

**Metodología y plan de tratamiento del Riesgo de
seguridad y privacidad de la información.
Instituto Nacional de Formación Técnica
Profesional**

**INFOTEP
SAN JUAN DEL CESAR, ENERO 2026**

© Instituto Nacional de Formación Técnica Profesional

Metodología y plan de tratamiento del Riesgo de seguridad y privacidad de la información.

Rector: Dr.Luis Alfonso Pérez Guerra

Documento preparado Por: Alberto Álvaro Vega González

Contacto:

Email: contactenos@infotep.edu.co

www.infotep.edu.co

San Juan del Cesar, La Guajira - Colombia

INFOTEP, 2026

Prohibida la reproducción total o parcial, en cualquier medio o para cualquier propósito sin la autorización escrita del Instituto nacional de Formación Técnica Profesional

Tabla de contenido

Lista de Tablas	4
Lista de Figura	5
1. Introducción	1
2. Objetivos	5
2.1. Objetivo General	5
2.2. Objetivos específicos.....	5
3. Identificación de las partes interesadas.....	7
4. Referencias Normativas	8
5. Textos y definiciones	9
6. Establecimiento contexto.	1
7. Alcance/Aplicabilidad.....	1
8. Metodología de evaluación de riesgo	1
9. Activos, amenazas, vulnerabilidades e impactos.....	3
9.1. Inventario de activos	4
9.2. Identificar amenazas y vulnerabilidades	17
9.3. Identificar los impactos	18
10. Caracterización y Valoración de los Activos.....	20
11. Análisis de las Vulnerabilidades	24
12. Análisis y evaluación de riesgo.....	26
13. Cronograma de Actividades.....	32
Referencias Bibliograficas	34

Lista de Tablas

Tabla 1. Identificación de cuestiones.....	3
Tabla 2. Partes interesadas. Fuente Propia.....	7
Tabla 3. Inventario de Activos.....	4
Tabla 4. Amenazas.....	17
Tabla 5. Mapa de Riesgo Inherente	18
Tabla 6. Mapa de impactos	18
Tabla 7. Caracterización y Valoración de los Activos.....	20
Tabla 8. Escala de valoración activos	21
Tabla 9. Valoración de aplicaciones	22
Tabla 10. Valoración de Servicios.....	23
Tabla 11. Análisis de Vulnerabilidades	24
Tabla 12. Análisis y evaluación de Riesgo	26

Lista de Figura

Figura 1. DOFA de SGSI. Fuente propia.....	4
Figura 2. Metodología para la administración del riesgo	3
Figura 3. Diagrama de Red	21

1. Introducción

Las organizaciones, empresas y entidades, actualmente están creando conciencia, de la importancia que las informaciones representan para ellos, sin importar los tipos de datos, o el medio en el que se encuentran, sea físico o digital, considerándolo como el mayor activo que poseen.

La información como un activo, forma parte de la actividad cotidiana de las organizaciones y personas; los dispositivos móviles y equipos de cómputo almacenan información, la procesan y la transmiten, a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios.

Estos activos pueden ser afectados por eventos o incidentes, que pueden comprometer de alguna manera su integridad, confidencialidad y disponibilidad, causando un impacto adverso, en los procesos de negocio de la organización o de su misión, por ello la norma ISO 27001 la cual es un estándar internacional, contempla los requisitos necesarios, para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información.

El INFOTEP en la actualidad, se encuentra en crecimiento, y debe involucrar en sus procesos, estrategias para la protección de la información; por ello es indispensable, el desarrollo del análisis de riesgo de la seguridad de la información, aplicado a cada uno de los activos de información.

Partiendo de lo anterior, es importante conocer los detalles de la organización objeto de estudio, y lograr identificar con claridad las especificaciones, para el desarrollo de nuestra asignatura Gestión de seguridad de TI, y cumplir el con el objetivo de cada una de las actividades planificadas. Identificación de las cuestiones externas e Internas

El análisis DOFA, es una herramienta que realiza una evaluación, de las interacciones de los factores principales que se esperan que influyan, en el cumplimiento de los objetivos de la institución. En el desarrollo de esta actividad se utilizó como medio para conocer la realidad de la Institución interna y externamente, así mismo es una forma de retroalimentación, acerca de cómo se realiza el trabajo institucional, formando de esta manera los requisitos necesarios, tanto para la gestión de los procesos como para las tomas de decisiones.

Dentro de las dimensiones del análisis encontramos que:

- Cuestiones Internas:
 - Fortalezas Positiva
 - Debilidad Negativa
- Cuestiones Externas
 - Oportunidades Positivo
 - Amenazas Negativo

Para el levantamiento de la información expuesta a continuación, se realizó por medio de la técnica del reportero, entrevistas con las directivas y el personal del área de TI de la institución, cuyo resultado es plasmado en la Matriz DOFA que se muestra en la figura 1. y aprobado por comité de desarrollo administrativo de INFOTEP.

Tabla 1. Identificación de cuestiones

Cuestiones Internas	Cuestiones externas
• Compromiso para la implementación del Sistema de Gestión de Seguridad de la Información. • Falta de Licenciamiento de los equipos. • Falta de personal para el apoyo en la realización de las actividades del proceso. • Falta de Conciencia en temas de Seguridad. • Procedimientos no adecuados para la vinculación de personal. • Red Académica y Administrativa bajo la misma red física y lógica. • Suministro eléctrico y de internet inestable. • Exposición de contraseñas	• Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información). • Recursos provenientes del estado como lo son la estampilla pro desarrollo fronterizo y Recursos Cree no sean girados a tiempo para la ejecución de las actividades. • Afectaciones en algunos de los pilares de la información “Disponibilidad, confidencialidad e integridad” causado por ataques informáticos.

A continuación, se describe la matriz DOFA de la entidad:

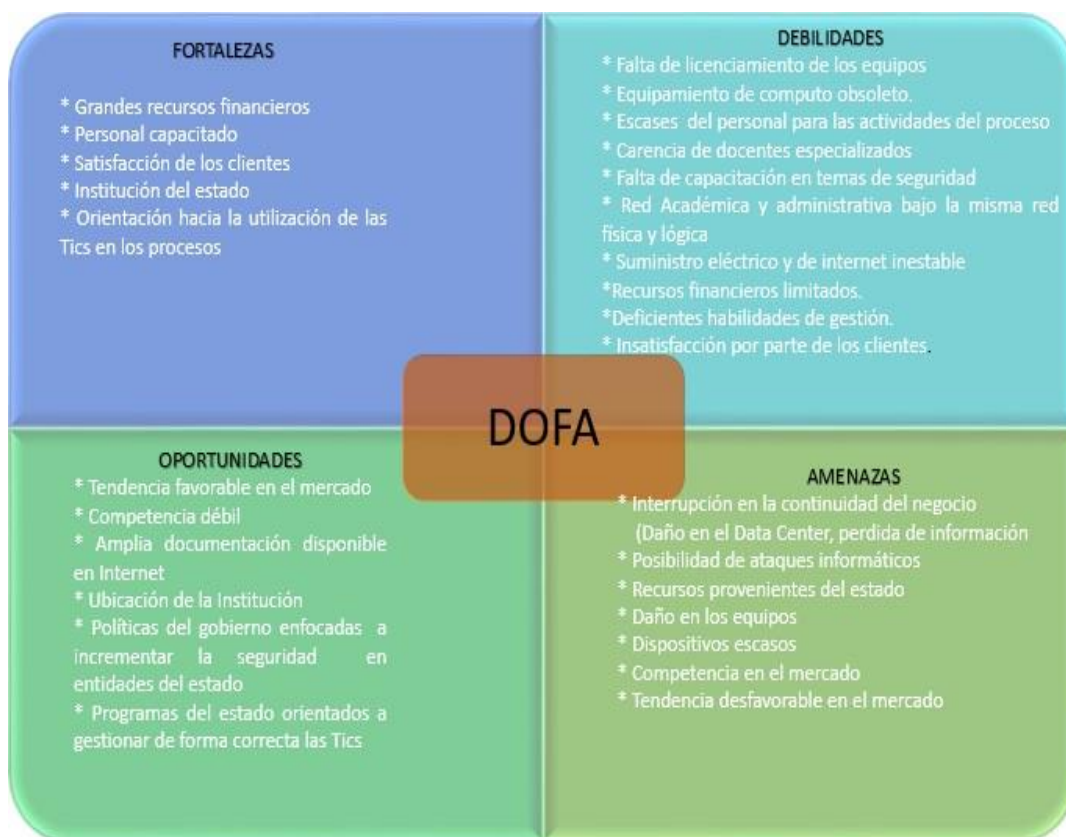


Figura 1. DOFA de SGSI. Fuente propia

2. Objetivos

2.1. Objetivo General

Determinar los lineamientos de buenas prácticas en Seguridad y Privacidad aplicables para el Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar, La Guajira.

2.2. Objetivos específicos

- Mediante la utilización del Modelo de Seguridad y Privacidad se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar al INFOTEP en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior del INFOTEP.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumplimiento de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.

- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior del INFOTEP para optimizar su articulación.

3. Identificación de las partes interesadas

Se realiza la identificación de las partes interesadas para el sistema de gestión de la seguridad de INFOTEP.

Tabla 2. Partes interesadas. Fuente Propia.

TIPO	PARTE INTERESADA	INTERÉS
INTERNOS	Máxima Autoridad “Representante Legal, Consejo Directivo”	Asegurar la integridad, disponibilidad, confidencialidad de sus activos de información
	Líderes de Proceso “Estratégico, Misional, Apoyo, Evaluación”	Generación y uso de los activos de información
	Población Académica “Estudiantes, Docentes, Graduados, Egresados”	Disponibilidad, integridad y confidencialidad de su información.
EXTERNOS	Entes de Control “Ministerio de educación Nacional, Ministerio de las TIC, Procuraduría, Contraloría, Contaduría”	Recepción de información de acuerdo con los requerimientos de cada entidad.
	Otros “Proveedores y Contratistas”	Cumplir las políticas del SGSI de la entidad en los entes externos, con el fin de garantizar su la seguridad de la

TIPO	PARTE INTERESADA	INTERÉS
		información

4. Referencias Normativas

A continuación, se relación las referencias normativas aplicables las cuales son definidas en el ITEM 5. Textos y definiciones.

Ley 1712 de 2014, Sobre la Transparencia y del Derecho de Acceso a la Información Pública Nacional

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales"

Resolución CRC 2258 de 2009. De la Comisión de Regulación de Comunicaciones: Ciberespacio

CONPES 3701 de 2011, Donde se establecen los Lineamientos de política para la Ciberseguridad y Ciberdefensa

Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones

Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012 Régimen General de Protección de Datos Personales.

ISO/IEC 27000, es un grupo de estándares internacionales titulados: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).

5. Textos y definiciones

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho

individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad

para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: 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. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. Establecimiento contexto.

Para definir y documentar el proceso de gestión de riesgos de seguridad de la información, como parte de la descripción del Instituto Nacional de Formación Técnica Profesional a continuación se detallan las partes interesadas del sistema, descripción del rol que desempeñan al igual que las actividades que ejecutan de la siguiente manera:

GRUPOS DE INTERÉS		
ROL	DESCRIPCIÓN	ACTIVIDADES
Director General	Responsable por el direccionamiento estratégico e impulso del SGSI	Aprobación y verificación del cumplimiento de las políticas de seguridad de la información. Hacer que los miembros del Comité Directivo sean conscientes de la criticidad de los activos de información y de su criticidad en el desarrollo de la misión de la Entidad. Divulgar las responsabilidades de seguridad de la información con base en los lineamientos del SGSI.
Oficial de Seguridad	Es el responsable por el SGSI	Definición, actualización y mantenimiento de los activos de información y asociados. Análisis de riesgos de seguridad de la información con base en lo establecido en el SGSI. Definición del plan de tratamiento de los riesgos de seguridad de la información. Ejecución del plan de tratamiento de los riesgos de seguridad de la información. Definición, actualización y difusión de las políticas, procedimientos y formatos del SGSI. Definición y generación de las métricas de seguridad de la información establecidas en el SGSI. Definición de los planes de entrenamiento y sensibilización para los funcionarios en lo referente a seguridad de la información.
Nivel directivo	Aplicar los lineamientos del SGSI al interior del área correspondiente, transmitiendo los objetivos de la seguridad de la información para cada uno de los roles que aplique	Liderazgo y apoyo continuo para la aplicación del SGSI al interior del área correspondiente. Alineación de los objetivos del área para que su cumplimiento este apoyado por el SGSI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad de la información para los roles definidos en el área correspondiente. Proveer los recursos necesarios para la implementación del SGSI al interior del área correspondiente. Apoyar la capacitación y entrenamiento requerido para que los funcionarios del área correspondiente cumplan con el SGSI. Aplicar el proceso disciplinario ante los incidentes de seguridad de la información originado por un funcionario del área correspondiente.
Comité Operativo de Seguridad de la	Lo integran todos los líderes de proceso	Validar la documentación propia del SGSI con cada dueño de proceso. Fomentar dentro de su dependencia la práctica de directrices de seguridad de información.

Información		Apoyar la identificación y actualización de activos y riesgos de seguridad de información. Apoyar la identificación e implementación de controles para la mitigación de riesgos de seguridad de información. Participar en las jornadas de implementación, mantenimiento y mejora del SGSI.
Propietario del Activo	Es el funcionario asignado de gestionar que el activo asignado bajo su responsabilidad	Gestión requerida para que la Entidad asigne los recursos necesarios para la implementación de los controles definidos en el SGSI protegiendo la Confidencialidad, Integridad y disponibilidad de la información del activo. Gestión requerida para que el o los custodios del activo estén informados sobre los controles aplicados a éste y que cuenten con los recursos necesarios para implementarlos. Verificar el cumplimiento de la Política de uso Aceptable del Activo. Actualización permanente de la información del activo en el SGSI. Implementación de los controles definidos en el SGSI para la protección del activo. Remediación de vulnerabilidades reportadas por el fabricante correspondiente o identificadas en las pruebas de vulnerabilidad. Reporte inmediato de incidentes de seguridad de la información
Custodio del Activo	Es el usuario final a quien se asigna el activo para el cumplimiento de las actividades diarias.	Comunicación permanente con el Propietario del activo para reportes de los resultados de la aplicación de los controles. Hacer cumplir la Política de uso Aceptable del Activo. Reporte inmediato de incidentes de seguridad de la información
Responsable del Riesgo	Líder del Proceso	Conocer la valoración actual del riesgo y verificar si se encuentra dentro del NRA definido por el INFOTEP. Gestión inmediata para el tratamiento definido en el SGSI cuando el riesgo se encuentre en una calificación por fuera del NRA. Cumplir con el reporte formal del riesgo a la Dirección General, cuando se detecte que su valoración supera el NRA. Seguimiento permanente a la aplicación de los controles requeridos para el tratamiento del riesgo que se constate que el nivel se encuentra dentro del NRA

7. Alcance/Aplicabilidad.

El presente documento aplica a toda la entidad, sus funcionarios, contratistas y terceros del Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar y la ciudadanía en general.

8. Metodología de evaluación de riesgo

Para la selección de la metodología de evaluación de riesgos se tuvieron en cuenta ISO 27005, Octave, RiskIT y la metodología para la gestión de riesgos del Departamento Administrativo de la Función Pública “DAFP”, siendo esta última la seleccionada para nuestro caso de estudio.

El DAFP es la “entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional” (DAFP, Información General). Como parte de sus funciones se elaboró la metodología de administración de riesgos para ser aplicada por todas las Entidades Públicas colombianas, ya sean de orden nacional o territorial, así como proveedores o terceros que deseen adoptarla (DAFP, Función Pública, 2011).

Debido a que la organización seleccionada como caso de estudio INFOTEP es una Entidad Pública se seleccionó esta metodología pues de esta manera se integra a los lineamientos del Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea, además esta metodología toma como referencia varios

aspectos de ISO31000 y se integra perfectamente a los demás modelos de gestión que el gobierno nacional ha sugerido para sus entidades públicas.

Para la aplicación de esta metodología específicamente hacia la gestión de riesgos de seguridad informática, el MinTIC ha publicado una guía de gestión de riesgos cuyo objetivo es “orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP” (MINTIC, 2016). En esa guía se detalla la forma en que se deben gestionar los riesgos y se toman algunos aspectos de ISO 27005.

En la siguiente imagen se muestran de manera detallada los pasos que esta metodología sugiere para la administración de riesgos, los cuales se irán profundizando en los siguientes puntos.

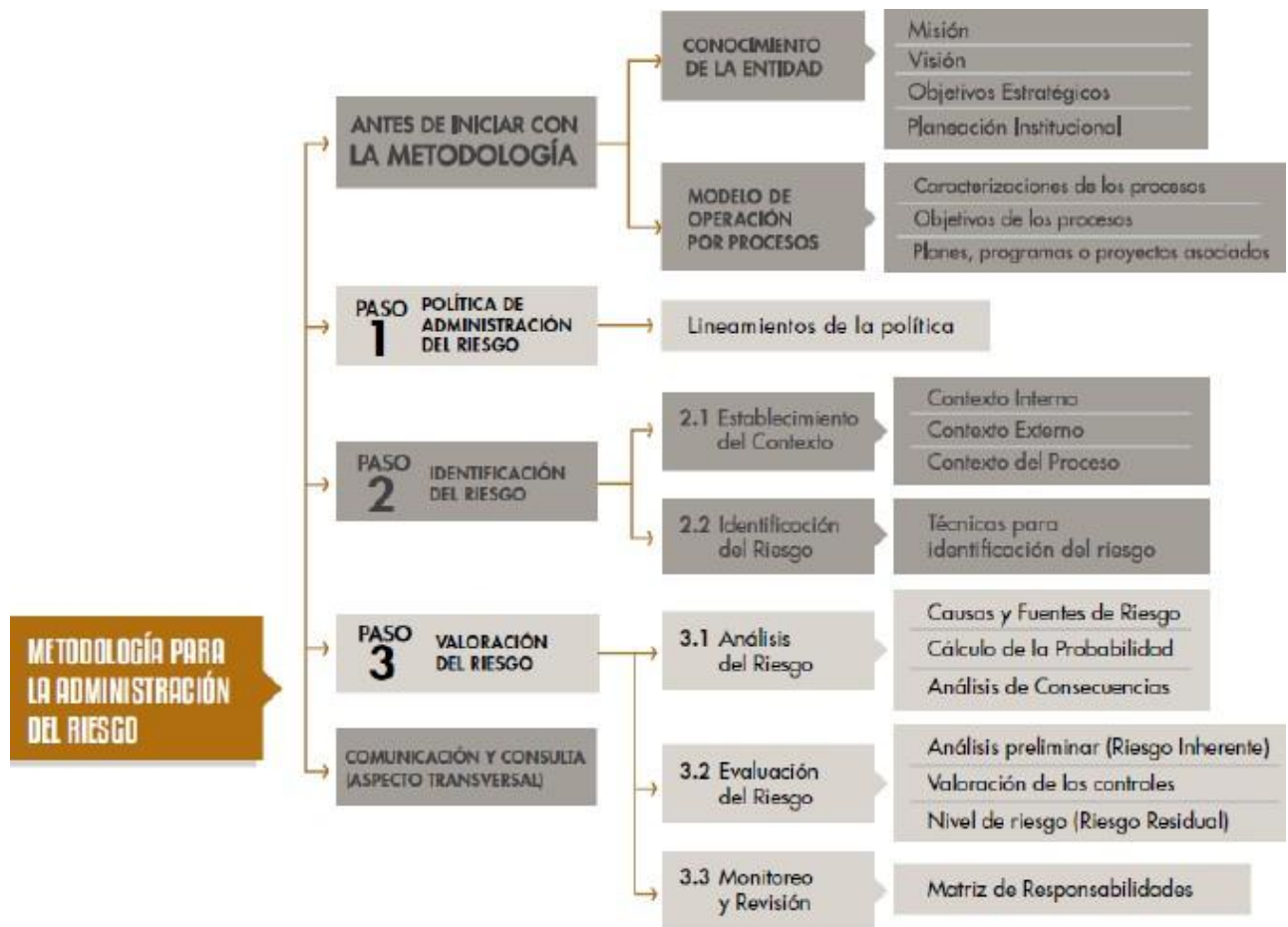


Figura 2. Metodología para la administración del riesgo

Como se puede observar, esta metodología no se enfoca sólo en la evaluación de riesgo, sino que contempla la gestión completa de los riesgos en todas sus etapas. En los capítulos 3, 4 y 5 se desarrollaron los pasos 1 y 2.1, por lo que los siguientes capítulos se enfocarán en la identificación, análisis y evaluación de los riesgos, es decir, del paso 2.2 de la metodología en adelante

