PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL INFOTEP

2026

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

TABLA DE CONTENIDO

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

1. INTRODUCCIÓN Y CONTEXTO ESTRATÉGICO

La gestión de riesgos de seguridad de la información en el **INFOTEP** no es un ejercicio técnico aislado, sino un componente transversal de la gobernanza institucional. En el contexto de la educación superior en el Archipiélago de San Andrés, Providencia y Santa Catalina, la información actúa como el activo estratégico que habilita la docencia, la investigación y la proyección social.

Este documento formaliza la respuesta institucional ante la incertidumbre, estableciendo las acciones concretas para modificar los riesgos identificados en el ecosistema digital de la entidad. Se fundamenta en el análisis del contexto interno (procesos académicos y administrativos) y externo (amenazas cibernéticas y condiciones de insularidad), asegurando que los controles implementados sean proporcionales al valor de los activos protegidos y al nivel de amenaza real.

1.1. Propósito del Plan en el Marco del MIPG y Gobierno Digital

El presente Plan de Tratamiento de Riesgos se articula como un instrumento de ejecución de la **Dimensión 7 (Control Interno)** y la **Política de Gobierno Digital** del Modelo Integrado de Planeación y Gestión (MIPG). Su propósito es dar cumplimiento a los requisitos del **Modelo de Seguridad y Privacidad de la Información (MSPI)** adoptado mediante el Decreto 1078 de 2015 y las resoluciones 02277 de junio de 2025 y la resolución 500 de 2021 del MinTIC.

Específicamente, este plan busca:

- **Fortalecer la confianza digital:** Garantizar a estudiantes, docentes y ciudadanos que sus datos están protegidos bajo estándares de seguridad reconocidos.
- **Asegurar la continuidad del servicio:** Minimizar la interrupción de los servicios educativos críticos frente a incidentes de seguridad, un requisito vital dada la dependencia tecnológica en la región insular.
- **Cumplimiento Normativo:** Evidenciar la "debida diligencia" en la gestión de riesgos exigida por los entes de control y la Ley de Protección de Datos Personales.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

1.2. Articulación con la Política General de Seguridad de la Información

Este plan es el brazo operativo de la **Política General de Seguridad de la Información** de INFOTEP. Mientras la política establece el "qué" (el compromiso de la Alta Dirección de proteger la confidencialidad, integridad y disponibilidad), este plan define el "cómo" (las acciones tácticas y técnicas para mitigar los riesgos que amenazan dichos principios).

La ejecución de este plan es responsabilidad directa de los dueños de los procesos y del Oficial de Seguridad Digital (CISO), y sus resultados alimentan la revisión por la dirección para la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

1.3. Apetito de Riesgo Institucional (Niveles de Aceptación Definidos)

El **Apetito de Riesgo** define el nivel de exposición que INFOTEP está dispuesto a aceptar en la búsqueda de sus objetivos misionales. De acuerdo con la **Metodología de Gestión de Riesgos (Versión 01)** aprobada por la institución, se establecen los siguientes criterios de aceptación y tratamiento:

- **Nivel de Aceptación:** INFOTEP define que **solo se aceptarán** (asumirán) aquellos riesgos cuya valoración residual se ubique en la **Zona de Riesgo Baja (B)**.
- **Niveles que Requieren Tratamiento Obligatorio:** Cualquier riesgo que, tras la evaluación inicial, se ubique en zonas Moderada, Alta o Extrema, deberá ser objeto de un Plan de Tratamiento (Reducir, Evitar, Compartir/Transferir) hasta llevarlo a niveles tolerables.

Matriz de Decisión Institucional:

Nivel de Riesgo (Zona)	Color	Criterio de Aceptación / Acción Requerida
BAJA (B)	Verde	**Zona de Aceptación.** Se asume el riesgo. No requiere controles adicionales inmediatos, solo monitoreo periódico.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

Nivel de Riesgo (Zona)	Color	Criterio de Aceptación / Acción Requerida
MODERADA (M)	Amarillo	**Zona de Tolerancia Condicionada.** Se debe evaluar si es rentable reducir el riesgo. Requiere monitoreo estricto y controles si es posible.
ALTA (A)	Naranja	**Zona Inaceptable.** Requiere tratamiento obligatorio para **Reducir, Evitar, Compartir o Transferir** el riesgo de manera prioritaria.
EXTREMA (E)	Rojo	**Zona Crítica.** Atención inmediata e imperativa. Se deben aplicar controles urgentes para **Reducir, Evitar o Transferir** el riesgo. La operación podría suspenderse si no se mitiga.

2. OBJETIVOS DEL PLAN

2.1. Objetivo General

Ejecutar las acciones de tratamiento necesarias para **reducir la exposición al riesgo** de seguridad de la información de **INFOTEP** a niveles aceptables, mediante la implementación efectiva de controles técnicos, físicos y administrativos basados en la norma **NTC-ISO/IEC 27001:2022**.

Este plan busca transformar el perfil de riesgo institucional, asegurando que las amenazas identificadas sobre la infraestructura tecnológica y los datos académicos no comprometan la capacidad de la entidad para cumplir su misión educativa y social en el Archipiélago, garantizando la sostenibilidad de la operación digital frente a escenarios de incertidumbre y ciberamenazas.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

2.2. Objetivos Específicos

Para alcanzar el propósito general, este plan se despliega en los siguientes objetivos tácticos:

- **Protección de Activos Críticos:** Blindar los activos de información clasificados como "Confidenciales" o "Críticos" (bases de datos de estudiantes, sistemas financieros y plataforma académica) contra accesos no autorizados, fugas de información y ataques de denegación de servicio, preservando los principios de confidencialidad, integridad y disponibilidad.
- **Cumplimiento Normativo y Legal:** Garantizar la conformidad con el marco legal colombiano vigente, específicamente la **Ley 1581 de 2012** (Protección de Datos Personales), la **Ley 1712 de 2014** (Transparencia) y los lineamientos de Seguridad y Privacidad de la Política de Gobierno Digital (Decreto 1078 de 2015), evitando sanciones legales y daños reputacionales.
- **Fortalecimiento de la Cultura de Seguridad:** Reducir la vulnerabilidad asociada al "factor humano" mediante la ejecución de estrategias de sensibilización que modifiquen comportamientos de riesgo en funcionarios, docentes y contratistas, consolidando una primera línea de defensa consciente y proactiva.
- **Resiliencia y Continuidad Operativa:** Implementar medidas de redundancia y recuperación (backups, planes de contingencia) que mitiguen el impacto de fallas tecnológicas o eventos naturales, asegurando la continuidad de los servicios educativos críticos ante las limitaciones de conectividad propias de la condición insular.

3. ALCANCE Y LÍMITES

El alcance de este Plan de Tratamiento de Riesgos se define para asegurar una cobertura integral de los activos que soportan la misión institucional. De acuerdo con la **Metodología de Gestión de Riesgos (Versión 01)**, el plan se aplica a **todos los activos de información identificados y valorados** en el inventario institucional, priorizando aquellos cuya materialización de riesgo impactaría significativamente la operación.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

3.1. Procesos Cubiertos

El plan cubre la totalidad de los procesos caracterizados en el mapa de procesos de la entidad, con especial énfasis en aquellos que gestionan datos sensibles o son esenciales para la continuidad del servicio educativo:

- **Procesos Misionales:** Gestión Académica, Formación Técnica, Investigación y Proyección Social.
- **Procesos Estratégicos:** Planeación Institucional y Gestión de Calidad.
- **Procesos de Apoyo:** Gestión Tecnológica (TI), Gestión del Talento Humano, Gestión Financiera, Gestión Documental y Atención al Usuario.
- **Procesos de Evaluación:** Control Interno y Control Disciplinario.

3.2. Activos de Información Críticos (Inventario Priorizado)

Para efectos del tratamiento de riesgos 2026, el alcance se centra en los activos de información que han sido clasificados con nivel **ALTO** o **MEDIO** en los criterios de Confidencialidad, Integridad y Disponibilidad, según la metodología de clasificación de activos de la entidad.

Se prioriza la protección de los siguientes grupos de activos:

1. **Información Digital:** Bases de datos de estudiantes (notas, datos personales), sistemas financieros y expedientes laborales.
2. **Software y Aplicaciones:** Portal Académico, Plataformas de Aprendizaje Virtual (LMS) y Sitio Web.
3. **Infraestructura Tecnológica (Hardware/Red):** Servidores (físicos y virtuales), equipos de borde (Firewall/Routers), infraestructura de red LAN/WLAN y Datacenter.
4. **Personas:** Funcionarios, docentes y contratistas que administran o tienen acceso privilegiado a la información.

3.3. Partes Interesadas (Sujetos del Alcance)

Las medidas de tratamiento de riesgo definidas en este documento son de obligatorio cumplimiento y aplicación para todas las partes interesadas que interactúan con los activos de información de **INFOTEP**:

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

- **Internas:** Alta Dirección, Servidores Públicos (administrativos), Docentes (planta y cátedra) y Comité Institucional.
- **Externas:** Estudiantes, Egresados, Proveedores de servicios tecnológicos (Terceros), Entes de Control y Ministerio de Educación Nacional.

4. MARCO NORMATIVO Y METODOLÓGICO

El diseño y ejecución de este plan se fundamenta en el cumplimiento del bloque de constitucionalidad y la normatividad vigente en materia de seguridad digital para entidades públicas.

4.1. Marco Legal

- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector TIC y se establecen los lineamientos de la estrategia de Gobierno en Línea (hoy Gobierno Digital).
- **Ley 1581 de 2012:** Disposiciones generales para la protección de datos personales y Decreto reglamentario 2693 de 2012.
- **Política Pública (CONPES):** CONPES 3701 de 2011 (Ciberseguridad), CONPES 3854 de 2016 (Seguridad Digital) y CONPES 3995 de 2020 (Confianza y Seguridad Digital).

4.2. Estándares Técnicos

- **NTC-ISO/IEC 27001:** Requisitos para el Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27002:** Código de prácticas para los controles de seguridad de la información.
- **Guía de Gestión de Riesgos del MinTIC:** Lineamientos técnicos base para el análisis de riesgos digitales.
- **Documento de Políticas de Seguridad de la Información:** Versión 1.0 de INFOTEP.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

4.3. Metodología de Valoración de Riesgos

Para la valoración de los riesgos inherentes, INFOTEP utiliza una matriz de calificación cualitativa de **5x5** que cruza la **Probabilidad** (Frecuencia/Factibilidad) con el **Impacto** (Consecuencias).

- **Escala de Probabilidad:** 1. Raro, 2. Improbable, 3. Posible, 4. Probable, 5. Casi Seguro.
- **Escala de Impacto:** 1. Insignificante, 2. Menor, 3. Moderado, 4. Mayor, 5. Catastrófico.

El cruce de estas variables determina la **Zona de Riesgo** inicial (Baja, Moderada, Alta, Extrema), la cual dicta la urgencia y obligatoriedad del tratamiento.

5. CRITERIOS PARA EL TRATAMIENTO DEL RIESGO

Una vez evaluados los riesgos, **INFOTEP** aplicará las siguientes reglas y criterios técnicos para seleccionar e implementar los controles, conforme a lo establecido en el numeral 13 de la metodología interna.

5.1. Opciones de Manejo del Riesgo

Para cada riesgo identificado, se seleccionará una de las siguientes opciones de manejo:

1. **Asumir el riesgo (Aceptar):** Aceptar la pérdida residual probable. Esta opción solo es válida si el riesgo se encuentra en Zona Baja.
2. **Reducir el riesgo (Mitigar):** Implementar acciones (controles) para disminuir la probabilidad de ocurrencia o el impacto.
3. **Evitar el riesgo:** Tomar acciones para eliminar la causa del riesgo, lo que puede implicar no iniciar o suspender la actividad que lo genera.
4. **Compartir o Transferir el riesgo:** Traspasar las pérdidas a terceros mediante seguros, outsourcing o contratos.

5.2. Criterios de Selección de Controles

La selección de nuevos controles se realizará basándose en la estructura de controles del **Modelo de Seguridad y Privacidad de la Información (MSPI)** y el **Anexo A de la norma ISO/IEC 27001**, clasificándolos en **Preventivos** (actúan

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

sobre la causa/probabilidad) o **Correctivos** (actúan sobre la consecuencia/impacto).

5.3. Metodología de Valoración de Controles (Efectividad)

Para determinar cuánto reduce un control el riesgo inherente, se aplicará la siguiente tabla de valoración, la cual asigna un puntaje máximo de **100 puntos** a cada control según su diseño y ejecución:

PARÁMETROS	CRITERIOS DE EVALUACIÓN	PUNTAJE MÁX.
Herramientas	¿Posee herramienta para ejercer el control? (Manual o Automática)	15
Documentación	¿Existen manuales, instructivos o procedimientos documentados?	15
Efectividad	¿Ha demostrado ser efectiva en el tiempo?	30
Responsables	¿Están definidos los responsables de la ejecución?	15
Seguimiento	¿La frecuencia de ejecución y seguimiento es adecuada?	25
TOTAL		**100 Puntos**

5.4. Cálculo del Riesgo Residual Esperado

El puntaje obtenido en la valoración de los controles determinará el desplazamiento (reducción) en la matriz de calor, definiendo así el **Riesgo Residual Esperado**:

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Puntaje entre 0 - 50:** El control es débil. Disminuye **0** cuadrantes.
- **Puntaje entre 51 - 75:** El control es satisfactorio. Disminuye **1** cuadrante en Probabilidad o Impacto.
- **Puntaje entre 76 - 100:** El control es fuerte. Disminuye **2** cuadrantes en Probabilidad o Impacto.

Nota: Este cálculo permite justificar técnicamente la inversión: "Si implementamos el WAF (Herramienta) y definimos el procedimiento (Documentación), obtendremos un puntaje >76, lo que reducirá el riesgo de Extremo a Moderado".

6. MATRIZ DE TRATAMIENTO DE RIESGOS (EL PLAN)

Esta sección detalla las acciones específicas para mitigar los riesgos ubicados en zonas **Alta (A)** y **Extrema (E)**. La selección de controles se basa en el **Anexo A de la NTC-ISO/IEC 27001:2022** y los proyectos de inversión definidos en el presupuesto 2025.

6.1. Riesgo 1: Ciberataques Externos y Ransomware

6.1.1. Descripción y Nivel de Riesgo Inherente

Descripción: Compromiso de la infraestructura tecnológica mediante la explotación de vulnerabilidades en servicios expuestos a internet (Portal Académico, Web) o infección por código malicioso (Ransomware) que cifra la información institucional.

- **Zona de Riesgo Inherente: EXTREMA (E)**.
- **Causa Raíz:** Falta de controles de seguridad perimetral a nivel de aplicación (Capa 7) y obsolescencia en gestión de parches.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

6.1.2. Plan de Acción y Controles Seleccionados

Opción de Manejo	Control ISO 27001 (Anexo A)	Acción / Proyecto 2026	Tipo	Entregable
REDUCIR	**A.8.26** Requisitos de seguridad de las aplicaciones	**Implementación de WAF:** Adquisición y configuración de Web Application Firewall para el Portal Académico.	Tecnológico	Reglas de filtrado activas.
REDUCIR	**A.8.8** Gestión de vulnerabilidades técnicas	**Gestión de Vulnerabilidades:** Escaneo trimestral automatizado y plan de remediación (parcheo).	Preventivo	Informes de escaneo y remediación.
REDUCIR	**A.8.20** Seguridad de las redes	**Renovación Firewall Perimetral:** Implementación de firewall de nueva generación con inspección profunda de paquetes (IPS).	Tecnológico	Equipo instalado y configurado.

6.1.3. Valoración del Control y Riesgo Residual Esperado

Aplicando la metodología de INFOTEP para el conjunto de controles:

- **Herramientas (15 pts):** Sí (WAF + NGFW).
- **Documentación (15 pts):** Sí (Se crearán procedimientos de configuración).
- **Efectividad (30 pts):** Alta (Bloqueo automático de ataques).
- **Responsables (15 pts):** Sí (Líder TI / Proveedor).

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Seguimiento (25 pts):** Sí (Monitoreo de logs 24/7).
- **PUNTAJE TOTAL PROYECTADO: 100 Puntos**.
- **Impacto en la Matriz:** Disminuye **2 Cuadrantes** en Probabilidad.

RESULTADO: El riesgo pasa de **Extremo (E)** a **MODERADO (M)**.

6.2. Riesgo 2: Fuga de Información y Datos Personales

6.2.1. Descripción y Nivel de Riesgo Inherente

Descripción: Divulgación no autorizada de datos sensibles de estudiantes (menores de edad), docentes o administrativos, ya sea por error humano, ingeniería social (Phishing) o exfiltración intencional.

- **Zona de Riesgo Inherente: ALTA (A)**.
- **Impacto Legal:** Sanciones de la SIC por incumplimiento de Ley 1581 de 2012.

6.2.2. Plan de Acción y Controles Seleccionados

Opción de Manejo	Control ISO 27001 (Anexo A)	Acción / Proyecto 2026	Tipo	Entregable
REDUCIR	**A.5.12** Clasificación de la información	**Inventario y Clasificación:** Actualización del inventario de activos con etiquetado de confidencialidad (Público, Reservado, Clasificado).	Admin.	Inventario de Activos v.2026.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

Opción de Manejo	Control ISO 27001 (Anexo A)	Acción / Proyecto 2026	Tipo	Entregable
REDUCIR	**A.6.3** Concienciación y formación	**Plan Cultura Segura:** Talleres de ingeniería social y simulación de Phishing para funcionarios.	Humano	Reporte de asistencia y evaluación.
REDUCIR	**A.8.12** Prevención de fuga de datos	**Protección Endpoint (EDR):** Despliegue de antivirus avanzado con control de dispositivos USB en equipos administrativos.	Tecnológico	Consola de gestión EDR.

6.2.3. Valoración del Control y Riesgo Residual Esperado

- **Puntaje Proyectado: 85 Puntos** (Fuerte componente de herramienta y capacitación).
- **Impacto en la Matriz:** Disminuye **2 Cuadrantes** en Probabilidad.

RESULTADO: El riesgo pasa de **Alto (A)** a **BAJO (B)**.

6.3. Riesgo 3: Indisponibilidad por Obsolescencia y Fallas (Continuidad)

6.3.1. Descripción y Nivel de Riesgo Inherente

Descripción: Interrupción prolongada de los servicios tecnológicos debido a obsolescencia de protocolos (IPv4), fallas de hardware o desastres naturales (Huracanes) propios de la insularidad.

- **Zona de Riesgo Inherente: ALTA (A)**.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

6.3.2. Plan de Acción y Controles Seleccionados

Opción de Manejo	Control ISO 27001 (Anexo A)	Acción / Proyecto 2026	Tipo	Entregable
EVITAR / REDUCIR	**A.8.21** Seguridad de los servicios de red	**Transición IPv4 a IPv6:** Ejecución del plan de implementación del protocolo IPv6 para cumplimiento normativo y sostenibilidad de la red.	Tecnológico	Red operando en Dual Stack.
COMPARTIR	**A.8.13** Copias de seguridad	**Backup en Nube (Inmutable):** Contratación de almacenamiento externo (fuera de la isla) para copias de seguridad críticas.	Tecnológico	Reportes de restauración exitosa.
REDUCIR	**A.5.29** Seguridad de la información en la interrupción	**Actualización BCP/DRP:** Pruebas de escritorio del Plan de Recuperación ante Desastres.	Admin.	Informe de simulacro.

6.3.3. Valoración del Control y Riesgo Residual Esperado

- **Puntaje Proyectado: 90 Puntos** (La tercerización del backup y la modernización a IPv6 son controles de alta efectividad).
- **Impacto en la Matriz:** Disminuye **2 Cuadrantes** en Impacto (al tener respaldo externo, el impacto de una falla local baja drásticamente).

RESULTADO: El riesgo pasa de **Alto (A)** a **MODERADO (M)**.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

6.4. Riesgo 4: Fraude Interno y Corrupción Digital

6.4.1. Descripción y Nivel de Riesgo Inherente

Descripción: Alteración no autorizada de notas, registros financieros o certificaciones por parte de usuarios internos con privilegios excesivos o falta de trazabilidad.

- **Zona de Riesgo Inherente: MODERADA (M)** (Se trata para prevenir escalamiento).

6.4.2. Plan de Acción y Controles Seleccionados

Opción de Manejo	Control ISO 27001 (Anexo A)	Acción / Proyecto 2025	Tipo	Entregable
REDUCIR	**A.5.3** Segregación de cometidos	**Revisión de Perfiles:** Auditoría de permisos en los sistemas y Portal Académico para garantizar segregación de funciones.	Admin.	Matriz de accesos validada.
REDUCIR	**A.8.15** Registros de eventos	**Auditoría de Logs:** Activación y revisión mensual de logs de auditoría en bases de datos críticas.	Detectivo	Informes de revisión de logs.

6.4.3. Valoración del Control y Riesgo Residual Esperado

- **Puntaje Proyectado: 70 Puntos** (Depende fuertemente de procedimientos manuales de revisión).
- **Impacto en la Matriz:** Disminuye **1 Cuadrante** en Probabilidad.

RESULTADO: El riesgo pasa de **Moderada (M)** a **BAJO (B)**.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

6.5. Resumen de Recursos Requeridos (Presupuesto)

Para ejecutar esta matriz, se requiere la aprobación de los siguientes recursos estimados en el PESI:

1. **Talento Humano:** Contratación del Oficial de Seguridad (CISO) para liderar la ejecución.
2. **Hardware/Software:** Firewall NGFW, WAF, Licencias EDR, Nube para Backups.
3. **Servicios:** Consultoría para Ethical Hacking y Transición IPv6.

7. INTEGRACIÓN CON EL SISTEMA DE GESTIÓN (MIPG)

La gestión de riesgos de seguridad de la información en **INFOTEP** se integra transversalmente con el **Modelo Integrado de Planeación y Gestión (MIPG)**, específicamente dentro de la **Dimensión 7: Control Interno**. De acuerdo con la metodología institucional, los riesgos de seguridad digital no se gestionan de forma aislada, sino que alimentan y se correlacionan con los demás mapas de riesgos de la entidad (Estratégicos, Operativos y de Corrupción) para asegurar una visión holística de la exposición institucional.

7.1. Relación con el Mapa de Riesgos de Corrupción

La seguridad de la información actúa como un control habilitador para la prevención de la corrupción. En este Plan de Tratamiento, se ha identificado una correlación directa entre las vulnerabilidades digitales y la posibilidad de materialización de hechos de corrupción, estableciendo los siguientes puntos de integración:

- **Integridad de la Información:** Los controles implementados en este plan para asegurar la integridad de bases de datos académicas y financieras (ej. auditoría de logs, segregación de funciones) mitigan directamente el **Riesgo de Corrupción** asociado a la manipulación indebida de notas, certificados o registros presupuestales.
- **Trazabilidad Digital:** La implementación de herramientas de monitoreo y gestión de eventos (SIEM/Logs) proporciona la evidencia digital necesaria para las investigaciones disciplinarias y fiscales, fortaleciendo la línea de defensa contra el fraude interno.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Reporte Unificado:** Los incidentes de seguridad que involucren alteración de información crítica serán reportados tanto al Comité de gestión de desempeño, activando los protocolos de gestión del riesgo de corrupción cuando aplique.

7.2. Relación con el Plan de Continuidad del Negocio (BCP/DRP)

El Plan de Tratamiento de Riesgos es el insumo preventivo fundamental para la **Gestión de la Continuidad del Negocio**. Existe una relación de interdependencia técnica y operativa:

- **Prevención vs. Recuperación:** Mientras este plan se enfoca en **reducir la probabilidad** de que ocurra un incidente (ej. implementando un Firewall o WAF), el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) se activan cuando los controles preventivos fallan y el riesgo se materializa (ej. impacto de un huracán o ataque de Ransomware exitoso).
- **Alimentación del BIA (Analisis de impacto de negocio):** La valoración de activos y riesgos de disponibilidad realizada en este plan actualiza el Análisis de Impacto al Negocio, permitiendo a INFOTEP priorizar qué servicios (ej. Plataforma Académica) deben recuperarse primero en caso de un desastre.
- **Controles Compartidos:** Las acciones de tratamiento clasificadas como "Correctivas" o de "Transferencia" en este plan (como la contratación de backups en la nube y enlaces redundantes) son, de facto, las estrategias de recuperación que dan viabilidad al DRP.

8. ESQUEMA DE MONITOREO Y REVISIÓN (LÍNEAS DE DEFENSA)

Para garantizar la efectividad, idoneidad y actualización de los controles de seguridad implementados, **INFOTEP** adopta el esquema de las **Tres Líneas de Defensa** establecido en la Dimensión 7 del MIPG. Este modelo asegura una segregación de funciones adecuada entre quienes gestionan el riesgo día a día, quienes supervisan y quienes auditan de manera independiente.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

8.1. Rol de la 1ra Línea de Defensa: Ejecución y Autocontrol

La primera línea está conformada por los **Líderes de Proceso** (Académico, Administrativo, TI) y los **Propietarios de los Activos de Información**. Son los responsables directos de la gestión operativa del riesgo.

- **Responsabilidades en el Plan:**
  - **Ejecución:** Implementar los controles técnicos y administrativos definidos en la Matriz de Tratamiento (Sección 6) dentro de los plazos establecidos.
  - **Autocontrol:** Verificar diariamente que los controles (ej. Backups, Antivirus, WAF) estén operando correctamente.
  - **Reporte:** Notificar inmediatamente al Oficial de Seguridad Digital (CISO) sobre cualquier incidente, falla en los controles o cambio en el entorno que pueda modificar el nivel de riesgo identificado.

8.2. Rol de la 2da Línea de Defensa: Monitoreo y Gestión de Riesgos

La segunda línea es liderada por el **Oficial de Seguridad Digital (CISO)** en articulación con la **Oficina de Planeación**. Su función es supervisar y apoyar la gestión del riesgo, asegurando que la metodología se aplique correctamente.

- **Responsabilidades en el Plan:**
  - **Metodología:** Mantener actualizada la Política y la Metodología de Gestión de Riesgos de Seguridad.
  - **Asesoría:** Acompañar a los líderes de proceso (1ra línea) en la identificación de nuevos riesgos y la definición de planes de acción.
  - **Consolidación:** Centralizar el Mapa de Riesgos de Seguridad Digital y monitorear los Indicadores de Riesgo (KRI) para detectar desviaciones.
  - **Evaluación de Controles:** Realizar pruebas periódicas (ej. simulacros, revisión de logs) para validar la eficacia de los controles reportados por la primera línea.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

8.3. Rol de la 3ra Línea de Defensa: Aseguramiento Independiente (Auditoría)

La tercera línea corresponde a la **Oficina de Control Interno**. Su rol es proporcionar aseguramiento objetivo e independiente a la Alta Dirección sobre la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI).

- **Responsabilidades en el Plan:**
  - **Auditoría Interna:** Incluir la "Gestión de Seguridad de la Información" como una unidad auditable dentro del Plan Anual de Auditoría.
  - **Verificación:** Evaluar si los controles descritos en este plan realmente se implementaron y si redujeron el riesgo según lo proyectado.
  - **Hallazgos:** Generar reportes de hallazgos y no conformidades cuando se evidencie que los controles no son efectivos o no se están ejecutando, exigiendo planes de mejoramiento.

8.4. Cronograma de Reportes a la Alta Dirección

El flujo de información sobre el estado de los riesgos hacia la Alta Dirección (Rectoría y Comité de Gestion de Desempeño) se realizará con la siguiente periodicidad, conforme a los lineamientos de la Guía MinTIC:

TIPO DE REPORTE	CONTENIDO	RESPONSABLE (Línea)	PERIODICIDAD
Informe de Avance de Controles	Estado de ejecución de los proyectos del plan de tratamiento (Avance físico/presupuestal).	CISO (2da Línea)	**Trimestral**
Reporte de Incidentes y Riesgos Materializados	Resumen de incidentes ocurridos, impacto real y efectividad de la respuesta.	CISO (2da Línea)	**Semestral** (o Inmediato si es Crítico)
Evaluación Independiente del SGSI	Informe de auditoría interna sobre el cumplimiento del MSPI y efectividad de controles.	Control Interno (3ra Línea)	**Anual**

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

TIPO DE REPORTE	CONTENIDO	RESPONSABLE (Línea)	PERIODICIDAD
Revisión por la Dirección	Toma de decisiones sobre recursos y aceptación de riesgos residuales.	Alta Dirección	**Anual**

9. INDICADORES DE GESTIÓN Y EFECTIVIDAD

La medición del desempeño del Plan de Tratamiento de Riesgos se realizará a través de dos dimensiones: **Gestión** (¿Estamos haciendo lo que planeamos?) y **Efectividad** (¿Lo que hicimos sirvió para reducir el riesgo?).

Los siguientes indicadores alimentarán el informe de revisión por la dirección y el reporte FURAG.

9.1. Indicadores de Impacto (Efectividad de Controles)

Estos indicadores miden el resultado final de la estrategia: la reducción de la exposición al riesgo y la capacidad de contener incidentes.

ID	NOMBRE DEL INDICADOR	DESCRIPCIÓN / OBJETIVO	FÓRMULA DE CÁLCULO	META 2026	PERIODICIDAD	RESPONSABLE
IND-01	**Efectividad en la Reducción del Riesgo**	Mide el porcentaje de riesgos críticos que lograron disminuir su valoración (Probabilidad o Impacto) tras la implement	No. Riesgos que bajaron de Zona / Total Riesgos Tratados x100	**> 80%**	Semestral	CISO / Planeación

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

ID	NOMBRE DEL INDICADOR	DESCRIPCIÓN / OBJETIVO	FÓRMULA DE CÁLCULO	META 2026	PERIODICIDAD	RESPONSABLE
		ación de controles.				
IND-02	**Materialización de Riesgos Priorizados**	Mide la frecuencia con la que se materializaron los riesgos que estaban siendo tratados (ej. Ciberataques exitosos vs. Intentos bloqueados).	No. de Incidentes de Seguridad Materializados asociados a Riesgos del Plan	**0 Críticos**	Trimestral	Líder TI
IND-03	**Efectividad de Controles Perimetrales (WAF/Firewall)**	Mide la eficacia de los nuevos controles tecnológicos implementados para bloquear amenazas externas.	No. Ataques Bloqueados por WAF/IPS /Total Intentos de Ataque Detectado X 100	**> 95%**	Mensual	Líder TI

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

9.2. Indicadores de Cumplimiento (Gestión del Plan)

Estos indicadores miden el avance físico y administrativo en la ejecución de las actividades propuestas en la Matriz de Tratamiento.

ID	NOMBRE DEL INDICADOR	DESCRIPCIÓN / OBJETIVO	FÓRMULA DE CÁLCULO	META 2026	PERIODICIDAD	RESPONSABLE
IND-04	**Ejecución del Plan de Tratamiento**	Mide el avance en la implementación de los controles (tecnológicos, físicos y administrativos) definidos en el cronograma.	No. Controles Implementados/ No. Controles Programados en el Periodo X100	**> 90 %**	Trimestral	CISO
IND-05	**Cobertura del Plan de Cultura**	Mide el porcentaje de funcionarios y docentes que han completado las capacitaciones de sensibilización (Control Humano).	No. Personas Capacitadas / Total Población Objetivo X 100	**> 85 %**	Semestral	Talento Humano

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

ID	NOMBRE DEL INDICADOR	DESCRIPCIÓN / OBJETIVO	FÓRMULA DE CÁLCULO	META 2026	PERIODICIDAD	RESPONSABLE
IND-06	**Remediación de Vulnerabilidades**	Mide la agilidad del equipo TI para cerrar las brechas técnicas detectadas en los escaneos.	No. Vulnerabilidades Críticas Corregidas / Total Vulnerabilidades Críticas Detectadas X 100	**100 %**	Trimestral	Líder TI

10. DECLARACIÓN DE RIESGO RESIDUAL

Una vez diseñado el plan de tratamiento y proyectada la efectividad de los controles seleccionados (WAF, IPv6, Cultura, Backups), se establece el perfil de **Riesgo Residual** de la entidad. Esta declaración confirma que las acciones propuestas son suficientes para llevar la exposición institucional a niveles tolerables.

10.1. Mapa de Calor Comparativo (Inherente vs. Residual Proyectado)

La implementación rigurosa de este plan generará el siguiente desplazamiento en el mapa de riesgos de **INFOTEP**, transformando un escenario crítico en uno gestionable:

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

RIESGO PRIORIZADO	ZONA DE RIESGO INHERENTE (Inicial)	CONTROLES CLAVE APLICADOS	ZONA DE RIESGO RESIDUAL (Proyectada)
R1. Ciberataques / Ransomware	**EXTREMA (E)** *(Probabilidad: Casi Seguro / Impacto: Catastrófico)*	• WAF + IPS • Gestión de Vulnerabilidades	**MODERADA (M)** *(Se reduce Probabilidad a 'Posible')*
R2. Fuga de Información	**ALTA (A)** *(Probabilidad: Probable)*	• DLP / Antivirus EDR • Cultura de Seguridad	**BAJA (B)** *(Se reduce Probabilidad a 'Improbable')*
R3. Indisponibilidad / Fallas	**ALTA (A)** *(Impacto: Mayor)*	• Transición IPv6 • Backup Inmutable en Nube	**MODERADA (M)** *(Se reduce Impacto a 'Menor' por Resiliencia)*
R4. Fraude Interno	**MODERADA (M)**	• Auditoría de Logs • Segregación de Funciones	**BAJA (B)** *(Se reduce Probabilidad por Disuasión)*

10.2. Justificación de Aceptación de Riesgos Residuales

De conformidad con la **Metodología de Gestión de Riesgos (Versión 01)** de INFOTEP, la Alta Dirección procede a la aceptación de los riesgos residuales bajo las siguientes premisas:

1. **Riesgos en Zona Baja (B):** Se aceptan plenamente. No requieren inversión adicional, solo el mantenimiento de los controles actuales.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

2. **Riesgos en Zona Moderada (M):** Se acepta convivir con este nivel de riesgo (R1 y R3) considerando que:
    - La inversión para reducirlos a "Baja" (ej. Data Center Tier IV redundante) superaría el beneficio obtenido (Costo-Beneficio).
    - Los controles de contingencia (Backups, Seguros) son suficientes para recuperar el servicio sin afectar la viabilidad institucional.
    - Se establece un compromiso de monitoreo trimestral obligatorio para evitar que vuelvan a zonas Altas.

Cualquier desviación que incremente el riesgo residual por encima de estos niveles deberá ser reportada inmediatamente al Comité Institucional de Coordinación de Control Interno para la asignación de recursos de emergencia.

11. CONTROL DE CAMBIOS Y APROBACIÓN

Este documento constituye la versión oficial del plan para la vigencia 2026 y ha seguido el debido proceso de revisión técnica y validación estratégica.

11.1. Firmas de Aprobación

La firma del presente documento formaliza la asignación del presupuesto requerido y la aceptación de los riesgos residuales descritos.

REGISTRO DE APROBACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre: Jonathan Marín Medicis	**Nombre:** Comité de Gestión y Desempeño	**Nombre:** (Rector/a) Chales Gallardo Humphries
Cargo: Contratista - Oficial de Seguridad Digital	**Cargo:** presidente del Comité	**Cargo:** Rector - Alta Dirección
Fecha: 05-11-2025	**Fecha:** 05-11-2025	**Fecha:** 05-11-2025

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

11.2. Historial de Versiones

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA VIGENCIA**	**NATURALEZA DEL CAMBIO**
01	5/11/2025	Creación del Plan de tratamiento de riesgos

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación