MANUAL DE POLÍTICAS 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
Vigilada MiniEducación

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

1. OBJETIVO DEL MANUAL

El presente Manual tiene como propósito fundamental articular la estrategia de seguridad digital de INFOTEP con su operación misional, mediante los siguientes objetivos específicos:

- Establecer el marco normativo técnico y estratégico: Definir las directrices de control y gobierno de seguridad digital que son de obligatorio cumplimiento para funcionarios, docentes, investigadores, estudiantes, contratistas y terceros de INFOTEP. Estas directrices buscan preservar las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información institucionales, asegurando la trazabilidad y la defensa en profundidad de la infraestructura tecnológica.
- Fomentar la apropiación de la cultura de ciberseguridad: Institucionalizar una cultura de ciber higiene y responsabilidad digital en toda la comunidad educativa, garantizando que las políticas aquí descritas no sean solo documentos estáticos, sino prácticas entendidas y aplicadas diariamente para la protección del conocimiento y los datos personales.
- Gestión de riesgos alineada a la Misión Institucional: Minimizar la superficie de ataque y mitigar el impacto de los riesgos de seguridad digital que podrían afectar la continuidad de los servicios críticos de formación técnica, proyección social e investigación. Esto asegura que los controles implementados habiliten, y no entorpezcan, la visión de INFOTEP de ser pionera en temas de insularidad y desarrollo regional.
- Garantizar el cumplimiento y la mejora continua: Asegurar la actualización dinámica de los lineamientos de seguridad digital frente a nuevas amenazas y cambios en el entorno tecnológico, dando estricto cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, la Ley de Protección de Datos Personales y demás normatividad vigente aplicable al sector educación.

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

2. ALCANCE DEL MANUAL

Las políticas, directrices y controles definidos en el presente Manual tienen un alcance integral y son de obligatoria observancia y cumplimiento para todos los actores que interactúan con el ecosistema de información de **INFOTEP**.

2.1. Sujetos de Aplicación:

El alcance cubre a todos los colaboradores públicos (funcionarios administrativos y directivos), personal docente, investigadores, población estudiantil, aprendices, practicantes, contratistas y terceros (proveedores, aliados estratégicos del sector productivo y entidades estatales) que tengan acceso, administren, procesen o custodien activos de información de la institución.

2.2. Cobertura sobre Activos y Procesos:

Este manual aplica transversalmente a:

Procesos Institucionales: Cubre la totalidad de los procesos Estratégicos, Misionales (Formación Técnica Profesional, Investigación y Proyección Social), de Apoyo y de Evaluación de INFOTEP.

Activos de Información: Abarca la información en cualquier formato (físico, digital, lógico, verbal) y en cualquier estado (en reposo, en tránsito o en procesamiento), incluyendo bases de datos académicas, propiedad intelectual derivada de investigaciones, sistemas financieros, infraestructura tecnológica (hardware, redes, software) e instalaciones físicas.

2.3. Ciclo de Vida de la Información:

El alcance se extiende a todo el ciclo de vida de la información institucional: desde su generación, recolección o creación, pasando por su clasificación,

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

almacenamiento, procesamiento y transmisión, hasta su disposición final, archivo o destrucción segura.

2.4. Extensión Territorial y Tecnológica:

Las políticas aplican dentro de las instalaciones físicas de INFOTEP en el departamento insular, así como en entornos de teletrabajo, trabajo remoto, movilidad, y en las infraestructuras tecnológicas tercerizadas o servicios en la nube (SaaS, PaaS, IaaS) que soporten la operación institucional.

3. DEFINICIONES

• **MSPI**: Modelo de Seguridad y Privacidad de la Información.
• **SGSI**: Sistema de Gestión de Seguridad de la Información.
• **Activo de Información**: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas) que tenga valor para la Entidad.
• **Confidencialidad**: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
• **Integridad**: Propiedad de la información que busca preservar su exactitud y completitud.
• **Disponibilidad**: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
• **Sistema de Gestión de Seguridad de la Información**: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
• **Controles**: Medida que permite reducir o mitigar un riesgo.
• **Amenaza**: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.

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

• **Autenticación**: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

• **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

• **Ciberseguridad**: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

• **Cifrado**: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

• **Criptografía**: Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.

• **Acceso Lógico**: restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como identificación, autenticación y autorización.

4. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL

INFOTEP, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios, proveedores y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta como esta descrito en las funciones y objetivos del contexto interno y externo de la entidad: Para cada política definida se debe establecer el responsable correspondiente, por ejemplo, para la política de RH podría mencionarse La dirección de Talento humano o la dependencia que tenga a cargo sus funciones será la responsable del cumplimiento y seguimiento de la política.

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

4.1 Política de Gobernanza y Organización Interna

INFOTEP establece un marco de gobierno de seguridad digital que garantiza la dirección estratégica, la asignación clara de responsabilidades y la integración de la seguridad en la cultura organizacional, asegurando que las decisiones de seguridad apoyen los objetivos misionales de educación e investigación.

4.1.1. Objetivo

Establecer un marco de gobierno y gestión de la seguridad digital en INFOTEP que defina una estructura organizacional clara, con roles y responsabilidades asignados, garantizando la segregación de funciones, el compromiso de la Alta Dirección y la articulación de la seguridad de la información con los objetivos misionales de docencia, investigación y proyección social.

4.1.2. Lineamientos de la Política

A. Estructura de Gobierno y Comités

- INFOTEP mantendrá activo el Comité de Gestión de Desempeño, presidido por la Rectoría. Este órgano será la máxima instancia de decisión estratégica en materia de seguridad digital, encargado de aprobar políticas, asignar recursos y revisar el estado del SGSI semestralmente.
- La seguridad digital debe ser parte integral de la toma de decisiones institucionales; por tanto, el Oficial de Seguridad Digital tendrá reporte directo en los comités directivos donde se decidan proyectos tecnológicos o cambios estructurales.

B. Asignación de Roles y Responsabilidades

- Se definen las responsabilidades de seguridad digital para todos los niveles de la Entidad, las cuales deben estar documentadas formalmente:

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

- Alta Dirección (Rectoría): Responsable final de la gestión del riesgo y de garantizar que los objetivos de seguridad se alineen con la Misión de formar talento humano idóneo para la región insular.
- Oficial de Seguridad Digital (CISO): Rol asesor e independiente, encargado de definir la estrategia, monitorear el cumplimiento y gestionar incidentes. Este rol debe tener independencia operativa de la Oficina de TI para garantizar auditoría objetiva.
- Oficina de Tecnología (TI): Responsable de la implementación técnica de los controles, la operación segura de la infraestructura y el soporte a los servicios académicos y administrativos.
- Líderes de Procesos: Propietarios de los activos de información y de los riesgos de sus áreas. Son responsables de clasificar la información y autorizar los accesos en sus respectivas dependencias.

C. Segregación de Deberes

- INFOTEP implementará controles para evitar que una sola persona tenga el control total sobre procesos críticos que puedan comprometer la integridad de los activos (quien administra la nómina no debe administrar la base de datos subyacente).
- En los casos donde la estructura de planta no permita una segregación total, se implementarán controles compensatorios como el monitoreo de logs y auditorías periódicas.

D. Contacto con Autoridades y Grupos de Especial Interés

- El Oficial de Seguridad Digital mantendrá canales de comunicación actualizados con autoridades relevantes (CSIRT Gobierno, Policía Nacional - Centro Cibernético, MinTIC) para la coordinación ante incidentes de alcance nacional.

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

- Se mantendrá contacto con redes académicas y de investigación y grupos de especial interés en ciberseguridad educativa para el intercambio de buenas prácticas y alertas tempranas de amenazas al sector educación.

E. Seguridad en la Gestión de Proyectos

- La seguridad digital debe abordarse en la gestión de proyectos (académicos, de investigación o administrativos) independientemente del tipo de proyecto.
- Se exigirá la identificación de riesgos de seguridad y requisitos de cumplimiento (ej. Ley 1581) desde la fase de concepción y diseño de cualquier nuevo servicio, software o cambio en la infraestructura de INFOTEP.

4.2 Política de Cultura, Formación y Toma de Conciencia

INFOTEP establecerá, documentará, implementará y mantendrá un Plan de Cultura y Toma de Conciencia en Seguridad Digital, dirigido a todos los colaboradores (docentes y administrativos), investigadores, estudiantes y terceros. Este plan busca mitigar los riesgos asociados al factor humano mediante la educación continua, asegurando que los usuarios entiendan sus responsabilidades y las consecuencias del incumplimiento de las políticas del SGSI.

4.2.1. Objetivo

Establecer los lineamientos estratégicos para la construcción, ejecución y medición del plan de toma de conciencia del SGSI. Este plan debe integrar actividades de sensibilización, capacitación técnica y comunicación estratégica, asegurando la cobertura total de la comunidad académica y administrativa de INFOTEP, con el fin de promover una cultura de ciberseguridad proactiva y el cumplimiento de los roles y responsabilidades definidos.

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

4.2.2. Lineamientos de la Política

A. Planificación y Alcance del Programa

- El Oficial de Seguridad Digital, en coordinación con Talento Humano y Bienestar Universitario, diseñará anualmente el Plan de Cultura de Seguridad Digital. Este plan debe identificar las necesidades de formación basándose en los riesgos identificados, los incidentes reportados y los cambios en la infraestructura tecnológica.
- El alcance del programa es obligatorio y transversal, cubriendo a:
    - Personal Administrativo y Directivo: Enfoque en manejo de información confidencial, protección de credenciales y normatividad (Ley 1581).
    - Personal Docente e Investigadores: Enfoque en propiedad intelectual, seguridad en la nube y protección de datos de investigación.
    - Estudiantes: Enfoque en uso responsable de recursos, ciberacoso, protección de datos personales y "ciber higiene".
    - Terceros y Proveedores: Inducción abreviada sobre políticas de acceso y confidencialidad.

B. Inducción y Reinducción Obligatoria

- INFOTEP incluirá módulos específicos de seguridad de la información y protección de datos personales en los procesos de inducción de nuevos funcionarios, docentes y estudiantes.
- Ningún usuario recibirá credenciales de acceso definitivas a los sistemas críticos (Académico, Financiero) sin haber completado y aprobado el módulo de sensibilización básico en seguridad digital.

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

C. Estrategias de Formación y Entrenamiento

- Sensibilización General: Campañas periódicas sobre amenazas comunes (Phishing, Ingeniería Social, Ransomware) utilizando canales institucionales (correo, intranet, carteleras digitales).
- Capacitación Técnica Especializada: El personal de la Oficina de TI y los administradores de sistemas recibirán formación técnica avanzada y certificada en ciberseguridad para garantizar la gestión competente de los controles tecnológicos.
- Simulacros de Ingeniería Social: Se realizarán ejercicios controlados (ej. pruebas de Phishing ético) al menos una vez al año para medir el nivel de susceptibilidad de la comunidad y reforzar el aprendizaje práctico.

D. Comunicación de la Seguridad

- Se establecerán canales oficiales para la difusión de alertas de seguridad tempranas y boletines informativos.
- Se comunicarán claramente las consecuencias disciplinarias, legales y operativas del incumplimiento de las políticas de seguridad, asegurando que los usuarios comprendan que la seguridad es una condición de empleo y permanencia académica.

E. Evaluación y Mejora Continua

- La eficacia del plan de formación no se medirá solo por asistencia, sino por evaluación de conocimientos adquiridos y cambio de comportamiento (ej. reducción en la tasa de clics en correos sospechosos).
- Se mantendrán registros documentados de todas las capacitaciones realizadas, listados de asistencia y resultados de evaluaciones como evidencia de cumplimiento ante auditorías y entes de control.

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 Política de Seguridad en la Adquisición y Desarrollo de Sistemas

INFOTEP integrará la seguridad digital como un componente funcional y no funcional obligatorio en todas las etapas del ciclo de vida de sus sistemas de información, abarcando desde la concepción y adquisición, hasta el desarrollo, mantenimiento y disposición final. Esto aplica tanto para soluciones institucionales (Académico), como para plataformas de aprendizaje (LMS) y desarrollos de software resultantes de proyectos de investigación.

4.3.1. Objetivo

Asegurar que la seguridad digital sea una parte integral de los sistemas de información de INFOTEP durante todo su ciclo de vida, garantizando que los productos de software (adquiridos o desarrollados) cumplan con los requisitos de confidencialidad, integridad y disponibilidad, minimizando las vulnerabilidades técnicas antes de su paso a producción, especialmente en sistemas que prestan servicios sobre redes públicas.

4.3.2. Lineamientos de la Política

A. Análisis y Especificación de Requisitos de Seguridad

- Antes de iniciar cualquier desarrollo interno o proceso de adquisición de software, el líder del proyecto (sea de TI, Académico o Investigación) debe identificar y documentar los requisitos de seguridad de la información.
- Estos requisitos deben incluir, según aplique: controles de autenticación y autorización robustos, cifrado de datos sensibles, gestión de sesiones, pistas de auditoría (logs) y cumplimiento normativo (ej. Ley 1581).
- La Oficina de TI validará estos requisitos antes de aprobar la viabilidad técnica del proyecto o la compra.

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

B. Seguridad en el Ciclo de Vida de Desarrollo (Secure SDLC)

- Metodología Segura: Todo desarrollo de software realizado por INFOTEP (incluyendo semilleros y grupos de investigación que desarrollen para la institución) debe seguir prácticas de codificación segura, alineadas con estándares de industria como OWASP Top 10, para mitigar vulnerabilidades comunes (inyección SQL, XSS, etc.).
- Segregación de Ambientes: Se deben mantener entornos estrictamente separados para Desarrollo, Pruebas (QA) y Producción. Los desarrolladores no deben tener acceso de modificación al ambiente de producción, y los datos reales de producción no deben usarse en ambientes de desarrollo sin previo enmascaramiento o anonimización.
- Control de Cambios: Cualquier modificación en el código fuente o configuración de sistemas en producción debe seguir el procedimiento formal de Gestión de Cambios, requiriendo aprobación y pruebas de regresión previas.

C. Seguridad en la Adquisición de Software y Servicios Tercerizados

En los procesos de contratación o compra de software y servicios en la nube (SaaS), se exigirá a los proveedores evidencia de cumplimiento de estándares de seguridad (ej. certificaciones ISO 27001, SOC2) y acuerdos de nivel de servicio (SLA) que garanticen la disponibilidad y la propiedad de los datos de INFOTEP.

Se deben establecer cláusulas contractuales que obliguen al proveedor a remediar vulnerabilidades de seguridad detectadas en sus productos en tiempos perentorios.

D. Pruebas de Seguridad y Aceptación

- Antes de la puesta en producción de nuevos sistemas o actualizaciones críticas, es obligatorio realizar pruebas de seguridad técnica. Esto incluye análisis

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

estático de código para desarrollos propios y/o escaneo de vulnerabilidades para aplicaciones web.

- No se autorizará el paso a producción de ningún sistema que presente vulnerabilidades críticas o altas sin remediar.

E. Protección de Datos de Prueba

- Se prohíbe el uso de bases de datos de producción que contengan Datos Personales (de estudiantes, docentes, empleados) o información confidencial en entornos de prueba o desarrollo, salvo que se apliquen mecanismos de anonimización, enmascaramiento o generación de datos sintéticos que impidan la identificación de los titulares.

4.4 Política de Desarrollo Seguro de Software

INFOTEP adopta un enfoque de "Seguridad desde el Diseño" y "Defensa en Profundidad" para todos los desarrollos de software, integrando controles de seguridad en cada fase del ciclo de vida de desarrollo, aplicable tanto a los sistemas administrativos como a las soluciones tecnológicas resultantes de proyectos académicos y de investigación.

4.4.1. Objetivo

Establecer y aplicar reglas, estándares y controles técnicos estrictos para el desarrollo de software y sistemas dentro de la entidad, asegurando que la seguridad digital esté diseñada e implementada desde la fase de codificación hasta el despliegue, minimizando vulnerabilidades y garantizando la integridad del código fuente y los ambientes de procesamiento.

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

4.4.2. Lineamientos de la Política

A. Estándares de Codificación Segura

- Todo desarrollo de software realizado internamente por la Oficina de TI, grupos de investigación o terceros contratados, debe adherirse a estándares de industria reconocidos, como el OWASP Top 10 (para aplicaciones web) o OWASP Mobile Top 10.
- Se prohíbe el uso de prácticas de programación inseguras conocidas, tales como: credenciales embebidas en código, falta de validación de entradas, manejo inadecuado de errores que revele información del sistema y uso de componentes de terceros con vulnerabilidades conocidas (CVEs).

B. Segregación de Ambientes y Control de Cambios

- INFOTEP mantendrá una separación lógica y, cuando sea posible, física, entre los ambientes de Desarrollo, Pruebas y Producción.
- Los desarrolladores no tendrán permisos de escritura ni capacidad de despliegue directo en el ambiente de Producción. El paso a producción es responsabilidad exclusiva del personal de Operaciones/Infraestructura, previa aprobación del control de cambios y validación de seguridad.
- Los datos reales de producción no deben ser copiados a los ambientes de desarrollo o pruebas, a menos que sean sometidos a procesos de anonimización o enmascaramientos irreversibles, garantizando el cumplimiento de la Ley 1581 de 2012.

C. Gestión y Seguridad del Código Fuente

- El código fuente es un activo crítico de INFOTEP. Debe ser almacenado en repositorios institucionales centralizados con control de versiones, con acceso restringido basado en roles y auditoría de cambios habilitada.

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

- Se debe realizar una revisión de código por un par técnico o líder de desarrollo antes de fusionar cambios a las ramas principales, verificando no solo la funcionalidad sino la ausencia de brechas de seguridad.

D. Pruebas de Seguridad en el Desarrollo

- Se integrarán pruebas de seguridad automáticas y manuales en el ciclo de desarrollo:
- Análisis Estático: Escaneo del código fuente para detectar vulnerabilidades en etapas tempranas.
- Análisis Dinámico: Pruebas sobre la aplicación en ejecución en el ambiente de pruebas antes del paso a producción.
- Para desarrollos críticos o que expongan datos sensibles de estudiantes o investigación, se exigirá la realización de pruebas de penetración periódicas o previas al lanzamiento.

E. Seguridad en Desarrollo Tercerizado

- Cuando el desarrollo sea realizado por proveedores externos, INFOTEP exigirá contractualmente que el proveedor demuestre el cumplimiento de prácticas de desarrollo seguro.
- La institución se reserva el derecho de auditar el código entregado y de rechazar entregables que contengan vulnerabilidades de seguridad de nivel Alto o Crítico, las cuales deberán ser remediadas por el proveedor sin costo adicional antes de la aceptación final.

F. Desarrollo en Proyectos de Investigación

- El software desarrollado en el marco de proyectos de investigación o semilleros que vaya a ser expuesto en la red institucional o a internet debe someterse a una validación de seguridad simplificada por parte de la Oficina de TI antes de

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

su publicación, para asegurar que no se convierta en un vector de ataque para la infraestructura de INFOTEP.

4.5 Política de Entorno de Trabajo Seguro (Escritorio y Pantalla Limpios)

INFOTEP adopta la directriz de "Cero Confianza" en el entorno físico y lógico del puesto de trabajo, exigiendo que todos los funcionarios, docentes y contratistas protejan la información sensible contra accesos no autorizados, pérdidas o daños, tanto en horarios laborales como fuera de ellos.

4.5.1. Objetivo

Definir los lineamientos técnicos y de comportamiento para mantener el entorno de trabajo físico (escritorio) y lógico (pantalla) despejados de información confidencial o sensible cuando no estén en uso, reduciendo la superficie de exposición ante amenazas internas o externas y garantizando la confidencialidad de los datos académicos y administrativos.

4.5.2. Lineamientos de la Política

A. Protección del Entorno Físico (Escritorio Limpio)

- Custodia de Documentación: No deberán dejarse documentos físicos con información clasificada, sensible o confidencial (ej. exámenes, listados de notas, historias laborales, informes financieros) expuestos sobre la superficie del escritorio, impresoras o áreas comunes cuando el puesto de trabajo esté desatendido, ni siquiera por periodos cortos.
- Almacenamiento Seguro: Al finalizar la jornada laboral, o durante ausencias prolongadas, toda la documentación sensible y los medios de almacenamiento

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

extraíbles (memorias USB, discos duros externos, tokens) deben ser resguardados en cajoneras, archivadores o armarios bajo llave.

- Pizarras y Tableros: La información escrita en pizarras o tableros de oficinas y salas de juntas que contenga datos sensibles o estratégicos debe ser borrada completamente al finalizar la reunión.

B. Protección del Entorno Lógico (Pantalla Limpia)

Bloqueo de Sesión: Es obligatorio bloquear la sesión del equipo de cómputo cada vez que el usuario se retire de su puesto de trabajo, independientemente de la duración de la ausencia. Se promoverá el uso del comando rápido de bloqueo (ej. `Win + L` en Windows) como hábito de ciber higiene.

Configuración de Inactividad: La Oficina de TI configurará, mediante políticas de dominio (GPO), la activación automática de un protector de pantalla o bloqueo de sesión tras un periodo máximo de inactividad (ej. 5 a 10 minutos), requiriendo autenticación (contraseña) para retomar la sesión.

Cierre de Sesión: Al finalizar la jornada, los usuarios deben cerrar sesión completamente o apagar sus equipos, salvo instrucción contraria de TI para ventanas de mantenimiento o actualizaciones nocturnas.