9. Activos, amenazas, vulnerabilidades e impactos

9.1. Inventario de activos

Según la metodología, en la etapa de identificación de riesgos, es necesario primero realizar un inventario de todo aquello que tiene valor para la entidad, y que, por lo tanto, requiere de protección. Esta identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo (MINTIC, 2016). Para la realización del inventario, se tuvieron en cuenta aquellos activos de información que tienen algún valor para el INFOTEP, los cuales fueron tabulados en un archivo de Excel, al cual se puede ingresar por medio de la dirección electrónica:

https://1drv.ms/x/s!AgwCgAzPGvb_gqRYuDBLPsAdXnCOaw

Tabla 3. Inventario de Activos

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
1	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	ACUERDOS	Información emanada por el concejo directivo.
2	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	ACTAS	Información emanada por el Comité de desarrollo administrativo y propias del cargo de vicerrector administrativo y financiero.
3	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	CERTIFICACIONES	Información propia del cargo de Vicerrector Administrativo y Financiero.
4	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	RESOLUCIONES	Información propia del cargo de Vicerrector Administrativo y Financiero.
5	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	SOLICITUD DE CDP	Solicitudes de disponibilidad presupuestal.
6	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	CUMPLIDO DE COMISION	Aprobación de comisiones. Legalización de los viajes
7	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	INSCRIPCIONES	
8	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	CONVENIOS	Lineamientos que definen los principios de funcionamiento de los convenios.
9	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	CONTRATOS	Actas de juntas y reuniones de seguimiento que se desarrolla en el contexto de avance de convenios y contratos.
10	Vicerrectoría Administrativa y Financiera	ACTOS ADMINISTRATIVOS	PRESUPUESTO	Informes técnicos y financieros de la ejecución del convenio.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
11	Vicerrectoría Administrativa y Financiera	CONTRATACION	DE OBRAS	Publicación de todo el proceso de contratación.
12	Vicerrectoría Administrativa y Financiera	CONTRATACION	PRESTACION DE SERVICIOS	Publicación de todo el proceso de contratación.
13	Vicerrectoría Administrativa y Financiera	CONTRATACION	INTERVENTORIA	Publicación de todo el proceso de contratación.
14	Vicerrectoría Administrativa y Financiera	CONTRATACION	SUMINISTRO	Publicación de todo el proceso de contratación.
15	Admisión, Registro y Control Académico	INSCRIPCION, SELECCIÓN Y ADMISION	SOLICITUD DE DOCUMENTOS	Lista de documentos requeridos para la inscripción
16	Admisión, Registro y Control Académico	INSCRIPCION, SELECCIÓN Y ADMISION	ACTA DE COMPROMISO	Documento de acta de compromiso firmada por el estudiante
17	Admisión, Registro y Control Académico	INSCRIPCION, SELECCIÓN Y ADMISION	LISTA DE CHEQUEO	Lista de chequeo
18	Admisión, Registro y Control Académico	INSCRIPCION, SELECCIÓN Y ADMISION	LISTA DE INSCRITOS	Listado de inscritos por programas de formación ofertados
19	Admisión, Registro y Control Académico	INSCRIPCION, SELECCIÓN Y ADMISION	LISTA DE ADMITIDOS	Lista de admitidos por programas de formación ofertados
20	Admisión, Registro y Control Académico	MATRICULAS ORDINARIA Y EXTRAORDINARIA	HOJA DE VIDA DE ESTUDIANTE	Hoja de Vida del estudiante con todos los documentos requeridos
21	Admisión, Registro y Control Académico	CONTROL ACADEMICO	CONCENTRADO DE NOTAS	Documento que contiene el acumulado de notas.
22	Admisión, Registro y Control Académico	CONTROL ACADEMICO	CERTIFICADO DE NOTAS	Certificación de las notas
23	Admisión, Registro y Control Académico	CONTROL ACADEMICO	CONSTANCIA DE ESTUDIOS	Constancia de asistencia y aprobación del proceso educativo
24	Admisión, Registro y Control Académico	CONTROL ACADEMICO	TERMINACION ACADEMICA	Documento que registra el proceso de terminación académica.
25	Admisión, Registro y Control Académico	CONTROL ACADEMICO	ACTA DE GRADO	Documento que contiene todos los datos contenidos en el Diploma de Grado, por ello puede ser utilizado para cualquier trámite legal, tanto a nivel nacional como Internacional.
26	Admisión, Registro y Control Académico	CONTROL ACADEMICO	DIPLOMA DE GRADO	Documento expedido por una la entidad, con firmas, sellos y los datos del estudiante, que acredita un grado académico.
27	Presupuesto	ANTEPROYECTO DE PRESUPUESTO	ANTEPROYECTO DE PRESUPUESTO	Es el conjunto de objetivos, actividades, consultas, estudios y documentos que se realizan al interior de la Alcaldía de cara a la elaboración del proyecto de presupuesto.
28	Presupuesto	ELABORACION DE CDP	ELABORACION DE CDP	
29	Presupuesto	REPORTE DE EJECUCION	EJECUCION Y CONTROL DEL	Comprende los procesos

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
		PRESUPUESTAL	PRESUPUESTO	relacionados con el recaudo de los ingresos y su uso para el funcionamiento oportuno.
30	Presupuesto	PROPUESTA DE EJECUCION PRESUPUESTAL	PROPUESTA DE EJECUCION PRESUPUESTAL	
31	Presupuesto	TRASLADO PRESUPUESTAL	TRASLADO PRESUPUESTAL	
32	Presupuesto	MODIFICACIONES PRESUPUESTAL	MODIFICACIONES PRESUPUESTAL	Se desarrolla actividades de adiciones, reducciones, y traslados En estos informes se reflejan los compromisos, las obligaciones o cuentas por pagar y los pagos realizados por el INFOTEP, de forma acumulada en un período determinado, sobre las asignaciones de recursos por concepto del gasto (funcionamiento, transferencias, inversión). Las reservas son el resultado de hechos contractuales imprevistos, como la suspensión de los contratos u otras situaciones jurídicas, y, en todo caso, no constituyen forma ordinaria de adquirir compromisos.
33	Presupuesto	INFORME DE EJECUCION PRESUPUESTAL	INFORME DE EJECUCION PRESUPUESTAL	
34	Presupuesto	CONSTITUCIONES DE LAS RESERVAS PRESUPUESTALES	RELACION DE RESERVAS	
35	Contabilidad	IDENTIFICACION DE HECHOS CONTABLES	ESTADO FINANCIERO	Son informes que utilizan el Infotep para dar a conocer la situación económica y financiera y los cambios que experimenta la misma a una fecha o periodo determinado.
36	Contabilidad	CLASIFICACION CONTABLE	CLASIFICACION CONTABLE	Es el conjunto de registros donde se detallan de forma cronológica todas las transacciones que ocurren en un ente económico
37	Contabilidad	REGISTROS Y AJUSTES CONTABLES	REGISTROS Y AJUSTES CONTABLES	Es el diseño de registro contable que permite conocer el saldo real de una cuenta.
38	Contabilidad	ANALISIS, INTERPRETACION Y COMUNICACIÓN	ESTADOS FINANCIEROS	Son informes que utilizan el Infotep para dar a conocer la situación económica y financiera y los cambios que experimenta la misma a una fecha o periodo determinado. Es una relación entre cifras extractadas de los estados financieros y otros informes contables de una empresa con el propósito de reflejar en forma objetiva el comportamiento de la misma.
39	Contabilidad	ANALISIS, INTERPRETACION Y COMUNICACIÓN	INDICADORES FINANCIEROS	

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
40	Contabilidad	CONCILIACIONES BANCARIAS	EXTRACTOS	Documento en el que se recoge el saldo disponible de la cuenta y los movimientos que se han realizado durante el último mes.
41	Contabilidad	CONCILIACIONES BANCARIAS	LIBROS DE CONTABILIDAD	Son el soporte material en la elaboración de la información financiera. Pueden ser de carácter obligatorio o voluntario.
42	Contabilidad	CONCILIACIONES BANCARIAS	CONCILIACIONES BANCARIAS	Es un proceso que permite confrontar y conciliar los valores que la institución tiene registrados, de las cuentas bancarias, con los valores que el banco suministra por medio del extracto bancario.
43	Tesorería	RECAUDOS	PROPUESTA	Documento eficiente del recaudo y el ingreso de los mismos. Con el fin de entregar la información financiera.
44	Tesorería	RECAUDOS	RELACION	Documento que relaciona los recaudos financieros.
45	Tesorería	RECAUDOS	COMPROBANTES DE PAGOS	Es un documento formal que avala una relación comercial o de transferencia en cuanto a bienes y servicios se refiere.
46	Tesorería	RECAUDOS	PAGARÉ	Documento que extiende y entrega una persona a otra mediante el cual contrae la obligación de pagarle una cantidad de dinero en la fecha que figura en él.
47	Tesorería	RECAUDOS	RECIBO OFICIAL DE CAJA	Es un soporte de contabilidad en el cual constan los ingresos en efectivo o en cheque recaudados por el INFOTEP. El recibo de caja se contabiliza con un débito a la cuenta de la caja y el crédito de acuerdo con su contenido o concepto del pago recibido.
48	Tesorería	GIROS	LIBRO AUXILIARES	Es un libro, en el cual se debe anotar todas las operaciones que realiza la institución, con la entidad bancaria en la cual se mantiene la cuenta corriente.
49	Tesorería	GIROS	ORDENES DE PAGO	Es una orden de transferencia efectuada por el ordenante, a su banco para que pague a un tercero
50	Tesorería	PROGRAMA ANUAL DE CAJA	DISTRIBUCION DEL PAC	Es un instrumento de administración financiera mediante el cual se relaciona la distribución de los recursos disponibles para el Infotep.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
51	Tesorería	PROGRAMA ANUAL DE CAJA	PROPUESTA	Es un instrumento de administración financiera mediante el cual se verifica y aprueba el monto máximo mensual de los recursos disponibles para el Infotep.
52	Biblioteca	SELECCIÓN Y ADQUISICION DE MATERIAL BIBLIOGRAFICO	NECESIDADES BIBLIOGRAFICOS	Documento que relaciona las necesidades de los libros requeridos en la institución.
53	Biblioteca	SELECCIÓN Y ADQUISICION DE MATERIAL BIBLIOGRAFICO	LISTADO DE MATERIAL BIBLIOGRAFICO	Documento que relaciona el listado de las necesidades bibliográficas.
54	Biblioteca	PRESTAMO DE MATERIAL BIBLIOGRAFICO	INFORMES DE GESTION	Documento que presenta el informe de la gestión en el área de biblioteca.
55	Biblioteca	PRESTAMO DE MATERIAL BIBLIOGRAFICO	CONTROL DE USUARIOS	Formato que presenta el control de entrada y salida de los usuarios.
56	Biblioteca	PRESTAMO DE MATERIAL BIBLIOGRAFICO	FICHA DE PRESTAMO	Documento que registra los datos del usuario y el libro solicitado.
57	Biblioteca	PRESTAMO DE MATERIAL BIBLIOGRAFICO	ESTADISTICA DEL MATERIAL	Documento que relaciona la estadística del material bibliográfico.
58	Biblioteca	RECUPERACION DE MATERIAL BIBLIOGRAFICO	USUARIOS MOROSOS	Relación de usuarios morosos en biblioteca.
59	Biblioteca	PRESERVACION BIBLIOGRAFICA	MATERIAL A INTERVENIR	Documento donde se identifica, selecciona y se clasifica el material bibliográfico.
60	Bienestar	INGRESO DE ESTUDIANTES	SOLICITUD DE SUBSIDIO	Documento que contiene la solicitud del estudiante al subsidio estudiantil.
61	Bienestar	INGRESO DE ESTUDIANTES	RELACION DE ESTUDIANTES	Relación de estudiantes inscritos
62	Bienestar	INGRESO DE ESTUDIANTES	ENTREVISTA	Herramienta psicológica para el ingreso de estudiantes inscritos.
63	Bienestar	INGRESO DE ESTUDIANTES	TALLER PSICOLOGICO	Herramienta psicológica para el ingreso de estudiantes inscritos.
64	Bienestar	BIENESTAR INSTITUCIONAL	BIENESTAR INSTITUCIONAL	Servicio que se le presta a los estudiantes matriculados.
65	Bienestar	PETICION, QUEJAS Y RECLAMOS	PETICION, QUEJAS Y RECLAMOS	Solicitud de los usuarios con el servicio de atención al cliente.
66	Bienestar	PERMANENCIA CON CALIDAD	CONTROL DE CITAS PSICOLOGICAS	Documento que controla las citas psicológicas.
67	Compras y Mantenimiento	COMPRAS Y SERVICIOS ADMINISTRATIVOS	NECESIDADES Y REQUERIMIENTOS	Listado de necesidades y requerimientos de las diferentes áreas.
68	Compras y Mantenimiento	COMPRAS Y SERVICIOS ADMINISTRATIVOS	RADICACION DE NECESIDADES	Documento que registra las solicitudes presentadas de las necesidades y requerimientos.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
69	Compras y Mantenimiento	COMPRAS Y SERVICIOS ADMINISTRATIVOS	CLASIFICACION DE NECESIDADES	Documento que clasifica según las necesidades presentadas.
70	Compras y Mantenimiento	COMPRAS Y SERVICIOS ADMINISTRATIVOS	PLAN ANUAL DE ADQUISICION	Es el instrumento de administración financiera mediante el cual se verifica y aprueba el monto máximo mensual de recursos disponibles para el Infotep.
71	Compras y Mantenimiento	COMPRAS Y SERVICIOS ADMINISTRATIVOS	SEGUIMIENTO Y CONTROL DEL PAA	Documento que registra actividades de supervisión y control.
72	Compras y Mantenimiento	PLAN ANUAL DE ADQUISICION	REQUISICION DE COMPRA	Es una autorización al área de Compras y mantenimiento con el fin de abastecer bienes o servicios.
73	Compras y Mantenimiento	PLAN ANUAL DE ADQUISICION	COMPROBANTE DE INGRESO A ALMACEN	Es un soporte de contabilidad en el que se reflejan los ingresos en efectivo, cheque y otras formas de recaudo. Son documentos que registra el área de compras y mantenimientos, información referida a las compras, transferencias, bajas, ubicación, depreciación y valores que corresponden a cada bien de uso que posee el Infotep.
74	Compras y Mantenimiento	PLAN ANUAL DE ADQUISICION	TARJETA REGISTRO Y CONTROL DE EXISTENCIA	El Plan Anual de Adquisiciones es una herramienta para: facilitar a la Entidad, identificar, registrar, programar y divulgar sus necesidades de bienes, obras y servicios; y diseñar estrategias de contratación basadas en agregación de la demanda que permitan incrementar la eficiencia del proceso de contratación.
75	Compras y Mantenimiento	PLAN ANUAL DE ADQUISICION	ANALISIS DE MOVIMIENTO DE ALMACEN	Es el documento mediante el cual se formaliza la solicitud de pedidos y necesidades.
76	Compras y Mantenimiento	SALIDA DE MERCANCIA	PEDIDOS	Es el documento legal que identifica clara y detalladamente las salida física y real de un bien, cesando de esta manera la responsabilidad por la custodia, administración y conservación por parte del encargado de la Bodega y quedando en poder y bajo la responsabilidad del funcionario destinatario.
77	Compras y Mantenimiento	SALIDA DE MERCANCIA	COMPROBANTE DE SALIDA	

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
78	Compras y Mantenimiento	CONTROL DE INVENTARIOS	INSPECCION DE BIENES	Documento que registra la inspecciona las cantidades y la calidad de los bienes. Si existen bienes no conformes o que no cumplen con las características de calidad establecidas, se apartan y se identifican con la tarjeta de “Producto No conforme”, para evitar su entrega no intencional al usuario; luego se informa al proveedor para que proceda según sus políticas de devoluciones.
79	Compras y Mantenimiento	CONTROL DE INVENTARIOS	SOLICITUD DE TRASLADO DE BIENES	Documento que registra el traslado de bienes devolutivos, es un movimiento de inventario que solicitan los funcionarios del Infotep, con el fin de transferir la responsabilidad de su custodia, control y manejo de los bienes solicitados; este se podrá efectuar si cuenta con autorización del responsable de la dependencia a la cual pertenece el bien.
80	Compras y Mantenimiento	CONTROL DE INVENTARIOS	RELACION Y ACTUALIZACION DE INVENTARIOS	Revisión Física de Bienes Muebles y La Actualización Del Inventario
81	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	PLANILLA DE INSPECCION DE INFRAESTRUTURA	Documento que registra el estado del bien e inmueble
82	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	SOLICITUD DE MANTENIMEINTOS	Documento que contiene las solicitudes de mantenimiento de los bienes e inmuebles.
83	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	PLAN GENERAL DE MANTENIMIENTO	Documento que registra la Documentación que registra las necesidades de mantenimiento, el cronograma y ejecución de las actividades de mantenimiento.
84	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	CRONOGRAMA DE MANTENIMIENTO	Documento que registra las actividades de mantenimiento, con sus respectivas fechas y responsable.
85	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	HOJA DE VIDA EQUIPOS Y MANTENIMIENTO	Documento que especifica la información que identifica el equipo. Las partes que lo conforman y sus características, y el historial de mantenimientos preventivos y correctivos que se le han realizado.
86	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	REGISTRO DE MANTENIMIENTO	Documento que registra la actividad de mantenimiento, a las instalaciones, equipos y bienes. Mediante la utilización de recursos físicos, humanos, y tecnológicos, para minimizar y corregir fallas imprevistas.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
87	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	SEGUIMIENTO Y CONTROL AL PLAN DE MANTENIMIENTO	Documento que registra la supervisión, el control y seguimiento del mantenimiento preventivo y correctivo.
88	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	PRESTAMO DE INSTALACIONES FISICAS	Documento que especifica la información de las solicitudes de préstamo las instalaciones.
89	Compras y Mantenimiento	MANTENIMIENTO PREVENTIVO Y CORRECTIVO	SALIDA E INGRESO DE BIENES	Documento que especifica la entrada y salida de bienes del almacén.
90	Compras y Mantenimiento	CONTROL DE VEHICULOS	CRONOGRAMA GENERAL DE PRACTICA	Documento que registra la programación del uso vehicular.
91	Compras y Mantenimiento	CONTROL DE VEHICULOS	SALIDA DE VEHICULO	Autorización de salida de vehículos.
92	Compras y Mantenimiento	CONTROL DE VEHICULOS	PLANILLA DE ABORDAJE	Documento que especifica la información del viaje, origen, destino, motivo, fecha, entre otros.
93	Compras y Mantenimiento	CONTROL DE VEHICULOS	PRE-OPERACIONAL	Documento que contiene la identificación de peligros y valoración de riesgos hasta el control y gestión de los mismos con el fin de prevenir lesiones personales, daño a la propiedad, daño a terceros y eficiencia en las operaciones
94	Compras y Mantenimiento	CONTROL DE VEHICULOS	CONTROL DEL USO DE VEHICULOS	Documento que registra la información del control de vehículos.
95	Compras y Mantenimiento	CONTROL DE VEHICULOS	PLAN DE MANTENIMIENTO DE VEHICULOS	Plan que contiene las actividades previamente establecidas, con el fin de anticiparse a la ocurrencia de fallas en los vehículos.
96	Compras y Mantenimiento	CONTROL DE VEHICULOS	HOJA DE VIDA DEL VEHICULO	Establecer la metodología y las acciones para llevar a cabo en el mantenimiento preventivo y correctivo vehicular Documento que especifica la información que identifica el vehículo, sus características, y el historial de mantenimientos preventivos y correctivos que se le han realizado.
97	Control Interno	EVALUACION DEL SISTEMA DE CONTROL INTERNO	SEGUIMIENTO Y EJECUCION AL PLAN DE DESARROLLO	Es un instrumento de planeación construido de manera participativa, donde se establece un acuerdo entre todos los miembros de la institución para trabajar con los mismos propósitos y sobre las bases de las mismas políticas. En el Plan de Desarrollo Institucional se consignan, el componente estratégico y operativo como lo establece la Ley Orgánica de Planeación, sus objetivos o ejes estratégicos de desarrollo y

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
98	Control Interno	EVALUACION DEL SISTEMA DE CONTROL INTERNO	SEGUIMIENTO AL REPORTE DE INFORMACION	bienestar, las metas de resultados que se pretenden alcanzar, los programas y subprogramas que tuvieran a lugar, y los recursos que se van a invertir durante el periodo de Dirección. seguimiento al reporte del Sistema Nacional de Información de la Educación Superior (SNIES), Este sistema como fuente de información, en relación con las instituciones y programas académicos aprobados por el Ministerio de Educación Nacional, consolida y suministra datos, estadísticas e indicadores.
99	Control Interno	EVALUACION DEL SISTEMA DE CONTROL INTERNO	NORMOGRAMA	Documento que permite a las entidades públicas y privadas delimitar las normas que regulan sus actuaciones en desarrollo con su objeto misional. El normograma contiene las normas externas como leyes, decretos, acuerdos, circulares, resoluciones que afectan la gestión de la entidad y las normas internas como reglamentos, estatutos, manuales y, en general, todos los actos administrativos de interés para la entidad que permiten identificar las competencias, responsabilidades y funciones de las dependencias de la organización.
100	Control Interno	EVALUACION DEL SISTEMA DE CONTROL INTERNO	MATRIZ DE RIESGO POR PROCESOS	Documento que tiene el propósito de identificar los riesgos operacionales de mayor incidencia en la entidad, labor realizada de acuerdo con las normas técnicas de calidad nacional. Los programas de Auditoría son guías detalladas sobre los procedimientos y pruebas a realizar para cumplir con los objetivos y propósitos de la auditoría.
101	Control Interno	AUDITORIA INTERNA	PROGRAMA DE AUDITORIA	Los programas de Auditoría son guías detalladas sobre los procedimientos y pruebas a realizar y la extensión de las mismas para cumplir con los objetivos y propósitos de la auditoría. Los programas de Auditoría son guías detalladas sobre los

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
				procedimientos y pruebas a realizar y la extensión de las mismas para cumplir con los objetivos y propósitos de la auditoría. Los programas de Auditoría son guías detalladas sobre los procedimientos y pruebas a realizar y la extensión de las mismas para cumplir con los objetivos y propósitos de la auditoría. Documento que contiene las actividades de Auditoría que a lo largo del año serán desarrolladas por las diferentes Unidades o Comités de Auditoría, en coordinación con la Oficina de Gestión de la Calidad del establecimiento o sus equivalentes.
102	Control Interno	AUDITORIA INTERNA	PLAN DE AUDITORIA	
103	Control Interno	AUDITORIA INTERNA	ENCUESTA	Instrumento de investigación para obtener resultados de la auditoría.
104	Control Interno	AUDITORIA INTERNA	ACTA	Documento que registra y legaliza las actividades de la auditoría interna.
105	Control Interno	AUDITORIA INTERNA	INFORME DE AUDITORIA	Informe de auditoría interna que se presenta a alta dirección.
106	Control Interno	AUDITORIA INTERNA	PLAN DE MEJORAMIENTO	Documento que contiene las acciones s de mejora, resultado de la auditoría interna.
107	Control Interno	INFORMES ESCRITOS	INFORMES	Informes
108	Control Interno	PLAN DE MEJORAMIENTO INSTITUCIONAL	EVALUACION DEL PLAN DE MEJORAMIENTO	Documento que contiene acciones de mejora, resultado de la evaluación institucional.
109	Control Interno	PLAN DE MEJORAMIENTO POR PROCESO	EVALUACION DEL PLAN DE MEJORAMIENTO	Documento que contiene las acciones s de mejora de cada proceso, resultado de la auditoría interna.
110	Control Interno	PLAN DE MEJORAMIENTO INDIVIDUAL	SEGUIMIENTO AL PLAN DE MEJORAMIENTO	Documento con el seguimiento de dicho plan
111	Archivo	ACTAS	ACTA DE COMITÉ DE ARCHIVO	Documento por medio del cual se publica y aprueban documentos y actividades relacionadas con la gestión documental.
112	Archivo	ACTAS	ACTA DE ELIMINACION DOCUMENTAL	Documento por medio del cual se aprueba la eliminación de expedientes.
113	Archivo	RECEPCION DE DOCUMENTOS	RECEPCION DE DOCUMENTOS	Procedimiento que realiza la actividad de recibir y entregar la documentación de la entidad.
114	Archivo	INFORMES	INFORMES ESTADISTICOS	Informes estadísticos de la prestación del servicio de consulta de documentos.
115	Archivo	PRESTAMO DOCUMENTAL	REQUERIMIENTO DOCUMENTAL	Formato que presenta el usuario que requiere una consulta documental.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
116	Archivo	PRESTAMO DOCUMENTAL	PRESTAMO DOCUMENTAL	Formato que presenta el usuario que requiere un préstamo documental.
117	Archivo	PRESTAMO DOCUMENTAL	ENCUESTA	Instrumento de investigación para obtener información del servicio prestado.
118	Archivo	DISPOSICION FINAL	INFORME	Informe de disposición final.
119	Acreditación institucional	EVALUACION	EVALUACION DE ESTUDIANTES	Instrumentos de evaluación estudiantil
120	Acreditación institucional	EVALUACION	EVALUACION DE DOCENTE	Instrumentos de evaluación docente
121	Acreditación institucional	EVALUACION	EVALUACION PROGRAMA ACADEMICOS	Instrumentos de evaluación a programas académicos.
122	Acreditación institucional	ACREDITACION DE PROGRAMACION ACADEMICOS	CONDICIONES DE CALIDAD	Requisitos para obtener y renovar registro calificado.
123	Acreditación institucional	ACREDITACION DE PROGRAMACION ACADEMICOS	VERIFICACION EXTERNA	Requisitos para obtener y renovar registro calificado.
124	Acreditación institucional	ACREDITACION DE PROGRAMACION ACADEMICOS	ACTAS	Requisitos para obtener y renovar registro calificado.
125	Acreditación institucional	ACREDITACION DE PROGRAMACION ACADEMICOS	INFORME	Requisitos para obtener y renovar registro calificado.
126	Centro de Investigación	POLÍTICAS Y NORMAS DE INVESTIGACION	NORMATIVIDAD	Documento con políticas y normas de investigación.
127	Centro de Investigación	CONVOCATORIA	INSCRIPCION	Inscripción de proyectos de investigación.
128	Centro de Investigación	CONVOCATORIA	PROPUESTA	Documento con la propuesta de investigación.
129	Centro de Investigación	CONVOCATORIA	INFORME FINAL DE PROYECTOS	Informe de proyectos de investigación.
130	Centro de Investigación	REVISION DE PROYECTOS	MONOGRAFIAS	Documento que legaliza la revisión y seguimiento de los proyectos
131	Centro de Investigación	REVISION DE PROYECTOS	INFORME DE PRACTICAS	Documento que legaliza la revisión y seguimiento de los proyectos
132	Centro de Investigación	REVISION DE PROYECTOS	ACCION POR PROGRAMA	Documento que legaliza la revisión y seguimiento de los proyectos
133	Centro de Investigación	SEGUIMIENTO A PROYECTOS	PLANIFICACION	Documento que legaliza la revisión y seguimiento de los proyectos
134	Centro de Investigación	SEGUIMIENTO A PROYECTOS	PROYECTOS	Documento que legaliza la revisión y seguimiento de los proyectos
135	Centro de Investigación	SEMILLEROS DE INVESTIGACION	CONVOCATORIA	Invitación a pertenecer a semilleros de investigación.
136	Centro de Investigación	SEMILLEROS DE INVESTIGACION	OFICIALIZACION DE GRUPOS DE SEMILLEROS	Documento que oficializa el grupo de semilleros.
137	Centro de Investigación	SEMILLEROS DE INVESTIGACION	CAPACITACION	Capacitaciones Investigación
138	Centro de Investigación	SEMILLEROS DE INVESTIGACION	CRONOGRAMA	Documento con las fechas planeadas para las actividades de investigación.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
139	Centro de Investigación	SEMILLEROS DE INVESTIGACION	ENCUESTA	Instrumento de Investigación
140	Planeación	ANTEPROYECTO DE PRESUPUESTO	ANTEPROYECTO DE PRESUPUESTO	Instrumento que propone la disponibilidad presupuestal de la entidad.
141	Planeación	BANCO DE PROYECTOS	BANCO DE PROYECTOS	Proyectos con necesidades de la institución, que garantizan la disponibilidad presupuestal
142	Planeación	INFORMES	INFORME GENERAL INSTITUCIONAL	Informe presupuestal
143	Planeación	INFORMES	INFORME ENTIDADES DEL ESTADO	Informe presupuestal
144	Planeación	MEDICION DE INDICADORES	MEDICION DE INDICADORES	Documento que realiza seguimiento a los indicadores de gestión.
145	Planeación	PLAN DE ACCION INSTITUCIONAL	PLAN DE ACCION INSTITUCIONAL	Documento que incluye las actividades requeridas en cada proceso anualmente.
146	Planeación	PROYECTO DE DESARROLLO EDUCATIVO	PROYECTO DE DESARROLLO EDUCATIVO	Documento que incluye las actividades misionales requeridas anualmente.
147	Planeación	SEGUIMIENTO Y CONTROL	SEGUIMIENTO Y CONTROL	Acciones de seguimiento y control a los proyectos y planes de acción.
148	Proyección Social	DESARROLLO, SEGUIMIENTOS Y CONTROL DE PROYECTOS	DESARROLLO, SEGUIMIENTOS Y CONTROL DE PROYECTOS	Acciones de seguimiento y control a los proyectos y planes de acción.
154	Proyección Social	PROYECCION A LA COMUNIDAD	Propuesta	Propuesta de proyección a la comunidad.
155	Proyección Social	PROYECCION A LA COMUNIDAD	Cronograma De Actividades	Cronograma De Actividades
156	Proyección Social	PROYECCION A LA COMUNIDAD	Informe	Informe de proyección a la comunidad.
157	Proyección Social	PROMOCION Y DIFUSION INSTITUCIONAL	Cronograma	Cronograma de promoción y difusión institucional.
158	Proyección Social	PROMOCION Y DIFUSION INSTITUCIONAL	Planilla De Promoción Institucional	Planilla De Promoción Institucional
159	Proyección Social	PROMOCION Y DIFUSION INSTITUCIONAL	Preinscripción De Estudiantes	Preinscripción De Estudiantes
160	Proyección Social	PROMOCION Y DIFUSION INSTITUCIONAL	Informe	Informe
161	Proyección Social	PROGRAMA DE EDUCACION CONTINUADA	Encuesta	Encuesta
162	Proyección Social	PROGRAMA DE EDUCACION CONTINUADA	Inscripción	Inscripción
163	Proyección Social	PROGRAMA DE EDUCACION CONTINUADA	Registro De Parcelación	Registro De Parcelación
164	Proyección Social	DESARROLLO DE CURSOS	DESARROLLO DE CURSOS	Desarrollo de cursos a egresados y estudiantes.
165	Proyección Social	PORTAFOLIO DE SERVICIOS	PORTAFOLIO DE SERVICIOS	Portafolio de servicios del Infotep.
166	Sistemas y Comunicación	APOYO AL SISTEMA TECNOLÓGICO	APOYO AL SISTEMA TECNOLÓGICO	Servicio de apoyo al sistema del Infotep.
167	Sistemas y Comunicación	RESPALDO DE INFORMACION	RESPALDO DE INFORMACION	Backup de la información.
168	Sistemas y Comunicación	COMUNICACIÓN INTERNA Y EXTERNA	COMUNICACIÓN INTERNA Y EXTERNA	Servicio de comunicación interna y externa en el Infotep.
169	Sistemas y Comunicación	DISEÑO DE IMÁGENES Y GRÁFICOS DE DIFUSION	DISEÑO DE IMÁGENES Y GRÁFICOS DE DIFUSION	Diseño de imágenes y gráficos.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
170	Sistemas y Comunicación	CREACION O MODIFICACION DE CORREOS	CREACION O MODIFICACION DE CORREOS	Manejo de correos institucionales.
171	Vicerrectoría Académica	ACTUALIZACION DEL PLAN DE ESTUDIO	ACTUALIZACION DEL PLAN DE ESTUDIO	Actualización del plan de estudio.
172	Vicerrectoría Académica	PROGRAMA ACADEMICO	PROGRAMA ACADEMICO	Programas académicos.
173	Vicerrectoría Académica	EVALUACION A LA PRESTACION DEL SERVICIO ACADEMICO	EVALUACION A LA PRESTACION DEL SERVICIO ACADEMICO	Evaluación de la prestación del servicio académico.
174	Vicerrectoría Académica	REGISTRO CALIFICADO DE PROGRAMA	REGISTRO CALIFICADO DE PROGRAMA	Requisitos para obtener y renovar registro calificado.
175	Vicerrectoría Académica	PLANIFICACION DOCENTE	PLANIFICACION DOCENTE	Actividades de planeación docente.
176	Vicerrectoría Académica	SATISFACCION DEL CLIENTE	SATISFACCION DEL CLIENTE	Satisfacción al cliente
177	Talento Humano	SELECCIÓN Y CONTRATACION DE PERSONAL	INSCRIPCION DE ASPIRANTES	Inscripción a vacante de personal
178	Talento Humano	SELECCIÓN Y CONTRATACION DE PERSONAL	LISTA DE ADMITIDOS Y NO ADMITIDOS	Listado de admitidos
179	Talento Humano	SELECCIÓN Y CONTRATACION DE PERSONAL	ACTAS	Documento que legaliza la selección y contratación de personal.
180	Talento Humano	INDUCCION Y REINDUCCION	EVALUACION DEL PROGRAMA DE INDUCCION Y REINDUCCION	Inducción a procesos.
181	Talento Humano	EVALUACION DE COMPETENCIAS	RESUMEN DE RESULTADOS DE EVALUACION DE DESEMPEÑO Y COMPETENCIAS	Evaluación de competencias del personal
182	Talento Humano	EVALUACIONES DE DESEMPEÑO	RESUMEN DE RESULTADOS DE EVALUACION DE DESEMPEÑO Y COMPETE	Evaluación de desempeño del personal.
183	Talento Humano	LIQUIDACION DE NOMINAS	LIBRANZAS	Liquidación de nóminas (libranzas)
184	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	SOLICITUD DE CAPACITACION	Solicitudes de capacitación a cada jefe de proceso.
185	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	ENCUESTA DE OPINION	Instrumento de Investigación, la encuesta de opinión.
186	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	ANALISIS DE RESULTADOS DE LA ENCUESTA	Estadísticas de capacitación y bienestar y estímulos.
187	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	PLAN DE CAPACITACION	Planeación de la capacitación anual
188	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	EVALUACION DE CAPACITACION	Evaluación de la capacitación,
189	Talento Humano	CAPACITACION, BIENESTAR, ESTIMULOS E INCENTIVOS	RESULTADO DE EVALUACION DE CAPACITACION	Resultado de la evaluación
190	Talento Humano	EVALUACIONES MEDICAS	PAZ Y SALVO	Documento Paz y salvo
191	Talento Humano	IDENTIFICACION DE PELIGRO Y EVACUACION DE RIESGO	PROGRAMA DE INSPECCIONES PLANEADAS	Programa de inspección de riesgos laborales.
192	Talento Humano	IDENTIFICACION DE PELIGRO Y EVACUACION DE RIESGO	MATRIZ DE IDENTIFICACION DE PELIGROS Y EVALUACION DE RIESGOS OCUPACIONALES	Instrumento de identificación de riesgos y peligros laborales.
193	Talento Humano	INVESTIGACION DE ACCIDENTE DE TRABAJO	ACTA	Documentos que legaliza la investigación del accidente laboral.
194	Talento Humano	SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO	CRONOGRAMA	Cronograma de seguridad y salud en el trabajo.
195	Talento Humano	SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL	EVALUACION SISTEMA DE GESTION DE SEGURIDAD Y	Evaluación del Sistema de seguridad y salud en el trabajo.

