



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

POLÍTICA DE SEGURIDAD DIGITAL

MARIO FERNANDO DÍAZ PAVA
Rector

DIANA MARILY RODRIGUEZ RICAURTE
Asesor de Planeación

Diseño y elaboración:
YULI SHIRLEY GUARNIZO GARZON
Ingeniera de Sistemas

Espinal – 2026





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

CONTENIDO

1. INTRODUCCION	2
2. OBJETIVOS	2
3. ALCANCE	2
4. MARCO NORMATIVO.....	3
5. DEFINICIONES	6
6. CONTROLES Y POLITICAS.....	8
7. CONTROLES DE PERSONAS.....	13
8. CONTROLES FISICOS.....	13
9. CONTROLES TECNOLOGICOS	14
10. POLITICAS ESPECIFICAS	16
11. RESPONSABILIDADES.....	17
12. ROLES Y RESPONSABILIDADES	20
13. PLAN DE IMPLEMENTACION	21
14. CRONOGRAMA.....	24

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

1. INTRODUCCIÓN

La información es un activo estratégico para el Instituto Tolimense de Formación Técnica Profesional (ITFIP). Su adecuada protección es fundamental para garantizar la continuidad de los procesos académicos, administrativos y de investigación, así como para asegurar la confianza de estudiantes, docentes, funcionarios y demás partes interesadas.

La presente Política de Seguridad Digital se formula en cumplimiento de los lineamientos institucionales y de la normativa vigente en Colombia, alineada con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y con el estándar internacional ISO/IEC 27001, con el fin de establecer un marco claro para la gestión de la seguridad de la información.

2. OBJETIVOS

2.1 Objetivo General

Establecer los lineamientos, responsabilidades y controles necesarios para proteger la información del ITFIP, garantizando su confidencialidad, integridad y disponibilidad, frente a amenazas internas y externas.

2.2 Objetivos Específicos

- Proteger los activos de información del ITFIP frente a accesos no autorizados, pérdida, alteración o divulgación indebida.
- Definir roles y responsabilidades en materia de seguridad digital.
- Cumplir con la normativa legal y regulatoria aplicable en Colombia.
- Fortalecer la gestión de incidentes de seguridad de la información.
- Asegurar la continuidad de los servicios institucionales ante eventos disruptivos.
- Promover una cultura de seguridad digital en la comunidad institucional.

3. ALCANCE

Esta política aplica a:

- Todos los funcionarios, docentes, contratistas, estudiantes y terceros que tengan acceso a la información y a los sistemas del ITFIP.
- Toda la información generada, procesada, almacenada o transmitida por el ITFIP, independientemente de su formato (digital, físico o verbal).

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592

Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

- Todos los activos tecnológicos, sistemas de información, redes, aplicaciones, dispositivos y servicios asociados.

4. MARCO NORMATIVO APLICABLE

La presente política se rige, los siguientes marcos normativos y de referencia:

NORMA	DESCRIPCION
Ley 23 1982	Sobre Derechos de Autor.
Ley 80 1993	Por la cual se expide el Estatuto General de Contratación de la Administración PÚBLICA.
Ley 1341 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1581 2012	Por el cual se dictan disposiciones generales para la protección de datos personales. HABEAS DATA.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Modificado en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de las Políticas de Gobierno Digital y Seguridad Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que las Políticas de Gobierno Digital y Seguridad Digital ÚLTIMA FECHA DE ACTUALIZACIÓN: 22 DE AGOSTO DE 2023.
Decreto 1414 de 2017	A través del cual se modificó la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones, asignando a la Dirección de Gobierno Digital, antes "Dirección de Gobierno en Línea"
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Directiva presidencial de 2019	Simplificación de la interacción digital entre los ciudadanos y el estado.
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

CONPES 3995 de 2020	Política nacional de confianza y seguridad digital.
Resolución 2893 2020	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones.
Resolución 1519 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Decreto 338 2022	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Resolución 460 de 2022	Por lo cual se expide el plan nacional de infraestructura de datos y su hoja de ruta en el desarrollo de la política de Gobierno Digital y se dictan los lineamientos generales para su implementación.
Decreto 1263 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Ley 2294 2023	Por la cual se expide el Plan Nacional de Desarrollo 2022-2026 “Colombia Potencia Mundial de la Vida” establece en su artículo 43 las medidas que implementará el Ministerio de las Tecnologías de la Información y las comunicaciones entre las que se encuentra el Fortalecimiento del Gobierno digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima



SC6793-1



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

	través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.
--	---

5. DEFINICIONES

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Documento CONPES 3854).

Ataque cibernético: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Documento Modelo Nacional Riesgo de Seguridad Digital).

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (Documento CONPES 3854).

Ciberespionaje: Es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas. (Documento CONPES 3854).

Ciberterrorismo: Es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo. (Documento CONPES 3854)

Ciberdelito (delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (Documento CONPES 3854).

Ciberlavado: Es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (Documento CONPES 3854).

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

(Documento CONPES 3854). Riesgo: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

Resiliencia: Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).

Seguridad de la información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

Seguridad digital o ciberseguridad: Conjunto de medidas de “Protección de



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Documento CONPES 3854).

6. CONTROLES Y POLITICAS

Política de Gestión de Activos

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Direccionamiento del Plan Estratégico Planeación, con el acompañamiento permanente del Grupo Interno de Trabajo de Sistemas, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y uso adecuado de los activos de información, con el objetivo de garantizar su protección.

1. **Inventario de Activos:** Los activos de información del Instituto Tolimense de Formación Técnica Profesional – ITFIP deberán ser identificados, clasificados, valorados y controlados, con el fin de garantizar su adecuado uso, protección y recuperación ante incidentes y desastres.

Para tal efecto, el ITFIP diseñará e implementará una metodología institucional que establezca los lineamientos necesarios para la gestión del inventario de activos de información, el cual deberá estar discriminado, como mínimo, por proceso y dependencia, tipo de activo, nivel de criticidad, clasificación de la información, ubicación, responsable, custodio y demás atributos que la institución defina.

2. **Protección:** Con el objetivo de establecer y aplicar los controles de seguridad físicos y digitales, las dependencias que tengan la custodia de la información generada en el marco de sus funciones serán responsables de proteger los activos de información, así como de mantener y actualizar el inventario de los activos relacionados con la prestación de sus servicios, incluyendo información física y digital, software, hardware y recurso humano.
Estas actividades se desarrollarán conforme a los lineamientos definidos por el Grupo Interno de Trabajo de Sistemas del ITFIP.

3. **Archivos de Gestion:** El Direccionamiento del Plan Estratégico y





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

Planeación, en coordinación con las dependencias responsables, deberá implementar los controles necesarios para garantizar que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de conformidad con las Tablas de Retención Documental (TRD) y las Tablas de Control de Acceso institucionales.

Lo anterior con el fin de proteger y preservar la confidencialidad, integridad y disponibilidad de la información física del ITFIP.

4. **Clasificación de la información:** El Direccionamiento del Plan Estratégico y Planeación, en coordinación con el Grupo Interno de Trabajo de Sistemas, implementará los mecanismos necesarios para la clasificación y rotulado de la información física y digital, de acuerdo con la metodología institucional de clasificación de la información establecida por el ITFIP.

Dichos mecanismos permitirán identificar el nivel de sensibilidad de la información y definir los controles de seguridad adecuados para su manejo, almacenamiento, transmisión y conservación.

Las firmas de los documentos que produzca el Instituto Tolimense de Formación Técnica Profesional – ITFIP serán válidas cuando se realicen mediante cualquiera de los siguientes mecanismos, garantizando en todo momento la confiabilidad, integridad, autenticidad y disponibilidad de la información y de los documentos expedidos por los servidores públicos y contratistas, en el marco de sus funciones y obligaciones:

- **Firma Manuscrita**

Firma realizada de forma autógrafa sobre documentos físicos, la cual será válida siempre que se asegure la custodia, integridad y conservación del documento conforme a las Tablas de Retención Documental (TRD) y los controles de acceso definidos por la institución.

- **Firma Escaneada**

Imagen digital de una firma manuscrita incorporada a un documento electrónico, utilizada para trámites internos de bajo riesgo, bajo los controles y lineamientos definidos por el Grupo Interno de Trabajo de Sistemas, sin perjuicio de las restricciones legales aplicables.

- **Firma Electrónica**

Mecanismo de identificación electrónica que permite vincular a una persona con un documento o mensaje de datos,



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

garantizando su autenticidad e integridad, de conformidad con la normativa vigente y los lineamientos institucionales del ITFIP.

- Firma Digital

Tipo de firma electrónica que utiliza un certificado digital emitido por una entidad de certificación acreditada, garantizando altos niveles de seguridad, integridad, autenticidad y no repudio, conforme a la legislación colombiana vigente.

El uso de cada tipo de firma deberá ajustarse al nivel de criticidad del documento, a su clasificación de la información y a los riesgos asociados según lo establecido por Direccionamiento del Plan Estratégico Planeación

Política de control de acceso

Los propietarios de los activos de información del Instituto Tolimense de Formación Técnica Profesional – ITFIP, teniendo en cuenta el tipo de activo, deberán establecer y aplicar medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios tecnológicos (en modalidad *on premise* o en la nube) e infraestructura física (instalaciones, oficinas y áreas restringidas). Estas medidas tendrán como finalidad mitigar los riesgos asociados al acceso no autorizado a la información, a la infraestructura tecnológica y a la infraestructura física, contribuyendo a salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional.

Los controles de acceso deberán definirse y gestionarse conforme a los lineamientos establecidos por el Grupo Interno de Trabajo de Sistemas, en coordinación con el Direccionamiento del Plan Estratégico Planeación.

política de Seguridad para la Relación con Proveedores

El Instituto Tolimense de Formación Técnica Profesional – ITFIP establecerá, a través del manual de contratación y demás disposiciones institucionales aplicables, los lineamientos necesarios para asegurar que la información que se genere, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión de contratos, convenios o acuerdos, sea tratada conforme a los principios de seguridad y privacidad de la información.

Así mismo, mediante el seguimiento a la ejecución contractual, se garantizará que los supervisores o responsables de los contratos, convenios o acuerdos apliquen y hagan cumplir las políticas y procedimientos de seguridad de la información durante toda su ejecución.

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

Estos lineamientos deberán ser comunicados oportunamente a los proveedores y terceros, a través de los canales institucionales dispuestos por el ITFIP, y su cumplimiento será de carácter obligatorio.

Política de Gestión de Incidentes de Seguridad y Privacidad de la Información

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Responsable de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los servidores públicos y contratistas el reporte oportuno, seguimiento y tratamiento de los incidentes relacionados con la seguridad y privacidad de la información.

El ITFIP asignará los responsables para la gestión de los incidentes, quienes se encargarán de su análisis, investigación, atención y cierre, de acuerdo con los procedimientos institucionales establecidos.

La Alta Dirección del ITFIP o su delegado será la única instancia autorizada para realizar pronunciamientos oficiales y reportes de incidentes ante autoridades competentes, entes de control, medios de comunicación y terceros externos, conforme a la normativa vigente y a los actos administrativos que correspondan.

Política de Continuidad de la Operación de los Servicios

El Instituto Tolimense de Formación Técnica Profesional – ITFIP dispondrá los planes necesarios para garantizar la continuidad de la operación de sus servicios, los cuales serán ejecutados por los líderes de los procesos institucionales.

El Responsable de Seguridad y Privacidad de la Información, en conjunto con el Direccionamiento del Plan Estratégico y Planeación, liderará la elaboración y actualización del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de la Operación de los Servicios (BCP).

El Plan de Continuidad de los Servicios del ITFIP incluirá el Plan de Continuidad de Tecnologías de la Información, así como los Planes de Emergencia y Contingencia, y demás estrategias orientadas a asegurar la continuidad de la prestación del servicio institucional.

El Grupo Interno de Trabajo de Sistemas será responsable de liderar, implementar y mantener actualizado el Plan de Continuidad de las TIC o Plan de Recuperación ante Desastres Tecnológicos (DRP), alineado con el BIA y el BCP, incorporando escenarios de falla, estrategias de recuperación, roles y responsabilidades, planes de comunicación y pruebas periódicas, con el fin de garantizar la disponibilidad y acceso

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

oportuno a los sistemas, datos y aplicaciones críticas ante eventos disruptivos.

Política Legal y de Cumplimiento

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Responsable de Seguridad y Privacidad de la Información o quien haga sus veces, velará por la identificación, documentación, actualización y cumplimiento de los requisitos legales y regulatorios relacionados con la seguridad y privacidad de la información, de conformidad con lo establecido por el Gobierno Nacional y la normativa vigente.

Dentro de estos requisitos se incluyen, entre otros, los relacionados con derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública y demás disposiciones aplicables. Para tal fin, el ITFIP dispondrá de una Matriz de Requisitos Legales, como instrumento de control, seguimiento y verificación de cumplimiento. Así mismo, el ITFIP establecerá, divulgará y mantendrá actualizada la Política de Tratamiento de Datos Personales, conforme a la normativa vigente.

Politica de privacidad

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Responsable de Seguridad y Privacidad de la Información o quien haga sus veces, implementará los controles técnicos, administrativos y organizacionales necesarios para la protección de la información personal de los servidores públicos, contratistas, estudiantes y demás partes interesadas externas, en los términos del artículo 15 de la Constitución Política de Colombia, la Ley 1581 de 2012 y sus decretos reglamentarios.

Política de Protección de la Información

El Instituto Tolimense de Formación Técnica Profesional – ITFIP adoptará estándares y buenas prácticas para garantizar la confidencialidad, integridad y disponibilidad de sus activos de información.

Los servidores públicos, contratistas y colaboradores deberán identificar y clasificar los activos de información según su nivel de sensibilidad y aplicar los controles de protección correspondientes,





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

de acuerdo con su tratamiento y criticidad.

Para efectos de contratos, convenios o acuerdos, se considerará información confidencial aquella definida por la normativa vigente, especialmente la Ley 1712 de 2014, manteniéndose la obligación de confidencialidad incluso después de finalizada la relación contractual o laboral. El ITFIP promoverá la suscripción de acuerdos o cláusulas de confidencialidad con las partes que requieran acceso a información restringida o confidencial.

Política de Seguridad de la Información en la Gestión de Proyectos

El Direccionamiento del Plan Estratégico y Planeación del ITFIP incorporará los requerimientos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación en la metodología institucional de gestión de proyectos, garantizando su implementación desde las fases iniciales.

El Control Interno incluirá en su plan de auditorías la verificación del cumplimiento de estos lineamientos, y las áreas responsables de la contratación velarán porque los estudios previos y contratos contemplen los requisitos asociados a la Política Institucional de Seguridad y Privacidad de la Información.

7. CONTROLES DE PERSONAS

7.1. Política de Seguridad de los Recursos Humanos

El ITFIP aplicará los lineamientos normativos y procedimientos internos en los procesos de selección, vinculación y retiro del personal, realizando las verificaciones necesarias para asegurar la confiabilidad de la información suministrada.

Así mismo, promoverá la conciencia y apropiación de responsabilidades en materia de seguridad de la información, seguridad digital y continuidad de los servicios, mediante cláusulas contractuales, divulgación a través de supervisores y acciones de sensibilización, con el fin de reducir riesgos y prevenir el uso indebido de los recursos institucionales.

8. CONTROLES FISICOS

8.1. Política de Seguridad Física y del Entorno

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Direccionamiento del Plan Estratégico y Planeación, con el apoyo del Grupo Interno de Trabajo de Sistemas y las dependencias





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

responsables, adoptará medidas de seguridad física y del entorno para proteger el perímetro de seguridad de sus instalaciones.

Estas medidas estarán orientadas a controlar el acceso y la permanencia de personas en oficinas, instalaciones y áreas restringidas, especialmente aquellas destinadas al procesamiento o almacenamiento de información sensible y a la infraestructura tecnológica, con el fin de mitigar riesgos, amenazas externas o ambientales y salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional.

El ITFIP garantizará la protección de los datos personales recolectados de servidores públicos, contratistas y visitantes, y establecerá mecanismos alternativos para aquellos casos en los que no se autorice su tratamiento, conforme a la normativa vigente.

9. CONTROLES TECNOLOGICOS

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Grupo Interno de Trabajo de Sistemas, será responsable de la operación y administración de los recursos tecnológicos que soportan la prestación de los servicios institucionales, garantizando la confidencialidad, integridad y disponibilidad de la información.

El ITFIP implementará controles de operación, incluyendo la gestión de cambios en los ambientes de producción, así como mecanismos de control para los ambientes de desarrollo y prueba, asegurando que toda modificación a los sistemas de información sea autorizada y controlada.

Así mismo, se garantizará la capacidad de procesamiento de la plataforma tecnológica mediante proyecciones de crecimiento, y se implementarán mecanismos de contingencia, respaldo y recuperación ante desastres, con el fin de asegurar la disponibilidad de los servicios de TI.

El ITFIP realizará **copias de seguridad periódicas** de la información crítica, de acuerdo con los procedimientos institucionales definidos. El responsable de seguridad de la información verificará su adecuada ejecución, asegurando la posibilidad de recuperación ante fallas o incidentes. Las plataformas tecnológicas operadas por terceros deberán cumplir con los mismos lineamientos y controles establecidos por la institución.



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

9.1. Política de Seguridad del Sistema y de la Red

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Grupo Interno de Trabajo de Sistemas, garantizará la disponibilidad, integridad y confidencialidad de las redes y servicios tecnológicos, implementando y monitoreando mecanismos de seguridad que permitan prevenir, detectar y gestionar eventos o incidentes de seguridad y privacidad de la información.

El intercambio de información con partes interesadas internas y externas se realizará mediante mecanismos seguros, aplicando controles criptográficos cuando se requiera el uso de servicios web u otros medios tecnológicos, asegurando la integridad de la información intercambiada.

Todos los servidores públicos, contratistas y proveedores deberán suscribir acuerdos de confidencialidad y no divulgación, los cuales harán parte de la documentación laboral o contractual correspondiente, como requisito para el acceso a la información institucional.

9.1. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas

El Grupo Interno de Trabajo de Sistemas del ITFIP velará porque los sistemas de información, desarrollados interna o externamente, cumplan con los requisitos de seguridad durante sus fases de diseño, desarrollo, pruebas, puesta en producción y mantenimiento, conforme a la metodología institucional definida.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), esta dependencia será la responsable de adquirir, desarrollar, autorizar y recibir software, así como de avalar soluciones tecnológicas contratadas con terceros, garantizando su conveniencia, soporte, mantenimiento y seguridad.

Todo software que opere en el ITFIP deberá contar con la autorización previa del Grupo Interno de Trabajo de Sistemas y cumplir con los lineamientos técnicos y presupuestales establecidos, con el fin de asegurar la protección, soporte y recuperación de la información ante posibles incidentes.

9.2. Política de servicios en la nube

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Grupo Interno de Trabajo de Sistemas, será responsable de garantizar la seguridad, privacidad y continuidad de la información y de los servicios tecnológicos que se presten mediante plataformas de

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

computación en la nube, asegurando el cumplimiento de los niveles de servicio y de los lineamientos institucionales establecidos

Los contratos o convenios que involucren el uso de servicios en la nube deberán incluir obligaciones específicas relacionadas con la seguridad de la información, protección de datos, disponibilidad del servicio y mitigación de riesgos, conforme a la normativa vigente y a las políticas del ITFIP.

El uso de los servicios de computación en la nube estará exclusivamente destinado al cumplimiento de las funciones institucionales, quedando prohibido su uso para fines personales o no autorizados.

10. POLITICAS ESPECIFICAS

10.1. Política de seguridad de la sede electrónica

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Grupo Interno de Trabajo de Sistemas, será responsable de la administración y gestión de la sede electrónica institucional, integrando en ella los portales web, plataformas, aplicaciones, ventanillas únicas y demás soluciones digitales del ITFIP.

Para la operación de la sede electrónica, se definirán e implementarán, en coordinación con las dependencias responsables de los trámites y servicios, las medidas jurídicas, organizativas y técnicas necesarias para garantizar la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios digitales.

La sede electrónica dispondrá de canales digitales oficiales claramente identificados para la recepción de solicitudes, peticiones y comunicaciones de los ciudadanos y partes interesadas.

La emisión, recepción y gestión de comunicaciones oficiales por medios electrónicos estará alineada con la gestión documental electrónica, incorporando los lineamientos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.

El Direccionamiento del Plan Estratégico y Planeación, en articulación con las dependencias responsables, establecerá las estrategias archivísticas necesarias para asegurar el tratamiento adecuado, la conservación y el acceso a largo plazo de los documentos electrónicos, conforme a los principios definidos por el Archivo General de la Nación.

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592

Correo: info@itfip.edu.co El Espinal – Tolima





11. RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS.

11.1. Política de seguridad digital

Todos los servidores públicos y contratistas del Instituto Tolimense de Formación Técnica Profesional – ITFIP que hagan uso de los recursos tecnológicos institucionales son responsables de cumplir las políticas de uso aceptable, entendiendo que un uso inadecuado puede afectar la continuidad de la operación de los servicios y el cumplimiento de la misión institucional.

El correo electrónico institucional, administrado por el Grupo Interno de Trabajo de Sistemas, es una herramienta destinada exclusivamente al desarrollo de funciones institucionales y deberá utilizarse bajo los siguientes principios generales:

- Solo se autoriza el uso del correo electrónico institucional asignado por el ITFIP, el cual cumple con los requerimientos técnicos y de seguridad necesarios para la protección de la información.
- El correo institucional deberá emplearse únicamente para comunicaciones oficiales, quedando prohibido su uso con fines personales, comerciales o ajenos a los propósitos institucionales.
- Se promoverá el uso del correo electrónico como medio preferente para el intercambio de información, cuando la normativa lo permita, en concordancia con la eficiencia administrativa.
- El ITFIP implementará controles tecnológicos para prevenir la pérdida o fuga de información, así como para detectar correos sospechosos, spam o posibles incidentes de seguridad.
- Todo mensaje sospechoso, spam o cadena deberá ser reportado como incidente de seguridad a través de los canales institucionales definidos.
- Está prohibido el envío o reenvío de contenidos ofensivos, ilegales, no autorizados, clasificados o reservados, así como la divulgación de información institucional por medios no autorizados.
- Las cuentas de correo institucional no deberán registrarse en sitios externos ajenos a la actividad institucional.
- El ITFIP se reserva el derecho de monitorear, respaldar y controlar el uso del correo electrónico institucional, informando previamente a los usuarios al inicio de la relación laboral o contractual, conforme a la normativa vigente



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

11.2. Política de Uso de Internet

El Instituto Tolimense de Formación Técnica Profesional – ITFIP, a través del Grupo Interno de Trabajo de Sistemas, en coordinación con el Responsable de Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación en Internet basadas en categorías, perfiles de usuario, jerarquía y funciones, con el fin de garantizar un uso seguro y adecuado de este recurso tecnológico.

El acceso a los servicios de Internet estará determinado por el rol y las funciones asignadas, y deberá utilizarse exclusivamente para fines institucionales, previa autorización del jefe o supervisor correspondiente.

Los servidores públicos y contratistas deberán abstenerse de:

- Acceder a sitios web, portales o aplicaciones no autorizadas por la política institucional.
- Enviar, descargar o visualizar contenidos ofensivos, ilegales, obscenos, injuriosos o que vulneren derechos de autor.
- Descargar software o archivos de fuentes externas no confiables.
- Propagar de manera intencional virus o código malicioso.

El ITFIP se reserva el derecho de monitorear y controlar el uso del servicio de Internet, así como de restringir accesos, horarios de conexión, descargas y servicios, cuando sea necesario para proteger la seguridad de la información, la continuidad de los servicios y el cumplimiento de la misión institucional, informando previamente a los usuarios conforme a la normativa vigente.

11.3. Uso de los Recursos Tecnológicos

Los recursos tecnológicos de la entidad son herramientas de apoyo al cumplimiento de las funciones y obligaciones laborales o contractuales, por lo que su uso debe ser exclusivamente institucional, responsable y conforme a las políticas establecidas.

Los empleados públicos y contratistas son responsables del adecuado uso, custodia y protección de los equipos asignados, los cuales no pueden ser utilizados con fines personales ni por terceros no autorizados. Solo está permitido el uso de software licenciado o expresamente autorizado por la Unidad de Gestión Tecnológica, que también es la única dependencia autorizada para instalar, modificar, trasladar, administrar o reparar los recursos tecnológicos.

- El acceso a la red institucional, incluyendo el uso de equipos no institucionales, dispositivos móviles personales y redes WiFi, deberá ser informado, autorizado, autenticado y controlado por la Unidad de Gestión Tecnológica, conforme a los lineamientos de

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592
Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

seguridad definidos.

- El uso de dispositivos externos de almacenamiento será monitoreado para prevenir fugas de información.
- Se deben realizar copias de seguridad de la información, reportar oportunamente cualquier pérdida de equipos, información o incidentes de seguridad, y utilizar únicamente las herramientas tecnológicas oficiales para la gestión de la información digital.
- Está prohibido almacenar contenidos no institucionales, vulnerar derechos de autor, realizar conexiones eléctricas no autorizadas, ingerir alimentos cerca de equipos tecnológicos y utilizar software o servicios tecnológicos para fines personales.
- Los equipos deberán permanecer apagados cuando no estén en uso, con el fin de proteger la seguridad de la información y optimizar los recursos.
- El incumplimiento de estas disposiciones podrá dar lugar a acciones disciplinarias, administrativas o legales, según corresponda.

11.4. Uso de Sistemas y Almacenamiento Institucional

Todos los empleados públicos y contratistas son responsables de proteger la información institucional a la que acceden, evitando su pérdida, alteración, destrucción, uso indebido o divulgación no autorizada.

- Las credenciales de acceso a los sistemas de información son personales e intransferibles, y cada usuario es responsable de su uso, cambio periódico y de todas las acciones realizadas desde su cuenta. En caso de ausencia, retiro o terminación contractual, los accesos serán bloqueados o suspendidos de forma inmediata, y la información será almacenada en los repositorios institucionales.
- Al finalizar la relación laboral o contractual, el jefe inmediato o supervisor asumirá la custodia de los activos de información, garantizando la protección de los derechos de propiedad intelectual y evitando que el funcionario o contratista retire información institucional. Asimismo, deberá cumplirse el paz y salvo conforme a los procedimientos establecidos.
- El uso de los sistemas de almacenamiento institucionales debe ser consciente y exclusivo para información de carácter institucional, debidamente clasificada y con controles de acceso adecuados para asegurar su confidencialidad, integridad y disponibilidad.
- La creación y custodia de copias de seguridad solo podrá realizarse bajo solicitud del jefe inmediato o supervisor, y serán administradas por la Unidad de Gestión Tecnológica conforme a las políticas de retención vigentes.

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592

Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

- El cumplimiento de la normativa de derechos de autor y propiedad intelectual es obligatorio para todos los funcionarios, contratistas y terceros vinculados a la entidad.

12. ROLES Y RESPONSABILIDADES

12.1. Alta Dirección

- Aprobar la Política de Seguridad Digital.
- Asignar recursos necesarios para su implementación y mantenimiento.

12.2. Responsable de Seguridad de la Información

- Coordinar la implementación de la política.
- Supervisar el cumplimiento de los controles de seguridad.
- Gestionar los incidentes de seguridad de la información.

12.3. Área de Tecnologías de la Información

- Implementar y administrar los controles técnicos de seguridad.
- Mantener la infraestructura tecnológica segura y actualizada.

13. PLAN DE IMPLEMENTACIÓN

13.1. Fases

- Diagnóstico Inicial

Identificar el estado actual de la seguridad y privacidad de la información del ITFIP mediante el inventario y clasificación de activos de información, revisión de controles existentes, análisis de cumplimiento normativo y evaluación de riesgos asociados a los procesos misionales, estratégicos y de apoyo.

- Fase 2. Planeación

Definir el alcance del Plan de Implementación, priorizar riesgos, establecer objetivos, responsables, recursos y cronograma. En esta fase se alinean las políticas de seguridad de la información con la normatividad vigente y los lineamientos institucionales del ITFIP.

- Definición y Ajuste de Controles



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

Diseñar, actualizar y formalizar los controles administrativos, técnicos y físicos necesarios para proteger la información, incluyendo control de accesos, uso aceptable de recursos tecnológicos, gestión de incidentes, continuidad del servicio y protección de datos personales.

- Fase 4. Implementación

Poner en marcha los controles definidos, tanto a nivel tecnológico como procedimental, asegurando su aplicación en todos los procesos y dependencias del ITFIP. Incluye la implementación de medidas de seguridad en sistemas de información, redes, infraestructura y servicios digitales.

- Fase 5. Sensibilización y Capacitación

Capacitar y sensibilizar a funcionarios, contratistas y partes interesadas sobre sus responsabilidades frente a la seguridad y privacidad de la información, promoviendo una cultura institucional de protección de la información en el ITFIP.

- Fase 6. Seguimiento y Evaluación

Realizar monitoreo periódico al cumplimiento del plan y la efectividad de los controles implementados, gestionar incidentes de seguridad y efectuar auditorías internas para identificar oportunidades de mejora.

- Fase 7. Mejora Continua

Actualizar de manera permanente el Plan de Implementación, los controles y las políticas de seguridad de la información, considerando los resultados del seguimiento, los cambios normativos, tecnológicos y organizacionales del ITFIP.

14. CRONOGRAMA DE IMPLEMENTACIÓN (PROPUESTO)

El presente cronograma establece las actividades necesarias para implementar de manera progresiva la Política de Seguridad Digital en el Instituto Tolimense de Formación Técnica Profesional – ITFIP, en concordancia con el MSPI de MinTIC y la norma ISO/IEC 27001.

ACTIVIDAD	DESCRIPCION	RESPONSABLE	ENTREGABLE	PLAZO
Diagnostico estado actual	Evaluar el estado de la seguridad y privacidad de la	Direccionamiento de Plan Estratégico y Planeación Grupo	Informe de diagnósticoInventario de activos	1 mes



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

	información, inventariar activos y revisar cumplimiento normativo	Interno de Trabajo de Sistemas		
Planeación del MSPI	Definir alcance, objetivos, roles, recursos y cronograma del MSPI en el ITFIP	Direccionamiento de Plan Estratégico y Planeación	Plan de Implementación aprobado	2 meses
Análisis y tratamiento de riesgos	Identificar, analizar y priorizar riesgos de seguridad de la información y definir planes de tratamiento	Grupo Interno de Trabajo de Sistemas	Matriz de riesgosPlan de tratamiento	3 y 4 meses
Definición y adopción de políticas	Formalizar políticas de activos, acceso, uso aceptable, incidentes, continuidad, privacidad y nube	Grupo Interno de Trabajo de Sistemas Asesoría Jurídica	Políticas adoptadas	3 y 4 meses
Implementación de controles	Implementar controles técnicos, administrativos y físicos definidos en las políticas Grupo Interno de Trabajo de Sistemas	Grupo Interno de Trabajo de Sistemas	Controles implementados	5 y 6 meses

“EDUCACIÓN SUPERIOR CON CALIDAD PARA TODOS”

Calle 18 Carrera 1ª Barrio ARKABAL Celular Atención al Ciudadano 316 6254592

Correo: info@itfip.edu.co El Espinal – Tolima





“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional
NIT 800.173.726.0
www.itfip.edu.co

Gestión de incidentes	Establecer y operar el procedimiento de reporte, análisis y atención de incidentes	Grupo Interno de Trabajo de Sistemas	Registros de incidentes Procedimiento operativo	6 meses
Continuidad del servicio	Elaborar y aplicar el BIA, BCP y Plan de Recuperación ante Desastres TIC	Grupo Interno de Trabajo de SistemasPlaneación	BIA-BCP-DRP	6 y 7 meses
Capacitación y sensibilización	Capacitar a funcionarios y contratistas en seguridad digital y uso aceptable	Talento Humano Grupo Interno de Trabajo de Sistemas	Registros de capacitación	7 meses
Seguimiento y auditoría	Monitorear cumplimiento del MSPI y realizar auditorías internas	Control Interno	Informes de seguimiento	8 y 9 meses
Actualización del MSPI	Ajustar políticas, riesgos y controles según resultados y cambios institucionales	Planeación de Sistemas	Plan de mejora continua	10 meses

Este cronograma se encuentra alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma ISO/IEC 27001



“ITFIP” INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Establecimiento público adscrito al Ministerio de Educación Nacional

NIT 800.173.726.0

www.itfip.edu.co

15. BIBLIOGRAFIA

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2021). *Resolución 500 de 2021 – Modelo de Seguridad y Privacidad de la Información (MSPI)*.

<https://www.mintic.gov.co/portal/715/w3-article-162626.html>

(Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (s. f.). *Modelo de Seguridad y Privacidad de la Información (MSPI)*.

<https://www.mintic.gov.co/portal/715/w3-article-403045.html>

(Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (s. f.). *Lineamientos para el fortalecimiento de la seguridad digital en entidades públicas*.

<https://www.mintic.gov.co/portal/715/w3-article-399981.html>

(Consulta: 2025)

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 – Information security management systems*.

<https://www.iso.org/standard/82875.html>

(Consulta: 2025)

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012 – Protección de Datos Personales*.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

(Consulta: 2025)