C. Seguridad en Dispositivos de Impresión

- Los documentos enviados a imprimir que contengan información sensible deben ser retirados inmediatamente de la bandeja de salida de la impresora.
- En lo posible, se implementará la "impresión segura" (retención de impresión hasta que el usuario se autentique en el dispositivo) para áreas críticas como Rectoría, Talento Humano y Registro Académico.

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

4.6 Política de Seguridad Física y de Instalaciones

INFOTEP implementará un enfoque de "Defensa en Profundidad" para la seguridad física, estableciendo anillos de protección concéntricos que van desde el perímetro del campus hasta los activos más críticos (Centro de Datos, Archivo de Gestión, Laboratorios de Investigación), garantizando que solo el personal autorizado tenga acceso físico a la información y a la infraestructura que la soporta.

4.6.1. Objetivo

Minimizar los riesgos de daños, interferencias, robo o accesos físicos no autorizados a la información y a las instalaciones de procesamiento de INFOTEP. Esto se logrará mediante la definición de perímetros de seguridad, controles de acceso físico y protección contra amenazas ambientales, asegurando la continuidad operativa de los servicios académicos y administrativos.

4.6.2. Lineamientos de la Política

A. Perímetros de Seguridad Física

- **INFOTEP** clasificará sus instalaciones físicas en zonas de seguridad según la criticidad de los activos alojados:
    - **Zona Pública:** Áreas de libre circulación (jardines, cafeterías, pasillos generales).
    - **Zona Controlada:** Áreas de trabajo administrativo y académico (oficinas, salas de profesores, aulas de cómputo), donde el acceso requiere identificación institucional.
    - **Zona Restringida (Áreas Seguras):** Espacios que alojan información sensible o infraestructura crítica, tales como el Centro de Datos, cuartos de comunicaciones (Racks/Switches), Archivo Central y Laboratorios de Investigación con equipos especializados.

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

B. Controles de Acceso Físico

- **Control de Ingreso:** El acceso a las "Zonas Restringidas" estará protegido por mecanismos de control sólidos (ej. cerraduras electrónicas, biometría o tarjetas de proximidad) que generen registros de auditoría (logs) de entrada y salida.
- **Visitantes:** Todo personal externo (proveedores, visitantes) que requiera ingresar a una Zona Controlada o Restringida deberá registrarse en portería, portar un distintivo visible en todo momento y estar acompañado por un funcionario de **INFOTEP**, salvo excepciones autorizadas formalmente.
- **Revocación de Acceso:** Los derechos de acceso físico deben ser revocados inmediatamente tras la terminación del vínculo laboral o contractual, o cuando cambien las funciones del usuario.

C. Protección contra Amenazas Ambientales y del Entorno

- Las instalaciones críticas (especialmente el Centro de Datos y Archivo) deben contar con protecciones diseñadas contra desastres naturales o fallas de infraestructura, incluyendo:
    - **Sistemas de Detección y Extinción de Incendios:** Adecuados para equipos electrónicos (ej. agentes limpios) y documentos físicos.
    - **Control Ambiental:** Sistemas de aire acondicionado de precisión para mantener temperatura y humedad en rangos operativos.
    - **Respaldo de Energía:** Sistemas de Alimentación Ininterrumpida (UPS) y plantas eléctricas para proteger los equipos contra fallas de energía y picos de voltaje, asegurando el cierre controlado de sistemas o la continuidad operativa.

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

D. Seguridad del Cableado

- El cableado de energía y de telecomunicaciones que transporta datos o soporta servicios de información debe estar protegido contra intercepciones, interferencias electromagnéticas o daños físicos (ej. mediante el uso de ductos, canaletas cerradas o fibra óptica), especialmente en áreas de alto tráfico estudiantil.

E. Mantenimiento de Equipos

- Los equipos críticos (servidores, equipos de red, aires acondicionados, UPS) deben recibir mantenimiento preventivo y correctivo periódico, conforme a las especificaciones del fabricante, para asegurar su disponibilidad e integridad. Las actividades de mantenimiento deben quedar registradas formalmente.

F. Trabajo en Áreas Seguras

- El personal que trabaje dentro de áreas seguras (ej. técnicos en el Data Center) no debe ingresar dispositivos de grabación (cámaras, celulares) no autorizados, ni consumir alimentos o bebidas que puedan poner en riesgo la infraestructura. Las puertas de estas áreas deben permanecer cerradas y bloqueadas cuando no estén en uso activo.

4.7 Política de Operaciones Tecnológicas Seguras

INFOTEP establecerá procedimientos documentados y controles técnicos rigurosos para la gestión de su infraestructura tecnológica, garantizando que las operaciones diarias de procesamiento de información se realicen de manera segura, predecible y monitoreada, minimizando el riesgo de interrupciones no planificadas o pérdida de datos.

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

4.7.1. Objetivo

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de INFOTEP, estableciendo responsabilidades y procedimientos para la gestión de cambios, la protección contra código malicioso, la realización de copias de seguridad y el monitoreo de la capacidad, con el fin de mantener la disponibilidad e integridad de los servicios críticos como la plataforma académica, los sistemas financieros y los repositorios de investigación.

4.7.2. Lineamientos de la Política

A. Documentación de Procedimientos Operativos

- La Oficina de TI mantendrá actualizados los **Procedimientos Operativos Estándar** para todas las actividades críticas de gestión de sistemas (ej. encendido y apagado de servidores, ejecución de procesos por lotes/batch, recuperación de servicios).
- Estos procedimientos deben estar disponibles para el personal autorizado y detallar las instrucciones precisas para evitar errores humanos que afecten la disponibilidad.

B. Gestión de Cambios

- **INFOTEP** implementará un proceso formal de Control de Cambios para cualquier modificación en los sistemas de información, redes o infraestructura de procesamiento.
- Todo cambio (actualización de software, parcheo de seguridad, cambio de configuración de red) debe ser:
    1. Solicitado y justificado formalmente.
    2. Evaluado en cuanto a su impacto y riesgo de seguridad.
    3. Probado en un ambiente de pre-producción.
    4. Aprobado por el líder del área antes de su aplicación.

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

5. Ejecutado con un **plan de retorno (rollback)** claro en caso de falla.

C. Gestión de Capacidad

- Se debe monitorear periódicamente la utilización de recursos (CPU, memoria, almacenamiento, ancho de banda) de los sistemas críticos.
- La Oficina de TI debe realizar proyecciones de capacidad futura, considerando los ciclos académicos de **INFOTEP** (ej. picos de demanda durante matrículas o cierre de notas), para asegurar la escalabilidad y evitar la denegación de servicio por saturación.

D. Protección contra Código Malicioso (Malware)

- Se implementarán controles de detección, prevención y recuperación contra código malicioso (Antivirus/EDR) en todos los activos tecnológicos de **INFOTEP** (servidores, estaciones de trabajo administrativas, equipos de laboratorios académicos).
- Las firmas de virus y agentes de seguridad deben actualizarse automáticamente. Se prohíbe a los usuarios desactivar estos controles.
- Se bloqueará la ejecución de software no autorizado o descargado de fuentes no confiables mediante políticas de control de aplicaciones.

E. Copias de Respaldo (Backups)

- **INFOTEP** aplicará una política de copias de seguridad rigurosa para proteger la información contra pérdida de datos (ej. por Ransomware o falla de disco).
- **Regla 3-2-1:** Se propenderá por mantener tres copias de los datos, en dos medios diferentes, con una copia fuera de sitio o en la nube inmutable.
- **Alcance:** Se deben respaldar diariamente las bases de datos académicas, financieras y los servidores de archivos críticos.

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

- **Pruebas de Restauración:** Se realizarán pruebas periódicas (mínimo semestrales) de restauración de backups para verificar su integridad y eficacia.

F. Gestión de Vulnerabilidades Técnicas

- La Oficina de TI obtendrá información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso (Sistemas Operativos, Bases de Datos, LMS).
- Se aplicarán los parches de seguridad críticos proporcionados por los fabricantes en un tiempo perentorio tras su liberación y prueba, priorizando los sistemas expuestos a internet.

G. Registros y Monitoreo

- Se habilitarán y protegerán los registros de auditoría (logs) que registren eventos de seguridad (inicios de sesión fallidos, uso de privilegios administrativos, errores de sistema).
- **Sincronización de Relojes:** Todos los sistemas de procesamiento de información de **INFOTEP** deben sincronizar sus relojes con una fuente de tiempo confiable (NTP) para asegurar la exactitud y correlación de los registros de eventos.

4.8 Política para el Trabajo Móvil y Remoto

4.8.1. Objetivo

Establecer los lineamientos de seguridad para el uso de dispositivos de computación móvil y comunicación (institucionales o personales autorizados) y asegurar la protección de la información de INFOTEP cuando es accedida,

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

procesada o almacenada en sitios de teletrabajo, trabajo en casa o durante desplazamientos, mitigando los riesgos de robo, pérdida, acceso no autorizado o interceptación de comunicaciones.

4.8.2. Lineamientos de la Política

A. Gestión de Dispositivos Móviles (Institucionales y BYOD)

- **Dispositivos Institucionales:** Todos los equipos portátiles (laptops, tabletas, celulares) propiedad de **INFOTEP** entregados a funcionarios o docentes deben contar con una configuración de seguridad base (línea base) que incluya: cifrado de disco duro/almacenamiento (ej. BitLocker), antivirus corporativo gestionado, y bloqueo de pantalla automático configurado.
- **Dispositivos Personales (BYOD):** Se permite el uso de dispositivos personales para acceder a servicios institucionales (correo, plataformas académicas) únicamente si el usuario acepta y cumple las normas de seguridad mínimas: mantener el sistema operativo actualizado, no realizar modificaciones no autorizadas al sistema y utilizar mecanismos de autenticación robustos (PIN, biometría).
- **Registro:** La Oficina de TI mantendrá un registro actualizado de los dispositivos móviles autorizados que tienen acceso a información sensible de la entidad.

B. Seguridad en el Teletrabajo y Trabajo Remoto

- **Entorno Físico:** El funcionario o docente en modalidad de teletrabajo debe garantizar que su entorno remoto ofrezca condiciones de seguridad física adecuadas para evitar que personas no autorizadas (incluidos familiares o visitantes) visualicen información confidencial en las pantallas o accedan a documentos impresos.

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

- **Uso Exclusivo:** Los equipos de cómputo suministrados por **INFOTEP** para el trabajo remoto son herramientas de uso exclusivamente laboral y académico. Está prohibido su uso por parte de terceros ajenos a la institución o para actividades personales que pongan en riesgo la seguridad (juegos, descargas ilegales).
- **Conexión Segura (VPN):** El acceso remoto a los sistemas de información internos (Financiero, Sistemas de Gestión Académica no expuestos a internet, Carpetas Compartidas) debe realizarse obligatoriamente a través de una Red Privada Virtual (VPN), proporcionada y configurada por la Oficina de TI.

C. Protección en Redes Públicas y Desplazamientos

- Se prohíbe el tratamiento de información sensible o confidencial conectándose a redes Wi-Fi públicas, abiertas o no confiables (ej. aeropuertos, cafeterías, hoteles) sin el uso de la VPN institucional. En su defecto, se recomienda el uso de redes de datos móviles (tethering 4G/5G) corporativas o personales.
- Durante los desplazamientos, los dispositivos nunca deben dejarse desatendidos en vehículos, áreas públicas o equipaje facturado. El usuario es responsable de la custodia física permanente del activo.

D. Prevención de Fuga de Información y Copias de Seguridad

- La información institucional generada en trabajo remoto no debe almacenarse localmente en el disco duro del dispositivo de forma permanente. Se debe trabajar directamente sobre las plataformas de nube institucional como lo es Google Drive o servidores de archivos conectados por VPN, para garantizar la realización de copias de seguridad centralizadas.
- En caso de pérdida o robo de un dispositivo móvil (institucional o personal con acceso a datos de la entidad), el usuario debe reportarlo inmediatamente

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

a la Mesa de Ayuda para proceder con el bloqueo de cuentas y, si es técnicamente posible, el borrado remoto de los datos institucionales.

4.9 Política de Seguridad en la Gestión del Talento Humano

INFOTEP integrará los requisitos de seguridad de la información en todas las etapas del ciclo de vida laboral de sus colaboradores, desde la selección y contratación, pasando por el desempeño de funciones, hasta la desvinculación o cambio de cargo. Esto aplica a funcionarios administrativos, personal docente, investigadores y contratistas de prestación de servicios.

4.9.1. Objetivo

Asegurar que los colaboradores y terceros sean aptos para los roles considerados, comprendan sus responsabilidades en materia de seguridad de la información y las cumplan. Asimismo, garantizar que los intereses de INFOTEP estén protegidos durante el proceso de vinculación, permanencia y, especialmente, en la terminación o cambio de la relación laboral o contractual.

4.9.2. Lineamientos de la Política

A. Antes del Empleo (Selección y Contratación)

- **Verificación de Antecedentes:** Para los candidatos a cargos que conlleven acceso a información confidencial o administración de sistemas críticos (ej. Tesorería, Admisiones, TI), **INFOTEP** realizará verificaciones de antecedentes, referencias y competencias técnicas, en conformidad con las leyes de privacidad vigentes.

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

- **Términos y Condiciones de Contratación:** Los contratos laborales y de prestación de servicios deben incluir cláusulas explícitas sobre responsabilidades de seguridad de la información.
- **Acuerdos de Confidencialidad:** Todo colaborador (incluyendo docentes hora cátedra e investigadores externos) deberá firmar un **Acuerdo de Confidencialidad y No Divulgación** antes de recibir acceso a los recursos de información. Este acuerdo debe proteger específicamente los datos personales de estudiantes y la propiedad intelectual institucional.

B. Durante el Empleo (Gestión y Concientización)

- **Responsabilidad de la Dirección:** La Alta Dirección y los jefes de área deben exigir a sus equipos el cumplimiento de las políticas de seguridad y motivar la participación en las actividades de sensibilización.
- **Educación y Formación:** Todos los empleados recibirán formación periódica adecuada y actualizaciones sobre las políticas y procedimientos de seguridad, relevante para sus funciones laborales (Ver Política 4.2).
- **Proceso Disciplinario: INFOTEP** establecerá un proceso formal (alineado con el Código Disciplinario Único y el Reglamento Interno de Trabajo) para sancionar a los colaboradores que hayan cometido violaciones a las políticas de seguridad, garantizando el debido proceso.

C. Terminación o Cambio de Empleo

- **Responsabilidades de Terminación:** Las responsabilidades de seguridad que subsisten tras la terminación del contrato (ej. datos sensibles) deben ser comunicadas claramente al colaborador al momento de su retiro.
- **Devolución de Activos:** Se debe establecer un procedimiento de "Paz y Salvo" que garantice la devolución de todos los activos de información (equipos de cómputo, tokens, tarjetas de acceso, llaves, documentación técnica) antes de la liquidación final.

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

- **Revocación de Derechos de Acceso:** Los derechos de acceso a las instalaciones y a los sistemas de información (cuentas de correo, sistemas de información y VPN) deben ser revocados o ajustados **inmediatamente** (el mismo día) tras la notificación de retiro o cambio de cargo. La oficina de Talento Humano debe notificar a TI sobre las novedades de personal con la debida antelación.

4.10 Política de Uso de Criptografía

INFOTEP implementará controles criptográficos robustos como medida técnica fundamental para proteger la confidencialidad, integridad, autenticidad y no repudio de la información institucional, especialmente aquella clasificada como Confidencial o Restringida, asegurando la protección de datos personales de la comunidad educativa y la propiedad intelectual generada en los procesos de investigación.

4.10.1. Objetivo

Asegurar el uso apropiado y eficaz de sistemas y técnicas criptográficas para proteger la información de INFOTEP contra el acceso no autorizado, la divulgación o la modificación, tanto cuando esta se encuentra almacenada como cuando se transmite a través de redes de comunicaciones, basándose en el análisis de riesgos y el nivel de clasificación del activo.

4.10.2. Lineamientos de la Política

A. Criterios de Uso de Cifrado

- **Información Sensible:** Se aplicará cifrado obligatorio a toda información clasificada como "Confidencial" o "Secreta", incluyendo bases de datos de

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

estudiantes, historias laborales, datos financieros y resultados de investigaciones no publicados.

- **Dispositivos Móviles:** Todos los dispositivos portátiles (laptops, tabletas, medios extraíbles) asignados a directivos, docentes investigadores o personal que maneje datos sensibles, deben tener activado el cifrado de disco completo.

B. Cifrado en Tránsito (Comunicaciones)

- Toda transmisión de información sensible o credenciales de autenticación a través de redes públicas (Internet) o redes inalámbricas debe estar protegida mediante protocolos de cifrado seguros y actualizados (ej. TLS 1.2 o superior).
- El acceso remoto a los servicios internos de **INFOTEP** se realizará exclusivamente a través de canales cifrados, como Redes Privadas Virtuales (VPN) con algoritmos robustos, prohibiendo el uso de protocolos inseguros (Telnet, HTTP, FTP) para operaciones administrativas o transaccionales.

C. Cifrado en Reposo (Almacenamiento)

- Las bases de datos críticas (Sistemas Académicos, sistema Financiero) deben implementar cifrado transparente de datos (TDE) o cifrado a nivel de columna para campos sensibles (contraseñas, números de identificación, datos biométricos).
- Las copias de seguridad (backups) que contengan información institucional deben estar cifradas antes de ser transferidas a medios de almacenamiento externos o servicios en la nube.

D. Gestión de Claves Criptográficas

- **Ciclo de Vida: INFOTEP**, a través de la Oficina de TI, establecerá un procedimiento formal para la gestión del ciclo de vida de las claves

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

criptográficas, que incluya su generación segura, distribución, almacenamiento protegido, rotación periódica, revocación y destrucción segura.

- **Separación de Roles:** Se debe garantizar la separación de funciones entre los administradores de las claves criptográficas y los administradores de los datos cifrados, para evitar accesos no autorizados o pérdida de disponibilidad.
- **Protección de Claves:** Las claves privadas y simétricas deben almacenarse en módulos de seguridad o bóvedas de claves seguras, nunca en archivos de texto plano o embebidas en el código fuente de las aplicaciones.

E. Estándares Técnicos Permitidos

- Se utilizarán únicamente algoritmos criptográficos estándar de la industria y de probada fortaleza (ej. AES-256 para datos, RSA-2048 o superior para claves asimétricas, SHA-256 o superior para integridad).
- Está prohibido el uso de algoritmos criptográficos obsoletos o comprometidos (ej. DES, MD5, SHA-1) en nuevos sistemas, y se establecerá un plan de migración para los sistemas legados que aún los utilicen.

4.11 Política de Cumplimiento Legal, Normativo y Contractual

INFOTEP gestionará la seguridad de la información no solo como una medida de protección técnica, sino como un componente esencial de cumplimiento legal, asegurando la conformidad con el marco jurídico colombiano, las regulaciones del sector educación y los compromisos adquiridos con terceros, aliados y el Estado.

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

4.11.1. Objetivo

Identificar, documentar y mantener actualizados los requisitos estatutarios, reglamentarios y contractuales pertinentes para evitar el incumplimiento de obligaciones legales relacionadas con la seguridad de la información. Esto busca mitigar el riesgo de sanciones legales, pérdida de reputación o incumplimiento de contratos, asegurando que el diseño, operación y administración de los sistemas de INFOTEP se adhieran estrictamente a la normatividad vigente.

4.11.2. Lineamientos de la Política

A. Identificación de la Legislación Aplicable

- La Oficina Jurídica, en coordinación con el Oficial de Seguridad Digital, mantendrá un inventario actualizado de las obligaciones legales y regulatorias relacionadas con la seguridad de la información y la ciberseguridad.
- Este marco normativo incluye explícitamente, pero no se limita a:
    - **Ley 1581 de 2012:** Régimen General de Protección de Datos Personales.
    - **Ley 1273 de 2009:** Delitos Informáticos.
    - **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública.
    - **Ley 23 de 1982 y Decisión 351 de la CAN:** Derechos de Autor y Propiedad Intelectual.
    - Normatividad del Archivo General de la Nación para la gestión documental electrónica.

B. Derechos de Propiedad Intelectual

- **Software Legal: INFOTEP** respetará los derechos de propiedad intelectual de los fabricantes de software. Se prohíbe estrictamente la instalación o uso

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

de software pirata o sin el licenciamiento adecuado en cualquier equipo institucional. Se realizarán auditorías periódicas de software para asegurar el cumplimiento.

- **Producción Intelectual Propia:** Se implementarán controles para proteger la propiedad intelectual generada por **INFOTEP** (investigaciones, publicaciones académicas, desarrollos tecnológicos propios), garantizando su integridad y evitando su filtración o plagio antes de su publicación oficial.

C. Protección de Registros y Gestión Documental

- Los registros institucionales importantes (académicos, financieros, historias laborales) deben ser protegidos contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y de negocio.
- Se deben aplicar las tablas de retención documental (TRD) para asegurar que la información se conserve por el tiempo exigido por la ley y se elimine de forma segura una vez cumplido dicho periodo, especialmente aquella que contenga datos sensibles.

D. Privacidad y Protección de Datos Personales (Habeas Data)

- **INFOTEP** garantizará la privacidad y la protección de los datos personales de estudiantes, docentes, funcionarios y proveedores, conforme a la Política de Tratamiento de Datos Personales de la entidad.
- Se implementarán controles técnicos (cifrado, control de acceso) y administrativos (avisos de privacidad, gestión de consentimientos) para asegurar que los datos solo se recolecten y procesen para las finalidades autorizadas.

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

E. Cumplimiento en Acuerdos Contractuales

- En todos los contratos, convenios o alianzas estratégicas (con el sector productivo, otras universidades o proveedores tecnológicos), se revisarán las cláusulas de seguridad de la información para asegurar que las contrapartes cumplan con los estándares de **INFOTEP**.
- Se establecerá el derecho de **INFOTEP** a auditar o solicitar evidencia de cumplimiento de seguridad a los proveedores críticos.

F. Revisión de la Seguridad de la Información

- Los sistemas de información y los controles de seguridad de **INFOTEP** deben ser sometidos a revisiones independientes (auditorías internas o externas) a intervalos planificados, para verificar el cumplimiento de las políticas y normas de seguridad.
- Los responsables de los sistemas deben realizar revisiones técnicas periódicas (ej. escaneo de cumplimiento) para asegurar que las configuraciones de hardware y software cumplan con las políticas de seguridad implementadas.

4.12 Política de Seguridad de las Redes y Comunicaciones

INFOTEP administrará y controlará sus redes de datos y comunicaciones (cableadas e inalámbricas) para proteger la información en tránsito y garantizar la disponibilidad de los servicios de conexión, impidiendo accesos no autorizados a la infraestructura tecnológica y asegurando la segregación lógica entre los servicios académicos, administrativos y públicos.

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

4.12.1. Objetivo

Garantizar la protección de la información en las redes y sus instalaciones de procesamiento, estableciendo controles técnicos y administrativos para asegurar la confidencialidad e integridad de los datos que viajan a través de las redes de INFOTEP, así como la disponibilidad y resiliencia de la infraestructura de comunicaciones ante ataques o fallas.

4.12.2. Lineamientos de la Política

A. Segregación y Segmentación de Redes

- **INFOTEP** no operará una red plana. Se implementará una estricta segmentación de la red mediante el uso de Redes de Área Local Virtuales (VLANs) y subredes, separando lógicamente el tráfico según su naturaleza y criticidad.
- Se definirán segmentos diferenciados para:
  - **Red Administrativa:** Exclusiva para funcionarios, con acceso a sistemas financieros y de gestión (ERP).
  - **Red Académica/Investigación:** Para laboratorios y equipos de docentes investigadores.
  - **Red Estudiantil/Pública:** Acceso a internet controlado, aislada totalmente de los servidores críticos y bases de datos institucionales.
  - **Zona Desmilitarizada (DMZ):** Para alojar servicios expuestos a internet (Portal Web, Campus Virtual) separándolos de la red interna (LAN).

B. Controles Perimetrales y de Seguridad de Red

- Se implementarán y mantendrán firewalls (cortafuegos) de nueva generación en los puntos de conexión con redes externas (Internet).

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

- La configuración de estos dispositivos seguirá la política de "denegar todo por defecto", permitiendo únicamente el tráfico estrictamente necesario para la operación.
- Se utilizarán Sistemas de Detección y Prevención de Intrusos (IDS/IPS) para monitorear y bloquear patrones de tráfico malicioso o intentos de explotación de vulnerabilidades en la red.

C. Seguridad en Redes Inalámbricas (Wi-Fi)

- Las redes inalámbricas institucionales utilizarán protocolos de cifrado robustos (WPA2/WPA3 Enterprise o superior).
- La autenticación de usuarios en la red Wi-Fi institucional/académica se realizará mediante credenciales individuales (usuario y contraseña institucional.
- La red Wi-Fi para invitados estará totalmente aislada de los recursos internos y se buscará la implementación de un portal cautivo.

D. Seguridad en el Intercambio de Información

- **Canales Seguros:** Toda transferencia de información sensible, confidencial o datos personales hacia entidades externas (Ministerio de Educación, Entidades Financieras, Aliados de Investigación) debe realizarse a través de canales cifrados (SFTP, HTTPS, VPN Site-to-Site, Correo Cifrado).
- **Acuerdos de Intercambio:** Antes de establecer conexiones dedicadas o interfaces de intercambio de datos automatizadas (APIs) con terceros, se deben formalizar acuerdos que especifiquen las responsabilidades de seguridad, los estándares técnicos y los niveles de servicio.

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

E. Protección del Acceso Remoto y VPN

- El acceso administrativo remoto a los dispositivos de red (switches, routers, firewalls) debe realizarse exclusivamente a través de protocolos cifrados (SSH, HTTPS) y desde estaciones de administración autorizadas y seguras.
- Las conexiones de teletrabajo o soporte externo hacia la red interna deben cursar obligatoriamente por una VPN Institucional con autenticación robusta, prohibiendo la exposición directa de servicios administrativos (RDP, SMB, SSH) a internet.

F. Monitoreo y Sincronización

- Se registrarán y monitorearán los eventos de seguridad de la red (logs de firewall, alertas de IPS).
- Todos los dispositivos de red deben estar sincronizados con una fuente de tiempo confiable (servidor NTP interno o externo autorizado) para garantizar la trazabilidad y el análisis forense en caso de incidentes.

4.13 Política de Continuidad Digital y Resiliencia

INFOTEP reconoce que, dada su ubicación geográfica insular y la creciente sofisticación de las ciberamenazas, la interrupción de servicios es un riesgo latente. Por tanto, la institución no solo se enfocará en la prevención, sino en la **resiliencia**: la capacidad de resistir, responder y recuperarse de incidentes disruptivos para garantizar la prestación del servicio educativo y administrativo.

4.13.1. Objetivo

Asegurar que los requisitos de seguridad de la información estén integrados en la gestión de la continuidad del negocio de INFOTEP, garantizando la disponibilidad

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

de los servicios tecnológicos críticos y la recuperación de la información en tiempos aceptables tras la ocurrencia de situaciones adversas, desastres naturales, fallas técnicas mayores o ciberataques.

4.13.2. Lineamientos de la Política

A. Análisis de Impacto y Evaluación de Riesgos

- **Análisis de Impacto al Negocio (BIA): INFOTEP** realizará y actualizará periódicamente un BIA para identificar los procesos misionales críticos (ej. Admisiones, Registro y Control, Plataforma LMS, Nómina) y determinar los tiempos máximos de interrupción tolerables (RTO - Recovery Time Objective) y el punto máximo de pérdida de datos aceptable (RPO - Recovery Point Objective).
- **Riesgos Específicos:** La evaluación de riesgos de continuidad debe considerar explícitamente amenazas derivadas de la **insularidad** (huracanes, fallas prolongadas de conectividad submarina o energía) y amenazas cibernéticas (Ransomware, ataques DDoS).

B. Planes de Continuidad y Recuperación (BCP/DRP)

- **Plan de Continuidad del Negocio (BCP):** Se desarrollará un marco de procedimientos para mantener la operación de la institución en modos de contingencia (incluso manuales) durante una crisis.
- **Plan de Recuperación de Desastres (DRP):** La Oficina de TI mantendrá un DRP técnico detallado que guíe paso a paso la restauración de la infraestructura tecnológica (servidores, redes, aplicaciones) en el sitio principal o en un sitio alterno (nube o físico), priorizando los servicios definidos como críticos en el BIA.

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

C. Alta Disponibilidad y Redundancia

- Para mitigar el riesgo de interrupción, los sistemas críticos de **INFOTEP** se diseñarán bajo principios de redundancia. Esto incluye, donde sea factible, enlaces de comunicaciones redundantes, clústeres de servidores y replicación de almacenamiento.
- Se implementarán estrategias de respaldo en la nube para garantizar que, ante un evento catastrófico en la sede física, los datos académicos y administrativos estén resguardados fuera de la zona de desastre.

D. Pruebas y Ejercicios de Continuidad

- Los planes de continuidad no son documentos estáticos. **INFOTEP** realizará pruebas periódicas (mínimo una vez al año) de sus planes BCP y DRP.
- Estas pruebas pueden variar desde ejercicios de escritorio (simulacros de toma de decisiones) hasta pruebas técnicas completas (restauración de backups, conmutación a sistemas de contingencia), con el fin de validar la efectividad de los procedimientos y entrenar al personal de respuesta.

E. Seguridad de la Información en la Continuidad

- Los controles de seguridad deben mantenerse incluso en situaciones de contingencia. El DRP debe garantizar que, al operar en modo de emergencia o en sitios alternos, se mantengan los niveles de seguridad requeridos (control de acceso, cifrado, monitoreo), evitando que la crisis se convierta en una oportunidad para brechas de seguridad.

F. Estrategia de Resiliencia ante Ciberataques (Ciber-Resiliencia)

- Se desarrollarán procedimientos específicos para la recuperación ante ataques destructivos (como Ransomware), que incluyan el aislamiento de redes, la limpieza de sistemas infectados y la restauración desde copias de

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

seguridad inmutables o fuera de línea, asegurando que los datos restaurados sean confiables antes de reiniciar la operación.

4.14 Política de Gestión de Incidentes de Ciberseguridad

INFOTEP reconoce que la prevención absoluta es imposible. Por tanto, establece un enfoque estructurado para la detección, reporte, evaluación y respuesta ante incidentes de seguridad, con el fin de minimizar el impacto en las operaciones académicas y administrativas, garantizar la recuperación del servicio y preservar la evidencia para fines forenses o legales.

4.14.1. Objetivo

Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los eventos, incidentes y debilidades de seguridad de la información reportados. El propósito es reducir el impacto adverso sobre la confidencialidad, integridad y disponibilidad de los activos de información y aprender de dichos eventos para prevenir su recurrencia.

4.14.2. Lineamientos de la Política

A. Obligatoriedad del Reporte

- Todo miembro de la comunidad **INFOTEP** (funcionarios, docentes, estudiantes, contratistas) tiene la **obligación** de reportar inmediatamente cualquier evento sospechoso, debilidad de seguridad observada o incidente confirmado a través de los canales oficiales establecidos (Mesa de Ayuda, correo de seguridad, línea telefónica).
- Se prohíbe a los usuarios intentar investigar o remediar incidentes de seguridad por su cuenta (salvo acciones de contención inmediata

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

autorizadas, como desconectar el cable de red), para evitar la alteración de evidencia digital.

B. Clasificación y Tipificación de Incidentes

- La Oficina de TI y el Oficial de Seguridad Digital establecerán una taxonomía para clasificar los incidentes según su **Tipo** (ej. Phishing, Ransomware, Fuga de Información, Denegación de Servicio, Intrusión) y su **Criticidad** (Baja, Media, Alta, Crítica).
- La priorización de la respuesta se basará en el impacto potencial sobre los procesos misionales (ej. afectación a inscripciones, pérdida de datos de investigación) y el número de usuarios afectados.

C. Equipo de Respuesta a Incidentes (CSIRT/CIRT)

- Se conformará un **Equipo de Respuesta a Incidentes de Seguridad** (interno o con apoyo de terceros especializados), liderado por el Oficial de Seguridad Digital.
- Este equipo tendrá la autoridad delegada por la Alta Dirección para tomar decisiones de emergencia durante un incidente, incluyendo la desconexión de sistemas críticos, el aislamiento de redes o la suspensión de servicios, si es necesario para contener una amenaza mayor.

D. Ciclo de Vida de la Gestión del Incidente

INFOTEP adoptará un procedimiento formal de respuesta que cubra las siguientes fases:

1. **Detección y Análisis:** Validación del reporte y determinación del alcance.
2. **Contención:** Acciones para limitar el daño (ej. aislar el servidor infectado).
3. **Erradicación:** Eliminación de la causa raíz (ej. eliminar el malware, cerrar la vulnerabilidad).

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. **Recuperación:** Restauración de servicios a la operación normal y monitoreo intensivo.
5. **Lecciones Aprendidas:** Análisis posterior para mejorar los controles.

E. Cadena de Custodia y Análisis Forense

- En incidentes que puedan derivar en procesos disciplinarios, legales o penales (ej. fraude interno, ataque externo), se debe garantizar la **cadena de custodia** de la evidencia digital.
- El análisis forense debe ser realizado por personal competente, asegurando que los medios originales no sean alterados (trabajando sobre imágenes forenses) y documentando detalladamente todos los hallazgos.

F. Comunicación del Incidente

- El manejo de la comunicación hacia las partes interesadas (Ministerio de Educación, estudiantes, autoridades) durante un incidente de seguridad será canalizado exclusivamente por la Oficina de Comunicaciones y la Alta Dirección, siguiendo el protocolo de gestión de crisis. Se debe evitar la divulgación de detalles técnicos que puedan ser explotados por los atacantes.

G. Gestión de Debilidades Técnicas

- Además de los incidentes, se deben reportar y gestionar las debilidades técnicas (vulnerabilidades) detectadas en los sistemas. La Oficina de TI debe evaluar y remediar estas debilidades de manera proactiva antes de que sean explotadas.

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

4.15 Política de Intercambio Seguro de Información

INFOTEP reconoce que la colaboración es esencial para su misión educativa y de investigación. Por tanto, establece controles estrictos para proteger la información que es transferida tanto internamente (entre dependencias) como externamente (con el Ministerio de Educación, entidades financieras, aliados de investigación y el sector productivo), asegurando que el tránsito de datos no se convierta en el eslabón más débil de la cadena de seguridad.

4.15.1. Objetivo

Mantener la seguridad de la información transferida dentro de INFOTEP y entre la institución y cualquier entidad externa, estableciendo procedimientos formales, controles técnicos de cifrado y acuerdos legales que protejan la confidencialidad, integridad y autenticidad de los datos durante su transporte, impidiendo su interceptación, copia no autorizada, modificación o direccionamiento erróneo.

4.15.2. Lineamientos de la Política

A. Formalización de Acuerdos de Intercambio

- Antes de establecer cualquier flujo regular de intercambio de información sensible o datos personales con un tercero, se deben formalizar **Acuerdos de Intercambio de Información**.
- Estos acuerdos deben especificar: las responsabilidades de cada parte en caso de incidentes, los estándares técnicos de transmisión (protocolos, cifrado), la clasificación de los datos y los requisitos de eliminación segura al finalizar el intercambio.

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

B. Uso de Canales Seguros y Protocolos Cifrados

- **Transferencia de Archivos:** Toda transferencia de archivos que contenga datos institucionales (ej. reportes a SNIES/SPADIES, nómina bancaria) debe realizarse a través de protocolos seguros como **SFTP** (Secure File Transfer Protocol) o **HTTPS**, garantizando el cifrado del canal. Se prohíbe el uso de FTP plano.
- **Correo Electrónico:** El intercambio de información sensible por correo electrónico debe implementar mecanismos de cifrado de adjuntos o del mensaje (ej. S/MIME, IRM) o realizarse mediante enlaces seguros a repositorios institucionales (Google Drive) con permisos de acceso restringidos y expiración de enlace.

C. Interoperabilidad y Servicios Web (APIs)

- Las integraciones sistema a sistema (Machine-to-Machine) mediante Servicios Web (REST/SOAP) deben estar protegidas mediante:
  - **Autenticación Robusta:** Uso de tokens de seguridad (OAuth2, API Keys) y no credenciales de usuario final.
  - **Cifrado en Tránsito:** Uso obligatorio de TLS 1.2 o superior.
  - **Validación de Origen:** Restricción de direcciones IP autorizadas para consumir el servicio.

D. Intercambio mediante Medios Físicos y Portátiles

- Se debe minimizar el uso de medios físicos (USB, Discos Externos) para el transporte de información. Cuando sea estrictamente necesario e inevitable:
  - El dispositivo debe estar **cifrado por hardware o software** (ej. BitLocker).

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

- Se debe utilizar un mecanismo de entrega segura (correo certificado o mensajero de confianza) con acuse de recibo, asegurando la cadena de custodia.
- Las contraseñas de descifrado nunca deben enviarse junto con el medio físico; deben transmitirse por un canal alterno (ej. llamada telefónica, SMS).

E. Prevención de Fuga de Información (DLP)

- **INFOTEP** implementará, en la medida de lo posible, soluciones de Prevención de Pérdida de Datos (DLP) en el perímetro de la red y en los servicios de correo, para detectar y bloquear la transmisión no autorizada de datos sensibles (ej. patrones de números de cédula masivos) hacia dominios externos no confiables.

F. Mensajería Instantánea y Nube Personal

- Se prohíbe el uso de aplicaciones de mensajería instantánea personal (WhatsApp, Telegram) o servicios de almacenamiento en nube personal no federados (Dropbox personal, Google Drive personal) para el intercambio oficial de documentos institucionales clasificados como Confidenciales o Restringidos, debido a la falta de control y trazabilidad sobre dichos datos.

4.16 Política de Seguridad en la Cadena de Suministro (Proveedores)

INFOTEP entiende que la tercerización de servicios y el uso de proveedores tecnológicos son necesarios para su operación y modernización; sin embargo, establece que la responsabilidad sobre la seguridad de la información es intransferible. Por tanto, extenderá sus controles de seguridad hacia toda su cadena

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

de suministro, asegurando que los terceros operen bajo estándares homologables a los institucionales.

4.16.1. Objetivo

Establecer los lineamientos para asegurar la protección de los activos de información de INFOTEP que sean accesibles a los proveedores o que sean procesados por ellos. El fin es mitigar los riesgos asociados al acceso de terceros, garantizando que se mantengan los niveles acordados de seguridad de la información y prestación de servicios, y asegurando la integridad de la cadena de suministro tecnológica.

4.16.2. Lineamientos de la Política

A. Seguridad en la Selección y Contratación

- **Evaluación de Riesgos:** Antes de contratar cualquier servicio que implique acceso, procesamiento o almacenamiento de información institucional (ej. Servicios en Nube, Soporte de Software, Mensajería Masiva), el líder del proceso y la Oficina de TI deben realizar una evaluación de riesgos del proveedor.
- **Criterios de Selección:** La seguridad de la información será un criterio ponderable en los procesos de selección y licitación. Se privilegiará a proveedores que demuestren certificaciones vigentes (ISO 27001, SOC2 Tipo II) o madurez comprobable en ciberseguridad.

B. Aspectos de Seguridad en Acuerdos y Contratos

Todo contrato o acuerdo de nivel de servicio (ANS/SLA) con terceros debe incluir cláusulas de seguridad explícitas y vinculantes ("Anexo de Seguridad"), que abarquen:

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

- **Confidencialidad:** Firma obligatoria de Acuerdos de Confidencialidad (NDA) por parte del proveedor y su personal asignado.
- **Propiedad de la Información:** Declaración explícita de que los datos procesados pertenecen exclusivamente a **INFOTEP** y no pueden ser utilizados por el proveedor para fines propios (minería de datos, comercialización).
- **Cumplimiento Normativo:** Obligación del proveedor de cumplir con la Ley 1581 de 2012 (Protección de Datos) y reportar cualquier brecha de seguridad a **INFOTEP** en un tiempo máximo (ej. 4 a 24 horas).
- **Derecho a Auditar: INFOTEP** se reserva el derecho de auditar, o solicitar auditorías de terceros, sobre los controles de seguridad del proveedor.

C. Gestión de la Prestación del Servicio

- **Monitoreo y Revisión: INFOTEP** supervisará regularmente el cumplimiento de los requisitos de seguridad por parte del proveedor. Esto incluye la revisión de informes de servicio, reportes de incidentes y la validación de los niveles de disponibilidad (SLA) pactados.
- **Control de Cambios del Proveedor:** El proveedor debe notificar con antelación cualquier cambio en su infraestructura, ubicación geográfica de los datos o subcontratación que pueda impactar la postura de seguridad o el cumplimiento legal de **INFOTEP**.

D. Seguridad en la Cadena de Suministro de TIC

- Para la adquisición de hardware y software crítico, se exigirá a los proveedores garantías sobre la integridad del producto, asegurando que no ha sido manipulado ni contiene puertas traseras desde su fabricación hasta su entrega.

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

- Se prohíbe la adquisición de equipos o software que se encuentren en listas de exclusión por riesgos de seguridad nacional o ciberseguridad reconocidos internacionalmente.

E. Terminación del Servicio y Transición

- Los contratos deben definir claramente las obligaciones de seguridad a la finalización del servicio, incluyendo:
  - **Borrado Seguro:** Eliminación certificada de toda la información de **INFOTEP** de los sistemas del proveedor.
  - **Devolución de Activos:** Retorno de equipos, tokens o credenciales.
  - **Revocación de Accesos:** Deshabilitación inmediata de cuentas de usuario y conexiones VPN.

4.17 Política de Clasificación y Manejo de la Información

INFOTEP reconoce que la información es un activo heterogéneo y que no todos los datos requieren el mismo nivel de protección. Por tanto, establece un marco formal para categorizar la información según su valor, sensibilidad y criticidad, asegurando que los recursos de seguridad se apliquen de manera proporcional y efectiva, cumpliendo con los mandatos de la Ley 1712 de 2014 (Transparencia) y la Ley 1581 de 2012 (Habeas Data).

4.17.1. Objetivo

Proporcionar a los colaboradores, docentes, investigadores y terceros de INFOTEP un esquema estandarizado para la clasificación, etiquetado y manejo seguro de la información. El propósito es garantizar que cada activo de información reciba el nivel de protección adecuado durante todo su ciclo de vida (creación, almacenamiento,

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

transmisión y destrucción), evitando tanto la fuga de información sensible como la restricción innecesaria de información pública.

4.17.2. Lineamientos de la Política

A. Esquema de Clasificación de la Información

INFOTEP adoptará un esquema de clasificación de tres (3) niveles, alineado con la normativa colombiana y las mejores prácticas:

1. **Información Pública:** Información que puede ser divulgada sin restricciones a cualquier persona dentro o fuera de la institución (ej. oferta académica, estados financieros publicados, investigaciones de acceso abierto). Su divulgación no causa daño a la entidad.
2. **Información de Uso Interno:** Información relacionada con la operación, gestión y administración de **INFOTEP** cuyo acceso está limitado a los funcionarios y docentes para el ejercicio de sus funciones (ej. actas de comités internos, borradores de políticas, correos institucionales operativos). Su divulgación no autorizada podría causar impacto operativo o reputacional moderado.
3. **Información Restringida (Confidencial / Reservada):** Información crítica cuya divulgación no autorizada causaría daños graves a la institución, a terceros o violaría leyes vigentes. Incluye:
    - **Datos Personales Sensibles:** Historias clínicas, datos biométricos, situación socioeconómica de estudiantes.
    - **Propiedad Intelectual:** Resultados de investigaciones no publicadas.
    - **Seguridad:** Credenciales de acceso, configuraciones de seguridad de la red, llaves criptográficas.

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

B. Responsabilidad de Clasificación (Asset Owners)

- El **Propietario del Activo de Información** (Líder del Proceso que genera o custodia la información) es el único responsable de determinar la clasificación inicial del documento, base de datos o archivo, basándose en el impacto de una posible divulgación.
- La Oficina de TI proveerá las herramientas, pero no define la clasificación del contenido misional.

C. Etiquetado y Marcado de la Información

- Todo documento o medio digital que contenga información clasificada como **Uso Interno** o **Restringida** debe portar una etiqueta visual clara (marca de agua, encabezado o pie de página) que indique su nivel de clasificación.
- Los sistemas de información (ERP, LMS) deben configurarse para mostrar etiquetas de clasificación en las pantallas de entrada y reportes que contengan datos sensibles.

D. Manejo Seguro según Nivel de Clasificación

Se establecen controles diferenciados para cada nivel:

- **Almacenamiento:** La información **Restringida** debe almacenarse cifrada o en repositorios con control de acceso estricto (ACLs) y auditoría activada. Nunca debe almacenarse en nubes públicas no corporativas ni en equipos personales sin protección.
- **Transmisión:** La información **Restringida** debe transmitirse cifrada (correo cifrado, SFTP, HTTPS). La información de **Uso Interno** debe transmitirse por canales institucionales oficiales.
- **Impresión y Copia:** Se prohíbe la impresión desatendida de información **Restringida**. Las copias físicas deben ser limitadas al mínimo necesario y custodiadas bajo llave.

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

E. Reclasificación y Desclasificación

- La clasificación de la información no es estática. Los propietarios de la información deben revisar periódicamente (al menos una vez al año) si la clasificación asignada sigue siendo vigente.
- La información que pierda su sensibilidad (ej. una investigación una vez publicada) debe ser desclasificada a **Pública** para facilitar su difusión, siguiendo el principio de máxima publicidad de la Ley 1712.

F. Destrucción Segura de Información Clasificada

- Los medios físicos (papel) y digitales (discos duros, USB) que contengan información **Restringida** o de **Uso Interno** deben ser destruidos de manera que la información no pueda ser recuperada (triturado cruzado, desmagnetización o borrado seguro de datos), antes de su desecho o reasignación. No basta con el borrado simple o el reciclaje directo.

4.18 Política de Uso Responsable de Recursos Tecnológicos

INFOTEP provee recursos tecnológicos significativos para apoyar las actividades de docencia, investigación, extensión y administración. El uso de estos recursos es un privilegio, no un derecho, y conlleva la responsabilidad de utilizarlos de manera ética, legal y eficiente, evitando conductas que pongan en riesgo la seguridad de la información o la reputación institucional.

4.18.1. Objetivo

Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información de INFOTEP, estableciendo las reglas de comportamiento aceptable para el uso de los recursos tecnológicos asignados (hardware, software, correo

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

electrónico, acceso a internet y redes sociales), asegurando que sean utilizados principalmente para el cumplimiento de las funciones misionales y administrativas, y previniendo su uso para actividades ilícitas o no autorizadas.

4.18.2. Lineamientos de la Política

A. Principios Generales de Uso

- **Propiedad Institucional:** Todos los recursos tecnológicos (equipos de cómputo, tabletas, cuentas de usuario, datos almacenados) suministrados por **INFOTEP** son propiedad exclusiva de la institución.
- **Uso Aceptable:** Se autoriza el uso de los recursos para el desempeño de las funciones laborales y académicas. Se permite un uso personal incidental, esporádico y razonable, siempre que no interfiera con la productividad, no consuma recursos excesivos (ancho de banda, almacenamiento), no infrinja la ley y no viole las políticas de seguridad.
- **Prohibiciones Expresas:** Está estrictamente prohibido utilizar los recursos de **INFOTEP** para:
    - Actividades ilegales o que violen derechos de autor.
    - Acoso, discriminación, intimidación o difusión de material ofensivo (Ciberacoso).
    - Actividades comerciales personales o con fines de lucro ajenos a la institución.
    - Hacking, escaneo de puertos o ataques a sistemas internos o externos.

B. Uso de Servicios de Internet y Navegación

- **Filtrado de Contenido:** El acceso a Internet estará mediado por soluciones de seguridad perimetral (Proxy/Firewall) que bloquearán categorías de sitios web considerados de riesgo o inapropiados, tales como: pornografía,

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

apuestas, sitios de hacking, malware, y sitios que promuevan la violencia o el odio.

- **Consumo de Ancho de Banda:** Se priorizará el tráfico académico y administrativo crítico. Se restringirá o limitará el acceso a sitios de entretenimiento (streaming de video, música) y descarga masiva de archivos (P2P, Torrents) en la red administrativa y en horarios de alta demanda académica.

C. Uso del Correo Electrónico Institucional

- **Canal Oficial:** El correo electrónico con dominio @infotep.edu.co es el medio oficial de comunicación. Su uso es obligatorio para todas las comunicaciones formales.
- **Buenas Prácticas:**
  - No se debe utilizar la cuenta institucional para suscribirse a servicios personales no relacionados con la labor (ej. redes sociales personales, sitios de citas, comercio electrónico).
  - Está prohibido el envío de correos masivos no solicitados (SPAM) o cadenas de mensajes.
  - Se debe tener extrema precaución con los archivos adjuntos y enlaces de remitentes desconocidos para prevenir ataques de Phishing.

D. Uso de Software y Respeto a la Propiedad Intelectual

- **Licenciamiento:** Únicamente se permite la instalación y uso de software que cuente con el debido licenciamiento institucional o que sea Software Libre/Open Source autorizado por la Oficina de TI.
- **Instalación de Software:** Los usuarios no tienen permisos administrativos para instalar software en los equipos institucionales. Cualquier requerimiento de software adicional debe ser solicitado a la Mesa de Ayuda para su

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

evaluación técnica y de seguridad. La instalación de software "pirata" o "crackeado" es causal de falta grave.

E. Uso de Redes Sociales y Reputación Digital

- **Cuentas Institucionales:** Solo el personal autorizado por la Oficina de Comunicaciones puede crear o administrar cuentas de redes sociales a nombre de **INFOTEP**.
- **Publicación de Información:** Está prohibido publicar información clasificada como "Uso Interno" o "Restringida" (ej. fotos de documentos sensibles, datos de estudiantes) en redes sociales personales o institucionales.

F. Monitoreo y Privacidad

- **Derecho de Inspección: INFOTEP** se reserva el derecho de monitorear, acceder, revisar y grabar el uso de sus recursos tecnológicos (incluyendo correos electrónicos, archivos y logs de navegación) cuando existan indicios de violación a las políticas de seguridad, requerimientos legales o necesidades operativas críticas, siempre respetando el debido proceso y la dignidad del trabajador/estudiante.
- **Inexistencia de Expectativa de Privacidad:** Los usuarios deben ser conscientes de que no existe una expectativa de privacidad total sobre la información almacenada o transmitida a través de los activos de la institución.

4.19 Política de Control de Acceso Lógico

INFOTEP reconoce que el control de acceso es la primera línea de defensa lógica para proteger sus activos de información. Por tanto, implementará mecanismos técnicos y administrativos estrictos para garantizar que los usuarios solo tengan acceso a los recursos necesarios para el desempeño de sus funciones legítimas,

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

impidiendo el acceso no autorizado a los sistemas académicos, financieros y de investigación.

4.19.1. Objetivo

Definir las directrices generales para limitar y controlar el acceso lógico a la información, las instalaciones de procesamiento y los servicios tecnológicos de INFOTEP. El objetivo es prevenir el acceso no autorizado, asegurar que el acceso otorgado sea coherente con la política de clasificación de la información y garantizar la trazabilidad de las acciones realizadas por los usuarios en los sistemas institucionales.

4.19.2. Lineamientos de la Política

A. Principios de Control de Acceso

- **Mínimo Privilegio:** A los usuarios se les otorgarán únicamente los permisos mínimos necesarios para realizar sus tareas laborales o académicas. El acceso "por defecto" debe ser denegado.
- **Necesidad de Saber:** El acceso a la información sensible se otorgará solo si es indispensable para la función del usuario, independientemente de su jerarquía en la institución.
- **Segregación de Funciones:** Se evitará otorgar permisos combinados que puedan generar conflictos de interés o riesgos de fraude (ej. la persona que solicita un pago no debe tener permisos para aprobarlo en el sistema financiero).

B. Gestión del Ciclo de Vida de Usuarios

- **Registro y Alta:** La creación de cuentas de usuario (ID) requiere una solicitud formal aprobada por el jefe inmediato o la autoridad académica

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

competente (Registro y Control). Se debe verificar la identidad del usuario antes de entregar las credenciales.

- **Modificación de Derechos:** Cuando un funcionario o docente cambie de cargo o funciones, sus derechos de acceso deben ser revisados y ajustados de inmediato para reflejar su nueva realidad, eliminando los permisos del cargo anterior.
- **Baja y Eliminación:** La Oficina de Talento Humano y Admisiones deben notificar a TI sobre la desvinculación de empleados o la deserción/graduación de estudiantes de manera inmediata. Las cuentas deben ser deshabilitadas el mismo día de la terminación del vínculo.

C. Gestión de Contraseñas y Autenticación

- **Complejidad:** Se exigirá el uso de contraseñas robustas (mínimo 8-12 caracteres, combinando mayúsculas, minúsculas, números y símbolos) para todos los sistemas.
- **Confidencialidad:** Las contraseñas son personales e intransferibles. Está prohibido compartirlas, escribirlas en lugares visibles o almacenarlas en scripts sin cifrar.
- **Rotación:** Los sistemas forzarán el cambio periódico de contraseñas (ej. cada 90 días para administrativos, cada semestre para estudiantes) y evitarán la reutilización de contraseñas antiguas.
- **Autenticación Multifactor (MFA):** Se implementará obligatoriamente el doble factor de autenticación (2FA) para el acceso a cuentas con privilegios administrativos, acceso remoto (VPN) y sistemas críticos expuestos a internet.

D. Gestión de Privilegios Especiales (Administradores)

- El uso de cuentas con privilegios de "Administrador" o "Root" se restringirá al mínimo número de personas posible (personal de TI autorizado).

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

- Estas cuentas no deben usarse para tareas cotidianas (leer correo, navegar en internet). Los administradores deben tener una cuenta estándar para uso diario y una cuenta administrativa separada para tareas de gestión.
- Todas las actividades realizadas con cuentas privilegiadas deben ser registradas y monitoreadas.

E. Revisión de Derechos de Acceso

- Los propietarios de los sistemas de información y la Oficina de TI realizarán revisiones periódicas (mínimo semestrales) de los derechos de acceso asignados, para detectar y eliminar cuentas huérfanas, permisos excesivos o accesos de personal que ya no labora en la entidad.

F. Control de Acceso a Aplicaciones y Código Fuente

- El acceso a los códigos fuente de las aplicaciones institucionales y a las herramientas de administración de bases de datos estará estrictamente restringido al personal de desarrollo y administración de bases de datos, respectivamente, y protegido mediante controles de acceso fuertes.

4.20 Política de Seguridad para Servicios en la Nube

INFOTEP entiende la computación en la nube (Cloud Computing) como un habilitador estratégico para la escalabilidad de sus servicios académicos y de investigación. Sin embargo, la migración a la nube no exime a la institución de su responsabilidad sobre la custodia de la información. Por tanto, se establecen controles para gestionar los riesgos derivados de procesar y almacenar datos institucionales en infraestructuras de terceros.

4.20.1. Objetivo

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

Definir los requisitos técnicos, legales y administrativos para la adopción, uso y gestión segura de servicios en la nube (SaaS, PaaS, IaaS) en INFOTEP. El propósito es maximizar los beneficios de la nube reduciendo el riesgo de pérdida de gobierno sobre los datos, accesos no autorizados, incumplimiento normativo (Ley 1581) o dependencia tecnológica excesiva.

4.20.2. Lineamientos de la Política

A. Evaluación de Riesgos y Selección de Servicios

- **Prohibición de "Shadow IT":** Está estrictamente prohibido que las áreas académicas o administrativas contraten o utilicen servicios en la nube para procesar información institucional sin la evaluación técnica previa de la Oficina de TI y la aprobación del Oficial de Seguridad Digital.
- **Clasificación Previa:** Antes de migrar cualquier servicio a la nube, se debe evaluar la sensibilidad de la información. La información clasificada como "Restringida" o "Datos Sensibles" (ej. historias académicas, investigaciones patentables) requiere controles de cifrado gestionados por **INFOTEP** antes de subir a la nube pública.

B. Modelo de Responsabilidad Compartida

- Para cada servicio en la nube contratado, se debe documentar claramente la matriz de responsabilidad compartida, delimitando qué controles de seguridad son responsabilidad del proveedor (ej. seguridad física del Data Center, parcheo del Hypervisor) y cuáles son responsabilidad exclusiva de **INFOTEP** (ej. gestión de usuarios, cifrado de datos, configuración de firewalls virtuales).

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

C. Soberanía de Datos y Cumplimiento Legal

- **Ubicación de los Datos: INFOTEP** privilegiará proveedores de nube que ofrezcan zonas de disponibilidad en Colombia o en países declarados con niveles "adecuados" de protección de datos por la Superintendencia de Industria y Comercio (SIC).
- **Propiedad:** Los contratos deben estipular explícitamente que la propiedad intelectual y los datos alojados pertenecen única y exclusivamente a **INFOTEP**, y que el proveedor no tiene derecho a utilizarlos para fines comerciales, minería de datos o publicidad.

D. Control de Acceso y Gestión de Identidades

- **Autenticación Robusta:** El acceso a consolas de administración de la nube (ej. Azure Portal, AWS Console, Admin de Google Workspace/Office 365) debe estar protegido obligatoriamente con **Autenticación Multifactor (MFA)**.
- **Federación:** En la medida de lo posible, la autenticación de usuarios finales debe federarse con el directorio institucional de **INFOTEP** (SSO - Single Sign-On) para centralizar el control de acceso y asegurar la revocación inmediata de permisos ante retiros.

E. Protección de Datos en la Nube (Segregación y Cifrado)

- **Segregación:** En entornos de nube pública multi-inquilino, se debe verificar que el proveedor garantice la segregación lógica efectiva para evitar que otros clientes accedan a los datos de **INFOTEP**.
- **Cifrado:** La información sensible debe estar cifrada tanto en tránsito (TLS/SSL) hacia la nube como en reposo (AES-256) dentro de los sistemas de almacenamiento del 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

F. Estrategia de Salida y Portabilidad

- Para evitar el secuestro tecnológico, todo contrato de servicios en la nube debe incluir cláusulas de salida que garanticen:
  - La devolución íntegra de los datos de **INFOTEP** en formatos estándar e interoperables (ej. CSV, SQL, JSON) al finalizar el contrato.
  - El borrado seguro y certificado de los datos en los discos del proveedor tras la migración.
  - Un periodo de transición razonable para migrar a otro proveedor o retornar a infraestructura local (On-premise).

G. Monitoreo y Auditoría en la Nube

- Se deben activar y revisar periódicamente los registros de auditoría (CloudTrail, Activity Logs) proporcionados por el servicio de nube, para detectar accesos anómalos, cambios de configuración no autorizados o descargas masivas de información.

4.21 Política de Gestión de Activos de Información

INFOTEP reconoce que la información, junto con los procesos y sistemas que la soportan, son activos fundamentales para su operación. Para protegerlos adecuadamente, primero es necesario saber qué se tiene, dónde está, quién es el responsable y qué valor aporta a la institución. Esta política establece las reglas para el inventario y control del ciclo de vida de los activos.

4.21.1. Objetivo

Garantizar la identificación, inventario, clasificación y control de todos los activos de información relevantes para el ciclo de vida de los procesos de INFOTEP. El

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

propósito es asignar responsabilidades claras de protección (propiedad), asegurar un nivel de seguridad acorde con la importancia del activo y prevenir el uso no autorizado, la pérdida o la modificación indebida de la información institucional almacenada en medios físicos o digitales.

4.21.2. Lineamientos de la Política

A. Inventario de Activos

- **Identificación: INFOTEP** mantendrá un inventario unificado y actualizado de todos sus activos de información. Esto no se limita al hardware (servidores, portátiles), sino que incluye:
    - **Activos de Información (Datos):** Bases de datos de estudiantes, resultados de investigación, expedientes financieros, software, contratos.
    - **Activos Físicos:** Equipos de cómputo, medios de comunicación, equipos de soporte (UPS, aire acondicionado).
    - **Activos de Servicio:** Servicios de conectividad, servicios en la nube, suministro eléctrico.
    - **Activos Humanos:** Personal con conocimientos críticos o acceso a información confidencial.
- **Mantenimiento:** El inventario debe revisarse y actualizarse periódicamente (mínimo una vez al año) o cuando ocurran cambios significativos (adquisiciones, bajas, cambios de proceso).

B. Propiedad de los Activos

- **Asignación de Responsable:** Todo activo de información identificado en el inventario debe tener un **"Propietario"** asignado. El propietario es el cargo o rol (no la persona específica) responsable de garantizar la clasificación y protección del activo a lo largo de su ciclo de vida.

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

- **Ejemplos de Propiedad:**
  - El *Propietario* de la Base de Datos de Notas es el Director de Registro y Control, no el Ingeniero de TI que administra el servidor (quien actúa como *Custodio*).
  - El *Propietario* de los datos de un proyecto de investigación es el Líder del Grupo de Investigación.

C. Uso Aceptable de los Activos

- Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y de los activos asociados a ella.
- Los usuarios que utilizan o tienen custodia de activos de información deben seguir las directrices de protección establecidas por el propietario del activo y la Oficina de TI (ej. no sacar equipos del campus sin autorización, no instalar software no autorizado).

D. Devolución de Activos

- Todos los empleados, docentes y contratistas deben devolver todos los activos institucionales que estén en su poder (equipos portátiles, teléfonos, tokens de autenticación, tarjetas de acceso, llaves y documentación técnica) al finalizar su contrato o acuerdo laboral.
- La Oficina de Talento Humano y la Oficina de Bienes/Almacén deben coordinar el proceso de paz y salvo para verificar la devolución íntegra antes de la liquidación final.

E. Gestión de Medios de Almacenamiento Removibles

- **Restricción:** Se restringirá el uso de medios extraíbles (memorias USB, discos duros externos) en equipos que procesen información crítica, para prevenir la fuga de datos o la infección por malware.

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

- **Cifrado:** Si es operativamente necesario el uso de medios removibles para el transporte de información institucional (ej. investigadores en trabajo de campo), dichos medios deben estar cifrados.
- **Borrado Seguro:** Antes de reutilizar, reasignar o desechar cualquier medio de almacenamiento (discos duros de computadores dados de baja, USBs), se debe realizar un proceso de borrado seguro o destrucción física para asegurar que la información contenida no pueda ser recuperada.

F. Movimiento Físico de Activos

- Los equipos, información o software no deben salir de las instalaciones de **INFOTEP** sin la debida autorización previa.
- El traslado de activos críticos (ej. servidores, equipos de red) debe contar con medidas de seguridad física adecuadas durante el transporte y un registro formal de la cadena de custodia.

5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- **SENSIBILIZACIÓN Y COMUNICACIÓN**

INFOTEP, definirá un "**Plan de Comunicación en Seguridad de la Información"** a través de su oficina de comunicación interna y externa y la Oficina TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación

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

de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

- **CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN**

INFOTEP, a través de sus áreas/procesos de Talento Humano y Contratación, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, la oficina y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones. La entidad implementara las estrategias adecuadas para crear y fortalecer una cultura, cambio y apropiación de Seguridad de la información, lo cual implica un cambio en el comportamiento de los colaboradores en relación a las políticas y directrices que deben cumplir. Esto debe generar la identificación de perfiles de conocimiento, público objetivo, temáticas identificadas para el año, y finalmente la medición de esta gestión.

6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del 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

7. SANCIONES

La política de Seguridad de la información que se adopte al interior de la entidad deberá estar sustentada por un acto administrativo.

La falta de conocimiento de los presentes lineamientos no libera al personal de **INFOTEP** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. La oficina de tecnologías de la información y las comunicaciones será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, la oficina TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

8. INFORMACIÓN DE CONTACTO

Cualquier inquietud relacionada con las políticas, favor remitirla al correo seguridaddigital@infotepsai.edu.co.

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

9. APROBACIÓN Y REVISIÓN DEL MANUAL DE POLÍTICAS

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

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA VIGENCIA**	**NATURALEZA DEL CAMBIO**
01	6/11/2025	Creación de documento manual de políticas

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