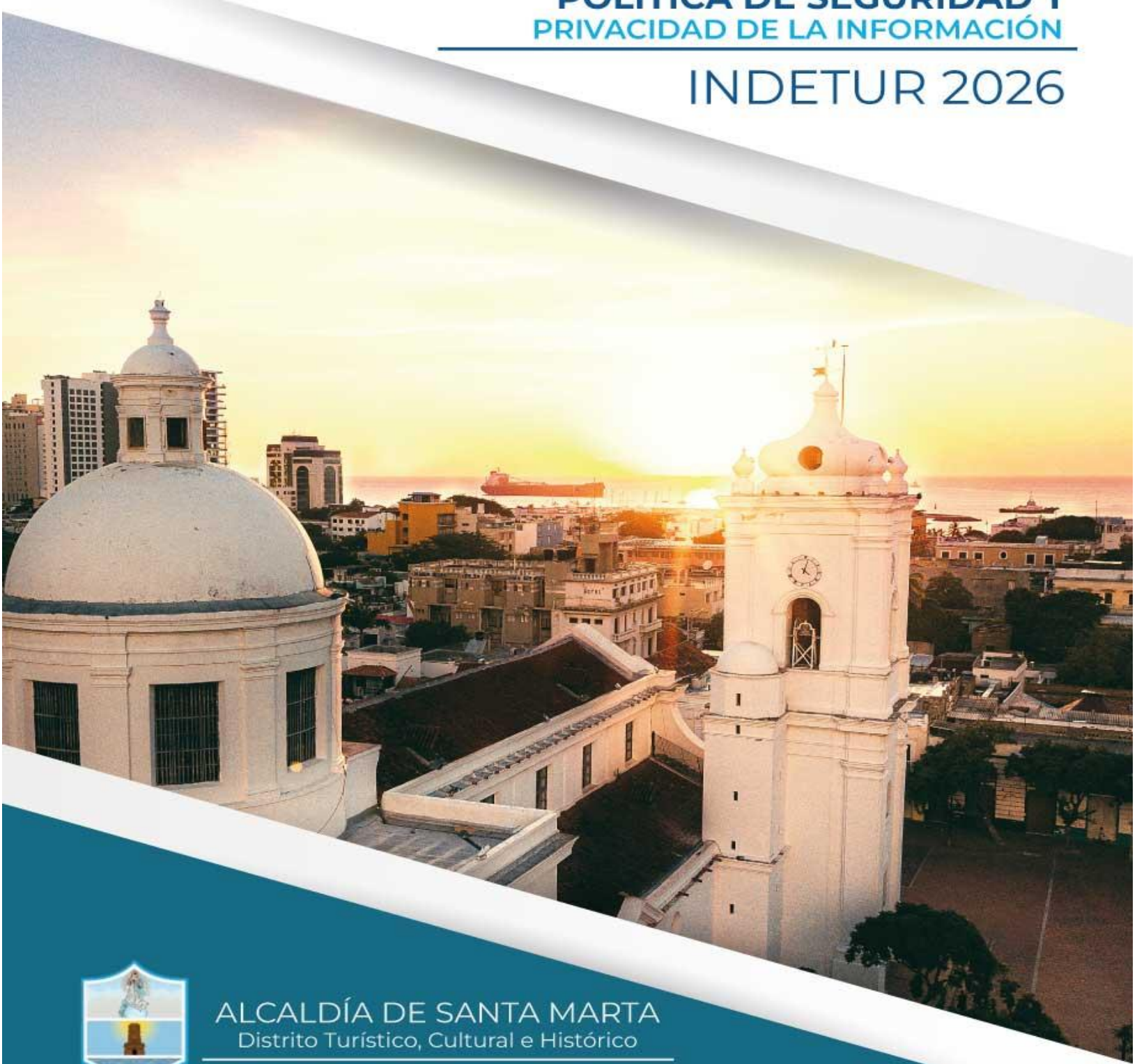
POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INDETUR 2026



ALCALDÍA DE SANTA MARTA
Distrito Turístico, Cultural e Histórico

Instituto Distital de Turismo
de Santa Marta

WWW.INDETUR.GOV.CO
CALLE 15 No 2 - 60 Ed. Bolivar Piso 3
@INDETURSMR

INSTITUTO DISTRITAL DE TURISMO DE SANTA MARTA

INDETUR

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Compromiso institucional con la protección, confidencialidad, integridad y disponibilidad de la información de INDETUR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – INDETUR			
Código:	INDETUR-TI-PSI-001	**Versión:**	1.0
Fecha de aprobación:	Mayo de 2026	**Próxima revisión:**	Enero de 2027
Elaboró:	Área de TI y Comunicaciones	**Aprobó:**	Dirección General – INDETUR
Clasificación:	Documento de uso interno / Divulgación general interna		
Aplica a:	Todos los funcionarios, contratistas y terceros con acceso a los sistemas de información de INDETUR		

Área de TI y Comunicaciones

Santa Marta D.T.C.H. – 2026

1. Declaración de la Política

El Instituto Distrital de Turismo de Santa Marta – INDETUR, en ejercicio de sus funciones como entidad pública del orden distrital y en cumplimiento de la normatividad vigente en materia de Gobierno Digital, seguridad de la información y protección de datos personales, declara su compromiso institucional con la seguridad de la información como un valor estratégico fundamental para el cumplimiento de su misión.

INDETUR reconoce que la información institucional es un activo de alto valor que debe ser protegido de manera permanente frente a amenazas internas y externas, garantizando en todo momento su:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
La información es accesible únicamente a personas y sistemas autorizados.	La información no ha sido alterada de forma no autorizada o accidental.	La información y los sistemas están accesibles cuando se necesitan.

La presente Política de Seguridad de la Información es de obligatorio cumplimiento para todos los funcionarios de planta, contratistas, pasantes, proveedores de servicios TI y cualquier tercero que acceda a los sistemas, redes o información de INDETUR.

2. Objetivo

Establecer los principios, directrices y reglas que deben seguir todos los actores relacionados con el uso y tratamiento de la información de INDETUR, con el fin de proteger sus activos de información, reducir los riesgos de seguridad digital y garantizar el cumplimiento de la normatividad colombiana aplicable.

3. Alcance

Esta política aplica a:

- Todos los funcionarios de planta y servidores públicos de INDETUR.
- Contratistas, consultores y prestadores de servicios con acceso a sistemas institucionales.
- Pasantes, aprendices SENA y personal en prácticas.
- Proveedores de servicios tecnológicos con acceso a la infraestructura de INDETUR.
- Todos los activos de información: equipos de cómputo, servidor institucional, correo electrónico, página web, redes, documentos digitales y datos personales.

4. Marco Normativo

Esta política se fundamenta en:

1. Constitución Política de Colombia – Art. 15 (habeas data) y Art. 20 (libertad de información).
2. Ley 1581 de 2012 – Protección de Datos Personales.
3. Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública.
4. Ley 527 de 1999 – Comercio electrónico y valor probatorio de mensajes de datos.
5. Decreto 1078 de 2015 – Política de Gobierno Digital (MinTIC).
6. Resolución 1519 de 2020 – Lineamientos de implementación de Gobierno Digital.
7. CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
8. Decreto 338 de 2022 – Gestión de incidentes de seguridad digital.
9. Ley 734 de 2002 – Código Disciplinario Único (conductas sancionables).
10. ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información (referencia técnica).
11. MSPI INDETUR v1.0 (2026) – Modelo de Seguridad y Privacidad de la Información.

5. Definiciones

Término	Definición
Activo de información	Todo recurso que tiene valor para la entidad y requiere protección: datos, software, hardware, redes y capital humano con conocimiento institucional.
Confidencialidad	Propiedad que asegura que la información es accesible solo por personas, procesos o sistemas autorizados.
Integridad	Propiedad que garantiza que la información y sus métodos de procesamiento son exactos y completos, y no han sido alterados sin autorización.
Disponibilidad	Propiedad que garantiza que la información y los sistemas son accesibles y utilizables cuando son requeridos.
Incidente de seguridad	Evento que afecta o amenaza la confidencialidad, integridad o disponibilidad de la información o los sistemas institucionales.
Dato personal	Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable (Ley 1581/2012).
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una amenaza para causar daño.

Término	Definición
Amenaza	Causa potencial de un incidente no deseado que puede causar daño a un sistema u organización.
Riesgo de seguridad	Combinación de la probabilidad de una amenaza y su impacto sobre los activos de información.
Control de acceso	Mecanismo que restringe el acceso a la información y los sistemas solo a usuarios autorizados.
Backup / Copia de seguridad	Copia de datos que puede utilizarse para restaurar la información original en caso de pérdida o daño.
Malware	Software diseñado para infiltrarse, dañar o ejecutar acciones no autorizadas en sistemas informáticos.
Phishing	Técnica de ingeniería social que busca engañar a usuarios para obtener credenciales u información confidencial.

6. Políticas Específicas de Seguridad

INDETUR adopta las siguientes doce (12) políticas específicas de seguridad de la información, de obligatorio cumplimiento institucional:

#	Política	Objetivo	Aplica a
1	**Control de Acceso y Gestión de Identidades**	Garantizar que solo usuarios autorizados accedan a los sistemas e información de INDETUR	*Todos los usuarios*
2	**Gestión de Contraseñas**	Establecer requisitos mínimos de seguridad para las credenciales de acceso institucional	*Todos los usuarios*
3	**Uso Aceptable de Activos de TI**	Definir el uso apropiado de los recursos tecnológicos de la entidad	*Todos los usuarios*
4	**Copias de Seguridad (Backups)**	Garantizar la disponibilidad y recuperación de la información institucional	*Jefe TI / Todas las áreas*
5	**Protección contra Malware y Ciberamenazas**	Prevenir la infección y propagación de software malicioso	*Todos los usuarios / Jefe TI*

#	Política	Objetivo	Aplica a
6	**Seguridad Física de la Infraestructura TI**	Proteger físicamente los activos tecnológicos críticos de la entidad	*Jefe TI / Administrativa*
7	**Gestión de Incidentes de Seguridad**	Establecer el proceso de reporte, atención y cierre de incidentes de seguridad	*Todos los usuarios / Jefe TI*
8	**Protección de Datos Personales**	Garantizar el tratamiento legal y seguro de datos personales conforme a la Ley 1581/2012	*Todos los usuarios*
9	**Correo Electrónico Institucional**	Definir el uso seguro y apropiado del correo electrónico de la entidad	*Todos los usuarios*
10	**Teletrabajo y Acceso Remoto**	Establecer condiciones de seguridad para el acceso a sistemas desde fuera de la sede	*Funcionarios en teletrabajo*
11	**Gestión de Proveedores y Terceros TI**	Controlar los riesgos de seguridad derivados del acceso de terceros a sistemas institucionales	*Jefe TI / Jurídica*
12	**Actualización y Parches de Seguridad**	Mantener los sistemas actualizados para reducir vulnerabilidades conocidas	*Jefe TI*

7. Desarrollo de las Políticas de Seguridad

Política 1: Control de Acceso y Gestión de Identidades

Todo acceso a los sistemas de información y recursos tecnológicos de INDETUR debe ser formalmente autorizado y gestionado por el Área de TI.

Directrices:

- Cada usuario tendrá una cuenta individual e intransferible. No se permite el uso compartido de cuentas.
- Los accesos se asignan según el principio de mínimo privilegio: solo los permisos necesarios para cumplir las funciones del cargo.
- El Área de TI mantendrá un registro actualizado de todos los usuarios con acceso a sistemas institucionales.
- Ante el retiro, traslado o cambio de funciones de un funcionario, sus accesos serán revocados o modificados dentro de las 24 horas siguientes a la notificación de Talento Humano.
- Los accesos temporales para contratistas o terceros tendrán fecha de vencimiento definida y serán eliminados al terminar la relación contractual.

- Se realizará auditoría semestral de cuentas de usuario activas para depurar accesos no vigentes.

Política 2: Gestión de Contraseñas

Las contraseñas son el principal mecanismo de autenticación. Su gestión segura es responsabilidad de cada usuario.

Requisitos de contraseña:

- Longitud mínima de 10 caracteres.
- Deben incluir: letras mayúsculas, minúsculas, números y al menos un carácter especial (!, @, #, $, %, etc.).
- No pueden contener el nombre del usuario, fecha de nacimiento, nombre de la entidad ni secuencias obvias (1234, abcd).
- Deben cambiarse obligatoriamente cada noventa (90) días.
- No se permite reutilizar las últimas 5 contraseñas.

Obligaciones del usuario:

- Nunca compartir la contraseña con compañeros, superiores o personal de soporte TI.
- No escribir contraseñas en papeles, notas adhesivas o documentos sin cifrar.
- Reportar de inmediato al Área de TI si sospecha que su contraseña fue comprometida.
- Activar el bloqueo automático de sesión por inactividad (máximo 10 minutos).

Política 3: Uso Aceptable de Activos de TI

Los equipos de cómputo, redes, software y demás recursos tecnológicos de INDETUR son de uso institucional y deben emplearse exclusivamente para el cumplimiento de las funciones asignadas.

Está permitido:

- Usar los equipos para actividades relacionadas con las funciones del cargo.
- Acceder a sitios web relacionados con las labores institucionales.
- Usar el correo institucional para comunicaciones de carácter oficial.

Está prohibido:

- Instalar software no autorizado por el Área de TI (juegos, aplicaciones personales, programas pirata).
- Acceder a contenido inapropiado, ilegal o no relacionado con las funciones institucionales.
- Conectar dispositivos de almacenamiento externos (memorias USB, discos duros) sin autorización previa del Área de TI.
- Desactivar, desinstalar o modificar herramientas de seguridad instaladas (antivirus, firewall).
- Usar recursos institucionales para actividades comerciales, políticas o personales.
- Acceder a redes sociales con fines personales durante la jornada laboral desde equipos institucionales.

Política 4: Copias de Seguridad (Backups)

INDETUR implementa un esquema de respaldo periódico para garantizar la recuperación de la información ante fallas, pérdidas o incidentes.

Esquema de backups:

- Backup diario: archivos críticos en uso activo (carpetas de trabajo de cada área).
- Backup semanal: copia completa del servidor institucional (cada viernes).
- Backup mensual: copia almacenada en medio externo o ubicación alternativa (último día hábil del mes).

Verificación:

- El Área de TI verificará la integridad de los backups mediante prueba de restauración trimestral.
- Se llevará registro de cada backup realizado con fecha, contenido y resultado.
- Los medios de backup externos serán almacenados en lugar seguro y diferente a la sede principal.

Política 5: Protección contra Malware y Ciberamenazas

INDETUR adoptará medidas técnicas y organizativas para prevenir la infección por malware, ransomware y otras ciberamenazas.

- Todos los equipos de cómputo tendrán instalado software antivirus/antimalware con licencia vigente y actualización automática de definiciones.
- El servidor institucional contará con firewall configurado con reglas de filtrado de tráfico.
- Está prohibido desactivar el antivirus o el firewall sin autorización explícita del Área de TI.
- Los usuarios no deben abrir archivos adjuntos de remitentes desconocidos ni hacer clic en enlaces sospechosos.
- El Área de TI aplicará parches y actualizaciones de seguridad del fabricante en cuanto estén disponibles.
- Cualquier equipo con sospecha de infección debe ser reportado inmediatamente al Área de TI y desconectado de la red.

Política 6: Seguridad Física de la Infraestructura TI

Los activos tecnológicos críticos de INDETUR requieren protección física adecuada para prevenir accesos no autorizados, daños o hurtos.

- El servidor institucional estará ubicado en espacio físico con acceso restringido mediante llave o control de acceso. Solo el Jefe TI y personal autorizado tendrán acceso.
- Se llevará registro de visitas y accesos al cuarto de servidores o área de TI.
- Los equipos de cómputo estarán inventariados con etiqueta de identificación institucional.
- Los usuarios aplicarán la política de escritorio limpio: pantalla bloqueada al ausentarse del puesto (máximo 10 minutos de inactividad).
- El servidor contará con sistema de alimentación ininterrumpida (UPS) para prevenir daños por cortes eléctricos.
- No se permitirá la reubicación de equipos institucionales sin autorización del Área de TI.

Política 7: Gestión de Incidentes de Seguridad

Todo evento que afecte o amenace la seguridad de la información de INDETUR debe ser reportado, atendido y documentado de manera oportuna.

Obligaciones del usuario:

- Reportar cualquier incidente o sospecha de incidente al Jefe TI inmediatamente (mismo día de detección).
- No intentar resolver el incidente por cuenta propia si no tiene los conocimientos técnicos para ello.
- Conservar evidencias del incidente (capturas de pantalla, correos, mensajes de error).

Proceso de atención (responsabilidad del Área TI):

12. Recepción y registro del incidente.
13. Clasificación por tipo y severidad (leve, moderado, grave, crítico).
14. Contención y mitigación del impacto.
15. Investigación de causas raíz.
16. Corrección y recuperación.
17. Cierre y documentación de lecciones aprendidas.
18. Notificación a la Dirección General si el impacto es significativo.

Política 8: Protección de Datos Personales

INDETUR garantiza el tratamiento legal, seguro y transparente de los datos personales que recibe en el ejercicio de sus funciones institucionales, en cumplimiento de la Ley 1581 de 2012.

- Solo se recolectarán datos personales estrictamente necesarios para las finalidades institucionales declaradas.
- Los titulares de datos personales serán informados sobre el tratamiento mediante el Aviso de Privacidad publicado en la página web de INDETUR.
- Los datos personales no serán compartidos con terceros sin autorización del titular, salvo mandato legal.
- Los datos personales serán almacenados con controles de acceso que restrinjan su consulta solo al personal autorizado.
- Los funcionarios que manejen datos personales deben guardar confidencialidad absoluta, incluso después de terminar su vínculo con la entidad.
- INDETUR mantendrá las bases de datos con datos personales registradas en el RNBD de la SIC.
- El responsable del tratamiento de datos personales es el Director General de INDETUR.

Política 9: Correo Electrónico Institucional

El correo electrónico institucional es un recurso oficial de comunicación y debe usarse de manera segura y responsable.

Uso permitido:

- Comunicaciones relacionadas con las funciones del cargo.
- Envío de documentos oficiales y notificaciones institucionales.

Está prohibido:

- Usar el correo institucional para comunicaciones personales, cadenas de mensajes o mensajes no solicitados (spam).
- Enviar información confidencial o datos personales sin las medidas de seguridad adecuadas.
- Abrir archivos adjuntos de remitentes desconocidos o sospechosos.
- Hacer clic en enlaces de correos que soliciten credenciales o información personal (phishing).
- Usar el correo institucional para actividades comerciales o políticas.

Buenas prácticas:

- Verificar siempre la identidad del remitente antes de responder solicitudes de información sensible.
- No responder correos de phishing. Reportarlos al Área de TI.
- Cerrar sesión del correo al terminar la jornada o al ausentarse del equipo.

Política 10: Teletrabajo y Acceso Remoto

Los funcionarios que realicen trabajo remoto o teletrabajo deben garantizar las mismas condiciones de seguridad que en la sede institucional.

- El acceso remoto a sistemas institucionales debe realizarse únicamente a través de conexiones seguras autorizadas por el Área de TI.
- Está prohibido acceder a sistemas de INDETUR desde redes WiFi públicas o no seguras sin VPN u otro mecanismo de protección.
- Los equipos personales utilizados para teletrabajo deben tener antivirus activo y sistema operativo actualizado.
- La información institucional no debe almacenarse en dispositivos personales o plataformas en la nube no autorizadas por la entidad.
- El funcionario en teletrabajo es responsable de garantizar que personas no autorizadas (familiares, terceros) no accedan a los sistemas institucionales desde su lugar de trabajo remoto.

Política 11: Gestión de Proveedores y Terceros TI

Los proveedores de servicios tecnológicos y terceros con acceso a sistemas de INDETUR deben cumplir los estándares de seguridad de la entidad.

- Los contratos con proveedores TI incluirán cláusulas de confidencialidad y obligaciones de seguridad de la información.
- El acceso de proveedores a sistemas institucionales será temporal, supervisado y con los mínimos privilegios necesarios.
- Al finalizar el contrato o la labor, el Área de TI revocará inmediatamente todos los accesos otorgados al proveedor.

- Los proveedores no podrán transferir, copiar ni divulgar información institucional a los que hayan tenido acceso en ejercicio del contrato.
- INDETUR realizará evaluación periódica del cumplimiento de los requisitos de seguridad por parte de sus proveedores TI.

Política 12: Actualización y Gestión de Parches de Seguridad

INDETUR mantendrá sus sistemas actualizados para minimizar la exposición a vulnerabilidades conocidas.

- El Área de TI evaluará y aplicará las actualizaciones de seguridad publicadas por los fabricantes de software y sistemas operativos en cuanto estén disponibles.
- Las actualizaciones críticas de seguridad se aplicarán dentro de los 15 días hábiles siguientes a su publicación oficial.
- Antes de aplicar actualizaciones en el servidor, se realizará backup completo.
- Está prohibido que los usuarios deshabiliten las actualizaciones automáticas de sus sistemas sin autorización del Área de TI.
- El Área de TI llevará registro de las versiones de software instaladas y las actualizaciones aplicadas.

8. Régimen de Sanciones

El incumplimiento de las disposiciones de esta Política de Seguridad de la Información constituye una falta disciplinaria y podrá dar lugar a las siguientes consecuencias, según la gravedad de la infracción:

Tipo de infracción	Ejemplos	Consecuencia posible
Leve	Compartir contraseña con un compañero. Usar equipo institucional para fines personales ocasionalmente.	Llamado de atención verbal. Requerimiento de capacitación en seguridad.
Moderada	Instalar software no autorizado. Ignorar reportes de incidentes. No actualizar contraseña en el plazo establecido.	Llamado de atención escrito. Reporte al superior jerárquico. Acción disciplinaria leve.
Grave	Acceder a información sin autorización. Divulgar información confidencial o datos personales. Sabotear sistemas institucionales.	Proceso disciplinario formal. Reporte a Control Interno. Posible denuncia penal según normativa vigente.

Las sanciones se aplicarán conforme al Código Disciplinario Único (Ley 734 de 2002) o la normativa que lo modifique o sustituya, sin perjuicio de las acciones penales o civiles que correspondan según la naturaleza de la infracción.

9. Compromisos de la Dirección

La Dirección General de INDETUR se compromete a:

- Aprobar y respaldar formalmente esta Política de Seguridad de la Información.
- Garantizar los recursos humanos, técnicos y presupuestales necesarios para su implementación.
- Promover una cultura de seguridad de la información en toda la entidad.
- Exigir el cumplimiento de esta política a todos los funcionarios y terceros relacionados con INDETUR.
- Revisar y actualizar esta política al menos una vez al año o cuando se presenten cambios significativos.

10. Responsabilidades

10.1 Director General

- Aprobar y comunicar oficialmente esta política.
- Garantizar su cumplimiento en todos los niveles de la entidad.
- Designar al Jefe TI como responsable de la gestión de seguridad de la información.

10.2 Jefe Área TI y Comunicaciones

- Implementar, mantener y hacer cumplir las políticas específicas de seguridad.
- Gestionar los controles técnicos: accesos, backups, antivirus, actualizaciones.
- Atender y documentar los incidentes de seguridad reportados.
- Capacitar y sensibilizar a los funcionarios en seguridad de la información.
- Elaborar informes periódicos de cumplimiento para la Dirección General.

10.3 Todos los Funcionarios y Contratistas

- Leer, comprender y cumplir esta Política de Seguridad de la Información.
- Reportar cualquier incidente o vulnerabilidad al Área de TI.
- Participar en las jornadas de capacitación en seguridad digital.
- No realizar acciones que pongan en riesgo la seguridad de la información institucional.

10.4 Oficina de Control Interno

- Verificar el cumplimiento de esta política en las auditorías internas.
- Emitir recomendaciones de mejora al proceso de seguridad de la información.

11. Capacitación y Sensibilización

INDETUR promoverá activamente la cultura de seguridad de la información mediante:

- Jornada anual de capacitación en seguridad digital para todos los funcionarios (ciberseguridad, phishing, contraseñas, datos personales).
- Socialización de esta política al inicio de cada vigencia y en la inducción de nuevos funcionarios y contratistas.
- Publicación de circulares periódicas con alertas de seguridad y buenas prácticas.
- Aprovechamiento de recursos gratuitos de MinTIC (Colombia Digital, cursos en línea de seguridad digital).
- Firma del Acuerdo de Confidencialidad y Uso Aceptable por parte de todos los usuarios al iniciar su vinculación con INDETUR.

12. Revisión y Actualización de la Política

Esta política será revisada y actualizada en los siguientes casos:

- Anualmente, durante el primer trimestre de cada vigencia.
- Cuando ocurran cambios significativos en la infraestructura tecnológica de INDETUR.
- Cuando se presenten incidentes de seguridad que evidencien brechas no contempladas.
- Cuando se emitan nuevas normativas o lineamientos de MinTIC, DAFP, SIC u otras entidades reguladoras.

El Jefe del Área de TI presentará la versión revisada a la Dirección General para su aprobación formal.

13. Historial de Versiones

Versión	Fecha	Elaboró	Descripción
1.0	Mayo 2026	Área TI y Comunicaciones	Elaboración inicial de la Política de Seguridad de la Información de INDETUR, conforme al MSPI v1.0 y lineamientos MinTIC.

DECLARACIÓN DE APROBACIÓN Y COMPROMISO INSTITUCIONAL

Los suscritos, en ejercicio de nuestras competencias, declaramos haber revisado, aprobado y adoptado la presente Política de Seguridad de la Información del Instituto Distrital de Turismo de Santa Marta – INDETUR, la cual es de obligatorio cumplimiento para todos los funcionarios, contratistas y terceros que accedan a los sistemas e información institucional.

Jose Egurrola Pedraza

Jefe Área TI y Comunicaciones

Elaboró y presentó

INDETUR – Santa Marta, Mayo 2026

Jose Domingo Davila

Director General – INDETUR

Aprobó

INDETUR – Santa Marta, Mayo 2026

Esta política entra en vigencia a partir de la fecha de su aprobación por la Dirección General y deroga cualquier disposición interna anterior sobre la misma materia.