## POLÍTICA GENERAL DE SEGURIDAD DIGITAL - TIC PARA LA GESTIÓN

**OBJETIVO**: Contrarrestar el incremento de las amenazas informáticas que afecten significativamente el uso de las TIC en el desempeño de las labores administrativas y misionales de la entidad, y afrontar retos en aspectos de seguridad cibernética, para crear un ambiente y unas condiciones que brinden protección en el ciberespacio, integridad, confidencialidad y la disponibilidad de la información que trata el Instituto Departamental de Antioquia “Indeportes”.

## POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”, con la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN” SGSI” estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”
- Garantizar la continuidad del negocio frente a incidentes.

El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de Seguridad que Soportan el Sistema de Gestión de Seguridad de la Información “SGSI” del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá su información de las amenazas originadas por parte del personal.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá el Data Center, Centros de Cableado y la infraestructura tecnológica que soporta sus procesos críticos.
- EL INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” implementará control de acceso a la información, sistemas y recursos de red.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## FORMATO DE POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del _INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

Minimizar el riesgo de los procesos misionales de la entidad.

- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”
- Garantizar la continuidad del negocio frente a incidentes

**Alcance/Aplicabilidad:**

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” y la ciudadanía en general.

**Nivel de cumplimiento:**

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen las 12 políticas generales de seguridad que soportan el SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN “SGSI” del INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES”:

- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá su información de las amenazas originadas por parte del personal.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” protegerá el Data Center, Centros de Cableados y la infraestructura tecnológica que soporta sus procesos críticos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” implementará control de acceso a la información, sistemas y recursos de red.

- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- El INSTITUTO DEPARTAMENTAL DE ANTIOQUIA “INDEPORTES” garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere

## POLITICAS ESPECÍFICAS PARA IMPLEMENTAR CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN

Para la implementación de controles en la seguridad de la información nos basaremos en el anexo 5A de la Norma Internacional ISO27001 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN “SGSI”, de la cual tanto en Modelo Integral de Planeación y Gestión “MIPG” como el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia “MINTIC” toman como referencia en materia de Gobierno Digital y seguridad Digital.

Anexo Controles según iso27001, son 14 controles Principales con sus respectivos sub niveles:

1. **POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**
    - 1.1. Orientación de la dirección para la gestión de la seguridad de la información
        - 1.1.1. Políticas para la seguridad de la Información
        - 1.1.2. Revisión de las políticas para la seguridad de la información
2. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
    - 2.1. Organización interna
        - 2.1.1. Roles y responsabilidades para la seguridad de la seguridad de la información
        - 2.1.2. Separación de deberes
        - 2.1.3. Contacto con las autoridades
        - 2.1.4. Contacto con grupos de interés especial
        - 2.1.5. Seguridad de la información en la gestión de proyectos
    - 2.2. Dispositivos móviles y teletrabajo
        - 2.2.1. Política para dispositivos móviles
        - 2.2.2. Teletrabajo
3. **SEGURIDAD DE LOS RECURSOS HUMANOS**
    - 3.1. Antes de asumir el empleo
        - 3.1.1. Selección
        - 3.1.2. Términos y condiciones del empleo
    - 3.2. Durante la ejecución del empleo

- 3.2.1. 2.2.1. Responsabilidad de la dirección
- 3.2.2. Toma de conciencia, educación y formación en la seguridad de la información
- 3.2.3. Proceso disciplinario

3.3. Terminación y cambio de empleo

- 3.3.1. Terminación o cambio de responsabilidades de empleo

**4. GESTION DE ACTIVOS**

4.1. Responsabilidad de activos

- 4.1.1. Inventario de los activos
- 4.1.2. Propiedad de los activos
- 4.1.3. Uso aceptable de los activos
- 4.1.4. Devolución de activos

4.2. Clasificación de la información

- 4.2.1. Clasificación de la información
- 4.2.2. Etiquetado de la información
- 4.2.3. Manejo de activos

4.3. Manejo de medios

- 4.3.1. Gestión de medios removibles
- 4.3.2. Disposición de los medios
- 4.3.3. Transferencia de medios físicos

**5. CONTROL DE ACCESO**

5.1. Requisitos del negocio para el control de acceso

- 5.1.1. Política de control de acceso
- 5.1.2. Acceso a redes y a servicios de red

5.2. Gestión de acceso de usuarios

- 5.2.1. Registro y cancelación de registro de usuarios
- 5.2.2. Suministro de acceso de usuarios
- 5.2.3. Gestión de derechos de acceso privilegiado
- 5.2.4. Gestión de información de autenticación secreta de usuario
- 5.2.5. Revisión de los derechos de acceso de usuarios
- 5.2.6. Retiro o ajuste de los derechos de acceso

5.3. Responsabilidad de los usuarios

- 5.3.1. Uso de información de autenticación secreta

5.4. Control de acceso a sistemas y aplicaciones

- 5.4.1. Restricciones de acceso a la información
- 5.4.2. Procedimiento de ingreso seguro
- 5.4.3. Sistema de gestión de contraseñas
- 5.4.4. Uso de programas utilitarios privilegiados
- 5.4.5. Control de acceso a códigos fuente de programas

**6. CRIPTOGRAFIA**

6.1. Controles criptográficos

- 6.1.1. Política sobre uso de controles criptográficos
- 6.1.2. Gestión de llaves

**7. SEGURIDAD FÍSICA Y DEL ENTORNO**

7.1. Áreas seguras

- 7.1.1. Perímetro de seguridad física
- 7.1.2. Control de accesos físicos
- 7.1.3. Seguridad de oficinas, recintos e instalaciones
- 7.1.4. Protección contra amenazas externas y ambientales

7.1.5. Trabajo en áreas seguras
7.1.6. Áreas de despacho y carga
7.2. Equipos
7.2.1. Ubicación y protección de los equipos
7.2.2. Servicios de suministro
7.2.3. Seguridad del cableado
7.2.4. Mantenimientos de equipos
7.2.5. Retiros de activos
7.2.6. Seguridad de equipos y activos fuera de las instalaciones
7.2.7. Disposición segura o reutilización de equipos
7.2.8. Equipos de usuario desatendido
7.2.9. Política de escritorio limpio y pantalla limpia
**8. SEGURIDAD DE LAS OPERACIONES**
8.1. Procedimientos operacionales y responsabilidades
8.1.1. Procedimientos de operación documentados
8.1.2. Gestión de cambios
8.1.3. Gestión de capacidad
8.1.4. Separación de los ambientes de desarrollo, prueba y operación
8.2. Protección contra códigos maliciosos
8.2.1. Controles contra códigos maliciosos
8.3. Copias de respaldo
8.3.1. Respaldo de la información
8.4. Registro y seguimiento
8.4.1. Registro de eventos
8.4.2. Protección de la información de registro
8.4.3. Registro del administrador y del operador
8.4.4. Sincronización de relojes
8.5. Control de software operacional
8.5.1. Instalación de software en sistemas operativos
8.6. Gestión de vulnerabilidad técnica
8.6.1. Gestión de la vulnerabilidad técnica
8.6.2. Restricciones sobre la instalación de software
8.7. Consideraciones sobre auditorías de sistemas de información
8.7.1. Controles de auditorías de sistemas de información
**9. SEGURIDAD DE LAS COMUNICACIONES**
9.1. Gestión de la seguridad de las redes
9.1.1. Controles de redes
9.1.2. Seguridad de los servicios de red
9.1.3. Separación en las redes
9.2. Transferencia de información
9.2.1. Políticas y procedimientos de transferencia de información
9.2.2. Acuerdos sobre transferencia de información
9.2.3. Mensajería electrónica
9.2.4. Acuerdos de confidencialidad o de no divulgación
**10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
10.1. Requisitos de seguridad de los sistemas de información
10.1.1. Análisis y especificación de requisitos de seguridad de la información
10.1.2. Seguridad de servicios de las aplicaciones en redes públicas

10.1.3. Protección de transacciones de los servicios de las aplicaciones
10.2. Seguridad en los procesos de desarrollo y de soporte
10.2.1. Políticas de desarrollo seguro
10.2.2. Procedimientos de control de cambios en sistemas
10.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
10.2.4. Restricciones en los cambios a los paquetes de software
10.2.5. Principios de construcción de los sistemas seguros
10.2.6. Ambientes de desarrollo seguro
10.2.7. Desarrollo contratado externamente
10.2.8. Pruebas de seguridad de sistemas
10.2.9. Prueba de aceptación de sistemas
10.3. Datos de prueba
10.3.1. Protección de datos de prueba
**11. RELACIONES CON LOS PROVEEDORES**
11.1. Seguridad de la información en las relaciones con los proveedores
11.1.1. Políticas de seguridad de la información para las relaciones con proveedores
11.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores
11.1.3. Cadena de suministro de tecnología de información y comunicación
11.2. Gestión de la prestación de servicios de proveedores
11.2.1. Seguimiento y revisión de los servicios de los proveedores
11.2.2. Gestión de cambios en los servicios de los proveedores
**12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
12.1. Gestión de incidentes y mejoras en la seguridad de la información
12.1.1. Responsabilidades y procedimientos
12.1.2. Reportes de eventos de seguridad de la información
12.1.3. Reportes de debilidades de seguridad de la información
12.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos
12.1.5. Respuesta a incidentes de seguridad de la información
12.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información
12.1.7. Recolección de evidencia
**13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**
13.1. Continuidad de seguridad de la información
13.1.1. Planificación de la continuidad de la seguridad de la información
13.1.2. Implementación de la continuidad de la seguridad de la información
13.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información
13.2. Redundancias
13.2.1. Disponibilidad de instalaciones de procesamiento de información
**14. CUMPLIMIENTOS**
14.1. Cumplimiento de requisitos legales y contractuales

14.1.1. Identificación de la legislación aplicable y de los requisitos contractuales
14.1.2. Derechos de propiedad intelectual
14.1.3. Protección de registros
14.1.4. Privacidad y protección de información de datos personales
14.1.5. Reglamentación de controles criptográficos

14.2. Revisiones de seguridad de la información
14.2.1. Revisión independiente de la seguridad de la información
14.2.2. Cumplimiento con las políticas y normas de seguridad
14.2.3. Revisión del cumplimiento técnico

**Nota**: Es posible que algunos de estos controles no sean necesarios implementar y otros ya estén implementados y solo sea documentar y estandarizar.