Id	Dependencia:	Categorías o Series de información:	Nombre o título de la información	Descripción de la información
		TRABAJO	SALUD EN EL TRABAJO	
196	Talento Humano	SIMULACROS	PLAN DE EMERGENCIA	Simulacros de plan de emergencia.
197	Talento Humano	SIMULACROS	REVISION DE BOTIQUIN	Revisión de Botiquín
198	Talento Humano	SIMULACROS	INSPECCION DE EXTINTORES	Inspección y revisión de extintores.
199	Talento Humano	SIMULACROS	EVALUACION DEL SIMULACRO	Evaluación del simulacro.
200	Talento Humano	ACOSO LABORAL	ACTAS	Actas de acoso laboral.
201	Talento Humano	NOVEDAD DE PERSONAL	CERTIFICACIONES	Certificación de novedades de personal
202	Talento Humano	NOVEDAD DE PERSONAL	SOLICITUD Y REGISTRO DE PERMISO	Solicitud y registro de permiso del personal
203	Talento Humano	NOVEDAD DE PERSONAL	REGISTRO DE INCAPACIDADES	Registro de incapacidades.
204	Talento Humano	NOVEDAD DE PERSONAL	INFORME DE AUSENTISMO LABORAL	Informe de ausentismo laboral
205	Talento Humano	NOVEDAD DE PERSONAL	PRESTAMO DE HISTORIAS LABORALES	Consulta de historias laborales.
206	Talento Humano	NOVEDAD DE PERSONAL	ACTAS	Actas de novedades de personal.
207	Talento Humano	NOVEDAD DE PERSONAL	PAZ Y SALVO	Paz y salvo

9.2. Identificar amenazas y vulnerabilidades

“Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo” (MINTIC, 2016)

A continuación, se muestran las amenazas identificadas para los activos de la institución.

Tabla 4. Amenazas

Tipo	Amenaza	Origen
Daño Físico	Incendios	A, D, E
	Contaminación, corrosión	A, D, E
	Destrucción del equipo o medios	A, D, E
Eventos naturales	Inundación, Fenómenos climáticos o meteorológicos	E

	Fenómenos sísmicos	E
Pérdida de los servicios esenciales	Pérdida de suministro de energía	A, E
	Falla en equipo de telecomunicaciones	A
	Hurto de equipo, medios o documentos	D
Compromiso de la información	Divulgación	D, A
	Manipulación con software	D
	Manipulación con hardware	D
	Espionaje remoto	D
Fallas técnicas	Mal funcionamiento del software	A
	Fallas del equipo	A
	Suplantación de identidad	D
Acciones no autorizadas	Procesamiento ilegal de datos	D
	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D

D= Deliberadas, A= Accidentales, E= Ambientales

9.3. Identificar los impactos

Tabla 5. Mapa de Riesgo Inherente

Casi seguro					R6	Extremo
Probable			R1 R3 R4			Alto
Posible		R2				Moderado
Improbable						Bajo
Raro			R5			
	Insignificante	Menor	Moderado	Mayor	Catastrófico	

Tabla 6. Mapa de impactos

PROBABILIDAD							
Casi seguro (A)	• Se ha presentado en el sector público o en el MEN más de una vez en el último año	Alto	Alto	Extremo	Extremo	Extremo	Extremo

		• Ocurrirá con alto nivel de certeza el próximo año					
	Probable (B)	• Se ha presentado en el sector público o en el MEN en el último año • Se espera que ocurra en la mayoría de los casos o circunstancias	Moderado	Alto	Alto	Extremo	Extremo
	Posible (C)	• Se ha presentado en el sector público o en el MEN en los últimos 2 años • Es probable que ocurra en esta vigencia	Bajo	Moderado	Alto	Extremo	Extremo
	Improbable (D)	• Se ha presentado en el sector público o en el MEN en los últimos 5 años • Es poco probable que ocurra esta vigencia	Bajo	Bajo	Moderado	Alto	Extremo
	Raro (E)	• No se ha presentado en el sector público o en el MEN en los últimos 5 años • El evento puede ocurrir sólo en circunstancias excepcionales	Bajo	Bajo	Moderado	Alto	Alto
Zona de riesgo baja : asumir el riesgo Zona de riesgo moderada : asumir el riesgo, reducir el riesgo Zona de riesgo alta : reducir el riesgo, evitar, compartir o transferir Zona de riesgo extrema : reducir el riesgo, evitar, compartir o transferir			Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)

10. Caracterización y Valoración de los Activos

Tabla 7. Caracterización y Valoración de los Activos

Tipo	Activo
Aplicaciones Informáticas	1. Sistema de Información Académica y de Gestión. Academusoft
	2. Sistema Contable y Financiero. DBS Financiero
	3. Sistema de Automatización de Bibliotecas. Openbiblio
	4. Acceso a publicaciones SPIP
	5. Sistema de Gestión Documental. Gestmail
	6. Gestión de contenidos Pagina Web Institucional. Jommla
	7. Sistema Operativo.
	8. Herramientas Software.
	9. Antivirus
Servicios	10. Servidor Sitios Web.
	11. Servidor Proxy.
	12. Servidor DNS
	13. Servidor DHCP
	14. Servidor Telefonía IP
	15. Servidor Bases de Datos
	16. Servidor Cámaras IP
	17. Servidor herramientas virtuales de aprendizaje.
Redes de Comunicaciones	18. Firewall / Equipo Unificado contra Amenazas.
	19. Equipos de computo
	20. Switch Administrable
Dispositivo Auxiliar	21. Cableado de Red

Tipo	Activo
Instalaciones	22. Sistema de Alimentación Ininterrumpida.
	23. Gabinete de Red
Personal	24. Asesor Tecnologías de Información y Comunicaciones
	26. Técnico Administrativo
	27. Técnico Administrativo Experto
	28. Contratista.

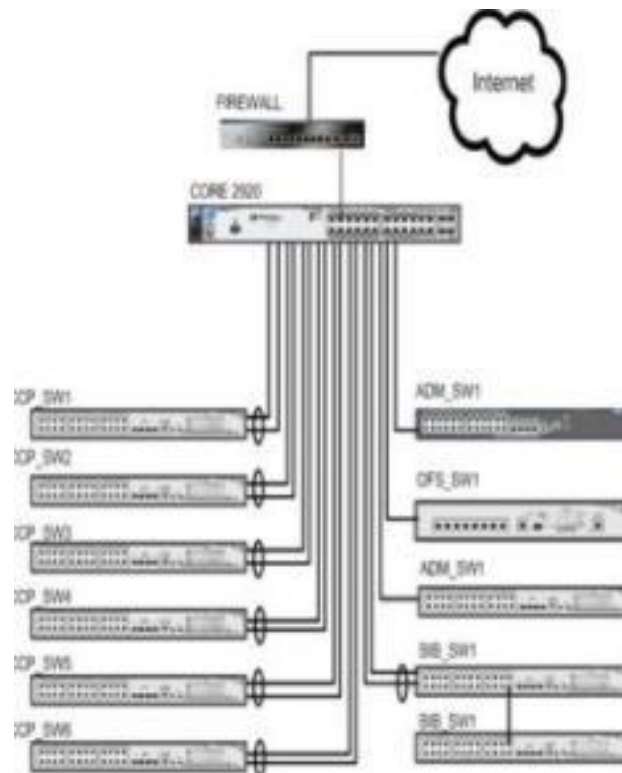


Figura 3. Diagrama de Red

Tabla 8. Escala de valoración activos

	Valor		Criterio
10	Extremo	E	Daño extremadamente grave.
9	Muy Alto	MA	Daño Muy grave
6-8	Alto	A	Daño grave.
3-5	Medio	M	Daño importante
1-2	Bajo	B	Daño Menor
0	Despreciable	D	Irrelevante a efectos prácticos

Valor a los Activos

Dimensiones de Seguridad. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información.
- [A] Autenticidad
- [T] trazabilidad

Tabla 9. Valoración de aplicaciones

Activo	Dimensiones de Seguridad

	D	I	C	A	T
Sistema de Información Académica y de Gestión	MA	MA	M	A	A
Sistema Contable y Financiero		A	A	A	
Sistema de Automatización de bibliotecas	M	A			
Acceso a publicaciones	M				
Sistema de Gestión Documental	A	A	A		
Gestión de contenidos Pagina Web Institucional	MA				
Sistema Operativo	MA	A			
Herramientas de Software	MA	A			
Antivirus	A				

Tabla 10. Valoración de Servicios

Activo	Dimensiones de Seguridad				
	D	I	C	A	T
Servidor WEB		MA	A		
Servidor Proxy	E	A			
Servidor DHCP	M	A			
Servidor telefonía IP	B	B			
Servidor de Base de Datos	E	MA		MA	A
Servidor de Camaras	B				
Servidor de herrameintas virtuales	M	M	M		

11. Análisis de las Vulnerabilidades

Tabla 11. Análisis de Vulnerabilidades

✓ Los desarrollos de nuevas funcionalidades del software de gestión documental no quedan registrados y/o actualizadas en el aplicativo de control de versiones, permaneciendo de manera local en el equipo del desarrollador.	✓ Manipulación no autorizada de la información que puede conllevar a la afectación del buen funcionamiento de la Institución.
✓ No hay definido un plan detallado de pruebas de seguridad a efectuar en las etapas del desarrollo de software.	✓ Afectación de la operación en la Institución debido a la indisponibilidad de la información
✓ No se realizan pruebas de seguridad sobre el software que permitan detectar vulnerabilidades de seguridad.	✓ Divulgación de información no autorizada por terceros por asignación excesiva de permisos sobre un rol.
✓ Ausencia de un plan de tratamiento de incidentes de seguridad.	
✓ Ausencia de configuraciones de seguridad en el aplicativo que permita solicitar el cambio de la contraseña con el aprovisionamiento del servicio de un usuario nuevo.	✓ Afectación en los ingresos económicos debido a la divulgación de las vulnerabilidades de seguridad del aplicativo
✓ • El software no cuenta con lineamientos de seguridad que establezca una frecuencia de renovación y cambio del password por parte del usuario.	
✓ • El sistema operativo de red instalado en algunos servidores no se encuentra licenciado ni actualizado	✓ • Eliminación de información clave para la Institución afectando la disponibilidad de la misma para el desarrollo de las actividades.
✓ • Ausencia de configuraciones de seguridad en los servidores.	✓ • Manipulación no autorizada de las configuraciones de los servicios de red, afectando la disponibilidad del servicio a los trabajadores de la Institución.
✓ • El respaldo de Backup se encuentra ubicado en los mismos servidores a los cuales les establecen las copias de respaldo	✓ • Pérdida de información que puede conllevar a la afectación de la Institución.
✓ • No se realiza un monitoreo constante de los eventos y registro de logs que permitan detectar posibles intrusiones y/o debilidades de seguridad.	✓ • Afectación de la operación de la Institución debido a la indisponibilidad de la información.

✓ El antivirus instalado en los servidores no se encuentra activo ni actualizado. ✓ Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en el área donde se encuentran instalados los servidores. ✓ • No existen configuraciones de seguridad establecidas en los servidores ni en los servicios de red que han sido implementados a través de la red corporativa.	✓ Divulgación de información no autorizada por terceros por asignación excesiva de permisos sobre los servidores.
✓ • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad relativa en cuarto de equipos (Centro de cómputo). ✓ • Deficiencias en las configuraciones de seguridad de la red inalámbrica, empleando un cifrado débil. ✓ • Pérdida de confidencialidad de información que puede ser sensible para la Institución, debido a que es compartida a través de la infraestructura de red de la misma, permitiendo su visualización a personas no autorizadas.	✓ • Pérdida de información que puede conllevar a la afectación de la Institución. ✓ Indisponibilidad de los servicios que se brindan a través de la red ocasionando tiempos no productivos del equipo de desarrollo de la Institución. ✓ • Pérdida de disponibilidad, integridad y confidencialidad de la información de la entidad, generando un impacto negativo en la continuidad del negocio.

12. Análisis y evaluación de riesgo

Con base en las amenazas identificadas se realizó la identificación de los riesgos y el análisis de la probabilidad de ocurrencia e impacto. Según nos dice MINTIC (2016), con estos datos se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

Tabla 12. Análisis y evaluación de Riesgo

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
Recurso Humano	a). Desconocimiento de código de ética, manual de políticas de seguridad	Mala aplicación de los principios éticos No aplicación de las políticas definidas por el INFOTEP. Incurrir en prácticas indebidas. Acciones equivocadas o destrucción uso no autorizado de equipos	Rara vez	Catastrófico	Alto
	b). Ausencia de planes de capacitación al personal y oportuno entrenamiento en seguridad de la información	Baja cultura frente al riesgo Indebida interpretación de la normatividad interna y externa de seguridad de la información	Eventualmente	Catastrófico	Extremo
	c). Inadecuada segregación y dependencia de funciones y responsabilidades. (por insuficiencia de personal)	Facilita el ocultamiento de errores o acciones fraudulentas.	Puede Ocurrir	Mayor	Extremo
	d). Procedimientos no adecuados de contratación	Destrucción de equipos y medios	Media	Media	Alto

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
	e). Ausencia de adecuados canales de comunicación	Incurrir en errores u omisiones por falta de conocimiento de normas, instrucciones, procedimientos, entre otros.	Eventualmente	Mayor	Alto
	f). Trabajos no supervisados e inexistencias de mecanismos de monitoreo	Hurto de medios o documentos procesamiento ilegal de datos	posible	alta	
	a). Abstenerse de divulgar /comunicar a quien corresponda información sobre la cual estén obligados a transmitir.	Posibles sanciones de los organismos de control. Que se tomen decisiones equivocadas y en contra de sus intereses.	Rara Vez	Catastrófico	Alto
Información	b). Generar y suministrar información inoportuna, inexacta y no confiable a nivel interno y externo de la firma comisionista, con respecto a las actividades, líneas de negocio y operaciones asociadas.	Entregar información deficiente al cliente para la toma de decisiones. Afectar la relación cliente-Firma bajo esquemas de canales deficientes de información. Retardar, frenar e incurrir en errores de diferentes procedimientos y operaciones de la firma.	Rara Vez	Catastrófico	Alto
	c). Divulgar información confidencial	Manipulación indebida de los diferentes actores. Incidir deliberadamente en beneficio propio o de terceros y en detrimento de otros. Sanciones y penalidades por parte de los entes de vigilancia y control. Conflicto de interés	Rara Vez	Catastrófico	Alto

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
Tecnología de la información	d). Uso de información privilegiada	Manipulación indebida de la información. Incidir deliberadamente en beneficio propio o de terceros y en detrimento de otros.	Eventualmente	Catastrófico	Extremo
	e). Uso indebido de información de los clientes sujeta a reserva.	Posibles sanciones por parte de los organismos de control. Poner en riesgo al cliente.	Puede Ocurrir	Mayor	Extremo
	f). Recibir documentación falsa para obtener tramites	Posible detrimento del ambiente. Eventuales investigaciones por entes fiscalizadores.	Rara Vez	Catastrófico	Alto
	a). Débil estructura de seguridad (ausencia de políticas, procedimientos y controles)	Acceso de usuarios no autorizados a los sistemas de información. Uso indebido de los registros. Realizar operaciones no autorizadas. Información insuficiente para detectar directos responsables.	Puede Ocurrir	Mayor	Extremo
	b). Continuidad en las operaciones de la entidad ante un evento fortuito (falta de un plan de contingencia).	Pérdidas económicas por parálisis operativa. Generar perjuicios económicos a los clientes. Incumplimiento.	Puede Ocurrir	Catastrófico	Extremo
	c). Fallas en la comunicación y operación de los sistemas de la entidad externa e internamente.	Pérdida de información. Pérdidas económicas por dificultad para operar. Pérdida de clientes Incremento de costos operativos. Eventuales sanciones por incumplimiento de operaciones. Pérdida de negocios	Probable	Catastrófico	Extremo

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
	d). Falta de integralidad de los sistemas de información	Errores en la manipulación de datos. Incremento de costos en el procesamiento de la información. Bajo nivel de confiabilidad en los datos procesados. Baja eficiencia en las actividades desarrolladas.	Eventualmente	Moderado	Moderado
	e). Tener instalado software ilegal en la entidad	Incumplimiento de la Ley 603 de 2000 sobre propiedad intelectual, lo cual genera sanciones penales, pecuniarias y civiles para la entidad. Pérdida del valor de la información. Sanciones por parte de entidades de vigilancia y control.	Puede Ocurrir	Mayor	Extremo
	f). Ausencia de procedimientos para cambios y modificaciones del software funcional utilizado.	Pérdida de eficiencia en el procesamiento de la información. Bajo nivel de respuesta ante los cambios de tipo legal y operativo.	Eventualmente	Moderado	Moderado
	g). Realizar adquisiciones inadecuadas de hardware y software	Pérdida económica por decisiones mal fundamentadas. Atraso tecnológico. Pérdida de información. Débil respuesta informática a los requerimientos operativos y administrativos.	Puede Ocurrir	Moderado	Alto
	h). Ausencia de procedimientos legales para la contratación de soporte postventa.	Demoras en los cambios requeridos ante necesidades del usuario o un mal funcionamiento del sistema. Pérdida del servicio por ausencia del proveedor.	Puede Ocurrir	Mayor	Extremo

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
Operativo	i). Obsolescencia de los sistemas de información (hardware y software)	Ineficiencia operacional. Probabilidad de errores en el procesamiento de información. Ineficiencia en el desarrollo de las actividades laborales.	Puede ocurrir	Moderado	Alto
	j). Ausencia de pólizas de cumplimiento con los proveedores.	No reconocimiento de daños y perjuicios en un procesamiento inadecuado de la información originado por fallas del sistema. Pérdidas económicas para la Firma. Falta de soporte ante daños en los sistemas	Puede Ocurrir	Mayor	Extremo
	a). Administrar inadecuadamente los riesgos cuantificables y no cuantificables	Pérdidas económicas asociadas a operaciones no identificadas con un riesgo particular. Incurrir en errores susceptibles de sanción por parte de los organismos de control. Incumplimiento de normas sobre administración de riesgos. Afectar el normal desarrollo de las operaciones de la firma.	Puede Ocurrir	Catastrófico	Extremo
	b). Ausencia de manuales normas, políticas y procedimientos para la operación. Para el uso correcto de medios de telecomunicaciones y mensajería.	Incurrir en errores por desconocimiento de la actividad. Evasión de responsabilidades por parte del funcionario que incumple la norma. Ineficiencia en la asignación y ejecución de funciones. Facilidad para defraudar la entidad. Uso no autorizado de equipos y red Ausencia de funciones y obligaciones de la entidad por desconocimiento.	Eventualmente	Mayor	Alto

CATEGORÍA	RIESGO ASOCIADO	POSIBLES CONSECUENCIAS	PROB. OCURRENCIA	MAGNITUD DEL IMPACTO	CLASIFICACION DEL RIESGO
	c). Desconocimiento del sistema de gestión de la seguridad de la información	Alta exposición al riesgo en la totalidad de las operaciones realizadas. Informalidad en el desarrollo de las actividades. Falta de efectividad en las actividades desarrolladas. Conflictos internos.			Extremo
	d). Errores operativos	Pérdidas económicas, de recursos de información, humanos y técnicos por ineficacia en las operaciones. Pérdida de imagen corporativa. Desconfianza de los clientes hacia el INFOTEP.	Probable	Mayor	Extremo
	e). Limitación de recursos físicos y humanos	Dificultad para la segregación de funciones. Dificultad para desarrollar las actividades propias del cargo. Ineficacia en el cumplimiento de las labores encomendadas. Incurrir en errores y facilitar su ocultamiento. Limitación en posibles ejecuciones.	Probable	Moderado	Alto
	f). Débil estructura de seguridad de la información en la corporación	Pérdidas por ilícitos internos y externos en contra de la entidad. Facilidad para hacer uso indebido de los recursos. Dificultad para la consecución de pruebas en procesos disciplinarios y judiciales. Fraude Interno/Externo	Probable	Catastrófico	Extremo

13. Cronograma de Actividades

Logro	Criterio	Actividad	Producto / Meta	Responsable	Fecha programada	Recursos
		Revisar y o actualizar la metodología para la identificación, valoración y tratamiento de riesgos de seguridad de la información.	Matriz con la Metodología	Sistemas & Comunicación	09/04/2026	Recursos técnicos y humanos
		Revisar y o actualizar la declaración de aplicabilidad de acuerdo al anexo A de la norma ISO 27001:2013.	Documento Declaración de aplicabilidad	Sistemas & Comunicación	09/04/2026	Recursos técnicos y humanos
Implementación del Plan de Seguridad y Privacidad de Información y de los Sistemas de Información	Gestión de riesgos de seguridad y privacidad de la información	Crear documentos soporte de la implementación de controles físicos y lógicos planeados dentro del plan de implementación del MSPI.	Documento soporte de la implementación de controles físicos y lógicos	Sistemas & Comunicación	09/05/2026	Recursos técnicos y humanos
		Crear un documento con el plan de continuidad de negocio	Documento plan de continuidad de negocio	Sistemas & Comunicación	09/05/2026	Recursos técnicos y humanos
	Busca Implementación del Plan de Seguridad y Privacidad de Información y de los Sistemas de Información	Implementar el plan de continuidad de negocio en lo concerniente a tecnología	Registros que evidencian la ejecución del plan de continuidad de negocio	Sistemas & Comunicación	28/07/2026	Recursos técnicos y humanos
		Crear formatos e informes de seguimiento de la aplicación de controles preventivos y reactivos	Registros de seguimiento de la aplicación de controles preventivos y reactivos	Sistemas & Comunicación	29/07/2026	Recursos técnicos y humanos

Logro	Criterio	Actividad	Producto / Meta	Responsable	Fecha programada	Recursos
		Crear formatos e informes de seguimiento de la ejecución de concientización y comunicación del MPSI.	Registros sobre informes de seguimiento de la ejecución de concientización y comunicación del MPSI	Sistemas & Comunicación	29/09/2026	Recursos técnicos y humanos
		Crear un documento del plan de tratamiento de incidentes	Documento del plan de tratamiento de incidentes	Sistemas & Comunicación	29/09/2026	Recursos técnicos y humanos
Monitoreo y Mejoramiento Continuo	Evaluación del desempeño	Crear un documento del plan de seguimiento y desempeño del MPSI.	Documento del plan de seguimiento y desempeño del MPSI.	Sistemas & Comunicación	21/12/2026	Recursos técnicos y humanos
		Crear formatos de seguimiento al plan de tratamiento de incidentes	Registros de seguimiento al plan de tratamiento de incidentes	Sistemas & Comunicación	21/12/2026	Recursos técnicos y humanos

Referencias Bibliograficas

Bolaños, M. C., & Galvis, M. R. (25 de 03 de 2014). *AUDITORÍA DE SI*. Obtenido de <https://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin>

CENTENO, R., & GIMÉNEZ, O. (SF). *proyectos, cultura organizacional y competencias de los gerentes de proyectos según el modelo spv*.

DAFP. (2011). *Función Pública*. Obtenido de <http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/>

DAFP. (s.f.). *Guía Administración del riesgo V3*. Obtenido de <http://www.funcionpublica.gov.co/guias>

DAFP. (s.f.). *Información General*. Obtenido de <http://www.funcionpublica.gov.co/informacion-general>

Derrien, Y. (1994). *Técnicas de la auditoría informática*. Marcombo.

MINTIC. (2016). *Guía de gestión de riesgos*.

MINTIC. (2010). *Modelo de Seguridad y Privacidad de la Información*. Recuperado el 27 de mayo de 2018 del sitio web: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

MINTIC. (2010). *Guía 5: Política general MSPI v1*. Recuperado el 27 de mayo de 2018 del sitio web: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf