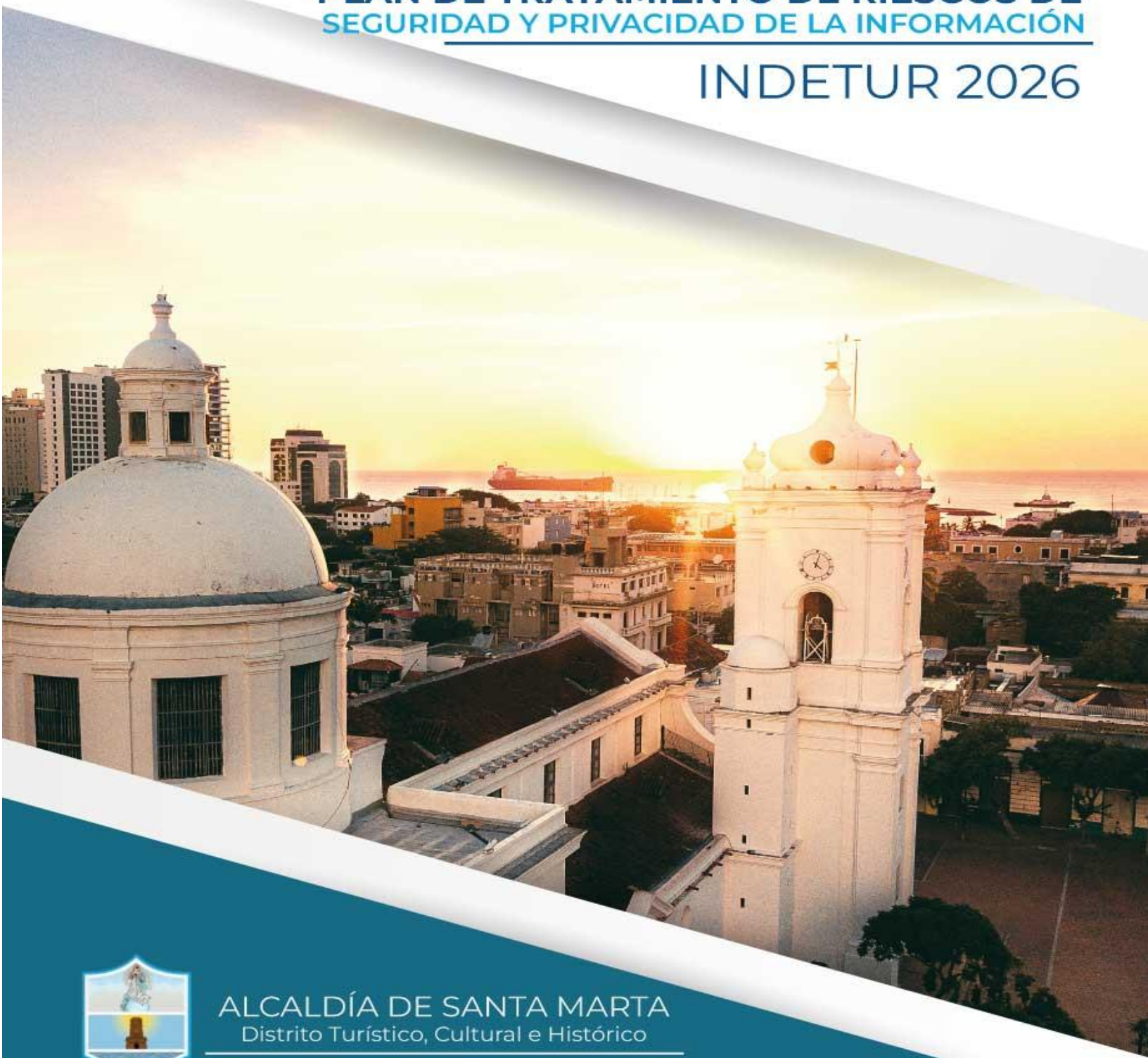
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL – INDETUR 2026			
Código:	INDETUR-TI-PTRS-001	**Versión:**	1.0
Fecha:	Mayo de 2026	**Vigencia:**	Enero – Diciembre 2026
Responsable:	Área TI y Comunicaciones	**Aprobó:**	Dirección General
Presupuesto estimado:	Menos de $5.000.000 COP	**Clasificación:**	Uso Interno

Área de TI y Comunicaciones

Santa Marta D.T.C.H. – 2026

1. Introducción

El presente Plan de Tratamiento de Riesgos de Seguridad Digital es el instrumento mediante el cual el Instituto Distrital de Turismo de Santa Marta – INDETUR define, prioriza y programa las acciones concretas para reducir los riesgos que amenazan la confidencialidad, integridad y disponibilidad de su información institucional.

Este plan se articula directamente con el Modelo de Seguridad y Privacidad de la Información (MSPI) de la entidad, complementa la Matriz de Riesgo Institucional y da cumplimiento a los lineamientos del CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital, el Decreto 338 de 2022 y los estándares del Marco de Referencia de Arquitectura Empresarial del Estado de MinTIC.

2. Objetivos

2.1 Objetivo General

Definir y ejecutar acciones de tratamiento proporcionales y sostenibles para reducir los riesgos de seguridad digital identificados en INDETUR durante la vigencia 2026, garantizando la protección de los activos de información institucionales.

2.2 Objetivos Específicos

- Identificar y valorar los riesgos de seguridad digital que afectan a INDETUR, incluyendo amenazas de ciberseguridad, privacidad y continuidad operacional.
- Definir acciones de tratamiento concretas, responsables, plazos y costos para cada riesgo identificado.
- Establecer indicadores de seguimiento que permitan medir la efectividad de los controles implementados.
- Garantizar el cumplimiento de la normatividad de Gobierno Digital, protección de datos personales y transparencia.
- Optimizar el uso de los recursos disponibles priorizando controles de gestión interna sin costo.

3. Alcance

El plan aplica a todos los activos de información, sistemas y procesos soportados por tecnología en INDETUR, e involucra a todos los funcionarios, contratistas y proveedores con acceso a la infraestructura institucional durante la vigencia 2026.

4. Marco Normativo

1. CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
2. Decreto 338 de 2022 – Gestión de incidentes de seguridad digital en entidades públicas.
3. Decreto 1078 de 2015 – Política de Gobierno Digital (MinTIC).
4. Ley 1581 de 2012 – Protección de Datos Personales.
5. Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública.
6. Resolución 1519 de 2020 – Lineamientos de implementación de Gobierno Digital.
7. ISO/IEC 27005:2022 – Gestión de riesgos de seguridad de la información (referencia técnica).
8. MSPI INDETUR versión 1.0 (2026) – Modelo de Seguridad y Privacidad de la Información.

5. Metodología de Valoración de Riesgos

Para la identificación y valoración de riesgos se utilizó la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP) en las Guías de Administración del Riesgo, adaptada al contexto de seguridad digital de MinTIC:

Probabilidad	Impacto	Zona de Riesgo	Opción de Manejo
Muy Alta (100%) Alta (80%) Media (60%) Baja (40%) Muy Baja (20%)	Catastrófico (100%) Mayor (80%) Moderado (60%) Menor (40%) Leve (20%)	EXTREMO ALTO MODERADO BAJO	Reducir Evitar Aceptar Transferir

6. Resumen Ejecutivo de Riesgos Identificados

Se identificaron un total de 9 riesgos de seguridad digital para INDETUR en la vigencia 2026. La siguiente tabla presenta el consolidado:

#	Riesgo	Prob.	Impacto	Zona	Opción	Responsable	Plazo
R-01	Acceso no autorizado por gestión débil de contraseñas y privilegios	Media 60%	Catastrófico 100%	**EXTREMO**	REDUCIR	Jefe TI	Mar 2026 (continuo)
R-02	Ciberataques (ransomware, DoS, DDoS) por obsolescencia tecnológica	Muy Alta 100%	Moderado 60%	**ALTO**	REDUCIR	Jefe TI / Proveedor	Jun 2026 (continuo)
R-03	Pérdida de trazabilidad e integridad de información digital	Baja 40%	Moderado 60%	**MODERADO**	REDUCIR	Jefe TI / Gestión Documental	Jun 2026
R-04	Modificación de información por personal no autorizado (riesgo de corrupción TI)	Muy Baja 20%	Moderado 60%	**MODERADO**	REDUCIR	Jefe TI	Abr 2026 (continuo)
R-05	Falla o indisponibilidad del servidor institucional	Baja 40%	Mayor 80%	**ALTO**	REDUCIR	Jefe TI	May 2026 (continuo)
R-06	Fuga o exposición de datos personales de ciudadanos y funcionarios	Baja 40%	Mayor 80%	**ALTO**	REDUCIR	Jefe TI / Jurídica	Jun 2026

#	Riesgo	Prob.	Impacto	Zona	Opción	Responsable	Plazo
R-07	Ingeniería social y phishing dirigido a funcionarios	Alta 80%	Moderado 60%	**ALTO**	REDUCIR	Jefe TI	Ago 2026
R-08	Incumplimiento de lineamientos de Gobierno Digital y transparencia (ITA)	Media 60%	Mayor 80%	**ALTO**	REDUCIR	Jefe TI / Planeación	Continuo 2026
R-09	Acceso físico no autorizado a equipos e infraestructura TI	Baja 40%	Mayor 80%	**ALTO**	REDUCIR	Jefe TI / Administrativa	Abr 2026

De los 9 riesgos identificados: 1 es de nivel EXTREMO (requiere atención inmediata), 5 son de nivel ALTO, y 3 son de nivel MODERADO. Todos tienen opción de manejo REDUCIR mediante controles de gestión interna o inversiones menores.

7. Fichas de Tratamiento por Riesgo

A continuación se presenta la ficha de tratamiento detallada para cada uno de los 9 riesgos identificados:

FICHA DE TRATAMIENTO: R-01			
Código:	R-01	**Zona de riesgo:**	**EXTREMO**
Nombre del riesgo:	Acceso no autorizado por gestión débil de contraseñas y privilegios		
Causa principal:	Ausencia de política robusta de contraseñas. Falta de revisión periódica de roles y privilegios de acceso.		
Probabilidad:	Media 60%	**Impacto:**	Catastrófico 100%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI
Plazo:	Mar 2026 (continuo)	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Implementar y documentar política formal de contraseñas (mínimo 10 caracteres, complejidad, cambio cada 90 días).		
2.	Realizar auditoría y depuración de cuentas de usuario activas en todos los sistemas.		
3.	Establecer revisión semestral de roles y privilegios con acta de verificación.		

4.	Activar bloqueo automático de sesión por inactividad (máximo 10 minutos).		
5.	Habilitar autenticación de dos factores (2FA) en correo institucional.		
Indicador de seguimiento:	% usuarios con contraseña actualizada ≥ 100%		
Estado actual:	**EN EJECUCIÓN**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-02			
Código:	R-02	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Ciberataques (ransomware, DoS, DDoS) por obsolescencia tecnológica		
Causa principal:	Restricciones presupuestales. Obsolescencia de software y hardware. Incumplimiento de ANS por proveedores.		
Probabilidad:	Muy Alta 100%	**Impacto:**	Moderado 60%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI / Proveedor
Plazo:	Jun 2026 (continuo)	**Costo estimado:**	$800.000 (licencias antivirus)
ACCIONES DE TRATAMIENTO			
1.	Aplicar parches y actualizaciones de seguridad disponibles del fabricante.		
2.	Instalar y mantener activo software antivirus/antimalware en todos los equipos.		
3.	Configurar firewall en el servidor institucional con reglas de filtrado básico.		
4.	Incluir en el plan de adquisiciones la renovación de equipos críticos obsoletos.		
5.	Verificar cumplimiento del Acuerdo de Nivel de Servicio (ANS) del contrato de soporte TI.		
Indicador de seguimiento:	0 incidentes por ciberataque en el período		
Estado actual:	**EN EJECUCIÓN**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-03			
Código:	R-03	**Zona de riesgo:**	**MODERADO**
Nombre del riesgo:	Pérdida de trazabilidad e integridad de información digital		
Causa principal:	Uso de documentos compartidos sin control de versiones. No utilización de herramientas de control de cambios.		
Probabilidad:	Baja 40%	**Impacto:**	Moderado 60%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI / Gestión Documental
Plazo:	Jun 2026	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Socializar y capacitar a funcionarios en el uso de control de versiones en documentos.		
2.	Definir estructura de carpetas y nomenclatura oficial para archivos digitales institucionales.		
3.	Establecer repositorio centralizado de documentos en el servidor institucional.		
4.	Implementar política de cero papel y gestión de documentos electrónicos.		
Indicador de seguimiento:	% documentos almacenados en repositorio centralizado		
Estado actual:	**PROGRAMADO**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-04			
Código:	R-04	**Zona de riesgo:**	**MODERADO**
Nombre del riesgo:	Modificación de información por personal no autorizado (riesgo de corrupción TI)		
Causa principal:	Ausencia de controles de auditoría. Acceso sin segmentación por rol. Personal con privilegios excesivos.		
Probabilidad:	Muy Baja 20%	**Impacto:**	Moderado 60%

Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI
Plazo:	Abr 2026 (continuo)	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Implementar logs de auditoría de acceso y modificación en sistemas críticos.		
2.	Aplicar principio de mínimo privilegio en todos los perfiles de usuario.		
3.	Realizar revisión mensual de logs de acceso al servidor y sistemas.		
4.	Fortalecer seguridad perimetral del servidor institucional.		
Indicador de seguimiento:	0 eventos de modificación no autorizada registrados		
Estado actual:	**EN EJECUCIÓN**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-05			
Código:	R-05	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Falla o indisponibilidad del servidor institucional		
Causa principal:	Ausencia de redundancia. Fallas de hardware por antigüedad. Interrupciones eléctricas. Sin plan de continuidad formal.		
Probabilidad:	Baja 40%	**Impacto:**	Mayor 80%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI
Plazo:	May 2026 (continuo)	**Costo estimado:**	$1.200.000 (UPS)
ACCIONES DE TRATAMIENTO			
1.	Ejecutar backups diarios (archivos críticos), semanales (servidor completo) y mensuales (copia externa).		
2.	Verificar trimestralmente la integridad de los backups mediante prueba de restauración.		
3.	Adquirir UPS (sistema de alimentación ininterrumpida) para el servidor.		

4.	Documentar procedimiento de recuperación ante desastres (DRP básico).		
5.	Evaluar migración parcial a servicios en la nube para información crítica.		
Indicador de seguimiento:	% backups realizados vs programados ≥ 95%		
Estado actual:	**EN EJECUCIÓN**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-06			
Código:	R-06	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Fuga o exposición de datos personales de ciudadanos y funcionarios		
Causa principal:	Ausencia de controles de privacidad. Envío de información sensible por correo sin cifrado. Incumplimiento Ley 1581/2012.		
Probabilidad:	Baja 40%	**Impacto:**	Mayor 80%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI / Jurídica
Plazo:	Jun 2026	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Publicar y socializar la Política de Tratamiento de Datos Personales de INDETUR.		
2.	Registrar las bases de datos ante la SIC en el RNBD (Registro Nacional de Bases de Datos).		
3.	Establecer procedimiento para el manejo de datos personales recibidos por trámites.		
4.	Capacitar a todos los funcionarios en obligaciones de la Ley 1581 de 2012.		
5.	Restringir el envío de información sensible por correo electrónico sin autorización.		
Indicador de seguimiento:	0 reportes de fuga de datos. Registro SIC activo.		
Estado actual:	**PROGRAMADO**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-07			
Código:	R-07	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Ingeniería social y phishing dirigido a funcionarios		
Causa principal:	Desconocimiento de amenazas digitales. Uso de correo institucional sin validación de remitentes. Falta de cultura en ciberseguridad.		
Probabilidad:	Alta 80%	**Impacto:**	Moderado 60%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI
Plazo:	Ago 2026	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Ejecutar jornada de capacitación en identificación de correos phishing y amenazas de ingeniería social.		
2.	Publicar circular interna con pautas de seguridad en el uso del correo institucional.		
3.	Activar filtros antispam en el servidor de correo institucional.		
4.	Simular ejercicio de phishing interno para medir nivel de concienciación (opcional).		
Indicador de seguimiento:	% funcionarios capacitados en ciberseguridad = 100%		
Estado actual:	**PROGRAMADO**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-08			
Código:	R-08	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Incumplimiento de lineamientos de Gobierno Digital y transparencia (ITA)		
Causa principal:	Desactualización de la página web institucional. Falta de publicación oportuna de información obligatoria. Ausencia de seguimiento al ITA.		
Probabilidad:	Media 60%	**Impacto:**	Mayor 80%

Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI / Planeación
Plazo:	Continuo 2026	**Costo estimado:**	$0 (gestión interna)
ACCIONES DE TRATAMIENTO			
1.	Mantener actualizada la página web conforme a los ítems obligatorios del ITA.		
2.	Realizar autoevaluación trimestral del cumplimiento ITA y corregir brechas identificadas.		
3.	Publicar el Aviso de Privacidad, índice de información clasificada y activos de información.		
4.	Articular con Planeación el reporte de avance en Gobierno Digital dentro del FURAG.		
Indicador de seguimiento:	% cumplimiento ITA ≥ 90% por período evaluado		
Estado actual:	**EN EJECUCIÓN**	**Seguimiento Control Interno:**	

FICHA DE TRATAMIENTO: R-09			
Código:	R-09	**Zona de riesgo:**	**ALTO**
Nombre del riesgo:	Acceso físico no autorizado a equipos e infraestructura TI		
Causa principal:	Servidor ubicado en área sin control de acceso adecuado. Equipos sin bloqueo físico. Ausencia de política de escritorio limpio.		
Probabilidad:	Baja 40%	**Impacto:**	Mayor 80%
Opción de manejo:	REDUCIR	**Responsable:**	Jefe TI / Administrativa
Plazo:	Abr 2026	**Costo estimado:**	$500.000 (cerraduras/señalización)
ACCIONES DE TRATAMIENTO			
1.	Garantizar que el servidor institucional esté ubicado en espacio con acceso restringido y controlado.		
2.	Implementar política de escritorio limpio: equipos bloqueados al ausentarse del puesto.		
3.	Etiquetar e inventariar físicamente todos los equipos de cómputo.		

4.	Establecer registro de visitantes y accesos al cuarto de servidores.		
Indicador de seguimiento:	Servidor en área restringida. 0 accesos físicos no autorizados.		
Estado actual:	**PROGRAMADO**	**Seguimiento Control Interno:**	

8. Cronograma de Ejecución 2026

El siguiente cronograma muestra los meses de ejecución programados para las acciones de tratamiento de cada riesgo:

#	Riesgo	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
R-01	Acceso no autorizado por gestión débil d…	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R-02	Ciberataques (ransomware, DoS, DDoS) por…	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R-03	Pérdida de trazabilidad e integridad de …		✓	✓	✓	✓	✓						
R-04	Modificación de información por personal…	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R-05	Falla o indisponibilidad del servidor in…	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R-06	Fuga o exposición de datos personales de…		✓	✓	✓	✓	✓						
R-07	Ingeniería social y phishing dirigido a …				✓	✓	✓	✓	✓				

#	Riesgo	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
R-08	Incumplimiento de lineamientos de Gobier…	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R-09	Acceso físico no autorizado a equipos e …		✓	✓	✓								

9. Presupuesto Estimado

El plan se ejecuta con un presupuesto total estimado inferior a $5.000.000 COP. La mayoría de las acciones se implementan mediante gestión interna sin costo adicional:

#	Acción / Inversión	Descripción	Valor estimado COP	Fuente / Observación
R-01	**Implementación 2FA correo**	Activación de doble factor en cuentas institucionales (Google Workspace u otro proveedor)	$0	*Sin costo adicional en plan actual*
R-02	**Licencias antivirus**	Adquisición o renovación de licencias antivirus/antimalware para equipos de la entidad	$800.000	*Plan de adquisiciones 2026*
R-05	**UPS para servidor**	Adquisición de sistema de alimentación ininterrumpida para el servidor institucional	$1.200.000	*Plan de adquisiciones 2026*
R-09	**Seguridad física TI**	Elementos de control de acceso físico al cuarto de servidores (cerradura, señalización)	$500.000	*Gestión Administrativa*
TODOS	**Capacitación ciberseguridad**	Jornada de sensibilización en seguridad digital para funcionarios (puede ser virtual y gratuita MinTIC)	$0	*Recursos MinTIC / Colombia Digital*
TODOS	**Gestión interna (restantes)**	Demás acciones ejecutadas con recursos propios del Área TI sin inversión adicional	$0	*Gestión propia del área TI*
TOTAL ESTIMADO				**$2.500.000 COP**

Nota: Las acciones de gestión interna (sin costo) son ejecutadas directamente por el Área TI como parte de sus funciones ordinarias y del contrato de soporte vigente.

10. Formato de Seguimiento Trimestral

El Jefe del Área TI diligenciará el siguiente formato trimestralmente, reportando el avance de las acciones de tratamiento a la Dirección General y a la Oficina de Control Interno:

#	Riesgo	Acción de tratamiento	T1 Ene-Mar	T2 Abr-Jun	T3 Jul-Sep	T4 Oct-Dic
R-01	Acceso no autorizado por gestión débil…	Implementar y documentar política formal de contraseñas (mínimo 10 caracteres, complejidad, cambio cada 90 días).				
R-02	Ciberataques (ransomware, DoS, DDoS) por obsolescencia…	Aplicar parches y actualizaciones de seguridad disponibles del fabricante.				
R-03	Pérdida de trazabilidad e integridad de…	Socializar y capacitar a funcionarios en el uso de control de versiones en documentos.				
R-04	Modificación de información por personal no…	Implementar logs de auditoría de acceso y modificación en sistemas críticos.				
R-05	Falla o indisponibilidad del servidor institucional…	Ejecutar backups diarios (archivos críticos), semanales (servidor completo) y mensuales (copia externa).				

#	Riesgo	Acción de tratamiento	T1 Ene-Mar	T2 Abr-Jun	T3 Jul-Sep	T4 Oct-Dic
R-06	Fuga o exposición de datos personales…	Publicar y socializar la Política de Tratamiento de Datos Personales de INDETUR.				
R-07	Ingeniería social y phishing dirigido a…	Ejecutar jornada de capacitación en identificación de correos phishing y amenazas de ingeniería social.				
R-08	Incumplimiento de lineamientos de Gobierno Digital…	Mantener actualizada la página web conforme a los ítems obligatorios del ITA.				
R-09	Acceso físico no autorizado a equipos…	Garantizar que el servidor institucional esté ubicado en espacio con acceso restringido y controlado.				

Escala de avance: 0% = No iniciado | 25% = En proceso | 50% = Avance significativo | 75% = Casi completado | 100% = Finalizado

11. Roles y Responsabilidades

11.1 Director General

- Aprobar el presente Plan de Tratamiento de Riesgos de Seguridad Digital.
- Garantizar los recursos presupuestales para la ejecución de las acciones que lo requieran.
- Recibir los informes trimestrales de seguimiento.

11.2 Jefe Área TI y Comunicaciones

- Liderar la implementación y seguimiento de todas las acciones de tratamiento.
- Elaborar los informes trimestrales de avance.

- Coordinar con otras áreas las acciones de tratamiento transversales.
- Actualizar el plan ante nuevos riesgos o cambios en el contexto institucional.

11.3 Todos los Funcionarios

- Cumplir las políticas de seguridad de la información.
- Reportar incidentes o situaciones de riesgo al Jefe TI.
- Participar en las jornadas de capacitación programadas.

11.4 Oficina de Control Interno

- Verificar la ejecución del plan en los seguimientos al Plan de Acción Institucional.
- Emitir recomendaciones de mejora al proceso de gestión de riesgos TI.

12. Revisión y Actualización

El Plan de Tratamiento será revisado en los siguientes casos:

- Trimestralmente, como parte del seguimiento al Plan de Acción Institucional.
- Cuando se materialice un incidente de seguridad digital.
- Cuando se identifiquen nuevas amenazas o vulnerabilidades no contempladas.
- Cuando se emitan nuevos lineamientos de MinTIC, DAFP o normativa aplicable.
- Al inicio de cada vigencia anual, para actualizar el plan al nuevo período.

APROBACIÓN Y FIRMAS

Jose Egurrola Pedraza	**Jose Domingo Davila**
Jefe Área TI y Comunicaciones	**Director General – INDETUR**
Elaboró y presentó	Aprobó