UNIDAD ACADÉMICA:

OFICINA DE POSTGRADOS

TEMA:

IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA GESTIÓN DE RIESGOS DE INFORMACIÓN BASADA EN LAS NORMAS ISO/IEC 27001 Y 27002 EN EL INSTITUTO TECNOLÓGICO SUPERIOR SUCRE

Proyecto de Investigación y Desarrollo previo a la obtención del título de Magíster en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo principal:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus Aplicaciones

Caracterización técnica del trabajo:

Desarrollo

Autor:

Ing. Flavio Eduardo López Vasco

Director:

Ing. Mtr. Javier Wilfrido Cóndor Cruz

Ambato – Ecuador

Enero 2019

Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre

Informe de Trabajo de titulación
Presentado ante la
Pontificia Universidad Católica del Ecuador
Sede Ambato

Por:

Flavio Eduardo López Vasco

En cumplimiento parcial de los
requisitos para el Grado de Magister en
Gerencia Informática

Pontificia Universidad Católica del Ecuador

Oficina de Postgrados
Enero 2019

Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre

Aprobado por:

María Fernanda San Lucas, Mg.
Presidente del Comité Calificador
Coordinadora de la Oficina de Postgrados

Verónica Maribel Pailiacho Mena, Mg.
Miembro Calificador

Javier Wilfrido Cóndor Cruz, Mg.
Miembro Calificador
Director de Proyecto

Hugo Rogelio Altamirano Villarroel, Dr.
Secretario General

Darío Javier Robayo Jácome, Mg.
Miembro Calificador

Fecha de aprobación:
Enero 2019

Ficha técnica

Programa: Magister en Gerencia Informática.

Tema: Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre.

Tipo de trabajo: Propuesta Metodológica y Tecnológica Avanzada.

Clasificación técnica del trabajo: Desarrollo

Autor: Flavio Eduardo López Vasco

Director: Ing. Javier Wilfrido Cóndor Cruz, Mtr.

Líneas de Investigación, Innovación y Desarrollo

Principal: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus Aplicaciones

Resumen Ejecutivo

El objetivo de esta investigación es implementar una metodología basada en las normas internacionales ISO/IEC 27001 y 27002 para la gestión de riesgos de información en el Instituto Tecnológico Superior "Sucre" [ITSS] de la ciudad de Quito, para dar cumplimiento al acuerdo N° 166 emitido por la Secretaría Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la Información. El proyecto se sustenta en la inexistencia de una Gestión de Riesgos de Seguridad de la Información, evidenciada a través de estrategias de seguridad de información ineficaces. El marco teórico analiza tanto normas de gestión de seguridad de la información como metodologías internacionales de gestión de riesgos de información. El proyecto es de intervención porque actúa materialmente de manera directa sobre un problema específico y la investigación es de tipo aplicada, cuasiexperimental, de nivel aplicativo, porque opera variables. El resultado del diagnóstico inicial de seguridad de la información en el ITSS, de 13% de conformidad respecto a ISO 27001, evidencia la poca importancia que recibía. Un procedimiento metodológico para la gestión de riesgos de información se adaptó y validó en el instituto, lo cual arrojó un nivel de conformidad de 38, 7%. Este trabajo propone las bases para futuras iniciativas en seguridad de la información que puedan ser implementadas en otros institutos tecnológicos superiores.

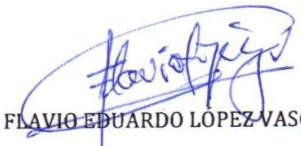
Declaración y Autorización

Yo: FLAVIO EDUARDO LÓPEZ VASCO con CC. 1712353596 autor del trabajo de graduación intitulado: "IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA GESTIÓN DE RIESGOS DE INFORMACIÓN BASADA EN LAS NORMAS ISO/IEC 27001 Y 27002 EN EL INSTITUTO TECNOLÓGICO SUPERIOR SUCRE", previa a la obtención del título profesional de Magíster en Gerencia Informática, en la Oficina de Postgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, enero 2019



FLAVIO EDUARDO LÓPEZ VASCO

CC. 171235359-6

Dedicatoria

A mi madre Martha y a mi padre Flavio Arturo, por su apoyo, amor, cuidado, acompañamiento y motivación.

A mis hijos Gabriel Eduardo y Emilia Victoria por motivar con su sola presencia todos mis logros y constituir el motivo para siempre salir adelante.

Reconocimientos

A la Pontificia Universidad Católica del Ecuador – Sede Ambato, a sus autoridades y personal administrativo y docente por la formación técnica y humanística recibida.

Al Instituto Tecnológico Superior Sucre, autoridades, personal docente y administrativo, en persona del doctor Santiago Illescas y magíster Fabián Cobos, rector y vicerrector, respectivamente; por su colaboración.

A Javier Cóndor Cruz Mtr. por su paciencia y respaldo, pues el asesoramiento y dirección de este trabajo de investigación por parte suya propician la concreción de un nuevo éxito académico.

Resumen

El objetivo de esta investigación es implementar una metodología basada en las normas internacionales ISO/IEC 27001 y 27002 para la gestión de riesgos de información en el Instituto Tecnológico Superior "Sucre" [ITSS] de la ciudad de Quito, para dar cumplimiento al acuerdo N° 166 emitido por la Secretaría Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la Información. El proyecto se sustenta en la inexistencia de una Gestión de Riesgos de Seguridad de la Información, evidenciada a través de estrategias de seguridad de información ineficaces. El marco teórico analiza tanto normas de gestión de seguridad de la información como metodologías internacionales de gestión de riesgos de información. El proyecto es de intervención porque actúa materialmente de manera directa sobre un problema específico y la investigación es de tipo aplicada, cuasiexperimental, de nivel aplicativo, porque opera variables. El resultado del diagnóstico inicial de seguridad de la información en el ITSS, de 13% de conformidad respecto a ISO 27001, evidencia la poca importancia que recibía. Un procedimiento metodológico para la gestión de riesgos de información se adaptó y validó en el instituto, lo cual arrojó un nivel de conformidad de 38, 7%. Este trabajo propone las bases para futuras iniciativas en seguridad de la información que puedan ser implementadas en otros institutos tecnológicos superiores.

Palabras claves: procedimiento metodológico, riesgos de información, gestión, ISO 27001, instituto tecnológico

Abstract

This research aims to implement a methodology based on the ISO/IEC 27001 and 27002 international standards for information risk management at Sucre Higher Technological Institute [ITSS] located in Quito, in order to comply with agreement Nº 166 enacted by the National Department for the Public Administration SNAP about the government information security model. The project was based on the lack of risk management of information security identified by inefficient information security strategies. The theoretical framework analyzes both information security management standards and international information risk management methodologies. The project directly intervenes in a specific problem using a quasi-experimental research method to be applied because it handles variables. The results from the initial assessment of information security at ITSS yielded that there is only 13% of compliance according to the ISO 27001, which shows little importance given to information security. Moreover, a methodological procedure for managing information risks is adapted and validated at ITSS which yielded a 38.7% of compliance. This study could be used as a foundation for future actions on information security, that can be implemented at technological institutes.

Key words: methodology, information risk, management, ISO 27001, technological institute

Tabla de contenidos

Lista de tablas

Lista de figuras

Capítulo 1

Introducción

Con el avance de la tecnología y especialmente Internet, se observa en titulares de prensa que en los últimos años se ha incrementado la incidencia de delitos relacionados con los sistemas de información tales como el fraude, la suplantación de identidad, el robo de contraseñas y de información confidencial. Por poner dos ejemplos; Según el diario La República con fecha 6 de abril de 2017, informa que "el Presidente de la República, Eco. Rafael Correa ha asegurado que hackers de EEUU violentaron la web del Consejo Nacional Electoral, CNE provocándole una caída de servicio por el tiempo 20 minutos el día de las elecciones de segunda vuelta" (La República., 2017) afectando de esta manera la reputación de esa institución frente a la ciudadanía ecuatoriana y los dos partidos políticos involucrados. De la misma forma, el diario El Comercio, el 9 de enero de 2016, dio a conocer que "Hackers registraron 366 títulos universitarios en la Senescyt y entregaron 600 licencias de conducir" (Ortiz, 2016) llegando a cobrar 10 000 dólares por el registro de un título de PhD y 1000 dólares por uno de licenciado o ingeniero, además de haber registrado fraudulentamente alrededor de 600 licencias de conducir, afectando no solamente a la institución en sí, sino reflejando el pésimo manejo de la confidencialidad de la información que debe primar en dicha institución pública.

A pesar de que amenazas a la información siempre han existido, en la actualidad, el accionar de personas malintencionadas, dedicadas a explotar vulnerabilidades en los sistemas es más especializado y deja como consecuencia caos, perjuicio económico y denigra la imagen de las organizaciones (Oliveira, 2016). Gómez Fernández (2012) advierte que ante tal escenario las empresas deben estructurar metódica y documentadamente, estrategias y controles que garanticen la gestión de sus procesos de negocio, dándole la debida importancia dentro de ellos al aseguramiento de la información.

De manera paralela al aparecimiento de amenazas a la seguridad de la información, también se han desarrollado normas y reglamentos con las cuales se puede preservar la seguridad. La gestión adecuada de la seguridad de la información se ha vuelto algo intrínseco a la supervivencia de las organizaciones. De ahí que la adopción de medidas de protección hacia activos de información críticos se haya vuelto importante. Sin ellos, no se garantiza la eficacia de las inversiones en las que pudiera

incurrir cualquier organización, es más, se ha llegado a decir que la seguridad de la información es función de una adecuada administración de ciertos factores y métricas de seguridad antes que de la adquisición de tecnología y herramientas de última generación. El criterio cierto pasa por implementar las primeras para luego con buen criterio escoger e implementar las segundas. (Hideo Ohtoshi, 2008)

El presente proyecto implementa una metodología para la gestión de riesgos de la información para el Instituto Tecnológico Superior Sucre ITSS, de la ciudad de Quito en cumplimiento con el acuerdo N° 166 emitido por la Secretaría Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la Información.

Para tal efecto se efectúa una investigación documental acerca de los requerimientos del mencionado acuerdo; también sobre la institución donde se valida la metodología, recopilándose documentos relacionados con su historia, marco legal, estructura organizacional y carreras que oferta; y también, sobre las normas de seguridad de información: INEN-ISO/IEC 27001 (2014), la cual recomienda el establecimiento de un sistema de gestión de seguridad de la información, SGSI, con la finalidad de coordinar normativas, políticas y procesos de seguridad al interior de las organizaciones contando para el efecto con un macro proceso: la gestión de riesgos; INEN-ISO/IEC 27002 (2014), que es un manual de buenas prácticas de seguridad de la información que soporta a través de 114 controles, los requerimientos de seguridad del SGSI mencionado; e, INEN-ISO/IEC 27005 (2012) que da especificaciones respecto al macro proceso de gestión de riesgos de información. La investigación analiza metodologías internacionales de gestión de riesgos de información vigentes, llegando a determinar que para dar cumplimiento a los requerimientos especificados en las normas ISO es recomendable adaptar el proceso de gestión de riesgos del Modelo de Sistema de Gestión de Seguridad de la Información basado en la norma NTC ISO/IEC 27001 para instituciones públicas de Educación Básica de la Comuna Universidad de Pereira, desarrollado por Alejandra Benavides y Carlos Blandón (2017) en lo que respecta a Gestión de Riesgos.

1.1. Presentación del Trabajo

En cumplimiento de lo enunciado en la introducción, se realiza una adaptación al citado Modelo de SGSI de Benavides y Blandón. Esto último se fundamenta en el hecho que las normas ISO/IEC de la familia 27000 orientan sobre lo que ha de hacerse para asegurar la información (el que) pero no precisan una metodología en particular (el cómo). El proceso inicial dentro de la metodología consiste en efectuar el diagnóstico inicial de brechas de cumplimiento normativo y diagnóstico de madurez del SGSI al interior del ITSS, adaptando para tal efecto la encuesta contenida en el Modelo de la Consejería

de TIC de la Alcaldía Mayor de Bogotá. Las preguntas están redactadas contando como insumo los controles contenidos en la norma ISO 27001 (2014); y estructuradas en tres columnas de acuerdo siguiendo el esquema: un campo para el texto de la pregunta; un campo para el registro del grado de cumplimiento del control al cual hace referencia, clasificado en niveles de cumplimiento (satisfactorio, parcial, no cumple, no aplica) de acuerdo a recomendaciones contenidas en las mismas normas; y, un campo para el registro de evidencias. La encuesta está estructurada en tres partes, o logros de seguridad; la primera, diagnostica el Marco de Seguridad y Privacidad de la Información a través de quince preguntas, con un peso de 30% sobre el total; la segunda, diagnostica la Implementación del Plan de Seguridad y Privacidad de la Información a través de ciento catorce preguntas, con un peso del 40% del total; y, la tercera, donde se diagnostican los procesos de Monitoreo y Mejora Continua, utilizando para ello doce preguntas, con un peso de 30% sobre el total de la encuesta. Se han tabulado los resultados y se ha determinado el porcentaje de brechas de seguridad respecto a ISO 27001.

El segundo proceso empieza con el diseño de la definición del contexto de gestión de riesgos, sigue con el análisis y evaluación de riesgos, luego propone un plan de tratamiento y finaliza con la implementación de dicho plan. En su elaboración adapta el Modelo de Sistema de Gestión de Seguridad de la Información desarrollado por Alejandra Benavides y Carlos Blandón de la Universidad de Pereira, Colombia, en lo que respecta al proceso de Gestión de Riesgos de Seguridad de la Información. A continuación se hace una breve descripción de las actividades de este proceso: definición del contexto de la gestión de riesgos cuyo resultado se evidencia en un acta; inventario de activos de información, cuyos resultados se presentan en una matriz; determinación de factores de criticidad en los activos de información; valoración de dichos factores de criticidad, a través de la aplicación de un modelo matemático sobre los activos inventariados y posterior elaboración de una matriz de resumen; identificación de escenarios de riesgo asociados a los activos; valoración de la probabilidad de ocurrencia de los riesgos identificados; determinación de criterios de impacto potencial; cálculo de vulnerabilidad inherente a través de un modelo matemático y creación de la matriz de vulnerabilidad inherente, donde se aplica dicho modelo a todos los escenarios de riesgo detectados; determinación de criterios para aceptabilidad de riesgo; creación de matrices de clasificación de vulnerabilidad inherente, presentando los riesgos de acuerdo a valores previamente calculados de vulnerabilidad inherente; identificación de controles existentes en una matriz donde se colocan los escenarios de riesgo detectados contrastándolos con los controles especificados en el Anexo de ISO 27001; cálculo de vulnerabilidad residual, a través de la aplicación un modelo matemático y elaboración de la matriz de cálculo de vulnerabilidad residual para cada escenario de riesgo; creación de matrices de

clasificación de vulnerabilidad residual. Luego, se hace el diseño del plan de tratamiento de riesgos, cuya valoración tiene el rango de inaceptable, donde constan estrategias, responsables y plazos. Como paso siguiente dicho plan de tratamiento se implementa, y se consigue un incremento en el nivel de conformidad de seguridad de la información que se almacena y gestiona al interior del ITSS al correr nuevamente la matriz de análisis de brechas descrito en el primer proceso.

1.2. Descripción del documento

El primer capítulo introduce y presenta el trabajo de investigación así como también describe la estructura del documento.

El segundo capítulo presenta información técnica básica, realiza un análisis de la situación actual del ITS Sucre: su historia, entes reguladores, estructura organizacional, carreras que oferta y matrícula, tomado de (ITS Sucre, 2017), (Instituto Tecnológico Superior Sucre, 2016) y describe el problema detectado en el ITSS y los objetivos de este trabajo.

El tercer capítulo presenta el marco teórico, esto es, definiciones de seguridad, seguridad de la información, seguridad informática del autor (Espasa Calpe, 2005), sistema de gestión de seguridad de la información del autor INEN(2014) y su estructura; normas ISO, familia de normas ISO/IEC 27000, norma ISO/IEC 27001, norma ISO/IEC 27002, norma ISO/IEC 27005 del autor ISO (2013); describe también metodologías y modelos internacionales de gestión de riesgos de información de los autores (Insight Consulting, 2003), (Ministerio de Administraciones Públicas, 2005), (Federal Office for Information Security (BSI), 2005) ; en particular NIST SP 800 -30 (National Institute for Standards and Technology (NIST), 2002) y el Modelo de Sistema de Gestión de Seguridad de la Información basado en la norma NTC ISO/IEC 27001 para instituciones públicas de Educación Básica de la Comuna Universidad de Pereira (Benavides Sepúlveda & Blandón Jaramillo, 2017), Colombia.

El cuarto capítulo presenta la estructura de la metodología adaptada de gestión de riesgos, que considerando las condiciones particulares y específicas del ITS Sucre permite volver más confiable y seguro el uso de sus activos de información, el cumplimiento de la conformidad legal y el mantenimiento de su reputación y prestigio institucional; basada en el trabajo de los autores (INEN Servicio Ecuatoriano de Normalización, 2014), (INEN, Instituto Ecuatoriano de Normalización, 2014), (Instituto Ecuatoriano de Normalización, 2012), (ISOTools Excellence, 2017), (National Institute for Standards and Technology (NIST), 2002), (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016), (Benavides Sepúlveda & Blandón Jaramillo, 2017).

El quinto capítulo presenta pormenorizadamente los resultados de la aplicación de la metodología presentada en el capítulo cuatro, validada en los procesos de la Unidad de Titulación del ITS Sucre, componente institucional en el cual el rector del plantel autorizó llevar adelante la implementación, con la presentación y análisis de resultados obtenidos.

El sexto capítulo presenta las conclusiones a las que se llega con esta investigación y presenta recomendaciones para futuros estudios sobre la temática de Seguridad de la Información en el ámbito nacional y local.

Capítulo 2

Planteamiento de la Propuesta de Trabajo

2.1. Información técnica básica

Tema: Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre.

Tipo de trabajo: Propuesta Metodológica y Tecnológica Avanzada

Clasificación técnica del trabajo: Desarrollo

Líneas de investigación y desarrollo:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus Aplicaciones

2.2. Situación actual del Instituto Tecnológico Superior Sucre

Marco legal educativo

La Constitución Política de la República del Ecuador vigente (2008), en su artículo 3 numeral 1 "establece como deber del Estado garantizar sin discriminación alguna el efectivo goce de los derechos [...] en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes" (Asamblea Nacional Constituyente, 2008, pág. 16).

Después, la Ley Orgánica de Educación Superior, LOES (2010), cita a la Constitución enunciando que "el Art. 26 de la Constitución de la República del Ecuador establece que la educación es un derecho de las personas a lo largo de su vida y un deber ineludible e inexcusable del Estado" (Asamblea Nacional de la República del Ecuador, 2010, pág. 4)

Posteriormente, en la LOES se cita nuevamente a la Carta Magna que en su artículo 352 dice "el Sistema de Educación Superior estará integrado por universidades y escuelas politécnicas; institutos superiores técnicos, tecnológicos y pedagógicos; y conservatorios superiores de música y artes, debidamente acreditados y evaluados. Estas instituciones, sean públicas o particulares, no tendrán fines de lucro" (Asamblea Nacional de la República del Ecuador, 2010, pág. 5)

Nuevamente, se menciona en la Constitución Política, en su artículo 354 que "[…]Los institutos superiores tecnológicos […] se crearán por resolución del organismo encargado de la planificación, regulación y coordinación del sistema, previo informe favorable de la institución de aseguramiento de la calidad del sistema y del organismo nacional de planificación" (Asamblea Nacional Constituyente, 2008, pág. 163), además, que "La creación y financiamiento de nuevas casas de estudio y nuevas carreras universitarias públicas se supeditarán a los requerimientos del desarrollo nacional" (Asamblea Nacional Constituyente, 2008, pág. 163); y finalmente, enuncia que "El organismo encargado de la planificación […] y el organismo encargado para la acreditación […] podrán suspender […] a las universidades […] institutos superiores tecnológicos, técnicos y pedagógicos[…] así como solicitar la derogatoria de aquellas que se creen por ley" (Asamblea Nacional Constituyente, 2008, pág. 163).

En el artículo 15 de la Ley Orgánica de Educación Superior consta que "Los organismos públicos que rigen el Sistema de Educación Superior son: a) El Consejo de Educación Superior (CES); y, b) El Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES)" (Asamblea Nacional de la República del Ecuador, 2010, pág. 11)

Breve reseña histórica del ITS Sucre y de las carreras que oferta

El Instituto Tecnológico Superior Sucre, en adelante ITSS o ITS Sucre, se origina a partir del Colegio Técnico Nacional Sucre, que en un inicio fuera institución municipal para después pasar a pertenecer al Ministerio de Educación. En sus inicios, de 1959 a 1974, el colegio Sucre ofertó las profesiones manuales de Carpintería, Zapatería y Mecánica General. Con posterioridad (1996) el colegio Sucre es elevado a la categoría de Instituto Técnico Superior, mediante acuerdo del Ministerio de Educación N° 4191, ofreciendo en su nivel superior las especialidades de Electricidad y Electrónica Industrial, hecho que es ratificado por el CONESUP(Consejo Nacional de Educación Superior, hoy extinto), en 2000 al otorgarle el registro institucional. Con posterioridad, mediante acuerdo Nº 166 del CONESUP con fecha 23 de diciembre del 2003, la institución alcanza la categoría de Instituto Tecnológico Superior, con las carreras de Electricidad y Electrónica Industrial. En 2005 se crea la especialidad de Electromecánica, misma que es ratificada mediante el acuerdo N° 402 del CONESUP con fecha 14 de agosto de 2007, donde además, se crean las especialidades de Recursos Audiovisuales y Gestión Ambiental. Mediante resolución del Consejo de Educación Superior, CES, N° 140-01-2013, se crea la carrera de Técnicos en Atención Primaria de la Salud (TAPS).En 2014, a través de un convenio interinstitucional entre la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, SENESCYT, y el Ministerio de

Inclusión Económica y Social, MIES, se da inicio a la carrera de Tecnología en Desarrollo Infantil Integral, TDII (Instituto Tecnológico Superior Sucre, 2016, pág. 15). Finalmente, mediante resolución RPC-SO-03 No.034-2016 del Consejo de Educación Superior, CES, en su Artículo primero se crea la carrera de Tecnología Superior en Producción Textil el 20 de enero de 2016.

En la actualidad el ITSS es un establecimiento de Educación Superior, ubicado en la ciudad de Quito, que cuenta con dos sedes; una al sur, en el sector de San Bartolo y otra al norte, en sector de Mosquera Narváez y 10 de Agosto; orientada hacia la formación de profesionales técnicos de Nivel Superior con capacidad crítica, creativa y de liderazgo a través de una sólida formación académica con la finalidad de satisfacer las demandas laborales implícitas en el desarrollo económico, empresarial e industrial del país (ITS Sucre, 2017) Ofrece las carreras de Tecnología en Electrónica Industrial, Electromecánica Industrial, Electricidad Industrial en la Sede Sur, y las de Desarrollo Infantil Integral, Gestión Ambiental, Atención Primaria de la Salud, Realización y Producción Audiovisual y Producción Textil en el Campus Norte y cuenta con una población estudiantil de 1300 personas, 111 docentes y 4 personas de administrativos (datos a enero de 2018).

El organigrama estructural del ITSS se muestra en el Apéndice A.

Misión y visión del ITS Sucre

Misión

"Formar profesionales competitivos en diferentes áreas técnicas y tecnológicas, a través de la aplicación del conocimiento teoricopráctico especializado, que contribuya al cambio de la matriz productiva y permita el mejoramiento de la calidad de vida de la sociedad" (Instituto Tecnológico Superior Sucre, 2016, pág. 64).

Visión

"En 2020, consolidarnos como una institución de educación superior técnica y tecnológica, con altos estándares de calidad académica y científica, que permitan posicionarnos en el entornos local, nacional e internacional" (Instituto Tecnológico Superior Sucre, 2016, pág. 65).

Carreras que oferta el ITSS

Las carreras que ofrece el Instituto Tecnológico Superior Sucre se clasifican en tradicionales o emblemáticas (de asistencia presencial) y en duales. A continuación se hace una breve reseña de las primeras:

Tecnología Superior en Electricidad Industrial

Según la descripción proporcionada en la página web institucional del ITSS, esta "carrera integra conocimientos, metodologías, procedimientos, técnicas, tecnologías para mejorar la producción, operación y gestión de proyectos e instalaciones eléctricas, a fin de aumentar la competitividad del sector energético en el Ecuador" (ITS Sucre, 2018, pág. 1), es de modalidad presencial, es gratuita, está ubicada en el Campus San Bartolo, dura dos y medio años, en jornadas diurna y vespertina y otorga el título de Tecnólogo Superior en Electricidad. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación (ITS Sucre, 2018, pág. 1).

Tecnología Superior en Electromecánica Industrial

Esta tecnología "combina las áreas de electricidad, mecánica y electrónica para aplicarlas en el análisis de funcionamiento, operación, mantenimiento y control de máquinas herramientas y equipos industriales" (ITS Sucre, 2018, pág. 1), es de modalidad presencial, es gratuita, está ubicada en el Campus San Bartolo, dura dos y medio años, en jornadas diurna y vespertina y otorga el título de Tecnólogo Superior en Electromecánica. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación (ITS Sucre, 2017, pág. 1).

Tecnología Superior en Electrónica Industrial

"La carrera de Electrónica fue creada para satisfacer las necesidades del sector empresarial en las áreas de automatización, redes y telecomunicaciones para el desarrollo tecnológico sostenible de las industrias con responsabilidad ambiental y social" (ITS Sucre, 2018, pág. 1), es de modalidad presencial, es gratuita, está ubicada en el Campus San Bartolo, dura dos y medio años, en jornadas diurna y vespertina y otorga el título de Tecnólogo Superior en Electrónica. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación (ITS Sucre, 2018, pág. 1).

Tecnología en Gestión Ambiental

Esta tecnología "forma profesionales que aplican conocimientos, metodologías, técnicas y procedimientos relacionados con el monitoreo, control y gestión ambiental. Se encuentra enfocada al manejo, cuidado y conservación del medio ambiente y la biodiversidad" (ITS Sucre, 2018, pág. 1), es de

modalidad presencial, es gratuita, ubicada en el Campus Norte, dura tres años, en jornadas diurna, vespertina, nocturna y otorga el título de Tecnólogo Superior en Gestión Ambiental. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación (ITS Sucre, 2018, pág. 1).

Tecnología en Producción y Realización Audiovisual

Según la descripción proporcionada en la página web institucional del ITS Sucre, esta "carrera forma profesionales con capacidad para gestionar las etapas de pre-producción, producción y postproducción audiovisual para impulsar el desarrollo del cine y la industria cultural en el país[…]" (ITS Sucre, 2018, pág. 1), es de modalidad presencial, es gratuita, está ubicada en el Campus Norte, dura dos y medio años, en jornadas diurna y vespertina y otorga el título de Productor y Realizador Audiovisual equivalente a Tecnólogo Superior. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación (ITS Sucre, 2018, pág. 1).

A continuación, se hace una breve reseña de las carreras que en modalidad dual oferta el ITSS:

Técnico en Atención Primaria de la Salud [TAPS]

"La carrera forma Técnicos en Atención Primaria de Salud-TAPS con capacidad para desarrollar e implementar actividades de promoción y prevención que mejoren las condiciones de salud de las personas, la familia y la comunidad" (ITS Sucre, 2018, pág. 1), es de modalidad dual, es gratuita, ubicada en el Campus Norte, dura dos años, en jornada intensiva dos días por semana y otorga el título de Técnico Superior en Atención Primaria de Salud. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación y beca del Ministerio de Salud Pública (ITS Sucre, 2018, pág. 1).

Tecnología en Desarrollo Infantil Integral [TDII]

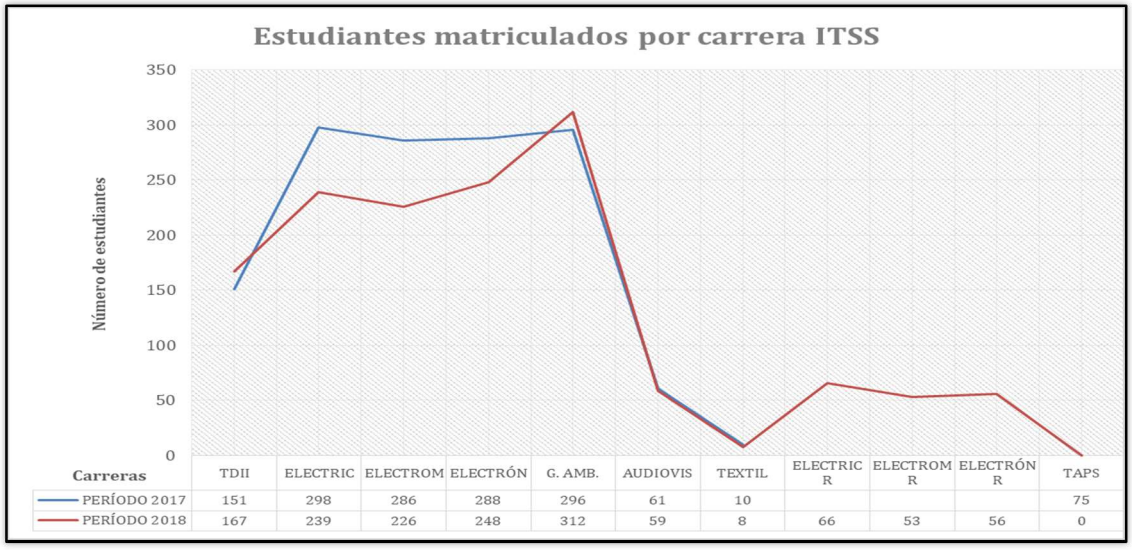
"La carrera perfila profesionales con formación teórica, metodológica, técnica e instrumental para intervenir en procesos de atención y educación de la primera infancia con enfoque biopsicosocial, pedagógico e intercultural" (ITS Sucre, 2018, pág. 1), es de modalidad dual, es gratuita, ubicada en el Campus Norte, dura dos y medio años, en jornada intensiva dos días por semana: viernes y sábados, otorga el título de Tecnólogo Superior en Desarrollo Infantil Integral. Tiene por requisitos el título de

bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación y una carta de aceptación en un CIBV/CDI (ITS Sucre, 2018, pág. 1).

Tecnología Superior en Producción Textil

"La carrera forma profesionales con conocimientos, habilidades y destrezas para planificar, ejecutar y evaluar procesos de producción textil, con alto rendimiento y calidad, a partir del manejo responsable y eficiente de los recursos" (ITS Sucre, 2018, pág. 1), es de modalidad dual, es gratuita, ubicada en el Campus Norte, dura dos y medio años, en jornada intensiva, otorga el título de Tecnólogo Superior en Producción Textil. Tiene por requisitos el título de bachiller, haber aprobado el examen de ingreso a la Educación Superior y la asignación de cupo de la SENESCYT, así como copia de cédula de ciudadanía y certificado de votación y una carta de aceptación en entidad receptora (ITS Sucre, 2017, pág. 1). A fines de enero de 2018 la carrera cuenta, según información proporcionada, con 8 estudiantes.

Figura 1: Estudiantes matriculados por carrera en el ITS Sucre en los años 2017 y 2018



Carreras	TDII	ELECTRIC	ELECTROM	ELECTRÓN	G. AMB.	AUDIOVIS	TEXTIL	ELECTRIC R	ELECTROM R	ELECTRÓN R	TAPS
PERÍODO 2017	151	298	286	288	296	61	10				75
PERÍODO 2018	167	239	226	248	312	59	8	66	53	56	0

Fuente: Unidad de TIC ITSS

Como presenta la Figura 1, elaborada con base en información proporcionada por la Unidad de Tecnologías de Información y Comunicación del ITS Sucre, se observa que el número de matriculados en el ITSS ha descendido, excepto para la Carrera de Gestión Ambiental y TDII. En el caso de las tecnologías en Electricidad, Electrónica y Electromecánica (Campus Sur) esto se debe a que el CEAACES ha aprobado el rediseño de carreras y los rediseños son considerados otras carreras. En el caso de la carrera de TAPS la caída del número de matriculados se debe a que se ha terminado su segunda cohorte

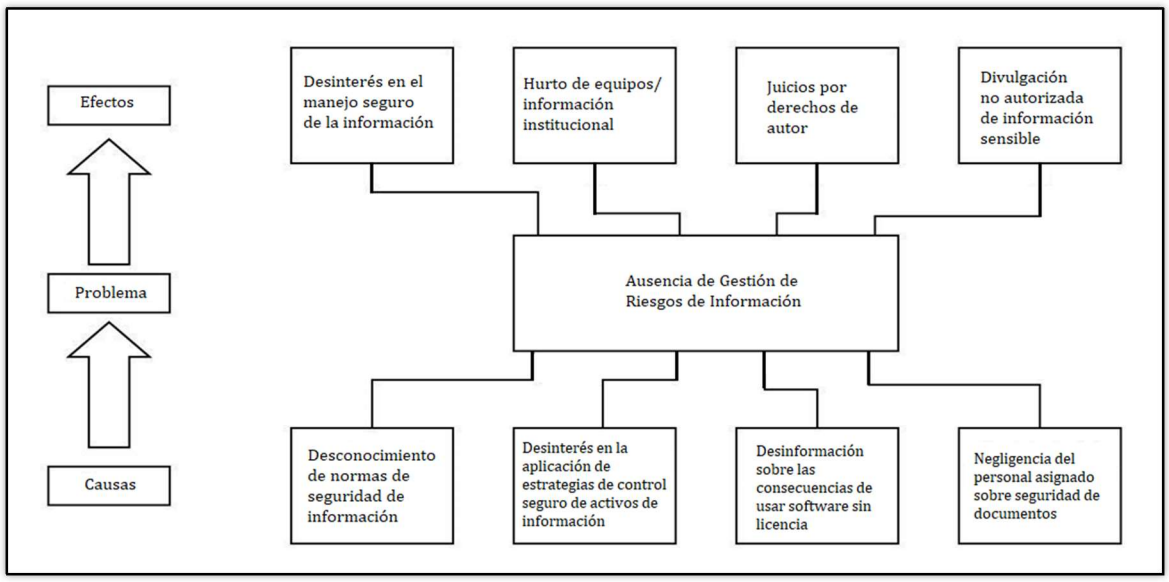
y se encuentra al momento en procesos de concursos de méritos y oposición en miras a abrir la tercera cohorte.

En la actualidad el ITSS cuenta con una Unidad de Tecnologías de la Información y Comunicación (Comisión de TIC) encargado, entre otras cosas, de administrar cinco laboratorios, cuatro al norte y uno en el sur, donde se dictan las clases de materias relacionadas a computación, gestionar la red wifi donde se distribuye el servicio de Internet en ambas sedes así como el arriendo y la gestión con un proveedor externo del sistema de calificaciones de la institución. Adicionalmente el instituto cuenta con tres computadores en secretaría de su sede norte, una en la unidad de bienestar estudiantil sede norte también, una en secretaría sede sur, una para la oficina de la Unidad de TIC, no se cuenta con servidores ni red intranet. La gestión de la seguridad de la información que se genera y custodia en nubes de tipo público también es responsabilidad esta dependencia.

El principal problema detectado, es el incumplimiento del Esquema Gubernamental de Seguridad de la Información, EGSI, publicado en el acuerdo Nro. 166 de la Secretaría Nacional de la Administración Pública SNAP con fecha 19 de septiembre de 2013 el cual se establece la aplicación de las normas de la familia ISO/IEC 27000 referentes a la Seguridad de la Información de manera obligatoria para las entidades de la Administración Pública en el Ecuador, para el cual tenían plazo las instituciones hasta marzo de 2015 (Secretaría Nacional de la Administración Pública, 2013).

Mediante una breve inspección inicial, se ha detectado que los activos de información; entendiéndose como tales a documentos físicos, lógicos y personal humano del ITS Sucre evidencian elevados grados de vulnerabilidad en cuanto su seguridad, que ante amenazas tales como hurto, accesos no autorizados tanto físicos como lógicos, virus informáticos, desastres naturales o cortes de fluido eléctrico; exponen a la institución a la afectación de su buen nombre, a pérdidas económicas o la interrupción de la prestación de los servicios. Situación que se agrava al no contar el instituto con un Marco de Gestión de Riesgos de Información, encargado de administrar tanto activos de información –entendiéndose como tales mobiliario físico y documentación, recursos humanos, hardware, software y procesos- como sus riesgos asociados, lo cual serviría dentro de un proceso de ande hacer la valoración de los mismos para coordinar, emitir y hacer cumplir normas, políticas y procedimientos de atención y tratamiento de riesgos. Todo esto, puede resumirse en el árbol de problemas que se presenta en la Figura 2.

Figura 2: Árbol de problemas



Fuente: Elaboración propia

En relación a lo expuesto, la realización de este trabajo se justifica por su utilidad práctica, pues ayudará a reducir de manera significativa las vulnerabilidades en los activos de información; y permitirá diseñar e implementar una metodología que respondiendo a las condiciones particulares y específicas del ITS Sucre permita volver más confiable y seguro el uso de sus activos de información, la conformidad legal y el mantenimiento de la reputación y prestigio institucional.

2.3. Preguntas Básicas

¿Cómo aparece el problema que se pretende solucionar?

Luego de realizar una primera inspección en la organización donde se implementa la metodología, se observaron los siguientes problemas; respecto a hardware y continuidad del negocio, carencia de UPS o plantas eléctricas de emergencia, y se corre el riesgo de pérdida de información de los equipos, y su daño ante un eventual apagón; respecto a software: existencia de software sin licencia y desactualizado, incluyendo los antivirus, por lo que los equipos están expuestos a virus, gusanos, troyanos, malware que pueden utilizar *exploits* y repercutir en el malfuncionamiento de Sistemas Operativos, robo de información confidencial de los usuarios, destrucción de aplicaciones de usuario además de convertirse en una vulnerabilidad de tipo legal para la organización por utilizar software sin licencia; dentro de software también: las actualizaciones de Sistema Operativo en los equipos de laboratorios están desactivados por que los equipos están expuestos a intrusiones no autorizadas, robo

o eliminación de información, ataques de denegación de servicio y escalamiento no autorizado de privilegios de usuarios. Además, respecto a seguridad física, no existe control sobre el acceso físico de personal no autorizado a oficinas y equipos en ambos campus, lo cual expone al instituto a robo, destrucción, modificaciones no autorizadas o borrado de información, destrucción o inutilización de equipos, de hecho ya se ha sufrido robo de proyectores e ingreso de ladrones a las instalaciones; respecto a seguridad lógica, se observó un deficiente control de acceso al sistema SAO-P, lo cual puede repercutir en suplantación de identidad y consecuentemente alteración de datos de notas de estudiantes e información de docentes y cursos, borrado de información, robo de claves de usuarios; en cuanto al recursos humanos, no existe una conciencia clara de seguridad documental así como no hay políticas claras y expresas de seguridad de la información por lo que el riesgo que se corre es el de borrado o eliminación tanto física como lógica de información, divulgación no autorizada/ robo de información confidencial o de los usuarios; destrucción de equipos.

¿Por qué se origina?

Los problemas anteriormente mencionados se originan en la carencia de una conciencia de seguridad entre usuarios de información de la entidad, el desconocimiento de estrategias de custodia segura de activos de información, desinformación sobre las consecuencias de uso de software sin licencia y desinterés del personal asignado sobre seguridad documental; debido a la ausencia de una cultura de Gestión de Riesgos de Información.

¿Dónde se origina?

Físicamente: tanto en el Campus Sur como en el campus Norte del ITS Sucre, que son los lugares donde están instalados los equipos informáticos y se custodia la información en formato físico; y, virtualmente, en el Internet.

2.4. Formulación de meta

Implementación de la gestión de riesgos de información a partir de normas internacionales ISO 27001 y 27002 en el ITS Sucre, a través de una metodología que permita reducir las vulnerabilidades de los activos de información de una manera significativa.

2.5. Objetivos

2.5.1. Objetivo General

Implementar una metodología de gestión de riesgos de información basada en ISO 27001 y 27002 para reducir los niveles de vulnerabilidad en los activos de información del ITS Sucre.

2.5.2. Objetivos Específicos

- Verificar el estado del arte en referencia a las normas internacionales ISO 27001 y 27002 para que la metodología se alinee a las necesidades institucionales.
- Elaborar un diagnóstico inicial de los activos de información del ITS Sucre para determinar el nivel de seguridad de los mismos.
- Adaptar una metodología de gestión de riesgos para reducir los niveles de vulnerabilidad.
- Aplicar la metodología adaptada con el fin de comprobar la vialidad técnica de la misma.

2.6. Delimitación funcional

¿Qué será capaz de hacer el producto final del trabajo de titulación?

El producto final de este trabajo permitirá al Instituto Tecnológico Superior Sucre contar con una línea base de Gestión de Riesgos de Seguridad de la Información para que los datos e información que ahí se generan y custodian sean administrados bajo estándares internacionales de seguridad con opción a continuar su aplicación, en función de su prioridad.

¿Qué no será capaz de hacer el producto final del trabajo de titulación?

El producto final del presente trabajo de titulación no será una certificación en normas de seguridad de la información, no abarca el diseño/ implementación de un Sistema de Gestión de Seguridad de la Información, ni elabora una Política de Seguridad de la Información para el ITS Sucre.

El producto final del presente trabajo de titulación no será un manual para la configuración de servidores de seguridad, firewalls y demás dispositivos de seguridad puesto que el enfoque de esta propuesta es generar una herramienta de tipo gerencial y no de tipo operativo.

Capítulo 3

Marco Teórico

3.1. Definiciones y conceptos

3.1.1. Seguridad

El diccionario de la lengua española de Espasa Calpe (2005) define a la seguridad como la cualidad de lo que es o está seguro o como la certeza del cumplimiento de algo. Sin embargo, también se la define como la ausencia de riesgo (Gutierrez Espinosa, 2013).

3.1.2. Información

Espasa Calpe (2005) define información como la agrupación de datos sobre alguna temática determinada; en tanto que, Benavides Sepúlveda & Blandón Jaramillo (2017) adicionan a lo anterior, que la información, generada y gestionada, tanto en formato digital como en impreso, sobre distintas actividades tanto internas como externas a las organizaciones se ha llegado a convertir en un elemento fundamental para su operatividad; además de servir como elemento de trazabilidad y pruebas dentro de la resolución de conflictos y no conformidades entre las partes interesadas del negocio.

3.1.3. Seguridad de la Información

El estándar internacional ISO/ IEC 27000 (2016) la define como la preservación de tres características fundamentales para la información: confidencialidad, integridad y disponibilidad; y, adicionalmente, otras propiedades, tales como la autenticidad, fiabilidad y no repudio.

La confidencialidad es definida como la característica de la información de no estar disponible o revelada a personas, organizaciones o procesos no autorizados (ISO /IEC , 2016).

La integridad es la propiedad de precisión y completitud en la información (ISO /IEC , 2016).

La disponibilidad, es, la característica de la información ser accesible y utilizable cuando se la requiera a pedido de un ente autorizado (ISO /IEC , 2016).

La autenticidad es la propiedad de que un ente es lo que dice ser (ISO /IEC , 2016).

El no repudio es la capacidad de probar la ocurrencia de un evento o acción atribuido y sus entidades originadoras (ISO /IEC , 2016).

La fiabilidad es la propiedad de la información de tener tanto un comportamiento como resultados previstos (Benavides Sepúlveda & Blandón Jaramillo, 2017).

La seguridad de la información, hace que las organizaciones puedan garantizar su continuidad del negocio, a través de una adecuada gestión de riesgos y la implementación acertada de controles que pueda mantenerlas competitivas, mientras se crea conciencia entre directivos y funcionarios respecto al empleo de mejores prácticas para la utilización de información (Benavides Sepúlveda & Blandón Jaramillo, 2017).

3.1.4. Seguridad Informática

La seguridad informática comprende el aseguramiento de los recursos tecnológicos de un sistema de información, entendiéndose como tales a su software, hardware o redes para que el acceso, utilización y almacenamiento de los mismos sea el previsto y autorizado (Torres Bermúdez, 2010).

La Seguridad de la Información, tal como la define la norma ISO/IEC 27000, abarca a la Seguridad Informática, puesto que aquella busca precautelar la confidencialidad, disponibilidad e integridad de la información contenida y gestionada, también, en activos de tecnología.

3.1.5. Sistema de Gestión de Seguridad de la Información SGSI

Sistema de gestión que planifica, organiza, dirige y controla la seguridad de la información a lo interno de una institución de acuerdo a las especificaciones dadas en la norma ISO/IEC 27001 bajo el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar propugnado por Edward Demig (INEN Servicio Ecuatoriano de Normalización, 2014).

3.1.6. ISO e IEC

ISO (International Standards Organization), es una organización internacional creada en el año 1947, con sede en Ginebra (Suiza) cuya misión es la consecución del establecimiento de normas comunes con ámbito mundial. Para tal efecto desde inicios de 1980 ha venido creando una serie de comités técnicos nacionales. Cuenta en la actualidad con 91 estados miembros (ISOTools, 2015).

IEC (Comisión Electrotécnica Internacional) es una organización, que junto a ISO, integra el sistema especializado para estandarización a nivel global (INEN Servicio Ecuatoriano de Normalización, 2014).

3.1.7. Normas ISO

Las normas ISO son un grupo de estándares internacionales encaminados a organizar la administración de una organización en sus distintos ámbitos. Su creciente prestigio y reconocimiento se debe a la creciente tendencia en la globalización de las economías así como la opinión de consumidores a nivel internacional. Estas normas son creadas por la Organización internacional para la normalización (ISO, por sus siglas en inglés) y están compuestas por patrones y guías relativos a sistemas y herramientas específicos de gestión empresarial (ISOTools, 2015).

3.1.8. Normas técnicas ecuatorianas ISO /IEC 27000

La familia de normas ISO/IEC 27000 es un conjunto de estándares que busca proveer a organizaciones de todo tipo, un marco de gestión de seguridad de la información, mismo que ha atravesado un proceso de creación y mejoramiento.

Para Freire (2014), la primera norma de la serie, ISO/IEC 27000 brinda una breve descripción de la serie de normas 27000, objetivos de cada una y el vocabulario a usarse. La versión más actual fue publicada el 15 de febrero de 2016 y no ha sido traducida aún al castellano.

3.1.9. Norma técnica ISO/IEC 27001

La norma NTE INEN- ISO/IEC 27001 (2014) Tecnología de la información- sistemas de gestión de la seguridad de la información, es una actualización de la norma británica BS 7799-2 (Federal Office for Information Security (BSI), 2005) que define la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y contempla su certificación. Trabaja en conjunto con la norma INEN- ISO/IEC 27002 (2014). Según Hideo Ohtoshi (2008) al implementar el SGSI según la norma ISO 27001 se sigue el ciclo PHVA donde se implementan controles definidos en el análisis de riesgos, como se presenta en la Figura 3.

Figura 3: Ciclo de Demig aplicado a un Sistema de Gestión de Seguridad de la Información

Fuente: (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Los requisitos exigidos por ISO 27001 para la implementación de un SGSI se pueden dividir en varias fases, como se presenta en la Figura 4.

Figura 4: Fases de un Sistema de Gestión de Seguridad de la Información según ISO 27001

Fuente: (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Como se observa en la Figura 3 los procesos de gestión y de análisis de riesgos son el núcleo del SGSI y son aquellos que transforman, por una parte, reglas y directrices de política de seguridad, y por otro, los objetivos del SGSI en planes específicos para la implementación de controles y mecanismos que tienen por meta minimizar amenazas y vulnerabilidades. No obstante lo anterior, Gómez Fernández (2012), afirma que la seguridad total en un SGSI es inalcanzable, pero a través de la aplicación de un proceso de mejora continua puede llegarse a niveles de aseguramiento satisfactorio, donde los riesgos a los que se halla expuesta la información están reducidos al mínimo.

La norma ISO 27001 está estructurada en 10 cláusulas que se detallan a continuación:

Tabla 1: Estructura de la norma ISO/IEC 27001:2014 con énfasis en gestión de riesgos

0.	**INTRODUCCIÓN**
1.	**OBJETO Y CAMPO DE ACCIÓN**
2.	**REFERENCIAS NORMATIVAS**
3.	**TÉRMINOS Y DEFINICIONES**
4.	**CONTEXTO DE LA ORGANIZACIÓN**
4.1	Comprender la organización y su entorno
4.2	Comprender las necesidades y expectativas de las partes interesadas
4.3	Determinar el alcance del Sistema de Gestión de Seguridad de la Información
4.4	Sistema de Gestión de Seguridad de la Información, SGSI
5.	**LIDERAZGO**
5.1	Liderazgo y compromiso respecto al SGSI
5.2	Política
5.3	Roles, responsabilidades y autoridades organizacionales
6.	**PLANIFICACIÓN**
6.1	Acciones para tratar los riesgos y las oportunidades
6.1.1	Generalidades
6.1.2	Valoración del riesgo de seguridad de la información
6.1.2.1	Establecer y mantener criterios de riesgo de seguridad de la información, SI
6.1.2.2	Asegurar que las valoraciones repetidas de riesgos de SI produzcan resultados consistentes, válidos y comparables
6.1.2.3	Identificar los riesgos de seguridad de la información
6.1.2.4	Analizar los riesgos de seguridad de la información
6.1.2.5	Evaluar los riesgos de SI.
6.1.3	Tratamiento de riesgos
6.1.3.1	Seleccionar opciones de tratamiento
6.1.3.2	Determinar todos los controles
6.1.3.3	Comparar los controles con los del Anexo A
6.1.3.4	Producir una declaración de aplicabilidad
6.1.3.5	Formular un plan de tratamiento de riesgos
6.1.3.6	Obtener la aprobación del plan de tratamiento de riesgos
6.2	Objetivos de seguridad de la información y planificación para conseguirlos
7.	**SOPORTE**
7.1	Recursos
7.2	Competencia
7.3	Concienciación
7.4	Comunicación
7.5	Información documentada
8.	**OPERACIÓN**
8.1	Planificación y control operacional
8.2	Evaluación de riesgos de seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información.
9.	**EVALUACIÓN DEL DESEMPEÑO**
9.1	Monitoreo, medición, análisis y evaluación.
9.2	Auditoría interna.
9.3	Revisión por la gerencia.
10.	**MEJORAS**
10.1	No conformidades y acción correctiva.
10.2	Mejora continua.
ANEXO A OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA	

Fuente: Elaboración propia basada en (INEN Servicio Ecuatoriano de Normalización, 2014)

Como se presenta en la Tabla 1 el requisito de proceso de gestión de riesgos se menciona en la cláusula sexta en lo que respecta a su planificación, específicamente en el numeral 6.1.2 para análisis y evaluación y 6.1.3 para tratamiento de riesgos; y en la cláusula octava, se menciona la implementación

de los procesos de evaluación de riesgos y tratamiento de riesgos, en los numerales 8.2 y 8.3, respectivamente.

3.1.10. Norma técnica ISO/IEC 27002

La norma ISO 27002 (2014) integra la familia de normas ISO 27000 para gestión de seguridad de la información. Apareció inicialmente como estándar británico BS-7799-1 (BS, 1999) y fue adoptada por ISO como ISO/IEC 17799 (ISO, 2005) y posteriormente nombrada como ISO/IEC 27002 Seguridad de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la información en 2006. Este documento reúne un conjunto de buenas prácticas de seguridad en el procesamiento de la información. No es una norma certificable, ni de gestión de riesgos, aunque contiene un capítulo que trata sobre ello. Recoge aspectos varios que han de ser considerados para administrar adecuadamente un sistema de información, mismo que no todos los controles recomendados llegaren a aplicarse en las instituciones (Hideo Ohtoshi, 2008). Su estructura se presenta a continuación.

Tabla **2:** Estructura de la norma ISO/IEC 27002:2014

0. INTRODUCCIÓN
1. ALCANCE Y CAMPO DE ACCIÓN
2. REFERENCIA Y NORMATIVAS
3. TÉRMINOS Y DEFINICIONES
4. ESTRUCTURA DE ESTA NORMA
4.1 Cláusulas
4.2 Categorías de control
5. POLITICAS DE CONTROL
5.1 Directrices de la Dirección en seguridad de la información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
6.1 Organización interna
6.2 Dispositivos para movilidad y teletrabajo
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
7.1 Antes de la contratación
7.2 Durante la contratación
7.3 Cese o cambio de puesto de trabajo
8. GESTIÓN DE ACTIVOS
8.1 Responsabilidad sobre los activos
8.2 Clasificación de la información
8.3 Manejo de los soportes de almacenamiento
9. CONTROL DE ACCESOS
9.1 Requisitos de negocio para el control de accesos
9.2 Gestión de acceso de usuario
9.3 Responsabilidades del usuario
9.4 Control de acceso a sistemas y aplicaciones

10. CIFRADO

10.1 Controles criptográficos

11. SEGURIDAD FISICA Y AMBIENTAL

11.1 Áreas seguras

11.2 Seguridad de los equipos

12. SEGURIDAD DE LAS OPERACIONES

12.1 Responsabilidades y procedimientos de operación

12.2 Protección contra código malicioso

12.3 Copias de seguridad

12.4 Registro de actividad supervisión

12.5 Control del software en explotación

12.6 Gestión de la vulnerabilidad técnica

12.7 Consideraciones de las auditorías de los sistemas de información

13. SEGURIDAD EN LAS TELECOMUNICACIONES

13.1 Gestión de la seguridad en las redes

13.2 Intercambio de información con partes externas

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1 Requisitos de seguridad de los sistemas de información

14.2 Seguridad en los procesos de desarrollo y soporte

14.3 Datos de prueba

15. RELACIONES CON LOS PROVEEDORES

15.1 Seguridad dela información en las relaciones con los proveedores

15.2 Gestión de la prestación del servicio por proveedores

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes de seguridad de la información y mejoras

17. ASPECTOS DE SEG. DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

17.1 Continuidad de la seguridad de la información

17.2 Redundancias

18. CUMPLIMIENTO

18.1 Cumplimiento de los requisitos legales contractuales

18.2 Revisiones de la seguridad de la información

Fuente: Elaboración propia basada en (INEN, Instituto Ecuatoriano de Normalización, 2014)

Como presenta la Tabla 2, ISO 27002 en su versión actual, define un total de 35 objetivos de control organizados en 14 dominios o áreas de control que incluyen cuestiones referidas al personal, ambientales, operaciones, desarrollo y mantenimiento de sistemas, continuidad de negocios, cumplimiento, que están especificados desde el dominio número 5 hasta el dominio número 18 (Ormella Meyer , 2014).

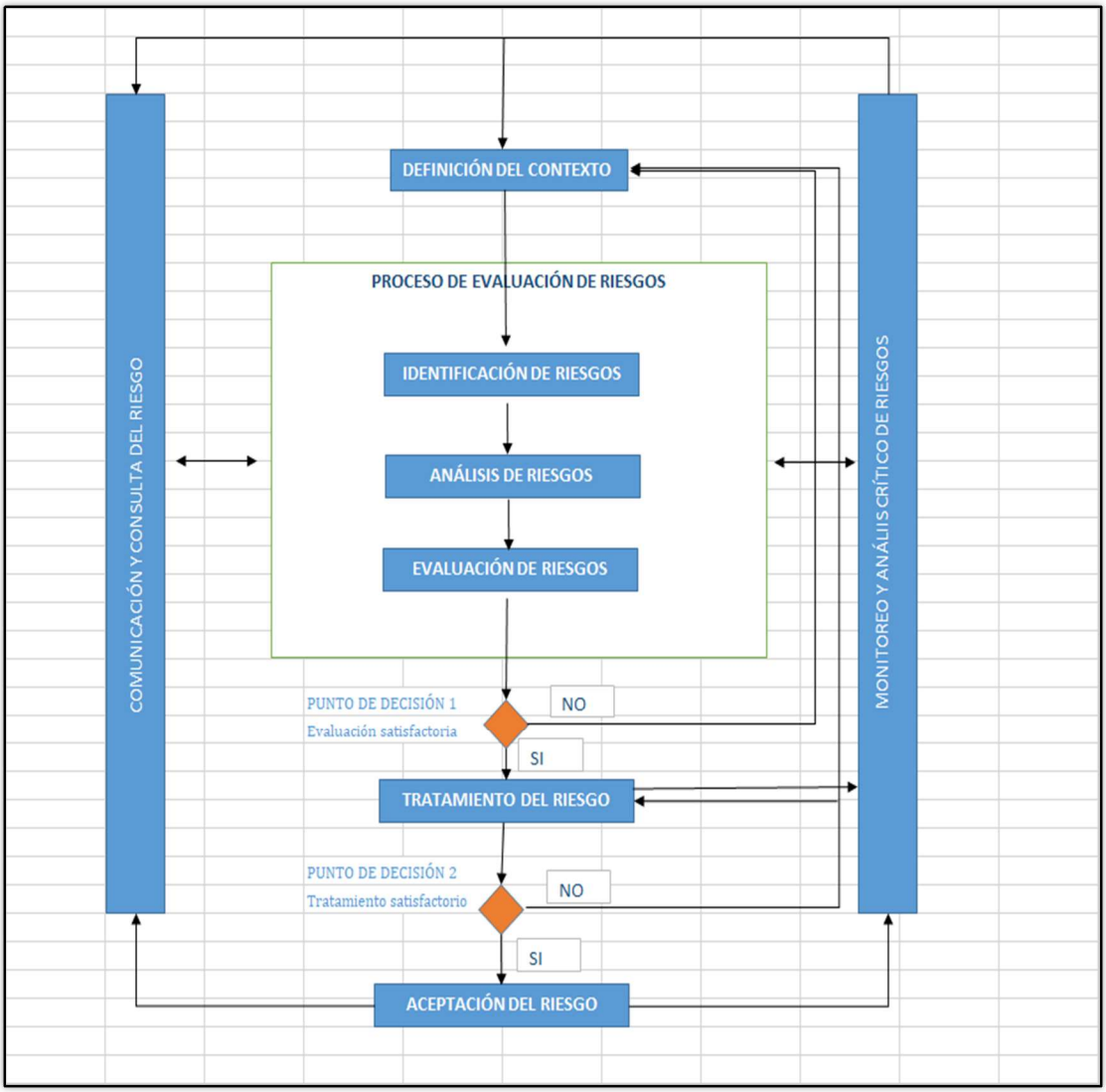
3.1.11. Norma técnica ISO/IEC 27005

La norma técnica ecuatoriana INEN/ISO 27005 (2012) apareció bajo la denominación ISO/IEC 13335:2 el año 2002 y fue adoptada por ISO, tomando su nombre actual en junio de 2008. Enuncia que dentro de lo que comprende un sistema de gestión de seguridad de la información se tiene como punto de partida los procesos de relevamiento, análisis y gestión de riesgos como aquellos que permiten a los administradores balancear presupuestos respecto al aseguramiento de activos críticos para la organización. ISO 27005 es la norma internacional encargada de la gestión de riesgos de seguridad de la información; y ofrece una serie de directrices para tal efecto. Esta norma está alineada con los requisitos de un SGSI definidos en la norma ISO 27001 (presentados en la Tabla 1). ISO 27005 no recomienda una metodología en particular para la gestión de riesgos de seguridad de información, ya que esta dependerá de varios factores tales como el alcance real del SGSI o la orientación comercial de la organización. La metodología seleccionada puede elegirse como la que mejor se adapte, como por ejemplo, a una evaluación de riesgos de alto nivel para posteriormente realizar el análisis de riesgos en profundidad en zonas de alto riesgo (ISOTools Excellence, 2014). Su última versión internacional corresponde al año 2011 y a nivel país, su equivalente del año 2012.

Al hablar de riesgo, este se define como una amenaza que aprovecha una vulnerabilidad dentro de un activo para provocar cierto perjuicio. Existe riesgo en todo el proceso que implica implantación de TI en una organización y para gestionarlo adecuadamente, se sugiere seguir un proceso estructurado, sistemático y estricto de análisis de riesgos para luego diseñar e implantar un plan para su tratamiento (ISOTools Excellence, 2017)

Según ISO 27005 la gestión de riesgo de información consiste en la definición del contexto, el proceso de evaluación de riesgos (que se subdivide en identificación, análisis y evaluación), el tratamiento de riesgos, aceptación del riesgo, comunicación y consulta del riesgo y monitoreo y análisis crítico de riesgos tal como se muestra en la figura 5.

Figura 5: Proceso de gestión de riesgos de seguridad de la información según ISO 27005



Fuente: (Instituto Ecuatoriano de Normalización, 2012)

El proceso de gestión de riesgos de seguridad de información presentado en la Figura 5, puede ser iterativo para las actividades de tratamiento de riesgos. Por cada iteración se puede ir ahondando los detalles de evaluación por cada repetición y de esta manera poder, minimizar recursos en la identificación de controles y asegurar que riesgos de alto impacto sean evaluados (Instituto Ecuatoriano de Normalización, 2012).

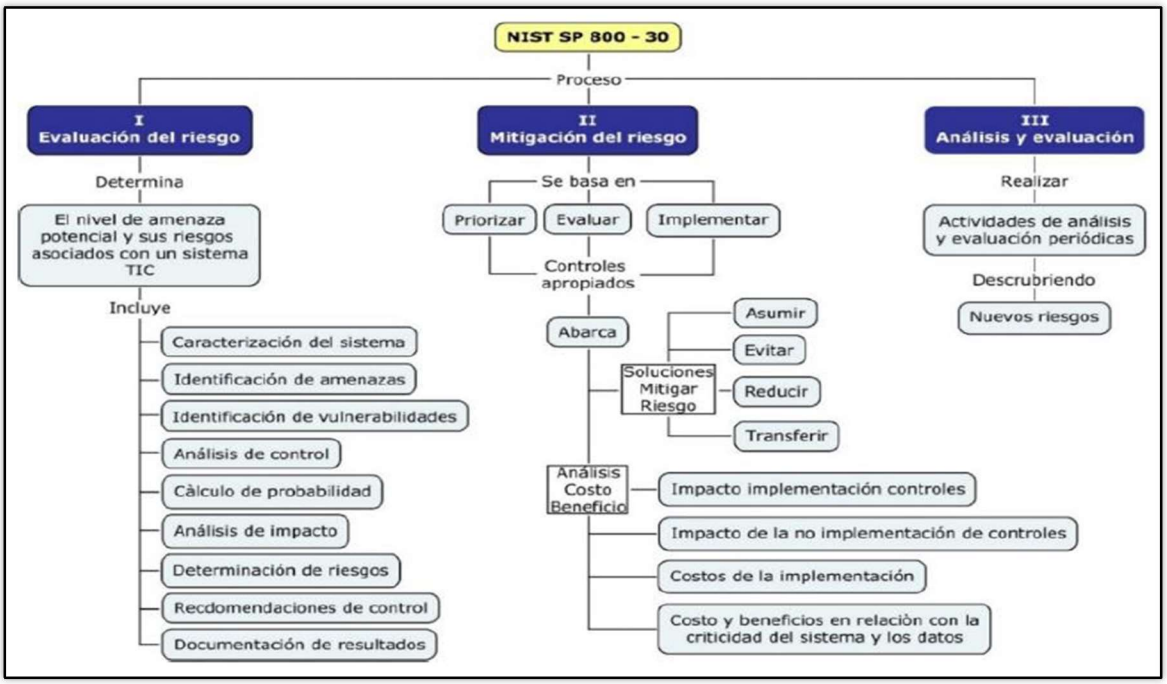
3.2. Metodologías internacionales de gestión de riesgos de información

Una vez revisadas las normas internacionales de gestión de seguridad de la información se procede a hacer una revisión bibliográfica de las metodologías de gestión de seguridad de información NIST800-30 y el Modelo Gubernamental Colombiano de Seguridad de Información, vigentes, tomando en consideración que están alineadas con las normas ISO/IEC 27001 y 27002. Posteriormente, se analiza el Modelo de SGSI de Benavides Sepúlveda y Blandón Jaramillo (2017), que, basado en las dos metodologías mencionadas, presenta una secuencia de actividades que guardan conformidad con las fases del Proceso de Gestión de Riesgos de Seguridad de la Información descrito en la norma ISO/IEC 27001 (2014).

NIST SP 800 – 30

SP 800-30, metodología desarrollada por el Instituto Estadounidense para Normalización y Tecnología, NIST, contiene una orientación detallada sobre lo que debe hacerse en análisis y gestión de riesgos, incluyendo listas de verificación, gráficos, diagramas de flujo, fórmulas matemáticas y referencias basadas en leyes y reglamentos estadounidenses (National Institute for Standards and Technology (NIST), 2002). Según Ohtoshi (2008) esta metodología la gestión de riesgos está compuesta por tres procesos: i) Análisis y evaluación de riesgos; ii) Mitigación de riesgos; iii) Estimación y análisis.

Figura 6: Procesos de la Metodología NIST SP 800-30



Fuente: (Benavides Sepúlveda & Blandón Jaramillo, 2017)

De acuerdo con Ohtoshi (2008) para SP 800-30 la gestión de riesgos es un proceso que procura equilibrar costos operativos y económicos de protección y ganancias obtenidos al proteger sistemas computacionales que apoyan la misión de la empresa, estructurados como se presenta en la figura 6, misma que se describe a continuación:

a. La **evaluación de riesgos**, es la primera actividad de esta metodología, usada para determinar el nivel de penetración de la amenaza potencial y el riesgo asociado. Las salidas de esta actividad ayudan a identificar los controles para la reducción de riesgos en la actividad siguiente que es mitigación de riesgo. Este proceso se compone de nueve actividades: i) Caracterización del sistema, ii) Identificación de amenazas; iii) Identificación de vulnerabilidades, iv) Análisis de controles, v) Determinación de probabilidad, vi) Análisis de impacto, vii) Determinación del riesgo, viii) Recomendaciones de controles, y, ix) Emisión documental de resultados.

b. La segunda actividad de gestión de riesgo según SP 800-30 es la **mitigación del riesgo**. La actividad abarca la priorización, estimación e implantación de controles adecuados, recomendados a partir del proceso de análisis y evaluación del riesgo. Como eliminar

totalmente los riesgos es algo improbable o imposible, es competencia de los gerentes responsables utilizar estrategias de menor costo e implantar controles adecuados para reducirlos hasta un nivel aceptable, minimizando el impacto negativo sobre recursos y sobre la misión de la empresa. La mitigación de riesgo comprende las siguientes actividades: i) Priorizar las acciones; ii) Evaluar; iii) Realizar un análisis costo/beneficio; iv) Selección de controles; v) Asignación de responsabilidades; vi) Desarrollo del plan de implementación de protección; vii) Implementación de controles seleccionados.

c. **Análisis y evaluación**. Debido al dinámico ambiente imperante en las instituciones: expansión y actualización de redes, aparecimiento de nuevos productos de software o nuevas versiones, renovación de la planilla de funcionarios organizacionales y de las políticas de seguridad a lo largo del tiempo; repercutirá en el surgimiento de nuevos riesgos lo que implica necesariamente su gestión sea un proceso en permanente evolución.

Modelo de Seguridad y Privacidad de Información del Gobierno de Colombia

El Ministerio de Tecnologías de Información y la Comunicación (2016) del gobierno de Colombia, ha desarrollado el "**Modelo de Seguridad y Privacidad de la Información**" para las organizaciones del sector público de su país. Dicho modelo de seguridad está elaborado acorde con los lineamientos de la norma ISO 27001, al igual que el "Esquema Gubernamental de Seguridad de la Información EGSI" (Secretaría Nacional de la Administración Pública, 2013) vigente en el Ecuador; pero va más allá, puesto que no solo especifica requerimientos de seguridad alineados con el estándar, sino que ofrece un set de 21 guías de implementación, todo esto bajo el nombre de "Biblioteca de Seguridad" descargables desde su web (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016). En particular para este trabajo es de interés el contenido de la **Guía No. 7**, guía de **Gestión de Riesgos**, que ha sido desarrollada con base en la norma ISO 27001 (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2016). Esta guía recomienda considerar siete etapas para el análisis de riesgos, que según Benavides Sepúlveda y Blandón Jaramillo (2017), son:

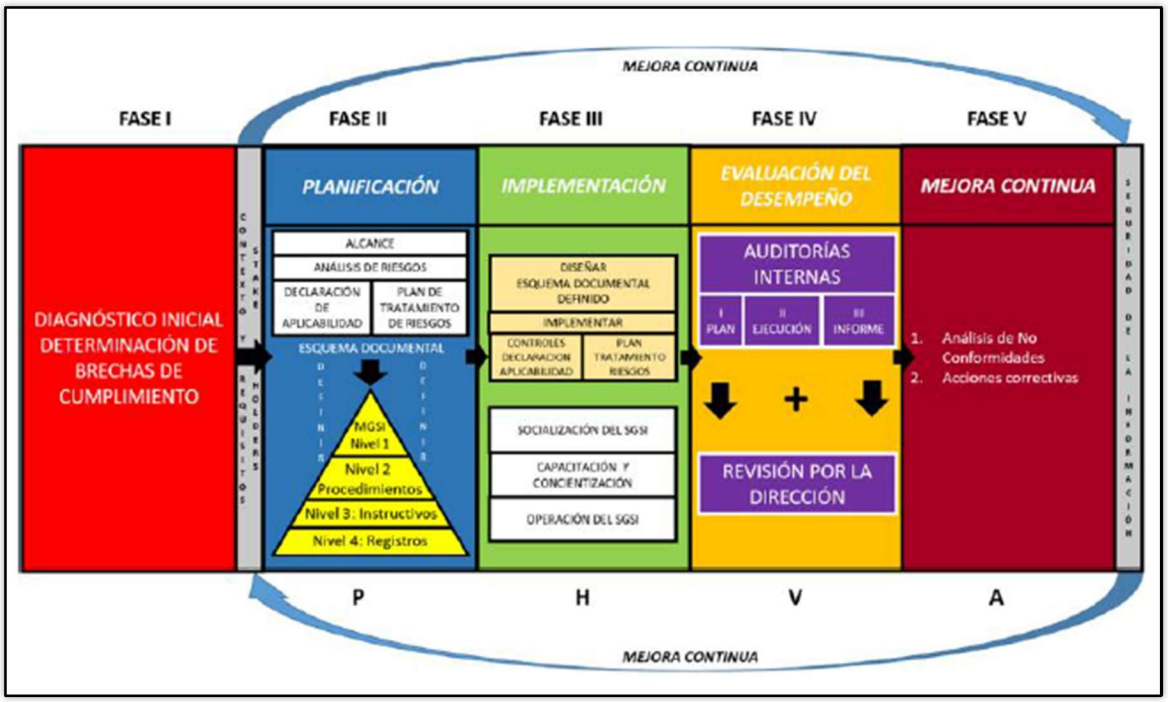
1. Identificación del riesgo.
2. Identificación de activos de información.
3. Identificación de amenazas sobre los activos identificados en el paso anterior.

4. Identificación de controles existentes.
5. Identificación de vulnerabilidades.
6. Valoración de vulnerabilidades.
7. Identificación de consecuencias.

Modelo de SGSI basado en ISO 27001 de Benavides y Blandón

Benavides Sepúlveda y Blandón Jaramillo (2017), proponen el **Modelo de Sistema de Gestión de Seguridad de la Información basado en la norma NTC ISO/IEC 27001 para instituciones públicas de Educación Básica de la Comuna Universidad de Pereira**, alineado con los requerimientos del Ministerio de Educación de Colombia y el Modelo de Seguridad y Privacidad antes mencionado. Su proceso de análisis y evaluación de riesgos "ha tenido en cuenta las directrices de la norma internacional ISO/IEC 27005 en conjunción los elementos de la norma (norteamericana) NIST 800-30" (Benavides Sepúlveda & Blandón Jaramillo, 2017, pág. 82) encuadrados en un SGSI que sigue los lineamientos de ISO 27001 e implementa controles detallados en ISO 27002.

Figura 7: Esquema general del modelo SGSI propuesto por Benavides y Blandón



Fuente: (Benavides Sepúlveda & Blandón Jaramillo, 2017, pág. 158)

En la Figura 7 se presenta el esquema correspondiente al Modelo de SGSI propuesto por Benavides y Blandón (2017), cuyas fases se describen a continuación.

Fase I Diagnóstico Inicial donde se determina el nivel de cumplimiento de los requisitos de seguridad de la información establecidos en ISO 27001 en la organización.

Fase II Planificación donde se hace la planeación del proceso de gestión de riesgo, requisito enunciado en ISO 27001, para cuyo cumplimiento se siguen las siguientes actividades:

1. **Definición del alcance** del SGSI según ISO 27001 para lo cual se escoge un departamento o dependencia administrativa en que se llevará a cabo el proceso. En el caso de un trabajo de Gestión de Riesgos de Información se utiliza la nomenclatura de **Definición de Contexto** tal como se indica en la norma ISO 27005 (2012).

2. Realización del proceso de **evaluación de riesgos** En lo cual se adapta la norma ISO 27005 (2012) y la metodología NIST SP-800 30 en concordancia con el numeral 6.1.2 de ISO 27001 (2014), para lo cual se llevan a cabo las siguientes actividades:

a. Realización del inventario de activos.

b. Determinación de los factores de criticidad en los activos.

c. Establecimiento de niveles de criticidad de los activos.

d. Determinación de los escenarios de riesgos.

e. Determinación de la calificación de la probabilidad de ocurrencia de riesgos.

f. Determinación del impacto potencial de los riesgos.

g. Cálculo de vulnerabilidad inherente derivada de los riesgos.

h. Establecimiento de parámetros de aceptabilidad de riego.

i. Elaboración de mapas de temperatura de vulnerabilidad inherente.

j. Identificación de los controles existentes en la institución según ISO 27002.

k. Cálculo de la vulnerabilidad residual.

l. Elaboración de mapas de vulnerabilidad residual.

Hasta aquí llega el proceso de evaluación de riesgos.

3. Implementación del **Plan de tratamiento de riesgos** detectados en la dependencia definida en el alcance y emisión de una **Declaración de Aplicabilidad**, en concordancia con los requisitos especificados en el numeral 6.1.3 en cuanto Planificación y 8.3 en cuento Operación de la norma ISO 27001 (2014). Según Benavides y Blandón (2017) hasta aquí llega el proceso de gestión de riesgos de información.

4. Establecimiento del esquema documental base para el SGSI, por niveles.

Fase III Implementación en esta fase la organización pone en marcha el SGSI a través de las siguientes actividades:

1. Diseño del esquema documental.

2. Implementación de controles definidos del Anexo A de ISO 27001.

3. Implementación del plan de gestión de riesgo definido.
4. Socialización del Sistema de Gestión de Seguridad de la Información.
5. Capacitación y concienciación.
6. Operación del Sistema.

Fase IV Evaluación del desempeño de lo planificado en la Fase I a través de procesos de:

1. Auditoría interna.
2. Revisión por parte de la dirección.

Fase V Mejora continua donde se analizan las causas que derivan en No conformidades de tal forma que los planes de mejora impidan la repetición de desviaciones, a través de las siguientes actividades:

1. Análisis de No conformidades o desviaciones.
2. Establecimiento de acciones correctivas.

Capítulo 4

Metodología

En este capítulo se presenta la Metodología adaptada del Modelo de Sistema de Gestión de Seguridad de la Información desarrollado por Alejandra Benavides y Carlos Blandón (2017) **en lo referente al proceso de gestión de riesgos de información**, con aplicación en el Instituto Tecnológico Superior Sucre, siguiendo las directrices de las normas ISO/IEC 27001 (2014), ISO/IEC 27002 (2014) e ISO/IEC 27005 (2012) en conjunción con NIST 800-30.

4.1. Diagnóstico inicial de seguridad de la información

Aunque esta actividad no conste dentro del Proceso de Gestión de Riesgos de Seguridad de la Información especificado por la norma ISO/IEC 27005 (2012), es el paso inicial para un Sistema de Gestión de Seguridad de la Información según ISO/IEC 27001 (2014). Para efectos del presente trabajo, sirve para tener una idea cierta de la situación actual de la seguridad de la información el ITS Sucre, razón por la cual se ha considerado su inclusión.

Entrando en materia, el primer proceso del modelo de SGSI de Benavides y Blandón (2017) se refiere al diagnóstico inicial de brechas de cumplimiento de requerimientos del estándar ISO 27001 (2014) y la determinación del grado de madurez que presenta una organización en temas de Seguridad de la Información. Luego de revisar documentación disponible en libros, artículos científicos y sitios web, así como el modelo antes citado se determinó la adaptación del Modelo de Diagnóstico de Seguridad de la Información según ISO 27001 creado por la Alta Consejería Distrital de TIC del Municipio de Bogotá, Colombia (Alta Consejería Distrital de TIC, 2015). Dicho instrumento, un aplicativo desarrollado en Microsoft Excel, permite determinar el nivel de madurez del SGSI de cual organización, en este caso el ITS Sucre, a través de un cuestionario estructurado en tres partes, denominados logros. A continuación, se presenta la descripción del propósito de cada uno de ellos, su peso en porcentaje de aporte sobre el total del diagnóstico de seguridad, así como de los subprocesos que componen a cada uno.

Tabla 3: Estructura del cuestionario de diagnóstico de SGSI

No. de logro	Descripción del Logro	% de peso sobre el total del diagnóstico	Subprocesos	% de peso del subproceso
1	Definición del Marco de Seguridad y Privacidad de la entidad	30%	Diagnóstico de Seguridad y Privacidad	10%
			Propósito de Seguridad y Privacidad de la Información	20%
2	Implementación del Plan de Seguridad y Privacidad	40%	Identificación y análisis de riesgos	20%
			Plan de tratamiento de riesgos, clasificación y gestión de controles	20%
3	Monitoreo y mejoramiento continuo	30%	Actividades de seguimiento, medición, análisis y evaluación	15%
			Revisión e implementación de acciones de mejora	15%

Fuente: Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

Diagnóstico de Logro 1: Definición del Marco de Seguridad y Privacidad de la Información

A continuación, se inicia el análisis del Logro No. 1, referente a la Definición del Marco de Seguridad y Privacidad. Como primer aspecto a considerar, se muestra el esquema sobre el cual se hace la ponderación del cumplimento para cada una de las preguntas que componen este logro.

Tabla 4: Descripción de la valoración para las preguntas del diagnóstico de Definición de Marco de Seguridad y Privacidad de la Información

DIAGNÓSTICO SGSI LOGRO 1: DEFINICIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)	
Por favor, conteste la siguiente encuesta:	
Estado	**Descripción**
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO 17001 versión 2014 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple al 100%
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2014) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona
No cumple	No existe y/o no se está haciendo.

Fuente: Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

En el análisis del Logro 1, mostrada en la Tabla 4, la valoración que reciben las preguntas se hace sobre sus tres posibles estados; el primero, denominado *cumplimiento satisfactorio,* se da cuando el requisito se cumple completamente según lo que exige la norma ISO 27001, está documentado y socializado, ha sido definido y aprobado y ha sido aplicado a todas las partes interesadas del SGSI ; el segundo estado posible, *cumple parcialmente*, se aplica cuando existe un cumplimiento parcial de los requerimientos de la norma, es decir, se tienen implementados controles, pero de manera diferente, es decir, estos ha sido definidos, aprobados y documentados, pero no se los gestiona; y, el tercer posible estado, *no cumple*, que se presenta cuando se tiene conocimiento del requisito especificado en la norma, sin embargo, no existe o no se ejecuta el control asociado.

En la Tabla 5 se presenta un desglose del Logro 1 presentando sus subprocesos, con pesos expresados en porcentajes, preguntas que los componen, así como las cláusulas de ISO 27001 relacionadas por cada uno y su respectiva valoración.

Tabla 5: Desglose del cuestionario de Logro 1

Subprocesos	% de peso del subproceso	Cláusula ISO/IEC 27001 involucrada	No. de pregunta	Detalle de la pregunta	Estado	% de peso de cada pregunta
Diagnóstico de Seguridad y Privacidad	10%	4. Contexto de la organización	1	Existe un autodiagnóstico del SGSI institucional	Cumple satisfactoriamente Cumple parcialmente No cumple	5% 2,5% 0%
		4. Contexto de la organización	2	Existencia de plan de trabajo inicial para implementar un SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	5% 2,5% 0%
Propósito de Seguridad y Privacidad de la Información	20%	5. Liderazgo	3	Aprobación por parte de dirección para el inicio del SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		4. Contexto de la organización	4	Están identificados aspectos organizacionales externos e internos que afectan el desarrollo del SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		6. Planificación	5	Están identificadas las partes interesadas	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		5. Liderazgo	6	Están evaluados objetivos y necesidades	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		5. Liderazgo	7	Existe el Comité de Seguridad Informática	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		4. Contexto de la organización	8	Se cuenta con una definición del alcance del SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		5. Liderazgo	9	Existe una política de seguridad de la información aprobada	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		6. Planificación	10	Están definidos roles, responsables	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		6. Planificación	11	Este un proceso de evaluación de riesgos	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		6. Planificación	12	Este una declaración de aplicabilidad	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		7. Soporte	12	Se ha evaluado la competencia del personal que tiene a su cargo una labor que afecta a la seguridad de la información	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		7. Soporte	13	Se ha evaluado la competencia del personal que tiene a su cargo una labor que afecta a la seguridad de la información	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		7. Soporte	14	Existe un modelo de comunicación interno y externo de seguridad de l información	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%
		7. Soporte	15	La información relacionada con el SGSI está debidamente documentada	Cumple satisfactoriamente Cumple parcialmente No cumple	20% 10% 0%

Fuente: Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

A continuación, la Tabla 6 presenta la estructura del cuestionario de diagnóstico de la Definición del Marco de Seguridad y Privacidad, Logro 1.

Tabla 6: Estructura del cuestionario del Logro 1

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	No cumple		Diligenciar autodiagnostico de seguridad de la informacion.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	No cumple		Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?			Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?			Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?			Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?			Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Cómite de Seguridad de la Información?			Definir mediante acto administrativo el comite de seguridad de la informacion que describa las responsabilidades de los integrantes, reuniones entre otros.

Fuente: (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

A continuación, se hace una breve descripción de la estructura del cuestionario de diagnóstico de Logro 1 presentado en la Tabla 6: número de pregunta, cuerpo de la pregunta, valoración de la pregunta, casillero para el registro de la evidencia física o digital que lo sustenta y un casillero para el registro de la recomendación que se debe considerar para dar cumplimiento al requisito. Cabe mencionar que el Logro 1 está relacionado en lo que respecta al Ciclo de Mejora Continua de Demig, con la Fase de Planificación. Los resultados de la aplicación del cuestionario del Logro 1 se presentan en el siguiente capítulo en el numeral 5.1.

Diagnóstico de Logro 2: Plan de Seguridad y Privacidad de la Información

Prosiguiendo con el diagnóstico, se procede con la descripción del cuestionario de diagnóstico del Plan de Seguridad y Privacidad de la Información o Logro 2. De manera similar al análisis de Logro 1, en el Logro 2 se hace una categorización sobre el valor que puede tomar el estado de un determinado control: "Cumple satisfactoriamente", "Cumple parcialmente", "No cumple" y, adicionalmente, el estado "No aplica" el cual se marca cuando el control no es aplicable para la organización. Esta categorización se presenta en la Tabla N° 7.

Tabla 7: Descripción de la valoración para las preguntas de diagnóstico del Logro 2

DIAGNÓSTICO SGSI LOGRO 2: IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (40%)	
Por favor, conteste la siguiente encuesta:	
Estado	**Descripción**
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO 17001 versión 2014 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple al 100%
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2014) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es compatible para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Fuente: Elaboración propia con base en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

A continuación, la Tabla 8 presenta una descripción de la estructura del Cuestionario del Logro 2, teniendo en cuenta que todo el logro analiza el cumplimiento de la Cláusula No. 8 de la norma ISO 27001 (2014), Operación. Este cuestionario contiene 114 preguntas que se corresponden con cada uno de los 114 controles de seguridad especificados en el Anexo A de la norma ISO 27001 (pormenorizados en la norma ISO 27002).

Tabla 8: Descripción de la estructura del cuestionario de Logro 2

Número de dominio	**Nombre dominio de control**				
Número de objetivo	**Nombre objetivo de control**				
Descripción del objetivo de control					
Número de control	Descripción del control	Pregunta por control	Estado	Evidencia	Peso por estado %
			Cumple satisfactoriamente Cumple parcialmente No cumple No aplica		40% 20% 0% 0%

Fuente: Elaboración propia basada en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

A continuación, se hace una breve descripción de la Tabla 8. Las preguntas están agrupadas por dominio de control (14 en total), cada dominio está compuesto por objetivos de control (35 en total) y estos a su vez por controles (114 en total). En los encabezados consta el número de dominio al que corresponde el control y por ende la pregunta, por ejemplo, A5, correspondiente a "Políticas de la seguridad de la Información" o A6, "Organización de la seguridad de la Información". Una vez presentado el número de dominio, el cuestionario se abre en diferentes objetivos de control; por ejemplo, A5.1 "Orientación de la dirección para la gestión de la seguridad de la información"; finalmente los objetivos de control se abren en controles, por ejemplo, A5.1 y A5.2 formulados como dos preguntas del cuestionario. Cada pregunta está estructurada de la siguiente manera: número de control, descripción del control, pregunta, estado del control y registro de evidencias. Para información más detallada respecto a la estructura del cuestionario de Logro 2 favor dirigirse al Apéndice B. El diagnóstico de Logro 2, como se muestra en la Tabla 8, aporta con un peso del 40% del total del diagnóstico distribuido de la siguiente manera: 20% por la Identificación y Análisis de Riesgos y 20% por Plan de tratamiento de riesgos, clasificación y gestión de controles.

A continuación, la Tabla 9 presenta la estructura del cuestionario de diagnóstico de Implementación del Plan de Seguridad y Privacidad de la Información, Logro 2, lleno con datos de prueba.

Tabla 9: Estructura del Cuestionario de Logro 2

ANEXO			ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	No cumple	No existe una política de seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple	Al no existir una política documentada no se puede revisar
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple parcialmente	Existe personal designado responsable de la seguridad de la información
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Cumple parcialmente	Existe separación de tareas y responsabilidades
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple parcialmente	Existe contacto con las autoridades pero no existe SGSI
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple	No existe contacto con especialistas

Fuente: (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

El Logro 2 está relacionado con la Fase de Ejecución dentro del Ciclo de Demig. Los resultados de la aplicación de este cuestionario se presentan en el siguiente capítulo en el numeral 5.1.

Diagnóstico de Logro 3: Procesos de Monitoreo y Mejoramiento Continuo

Finalmente, se procede al diagnóstico del Logro 3 del SGSI que correspondiente a procesos Monitoreo y Mejoramiento Continuo. De manera similar al análisis de Logro 1, en el Logro 3 se hace una categorización sobre el valor que puede tomar el estado de un determinado control: "Cumple satisfactoriamente", "Cumple parcialmente", "No cumple", estados que ya fueron descritos anteriormente, y se presentan en la Tabla 10.

Tabla 10: Descripción de la valoración del cuestionario del Logro 3

DIAGNÓSTICO SGSI LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30%)	
Por favor, conteste la siguiente encuesta:	
Estado	**Descripción**
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO 17001 versión 2014 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple al 100%
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2014) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona
No cumple	No existe y/o no se está haciendo.

Fuente: (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

En la tercera parte o logro, se verifica el cumplimiento de los procesos de Monitoreo y Mejora Continua a través de 12 preguntas, que se correlacionan con los procesos "Verificar" y "Actuar" del ciclo de Demig. Este logro tiene un peso del 30% del total distribuido de la siguiente manera: 15% atribuido a actividades de seguimiento, medición, análisis y evaluación (preguntas 1 al 6) y 15% por actividades de revisión e implementación de acciones de mejora (preguntas 7 al 12). En la Tabla 11 se presenta un desglose del cuestionario del Logro 3 presentando sus subprocesos con pesos, preguntas que los componen, así como las cláusulas de ISO 27001 relacionadas por cada una y su respectiva valoración.

Tabla 11: Desglose del cuestionario de Logro 3

Subprocesos	% de peso del subproceso	Cláusula ISO/IEC 27001 involucrada	No. de pregunta	Detalle de la pregunta	Estado	% de peso de cada pregunta
Actividades de seguimiento, medición, análisis y evaluación	15%	9.Evaluación del desempeño	1	Existe una metodología para dar seguimiento al desempeño del SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		9.Evaluación del desempeño	2	Existen auditorías internas al SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		9.Evaluación del desempeño	3	Existe un programa de auditorías aplicables al SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		9.Evaluación del desempeño	4	La alta dirección hace revisiones periódicas al SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		9.Evaluación del desempeño	5	Existe retroalimentación al desempeño del SGSI en las revisiones periódicas que hace la dirección	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		9.Evaluación del desempeño	6	Se documentan debidamente esas revisiones periódicas	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
Revisión e implementación de acciones de mejora	15%	10. Mejoras	7	Se da respuesta a las No Conformidades a la Seguridad de la Información en las auditorías	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		10. Mejoras	8	Se han implementado acciones respecto a las No conformidades	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		10. Mejoras	9	Se revisa la eficacia de las acciones correctivas mencionadas en la pregunta anterior	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		10. Mejoras	10	La entidad hace cambios al SGSI después de tomar acciones correctivas	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		10. Mejoras	11	Se documentan tales acciones correctivas debidamente	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%
		10. Mejoras	12	La entidad realiza procesos de mejora continua para el SGSI	Cumple satisfactoriamente Cumple parcialmente No cumple	15% 7,5% 0%

Fuente: Elaboración propia basada en (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

A continuación, la Tabla 12 presenta la estructura del cuestionario de diagnóstico de Monitoreo y Mejoramiento Continuo, Logro 3, lleno con datos de prueba.

Tabla 12: Estructura del Cuestionario de Logro 3

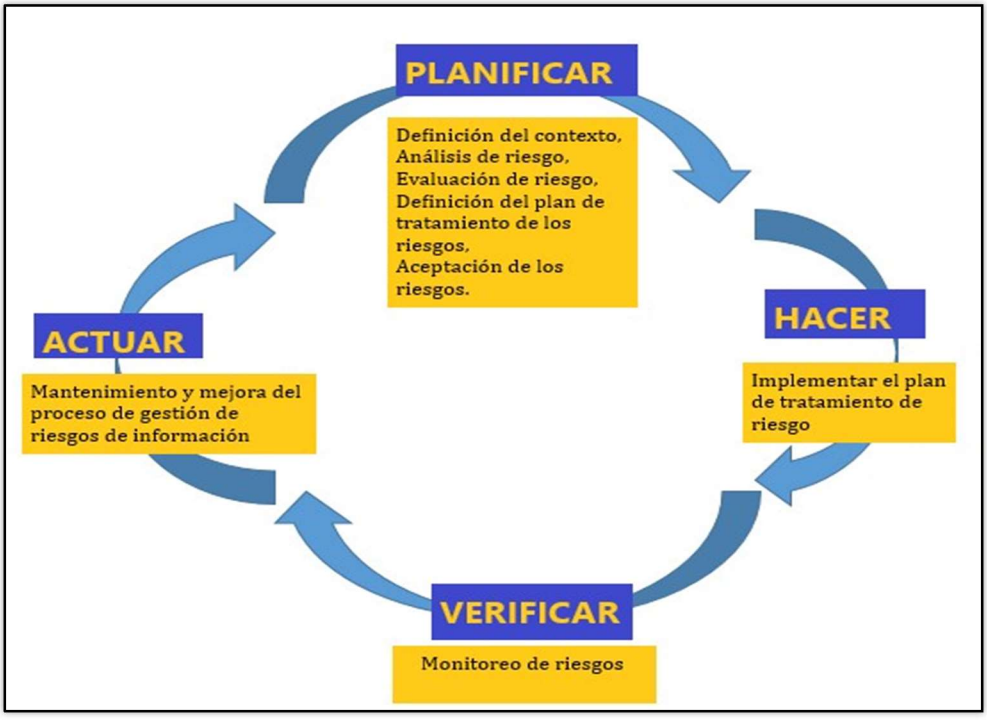
VERIFICAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de laInformación.?	No cumple	No existe un SGSI	Se debe tener en cuenta que se desea medir, cuando, quien realizará la mediciónу cuando se analizaran los resultados.
2	La entidad ha realizado auditorias internas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Se deben programar auditorias en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la Información.
3	La entidad cuenta con programas de auditorias aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	No existe un SGSI	Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periodicas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	No cumple	No existe un SGSI	
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	No existe un SGSI	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluacion de las no conformidades y acciones correctivas. Esta revisión debe incluir las decisiones relacionadas con las oportunidades de mejora

Fuente: (Ministerio de Tecnologías de la Información y las Comunicación, MinTIC, 2016)

Como se presenta en la Tabla 12, la estructura de las preguntas es similar al seguido en el cuestionario del Logro 1, de izquierda a derecha, número de pregunta, el texto de la pregunta (que está especificado en ISO 27001 versión 2014), la valoración de la pregunta, más un campo para el registro de la evidencia física o lógica y un campo reservado para recomendaciones especificadas en ISO 27001. Los resultados de la aplicación del cuestionario del Logro 3 son presentados en se presentan en el siguiente capítulo en el numeral 5.1.

Al finalizar, cabe recalcar que el Diagnóstico de Seguridad (Inicial) que se acaba de presentar se lo realiza sobre el proceso Sistema de Gestión de Seguridad de la Información como un todo y no únicamente sobre el proceso de Gestión de Riesgos de Seguridad de la Información, que es una parte de ese todo. Este diagnóstico puede ser aplicado sucesivamente en otras fases del desarrollo del SGSI para comprobar el cumplimiento de las especificaciones de ISO 27001 y dentro de los procesos de Monitoreo y Mejora Continua de la Gestión de Riesgos.

Figura 8: Alineamiento del proceso de SGSI y del proceso de Gestión de Riesgos de Seguridad de la Información



Fuente: Elaboración propia con base en (Instituto Ecuatoriano de Normalización, 2012)

En la Figura 8 se presentan las actividades componentes del proceso Gestión de Riesgos de Seguridad de la Información según ISO 27005(2012), para las cuatro fases del proceso de un SGSI según ISO 27001 (2014).

4.2. Definición del contexto de la gestión de riesgos de seguridad de la información

El paso siguiente dentro de la metodología adaptada de gestión de riesgos de seguridad de la información da cumplimiento al requisito descrito en el numeral 4.3 del estándar ISO 27001 (2014), los numerales 7 y 7.3 de la norma ISO 27005 (2012) y el Modelo de SGSI de Benavides y Blandón (2017); consiste en la definición del contexto del Proceso de Gestión de Riesgos de Seguridad de la Información. Luego de varias reuniones de trabajo con el rector y el vicerrector académico del ITS Sucre, en las que se analizaron las especificaciones pertinentes de las normas antes mencionadas y tomando en cuenta condiciones específicas de la información que se procesa y custodia en el plantel, el señor rector aprobó el proyecto y autorizó que la Implementación de la Metodología de Gestión de Riesgos de Seguridad de Información, fase práctica de este trabajo de investigación, se efectúe sobre los procesos que maneja la Unidad de Titulación del ITS Sucre, tanto en el Campus Norte como en el Campus Sur, puesto que dicha Unidad aglutina todos los procesos académicos del plantel que se derivan desde las ocho carreras. Las evidencias constan en los certificados que se presentan en el Apéndice C.

4.3. Proceso de evaluación de riesgos

4.3.1. Inventario de activos

Desde este proceso propiamente empieza la evaluación de riesgos de seguridad de la información y en su realización se adapta el Modelo de Benavides y Blandón (2017). Dicho modelo recomienda como primer paso realizar el levantamiento del inventario de activos sensibles a riesgos de información en la entidad definida en el alcance, para este estudio, se lo hace en la Unidad de Titulación del ITSS. Dichos activos pueden ser de tipo físico, como anaqueles, archivadores, carpetas de expedientes, espacios físicos; tecnológicos, como computadores, impresoras, dispositivos de acceso magnético; de tipo humano, como son secretarias, guardias, coordinadores de carrera o de titulación; de tipo lógico, software: sistemas operativos, procesadores de texto, hojas electrónicas, antivirus; procesos, como emisión de certificados académicos, elaboración y aplicación de exámenes complexivos, emisión de informes de aprobados, elaboración de promedios finales de titulación, etc. La estructura de la matriz

de inventario de activos se sigue el formato: número de activo, tipo de activo, descripción de activo, observaciones, tal como se presenta en la Tabla 13.

Tabla 13: Modelo de matriz de inventario de activos

N° activo	Tipo de activo	Descripción	Observaciones
1	Físico	Anaquel	Almacenamiento bibliográfico de las tesis de grado físicas y digitales de los graduados del ITSS
2	Físico	Archivador	Almacenamiento de las carpetas de estudiantes
3	Tecnológico	Computador de secretaría	Gestión bibliográfica de tesis en formato físico y digital, emisión de certificados académicos
4	Tecnológico	Impresora	Impresión de etiquetas de ordenamiento bibliográfico de las tesis, títulos de Tecnólogos, informes de estudiantes, constancias
5	Tecnológico	Regulador de voltaje	Protección de equipos utilizados para procesar información académica
6	Tecnológico	TAG de control de acceso	Dispositivo de lectura de tarjetas magnéticas de acceso a instalaciones, ingreso de códigos de acceso y emisión de alertas, en la Sede Sur
7	Tecnológico	Teléfono	Utilizado para atención al público, especialmente estudiantes, docentes y autoridades
8	Tecnológico	Tarjeta magnética	Dispositivo que permite acceder a instalaciones: aulas y oficinas en la Sede Sur
9	Humano	Secretaria	Persona responsable de elaboración de promedios, emisión de actas consolidadas de titulación, codificación de trabajos de titulación (tesis) físicos y digitales y archivo en vicerrectorado y su gestión y custodia, emisión de títulos, archivo de actas y documentos de respaldo en archivo en sala de lectura.
10	Humano	Guardia de seguridad	Control de ingreso/salida física y vehicular de personas a/de la institución. Custodia de bienes

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La matriz de inventario de activos de información completa se presenta en el numeral 5.3.1 del siguiente capítulo.

4.3.2. Determinación de los factores de criticidad de los activos

Una vez que se han identificado los activos de información sensibles se procede a determinar la criticidad de acuerdo a su disponibilidad, integridad y confidencialidad de acuerdo al modelo propuesto por Benavides y Blandón (2017) y adaptado por el autor. Esto se presenta en la Tabla 14.

Tabla 14: Factores de criticidad de activos de información de la Unidad de Titulación ITS Sucre

CRITERIO	FACTOR	CUESTIONAMIENTO
DISPONIBILIDAD	FINANCIERO	¿ Es posible que se genere afectación financiera por falta de disponibilidad del activo?
	LEGAL	¿ Es posible que se genere afectación legal por falta de disponibilidad del activo?
	IMAGEN	¿ Es posible que se genere afectación a la imagen del ITSS por falta de disponibilidad del activo?
INTEGRIDAD	FINANCIERO	¿ Es posible que se genere afectación financiera por cambios no autorizados en el activo?
	LEGAL	¿ Es posible que se genere afectación legal por cambios no autorizados en el activo?
	IMAGEN	¿ Es posible que se genere afectación a la imagen del ITSS por cambios no autorizados en el activo?
CONFIDENCIALIDAD	FINANCIERO	¿ Es posible que se genere afectación financiera por divulgación no autorizada de información sensible?
	LEGAL	¿ Es posible que se genere afectación legal por divulgación no autorizada de información sensible?
	IMAGEN	¿ Es posible que se genere afectación a la imagen del ITSS por divulgación no autorizada de información sensible?

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

4.3.3. Valoración de los factores de criticidad de los activos

Luego de realizar el inventario de activos y determinados los factores de criticidad que les corresponde, se procede a su valoración, adaptando para el efecto el modelo presentado por Benavides y Blandón (2017). A cada uno de los activos de seguridad inventariados se le asigna un valor entero 0 o 1 por criterio y factor de criticidad, de tal manera que el valor teórico máximo que pudiera llegar a tomar su criticidad 9. El valor real de criticidad de cada activo se calcula a partir de la siguiente fórmula:

$$NCA = \sum_{i=1}^{9} \frac{CFA}{MAX(CFA)}$$

Donde:

NCA es el nivel de criticidad del activo

CFA es la calificación de los factores para el activo

MAX (CFA) es el valor máximo posible de calificación de los factores para el activo

Con estos antecedentes se procede a levantar la matriz de valoración de criticidad para los activos de información de la Unidad de Titulación del ITSS, cuyo modelo se presenta en la Tabla 15:

Tabla 15: Modelo de matriz de valoración de criticidad de activos

N° activo	Descripción del activo	Tipo de Activo	Valoración de la de criticidad de los activos									Criticidad
			Confidencialidad			Integridad			Disponibilidad			
			Financ.	Legal	Imagen	Financ.	Legal	Imagen	Financ.	Legal	Imagen	
1	Anaquel	Físico	1	1	1	1	1	1	1	1	1	100%
2	Archivador	Físico	1	1	1	1	1	1	1	1	1	100%
3	Computador de secretaría	Tecnológico	0	1	1	0	0	0	0	1	1	44%
4	Impresora	Tecnológico	0	0	1	0	0	1	1	0	1	44%
5	Regulador de voltaje	Tecnológico	0	0	1	0	0	1	0	0	1	33%
6	TAG de control de acceso	Tecnológico	1	1	1	1	1	1	1	1	1	100%
7	Teléfono	Tecnológico	0	0	1	0	0	1	1	0	1	44%
8	Tarjeta magnética	Tecnológico	1	1	1	0	0	0	1	1	1	67%
9	Secretaria	Humano	1	1	1	1	1	1	1	1	1	100%
10	Guardia de seguridad	Humano	1	1	1	1	1	0	1	1	1	89%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La matriz de valoración de criticidad de activos de la Unidad de Titulación del ITS Sucre completa, se presenta en el numeral 5.3.3 del capítulo siguiente.

Una vez que se posee la criticidad de los activos se procede a su clasificación en cuatro niveles: alto, medio y bajo, como se presenta en la Tabla 16.

Tabla 16: Niveles de criticidad de activos de información de la Unidad de Titulación del ITSS

CRITERIO DE EVALUACIÓN	CALIFICACIÓN	CRITICIDAD
El activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información	>=33%	ALTO
El activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información	22%	MEDIO
El activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información	11%	BAJO
El activo no compromete la integridad, confidencialidad y disponibilidad de la información	0%	NO CRÍTICO

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

4.3.4. Identificación de riesgos asociados a los activos de información

Para el cumplimiento de esta actividad se utiliza las recomendaciones que trae el Anexo C de la norma ISO 27005 (2012) en lugar de utilizar el Modelo de SGSI de Benavides y Blandón (2017). Se realiza un inventario de riesgos asociados a los activos de información; estructurado de la siguiente manera: número de riesgo, riesgo (descripción), y, origen, que puede ser de tipo intencional (I), accidental (A) o de origen natural (N), cuyo modelo se presenta en la Tabla 17.

Tabla 17: Matriz modelo de escenarios de riesgo

N°	Riesgo	Origen
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	I
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	I
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	I
4	Afectación legal por pérdida de anillados o empastados de las tesis	A, I
5	Afectación legal por pérdida de actas consolidadas de titulación	I

Fuente: Elaboración propia

La matriz de escenarios de riesgo completa se presenta en el numeral 5.3.4 del siguiente capítulo.

4.3.5. Asignación de valor de probabilidad de riesgo

En esta actividad se retoma la adaptación del modelo de Benavides y Blandón (2017). Posterior al levantamiento de la matriz de riesgos, se establece un valor de probabilidad de ocurrencia del riesgo

de información para el período de un año, mismo que se establece tomando en consideración las características propias de la unidad objeto del análisis de riesgos. Esto es presentado en la Tabla 18.

Tabla 18: Valoración de probabilidad

VALOR	PONDERACIÓN DE PROBABILIDAD	DESCRIPCIÓN
3	alta	Si existe el riesgo de que se materialice una amenaza a la seguridad sobre un activo más de 5 veces en un año, la probabilidad es alta
2	media	Si existe el riesgo de que se materialice una amenaza a la seguridad sobre un activo entre 2 y 5 veces en un año, la probabilidad es media
1	baja	Si existe el riesgo de que se materialice una amenaza a la seguridad sobre un activo menos de 2 veces en un año, la probabilidad es baja

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

4.3.6. Valoración del impacto potencial

De manera similar a la valoración que se realizó a la probabilidad de ocurrencia de riesgos, debe hacerse una valoración a la materialización de riesgos (impactos) a la confidencialidad, integridad y disponibilidad de la información, misma que puede ser alta, moderada o baja. La valoración se realiza adaptando la guía de gestión de riesgo NIST 800-30 (2002) citada en el Modelo de SGSI de Benavides y Blandón (2017), como se presenta a continuación.

Tabla 19: Impacto potencial

CRITERIO	BAJO	MODERADO	ALTO
	1	2	3
CONFIDENCIALIDAD	La divulgación no autorizada de información sensible podría tener un efecto adverso limitado en las operaciones de la unidad de titulación del ITSS, sus activos de información o su personal	La divulgación no autorizada de información sensible podría tener un efecto adverso serio en las operaciones de la unidad de titulación del ITSS, sus activos de información o su personal	La divulgación no autorizada de información sensible podría tener un efecto adverso grave o catastrófico en las operaciones de la Unidad de Titulación del ITSS, sus activos o su personal
INTEGRIDAD	La modificación o destrucción imprevista de información sensible, herramientas o dispositivos podrían tener un efecto adverso limitado en las operaciones de la Unidad de Titulación del ITSS, sus activos o su personal	La modificación o destrucción imprevista de información sensible, herramientas o dispositivos podrían tener un efecto adverso serio en las operaciones de la Unidad de Titulación del ITSS, sus activos o su personal	La modificación o destrucción imprevista de información sensible, herramientas o dispositivos podrían tener un efecto adverso grave o catastrófico en las operaciones de la Unidad de Titulación del ITSS, sus activos o su personal
DISPONIBILIDAD	La interrupción del acceso a información sensible podría tener un efecto adverso limitado en las operaciones de la Unidad de Titulación del ITSS, sus activos o sus individuos	La interrupción del acceso a información sensible podría tener un efecto adverso serio en las operaciones de la Unidad de Titulación del ITSS, sus activos o sus individuos	La interrupción del acceso a información sensible podría tener un efecto adverso grave o catastrófico en las operaciones de la Unidad de Titulación del ITSS, sus activos o sus individuos

Fuente: Elaboración propia basada en (National Institute for Standards and Technology (NIST), 2002) citado por (Benavides Sepúlveda & Blandón Jaramillo, 2017)

4.3.7. Cálculo de la vulnerabilidad inherente

Una vez que se tiene ponderada la probabilidad de ocurrencia de riesgos y valorado su impacto potencial, se debe proceder al cálculo de la vulnerabilidad inherente. Para ello se adapta el Modelo de SGSI de Benavides y Blandón (2017) de la siguiente manera:

Primero se calcula el impacto total como la sumatoria de los impactos sobre la confidencialidad, integridad y disponibilidad de acuerdo a la fórmula: $Itotal = Ic + Ii + Id$

Donde:

Itotal = Impacto total

Ic= Valor de impacto sobre la confidencialidad

Ii= Valor de impacto sobre la integridad

Id= Valor de impacto sobre la disponibilidad

Segundo, se calcula la vulnerabilidad inherente para cada factor de seguridad (confidencialidad, integridad, disponibilidad). Para el cálculo de vulnerabilidad inherente por confidencialidad se utiliza la siguiente fórmula:

$$VIc = \frac{P * Ic}{Max(P * Ic)}$$

Donde:

VIc= Vulnerabilidad inherente de la confidencialidad

Ic= Valor de impacto por confidencialidad

P= Probabilidad

Max (P*Ic) = Máximo posible valor de la probabilidad por impacto. De acuerdo con Benavides y Blandón (2017) el valor máximo de la probabilidad es 3 y el valor máximo del impacto es 3, por ende, el denominador de la ecuación anterior es siempre 9.

Se procede de manera similar para el cálculo de la vulnerabilidad inherente de los otros dos factores, integridad y disponibilidad. Una vez que se tienen calculadas las tres vulnerabilidades inherentes se procede al cómputo de la vulnerabilidad inherente total, aplicando la siguiente fórmula:

$$VIt = \frac{P * (Ic + Ii + Id)}{Max(P * (Ic + Ii + Id))}$$

Donde:

VIt= Vulnerabilidad inherente total

Max$(P * (Ic + Ii + Id))$ = Máximo posible valor de la probabilidad por el impacto. De acuerdo con Benavides y Blandón (2017) el valor máximo de la probabilidad es 3 y el valor máximo combinado de los tres impactos es 9, por ende, el denominador de la ecuación anterior es siempre 27.

A continuación se presenta el modelo de matriz de vulnerabilidad inherente:

Tabla 20: Matriz modelo de vulnerabilidad inherente

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad inherente			
			Ic	Ii	Id	Itotal	VIc	VIi	VId	VIt
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	1	3	3	3	9	33%	33%	33%	33%
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	1	3	3	3	9	33%	33%	33%	33%
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	1	3	3	3	9	33%	33%	33%	33%
4	Afectación legal por pérdida de anillados o empastados de las tesis	2	3	3	3	9	67%	67%	67%	67%
5	Afectación legal por pérdida de actas consolidadas de titulación	1	3	3	3	9	33%	33%	33%	33%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La matriz de vulnerabilidad inherente se presenta en el siguiente capítulo, en el numeral 5.3.7.

4.3.8. Establecimiento de criterios de aceptación de riesgo

El siguiente paso es el establecimiento de criterios de aceptabilidad de riesgo. Para su cumplimiento se adapta el Modelo de SGSI de Benavides y Blandón (2017), y se genera la tabla de criterios de aceptabilidad de riesgo.

Tabla 21: Criterios de Aceptabilidad de Riesgo

Identificación	Criterio	Calificación
Verde	Aceptable	menor o igual a 25%
Amarillo	Tolerable	mayor a 25% y menor o igual a 50%
Rojo	Inaceptable	mayor a 50%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

4.3.9. Creación de mapas de temperatura de vulnerabilidad inherente

La siguiente actividad es la creación de las matrices/ mapas temperatura de vulnerabilidad inherente, que son herramientas gráficas a través de la cuales la alta dirección de la entidad puede saber qué activos dentro de su unidad administrativa precisan de mayor atención en función de su vulnerabilidad. A continuación, se presenta el modelo de matriz/mapa de temperatura de vulnerabilidad inherente para la confidencialidad de la información. Se debe contar con la información

de los riesgos proveniente de la matriz de vulnerabilidad inherente. Se crea una matriz en cuyo eje horizontal se colocan los impactos de confidencialidad y en el eje vertical los valores de probabilidad, se cruzan los valores formando un par ordenado (impacto, probabilidad). Con esos valores combinados se van ubicando en el mapa de vulnerabilidad inherente de la confidencialidad los números de cada uno de los escenarios de riesgo detectados. Luego, se observa el valor de vulnerabilidad inherente para confidencialidad que cada riesgo tiene y contando con los criterios de aceptabilidad de riesgos se van pintando las casillas del mapa: color verde para riesgos con vulnerabilidad inherente menor o igual a 25%, color amarillo para aquellos cuya vulnerabilidad inherente de confidencialidad es mayor a 25% pero inferior a 50% y de color rojo a aquellos cuyo valor porcentual de vulnerabilidad inherente de confidencialidad es mayor al 50%, como se muestra en la siguiente tabla modelo.

Tabla 22: Modelo de mapa de temperatura de vulnerabilidad inherente para la confidencialidad

CONFIDENCIALIDAD				
PROBABILIDAD	3	30,38,48	23,24,28	11,12,14,15,49
	2	19,20,25,26,27, 29,32,33,34,44	40,43,46,47,50	4,7,10,13,16,39
	1	8,37	17,18,36,45	1,2,3,5,6,9,21,2 2,31,35,41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Los mapas de temperatura de vulnerabilidad inherente para la confidencialidad, integridad y disponibilidad, así como el mapa de temperatura de vulnerabilidad inherente total, así como la interpretación de resultados de cada uno se presentan en el numeral 5.3.9 del siguiente capítulo.

4.3.10. Identificación de controles existentes

Para el cumplimiento de esta actividad se continúa con la adaptación del Modelo de SGSI de Benavides y Blandón (2017) y se elabora la Tabla de Controles Existentes para la Unidad de Titulación del ITS Sucre. Para su confección se utiliza la matriz de escenarios de riesgo detectados, las matrices del diagnóstico inicial llenas y la norma ISO 27002 (2014). Por cada escenario de riesgo detectado se reconoce el control existente reconocido por la norma ISO mencionada y se genera una matriz estructurada de la siguiente manera: número de riesgo, escenario de riesgo, código ISO 27002 del control, descripción del control actual, como se presenta en la Tabla 23.

Tabla 23: Modelo de Matriz de Controles Existentes en la Unidad de Titulación del ITS Sucre

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur, Bienestar Estudiantil Norte y computadores de coordinadores de carrera

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La Tabla de Controles Existentes consta en el numeral 5.3.10 del siguiente capítulo.

4.3.11. Cálculo de la vulnerabilidad residual

La existencia de controles implementados al interior de la Unidad de Titulación del ITSS, modifican los valores previamente calculados de vulnerabilidad inherente y se habla, entonces, de vulnerabilidad residual. Para su elaboración se adapta el Modelo de SGSI de Benavides y Blandón (2017) de la siguiente manera:

Primero se calcula el impacto residual total como la sumatoria de los impactos residual sobre la confidencialidad, integridad y disponibilidad, utilizando para el efecto la siguiente fórmula:

$$IRtotal = IRc + IRi + IRd$$

Donde:

IRtotal = Impacto residual total

IRc= Valor de impacto residual de confidencialidad

IRi= Valor de impacto residual de integridad

IRd= Valor de impacto residual de disponibilidad

Segundo, se calcula la vulnerabilidad residual para cada factor de seguridad: confidencialidad, integridad, disponibilidad. Para el cálculo de vulnerabilidad residual por confidencialidad de la información se utiliza la siguiente fórmula:

$$VRc = \frac{P * IRc}{Max(P * IRc)}$$

Donde:

VIc= Vulnerabilidad residual de confidencialidad

IRc= Valor de impacto residual de confidencialidad

P= Probabilidad

Max (P*IRc) = Máximo posible valor de la probabilidad por impacto residual. De acuerdo con Benavides y Blandón (2017) el valor máximo de la probabilidad es 3 y el valor máximo del impacto es 3, por ende, el denominador de la ecuación anterior es siempre 9.

Se procede de manera análoga para el cálculo de la vulnerabilidad residual de la integridad y de la disponibilidad. Una vez que se tienen calculadas las tres vulnerabilidades residuales se procede al cómputo de la vulnerabilidad residual total, misma que se halla con la siguiente fórmula:

$$VRt = \frac{P * (IRc + IRi + IRd)}{Max(P * (IRc + IRi + IRd))}$$

Donde:

VRt = Vulnerabilidad residual total

Max $(P * (IRc + IRi + IRd))$ = Máximo posible valor de la probabilidad por el impacto. De acuerdo con Benavides y Blandón (2017) el valor máximo de la probabilidad es 3 y el valor máximo combinado de los tres impactos es 9, por ende, el denominador de la ecuación anterior es siempre 27.

A continuación se presenta un modelo de matriz de vulnerabilidad residual.

Tabla 24: Modelo de matriz de vulnerabilidad residual

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad			
			IRc	IRi	IRd	IRtotal	VRc	VRi	VRd	VRt
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	1	3	3	3	9	33%	33%	33%	33%
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	1	3	3	3	9	33%	33%	33%	33%
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	1	3	3	3	9	33%	33%	33%	33%
4	Afectación legal por pérdida de anillados o empastados de las tesis	2	3	2	1	6	67%	44%	22%	44%
5	Afectación legal por pérdida de actas consolidadas de titulación	1	3	1	1	5	33%	11%	11%	19%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La Matriz de Vulnerabilidad Residual para la Unidad de Titulación del ITS Sucre se presenta en el numeral 5.3.11 del siguiente capítulo.

4.3.12. Creación de mapas de temperatura de vulnerabilidad residual

Con los valores tabulados de vulnerabilidad residual para la confidencialidad, integridad y disponibilidad, se cruzan los valores resultantes con los de probabilidad y siguiendo los criterios establecidos para la aceptabilidad de riesgo, se generan las matrices de clasificación de vulnerabilidad residual. Estas matrices, herramientas gráficas para la toma de decisiones, permiten optimizar los resultados obtenidos en las matrices de vulnerabilidad inherente, puesto que recalifican la vulnerabilidad al considerar los controles existentes. El proceso para su elaboración es similar al seguido en la elaboración de los mapas de temperatura de vulnerabilidad inherente por lo que se omite la descripción de su elaboración y se presenta a continuación un modelo de mapa de temperatura para la vulnerabilidad residual.

Tabla 25: Modelo de mapa de temperatura de vulnerabilidad residual

CONFIDENCIALIDAD				
PROBABILIDAD	3	28,30,38, 48	23,24	11, 12,49
	2	15,25,26,27,29,32 ,33,34,44	40,43,46,47, 50	4,14,39
	1	8,10, 19,20,22,37	17,18,36,45	1,2, 3,5,6,7,9,13,16, 21,31,35,41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Las matrices de vulnerabilidad residual para la confidencialidad, integridad y disponibilidad, así como la matriz de vulnerabilidad residual total se presentan en el numeral 5.3.12 en el siguiente capítulo.

Aquí termina el proceso de evaluación de riesgos de la información, según el numeral 8.2 de la norma ISO 27001 (2014).

4.4. Definición del Plan de Tratamiento de Riesgos

El proceso posterior a la Evaluación de Riesgos de Seguridad de la Información, consiste en la definición de un Plan para Tratamiento de riesgos. Para tal efecto se adapta el modelo de Benavides y Blandón (2017) y se define al plan mencionado, estructurado de la siguiente manera: se registra escenario de riesgo y plan de tratamiento de riesgo a seguir en su mitigación asociado; este último está compuesto de estrategia de seguridad de información a seguir, actividad, funcionario o entidad del ITS Sucre responsable de su ejecución, valor o presupuesto asignado por actividad, fecha de inicio y fecha de finalización. A continuación, se presenta en la Tabla 26 el Modelo de Matriz de Tratamiento de Riesgos que sigue la descripción realizada.

Tabla 26: Modelo de Matriz de Tratamiento de Riesgos

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	Actividad	Responsable	Fecha inicio	Fecha final
28. Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	Establecer/ revisar medidas que permitan garantizar el adecuado funcionamiento del Sistema de calificaciones SAO-P	Revisar el SLA o Acuerdo de nivel de servicio entre el proveedor del sistema SAO-P y el ITSS	Jurídico y TIC	1/3/2018	1/4/2018

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La Matriz de Tratamiento de Riesgos de la Unidad de Titulación del ITS Sucre se presenta en el numeral 5.6 en el siguiente capítulo. Hasta esta actividad se hace la adaptación del Modelo de SGSI de Benavides y Blandón (2017). Las siguientes actividades complementan el proceso de Gestión de Riesgos de Seguridad de la Información según la norma ISO 27005 (2012).

4.5. Aceptación del Riesgo

Como actividad final de la Fase de Planificación del Proceso de Gestión de Riesgos de Seguridad de la Información está la Aceptación de Riesgo. Para dar cumplimiento a este requerimiento de seguridad especificado en la norma ISO 27005(2017) se consideran los criterios de aceptabilidad de riesgos presentados en el numeral 4.3.8 con los cuales se elaboraron tanto la matriz de vulnerabilidad inherente como la de vulnerabilidad residual. De esta última, se consideran para su aceptación aquellos riesgos cuyo valor de vulnerabilidad residual es inferior al 50%, debido a las limitaciones presupuestarias a los cuales está expuesto este centro de estudios. Es necesario recalcar que el ITSS, no cuenta con autonomía financiera, sino que depende totalmente en este aspecto, de la SENESCYT. No obstante, se elabora el plan de tratamiento para los riesgos aceptados y es decisión de los niveles directivos institucionales su adición a la Implementación del Plan de Tratamiento de Riesgos, en función de la disponibilidad financiera.

4.6. Implementación del Plan de Tratamiento del Riesgo

Una vez terminada la Fase de Planificación, se implementa en la Unidad de Titulación del ITS Sucre el Plan de Tratamiento de Riesgo definido y descrito en el numeral 4.4. Esta actividad perteneciente al Proceso de Gestión de Riesgos de Seguridad de la Información da cumplimiento al requerimiento de seguridad de la información que consta en el numeral 8.3 de la norma ISO 27001 (2014).

4.7. Monitoreo Continuo de Riesgos

Una vez ejecutado el Plan de Tratamiento de Riesgos, es necesario someter tanto a riesgos como sus factores -valores de activos, impactos, probabilidades de ocurrencia- a un monitoreo y análisis crítico constante, dado que riesgos y factores carecen de un comportamiento estático a través del tiempo. En especial se debe monitorear en los siguientes casos: adición de nuevos activos a la Unidad de Titulación del ITS Sucre; cambios en la lógica de los procesos de la Unidad; detección de nuevas amenazas que puedan activarse interna o externamente a la entidad; la posibilidad de que nuevas vulnerabilidades posibiliten que alguna amenaza las explote; ocurrencia de incidentes de seguridad; vulnerabilidades previamente identificadas (Instituto Ecuatoriano de Normalización, 2012, págs. 37,38).

En caso de presentarse uno de los casos mencionados anteriormente, debe entrarse a un proceso de mejora continua del proceso de gestión de riesgos de información previa notificación a las partes involucradas, esto es coordinador de la Unidad y funcionarios de la misma, a través de los canales de comunicación y consulta pertinentes.

4.8. Mejora Continua del Proceso de Gestión de Riesgos de Seguridad de la Información

Una vez terminada la implementación del Plan de Tratamiento de Riesgo, una vez al año o en el caso que el proceso de monitoreo detecte cambios significativos tanto en riesgos como en sus factores, el Proceso de Gestión de Riesgos de Seguridad de la Información puede someterse a una nueva iteración.

4.9. Comunicación y Consulta

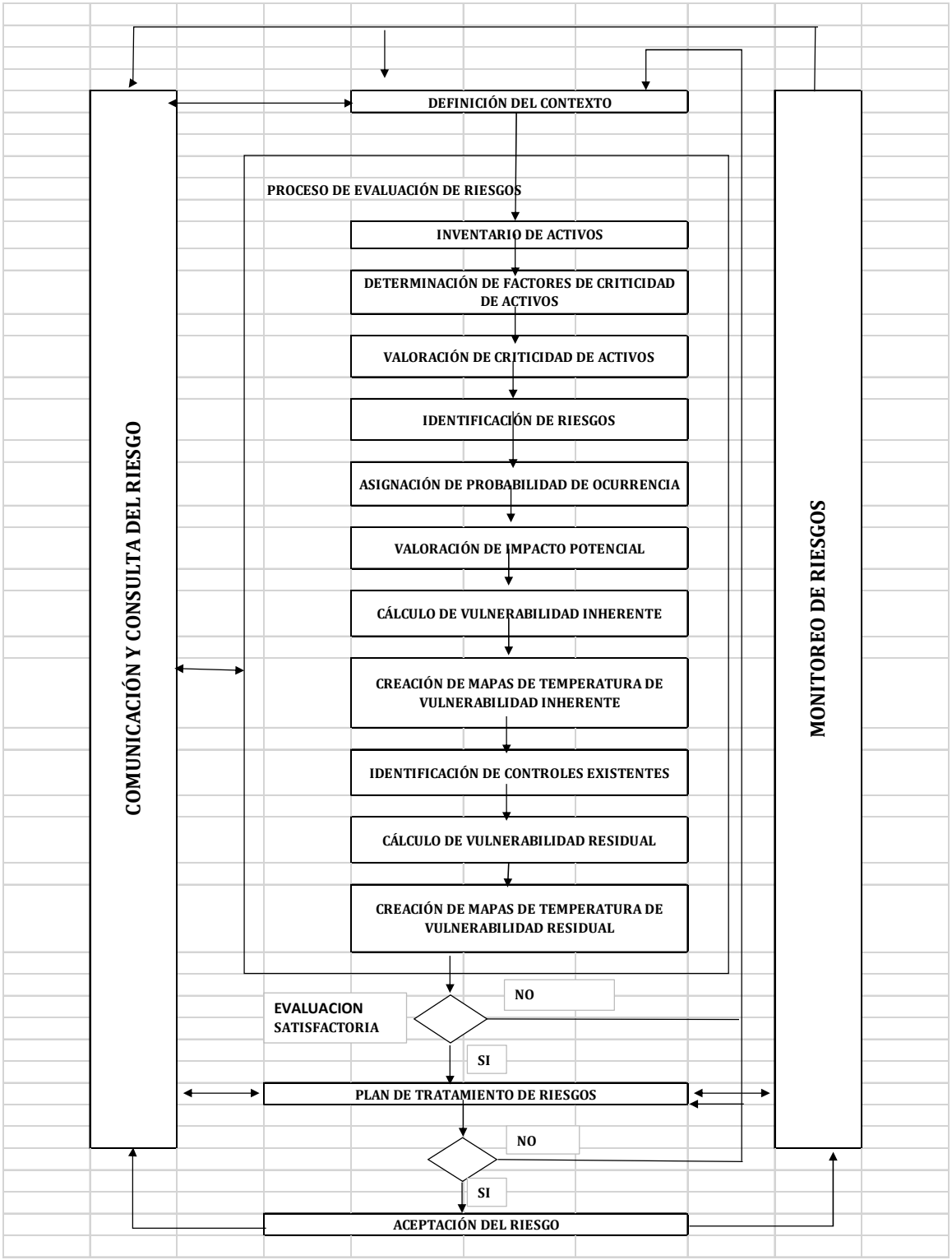
Comunicación y consulta es una actividad de apoyo a todo el proceso de Gestión de Riesgos de Seguridad de la Información existente dentro de la Unidad de Titulación del ITS Sucre, cuyo accionar es permanente, para lo cual se utiliza el correo electrónico institucional y cuya finalidad es ofrecer garantía de resultados de la gestión de riesgos así como el entendimiento continuo del proceso en sí así como de sus resultados (Instituto Ecuatoriano de Normalización, 2012, págs. 37,38).

Capítulo 5

Resultados

Este capítulo presenta los resultados de la Implementación de la Metodología de Gestión de Riesgos descrita en el capítulo 5, cuya estructura se presenta en la Figura 9.

Figura 9: Proceso de Gestión de Seguridad de la Información presentado en la Metodología



Fuente: Elaboración propia

5.1. Diagnóstico inicial de seguridad de la información

Para el cumplimiento de este primer proceso, descrito en el numeral 4.1, se aplicó la adaptación de la herramienta desarrollada en Microsoft Excel para determinar el nivel de madurez de los controles determinados en la norma ISO 27001 versión 2014 al Coordinador de la Unidad de TIC del ITSS, a la Encargada de Financiero y RR.HH. del ITSS, a la Encargada de Control de Activos del ITSS y a la abogada encargada de Jurídico del ITSS y se obtuvieron los resultados que se presentan en la Tabla 27:

Tabla 27: Resumen de resultados del diagnóstico de Definición de Marco de Seguridad y Privacidad de Información -Logro 1- en el ITSS

RESUMEN DEL DIAGNÓSTICO DE DEFINICIÓN DEL MARCO DE SEGURIDAD Y PRIVACIDAD -LOGRO 1- EN EL ITSS (SOBRE 30%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
3 a 15	Cumple satisfactoriamente	0	0	Propósito de Seguridad de Información
3 a 15	Cumple parcialmente	3	2,3%	
3 a 15	No cumple	10	0	
1	Cumple satisfactoriamente	0	0	Autodiagnóstico de S.I.
1	Cumple parcialmente	0	0	
1	No cumple	1	0	
2	Cumple satisfactoriamente	0	0	Creación plan inicial de proyecto que incluya prioridades y objetivos del SGSI
2	Cumple parcialmente	0	0	
2	No cumple	1	0	
TOTAL			2,3%	

Fuente: Elaboración propia

A continuación, se presenta la explicación de los resultados del Diagnóstico de Definición del Marco de Seguridad y Privacidad de la Información, Logro1. La ponderación que se aplica a este logro fue presentada en Tabla 5.

Del cuestionario del Logro 1, se obtuvieron únicamente 3 respuestas puntuables entre 13 posibles dentro del subproceso de Propósito de Seguridad de la Información, los cuales reciben valoración de 10% por cumplimiento parcial, lo que da

$\frac{3*10\%}{13}$ = **2,3%** de cumplimiento de requerimientos de seguridad de la información por Logro 1

A continuación, se presentan los resultados de la segunda parte del cuestionario, referente a la Implementación del Plan de seguridad y Privacidad de Información, Logro 2, en la Tabla 28. Se obtuvieron los siguientes resultados:

Tabla 28: Resumen de resultados del cuestionario de diagnóstico de Implementación del Plan de Seguridad y Privacidad de la Información en el ITSS (Logro 2)

RESUMEN DEL DIAGNÓSTICO DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -LOGRO 2- EN EL ITSS (SOBRE 40%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
1 a 114	Cumple satisfactoriamente	0	0	114 controles de seguridad de información desde A5.1.1 hasta A18.2.3
1 a 114	Cumple parcialmente	39	8,2%	
1 a 114	No cumple	56	0	
1 a 114	No aplica	19	10,0%	
Número de controles que aplican		95		
TOTAL			8,2%	

Fuente: Elaboración propia

A continuación, se presenta la explicación de los resultados del Logro2. La ponderación que se aplica a este logro fue presentada en Tabla 8.

Del cuestionario del Logro 2, se obtuvieron 39 respuestas puntuables entre 95 posibles, los cuales reciben valoración de 20% por cumplimiento parcial, lo que da

$\frac{39*20\%}{95}$ = **8,2%** de cumplimiento de requerimientos de seguridad de la información por Logro 2

Es importante puntualizar que el valor 95 se obtiene de restar el número de preguntas con valoración no aplica, 19, del total de preguntas de este cuestionario, 114.

A continuación, se presentan los resultados de la tercera parte del cuestionario, referente a la Implementación del Procesos de Monitoreo y Mejora Continua, Logro 3, en la Tabla 29. Se obtuvieron los siguientes resultados:

Tabla 29: Resumen de resultados del Cuestionario de Diagnóstico del Plan de Monitoreo y Mejora Continua en el ITSS (Logro 3)

RESUMEN DEL DIAGNÓSTICO DE DEFINICIÓN DEL PLAN DE MONITOREO Y MEJORA CONTINUA -LOGRO 3- EN EL ITSS (SOBRE 30%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
1 a 6	Cumple satisfactoriamente	0	0,0%	Monitoreo (Verificar)
1 a 6	Cumple parcialmente	0	0,0%	
1 a 6	No cumple	6	0,0%	
7 a 12	Cumple satisfactoriamente	0	0,0%	Mejora Continua (Actuar)
7 a 12	Cumple parcialmente	2	2,5%	
7 a 12	No cumple	4	0,0%	
TOTAL			2,5%	

Fuente: Elaboración propia

A continuación, se presenta la explicación de los resultados del Diagnóstico de Logro 3. La ponderación que se aplica a este logro fue presentada en Tabla 11.

Del cuestionario del Logro 3, se obtuvieron únicamente 2 respuestas puntuables entre 6 posibles dentro del subproceso de Mejora Continua, los cuales reciben valoración de 7,5% por cumplimiento parcial, lo que da

$\frac{2*7,5\%}{6}$ = **2,5%** de cumplimiento de requerimientos de seguridad de la información por Logro 3

Finalmente, como calificación final de evaluación de madurez del SGSI al interior del ITSS se obtuvo una calificación de 13% de conformidad respecto a la norma ISO 27001: 2014, como se presenta en la Tabla 30.

Tabla 30: Resumen consolidado de resultados del Diagnóstico Inicial de Seguridad en el ITSS

	FASE	**META**	**TOTAL EJECUTADO**
LOGRO1	PLANEAR	30%	2,3%
LOGRO2	HACER	40%	8,2%
LOGRO3	VERIFICAR	15%	0,0%
	ACTUAR	15%	2,5%
	TOTAL	100%	13,0%

Fuente: Elaboración propia

5.2. Definición del contexto de la gestión de riesgos de seguridad de la información

Este paso fue explicado en el numeral 4.2 del capítulo anterior. Las autoridades del ITS Sucre autorizaron que la Implementación de la Metodología de Gestión de Riesgos de Seguridad de Información se realice sobre los Procesos que maneja la Unidad de Titulación del ITS Sucre**,** tanto en el Campus Norte como en el Campus Sur. Como evidencia se cuenta con los certificados correspondientes emitidos por las autoridades del plantel, que se presentan en el Apéndice C.

5.3. Proceso de evaluación de riesgos

En este proceso se detalla paso a paso el proceso de implementación de análisis y evaluación de riesgos que parte desde el levantamiento de inventario de activos, sigue con la determinación y valoración de factores de criticidad, continúa con la identificación de escenarios de riesgos asociados, su probabilidad de ocurrencia e impacto, efectúa el cálculo de vulnerabilidad inherente, para luego de identificar controles existentes y calcular la vulnerabilidad remanente o residual, reconocer aquellos riesgos que precisan atención urgente por parte de las autoridades de la institución.

5.3.1. Inventario de activos

La Tabla 31 presenta el inventario de activos de información Unidad de Titulación del ITSS.

Tabla 31: Inventario de activos de información de la Unidad de Titulación del ITSS

N° activo	Tipo de activo	Descripción	Observaciones
1	Físico	Anaquel	Almacenamiento bibliográfico de las tesis de grado físicas y digitales de los graduados del ITSS
2	Físico	Archivador	Almacenamiento de las carpetas de estudiantes
14	Físico	Carpetas de estudiantes	Expedientes con información académica de los estudiantes desde su ingreso hasta su egreso (copias de cédula y papeleta, ficha de actualización de datos, matrículas, solicitudes, registro de materias
16	Físico	Vicerrectorado Sede Sur	Lugar de la Sede Sur donde se almacenan los anaqueles conteniendo las tesis de grado físicas y digitales (CDs) de los tecnólogos graduados en el ITSS
17	Físico	Sala de lectura Sede Sur	Lugar de la Sede Sur donde se ubican los archivadores con la documentación completa de los graduados
18	Físico	Unidad de Bienestar Estudiantil Norte	Lugar de la Sede Norte donde se almacenan físicamente y gestionan bibliográficamente las tesis de grado previo su envío a la sede sur para archivo
19	Físico	Coordinación de Carrera	Lugar donde se almacenan temporalmente las tesis, borradores y empastados, de grado de los graduados en el ITSS, así como también los CDs con los archivos digitales de las mismas
15	Físico	Secretaría Sede Sur	Lugar en el cual se llevan a cabo las actividades de gestión del proceso de Titulación y gestión de Tesis así como emisión de Títulos

9	Humano	Secretaria	Persona responsable de elaboración de promedios, emisión de actas consolidadas de titulación, codificación de trabajos de titulación (tesis) físicos y digitales y archivo en vicerrectorado y su gestión y custodia, emisión de títulos, archivo de actas y documentos de respaldo en archivo en sala de lectura.
10	Humano	Guardia de seguridad	Control de ingreso/salida física y vehicular de personas a/de la institución. Custodia de bienes
11	Humano	Coordinador de Titulación	Persona responsable de vigilar el cumplimiento y coordinar el proceso de titulación conjuntamente con los coordinadores de carrera del ITSS
12	Humano	Coordinador de Carrera	Persona responsable de dirigir el proceso de titulación en cada carrera tanto en la modalidad de trabajo teórico como examen complexivo. Responsable de la gestión de documentos físicos y digitales hasta su almacenamiento en la sede Sur. Responsable de coordinar la elaboración y toma de exámenes complexivos. Coordina con Titulación y Secretaría
13	Humano	Estudiante de sexto semestre	Persona que accede al proceso de titulación vía Ficha Técnica de dos maneras: vía examen complexivo o vía elaboración de trabajo teórico (tesis de grado)
20	Lógico	Sistema Operativo	Software base del equipo de Secretaría para el procesamiento de información
21	Lógico	Hoja de cálculo	Software aplicativo del equipo de Secretaría utilizado para gestión documental y búsquedas de Tesis
23	Lógico	Elaboración de cronograma de Titulación	Elaboración de cronograma de titulación por parte de la comisión encargada y su difusión entre coordinadores de carrera, docentes y estudiantes
22	Lógico	Antivirus	Software para protección contra aplicaciones peligrosas
24	Proceso	Emisión de Información Académica	Emisión de récord académico con notas para ser utilizada en el proceso de elaboración de promedios desde Coordinación de Carrera hasta Secretaría con el apoyo de Titulación
25	Proceso	Elaboración de la Ficha Técnica	Documento a llenarse en sexto semestre con asesoría del docente de la materia de Asesoría de Titulación donde se especifica la forma de titulación por la que opta el estudiante: tesis o examen complexivo
26	Proceso	Elaboración y aplicación del examen complexivo	Creación de reactivos para la toma de examen complexivo, recepción de dicho examen. Responsable coordinación de carrera
27	Proceso	Emisión de informe de aprobados de examen complexivo	Elaboración de listado de estudiantes aprobados bajo la modalidad de examen complexivo de coordinación de carrera a secretaría y titulación. Envío de calificaciones finales del proceso
28	Proceso	Defensa de tema de investigación de trabajo teórico (tesis)	Creación y cruce de información de tema, tutor y tribunales para defensas de tema de investigación
29	Proceso	Emisión de listado de estudiantes aprobados el tema	Emisión de listado de estudiantes cuyo tema de investigación ha sido aprobado desde Coordinación de Carrera a Secretaría para la emisión de oficios nombrando tutores y miembros de tribunal
30	Proceso	Gestión de elaboración de trabajos teóricos (tesis)	Proceso a cargo de coordinación de carrera: nombre de tutores y tribunal, cambios de tema, cambios de tutor, nombramiento de lectores de tesis, elaboración de informes de cumplimiento de capítulos
31	Proceso	Emisión de informe de aprobados en las defensas de tesis	Elaboración de listado de estudiantes aprobados bajo la modalidad de trabajo teórico (tesis) desde coordinación de carrera a secretaría y titulación. Envío de calificaciones finales del proceso
32	Proceso	Elaboración de promedios finales/ actas consolidadas de titulación	Proceso a cargo de secretaría sede sur donde se elaboran promedios finales de titulación y se emiten las actas consolidadas de titulación para el evento de graduación
33	Proceso	Emisión de títulos de tecnólogo	Proceso a cargo de secretaría sede sur

3	Tecnológico	Computador de secretaría	Gestión bibliográfica de tesis en formato físico y digital, emisión de certificados académicos
4	Tecnológico	Impresora	Impresión de etiquetas de ordenamiento bibliográfico de las tesis, títulos de Tecnólogos, informes de estudiantes, constancias
5	Tecnológico	Regulador de voltaje	Protección de equipos utilizados para procesar información académica
6	Tecnológico	TAG de control de acceso	Dispositivo de lectura de tarjetas magnéticas de acceso a instalaciones, ingreso de códigos de acceso y emisión de alertas, en la Sede Sur
7	Tecnológico	Teléfono	Utilizado para atención al público, especialmente estudiantes, docentes y autoridades
8	Tecnológico	Tarjeta magnética	Dispositivo que permite acceder a instalaciones: aulas y oficinas en la Sede Sur

Fuente: *Elaboración propia basada en* (Benavides Sepúlveda & Blandón Jaramillo, 2017)

5.3.2. Determinación de los factores de criticidad de los activos

Este paso implica el desarrollo de un componente teórico, el cual está explicado e ilustrado en el numeral 4.3.2

5.3.3. Valoración de los factores de criticidad de los activos

Este paso se aplica la fórmula explicada en el numeral 4.3.3 a cada uno de los activos de información detectados en la Unidad de Titulación, lo cual se presenta en la Tabla 32.

Tabla 32: Valoración de Criticidad de los Activos de Información de la Unidad de Titulación del ITSS

N° activo	Descripción del activo	Tipo de Activo	Valoración de la de criticidad de los activos									Criticidad
			Confidencialidad			Integridad			Disponibilidad			
			Financ.	Legal	Imagen	Financ.	Legal	Imagen	Financ.	Legal	Imagen	
1	Anaquel	Físico	1	1	1	1	1	1	1	1	1	100%
2	Archivador	Físico	1	1	1	1	1	1	1	1	1	100%
14	Carpetas de estudiantes	Físico	1	1	1	1	1	1	1	1	1	100%
16	Vicerrectorado Sede Sur	Físico	1	1	1	1	1	1	1	1	1	100%
17	Sala de lectura Sede Sur	Físico	1	1	1	1	1	1	1	1	1	100%
18	Unidad de Bienestar Estudiantil Norte	Físico	1	1	1	1	1	1	1	1	1	100%
19	Coordinación de Carrera	Físico	1	1	1	0	1	1	0	1	1	78%
15	Secretaría Sede Sur	Físico	1	1	1	1	1	1	1	1	1	100%

N° activo	Descripción del activo	Tipo de Activo	Valoración de la de criticidad de los activos									Criticidad
			Confidencialidad			Integridad			Disponibilidad			
			Financ.	Legal	Imagen	Financ.	Legal	Imagen	Financ.	Legal	Imagen	
9	Secretaria	Humano	1	1	1	1	1	1	1	1	1	100%
10	Guardia de seguridad	Humano	1	1	1	1	1	0	1	1	1	89%
11	Coordinador de Titulación	Humano	1	1	1	1	1	1	1	1	1	100%
12	Coordinador de Carrera	Humano	1	1	1	1	1	1	1	1	1	100%
13	Estudiante de sexto semestre	Humano	0	1	0	0	0	0	0	1	0	22%
20	Sistema Operativo	Lógico	0	0	1	1	0	1	0	0	1	44%
21	Hoja de cálculo	Lógico	1	1	1	1	1	1	1	1	1	100%
23	Elaboración de cronograma de Titulación	Lógico	1	1	1	1	1	1	1	1	1	100%
22	Antivirus	Lógico	0	0	1	0	1	1	0	1	1	56%
24	Emisión de Información Académica	Proceso	0	1	0	0	1	0	0	1	1	44%
25	Elaboración de la Ficha Técnica	Proceso	0	1	1	0	1	1	0	1	1	67%
26	Elaboración y aplicación del examen complexivo	Proceso	1	1	1	1	1	1	1	1	1	100%
27	Emisión de informe de aprobados de examen complexivo	Proceso	1	1	1	1	1	1	0	1	1	89%
28	Defensa de tema de investigación de trabajo teórico (tesis)	Proceso	1	1	1	0	1	0	0	1	0	56%
29	Emisión de listado de estudiantes aprobados el tema	Proceso	1	1	1	1	1	1	1	1	1	100%
30	Gestión de elaboración de trabajos teóricos (tesis)	Proceso	1	1	1	1	1	1	1	1	1	100%
31	Emisión de informe de aprobados en las defensas de tesis	Proceso	1	1	1	1	1	1	1	1	1	100%
32	Elaboración de promedios finales/ actas consolidadas de titulación	Proceso	1	1	1	1	1	1	1	1	1	100%
33	Emisión de títulos de tecnólogo	Proceso	1	1	1	1	1	1	1	1	1	100%

N° activo	Descripción del activo	Tipo de Activo	Valoración de la de criticidad de los activos									Criticidad
			Confidencialidad			Integridad			Disponibilidad			
			Financ.	Legal	Imagen	Financ.	Legal	Imagen	Financ.	Legal	Imagen	
3	Computador de secretaría	Tecnológico	0	1	1	0	0	0	0	1	1	44%
4	Impresora	Tecnológico	0	0	1	0	0	1	1	0	1	44%
5	Regulador de voltaje	Tecnológico	0	0	1	0	0	1	0	0	1	33%
6	TAG de control de acceso	Tecnológico	1	1	1	1	1	1	1	1	1	100%
7	Teléfono	Tecnológico	0	0	1	0	0	1	1	0	1	44%
8	Tarjeta magnética	Tecnológico	1	1	1	0	0	0	1	1	1	67%

Fuente: Elaboración propia

5.3.4. Identificación de riesgos asociados a los activos de información

El siguiente paso tiene que ver con el levantamiento del inventario de escenarios de riesgo relativo a los activos de información tal como se mencionó en el numeral 4.3.4 del capítulo anterior. Dichos riesgos fueron determinados después de sostener una reunión con el personal de la Unidad de Titulación del ITSS. Lo mencionado se presenta estructurado en la Tabla 33.

Tabla 33: Escenarios de riesgo de información de la Unidad de Titulación ITSS

N°	Riesgo	Origen
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	I
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	I
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	I
4	Afectación legal por pérdida de anillados o empastados de las tesis	A, I
5	Afectación legal por pérdida de actas consolidadas de titulación	I

N°	Riesgo	Origen
6	Afectación legal por pérdida de bancos de preguntas de los exámenes complexivos	A, I
7	Afectación legal por acceso no autorizado a cuentas de docentes del sistema SAO-P	A, I
8	Acceso a información confidencial de los estudiantes empleando contraseñas débiles generadas por default al momento de matricular a estudiantes	A, I
9	Afectación legal por alteración de calificaciones de estudiantes en el sistema SAO-P por acceso no autorizado a cuentas de docentes	A, I
10	Alteración de información de estudiantes o docentes en el sistema SAO-P por acceso no autorizado a cuentas de administrador	A, I
11	Acceso no autorizado al área de secretaría académica sede Sur por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A, I
12	Acceso no autorizado a las área de coordinación de carrera por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A, I
13	Acceso no autorizado a los anaqueles en vicerrectorado (sede sur) por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo	A, I
14	Acceso no autorizado a anaqueles de la sala de lectura (sede sur) por daño en candados o falta de mecanismos de control de acceso físico a estudiantes fuera del horario de clases	A, I
15	Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A, I
16	Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A, I
17	Acceso no autorizado a información de calificaciones de defensas de tesis/temas de tesis por ausencia de políticas de manejo confidencial de registro académico	A, I
18	Acceso no autorizado a exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	A, I
19	Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	A, I
20	Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico	A, I
21	Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur	A, I
22	Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	A, I
23	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	I
24	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	I
25	Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo	A
26	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por falta de mantenimiento preventivo programado	A
27	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	A

N°	Riesgo	Origen
28	Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	A
29	Demora en la atención de usuarios por demoras en el proceso de ingreso de calificaciones de exámenes complexivos o de los trabajos teóricos (tesis)	A
30	Desatención de los equipos de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios destinados a atención al público por parte de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte	A
31	Entrega de papel membretado institucional a personal no autorizado por parte de Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte	A
32	Fallos o demoras en atención al público por afectación de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte	A,I
33	Afectación por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte a causa de uso inadecuado de los recurso por parte de personal a cargo	A,I
34	Afectación de las comunicaciones por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte que afecta los drivers de las respectivas tarjetas de red	A,I
35	Pérdida de carpetas físicas de estudiantes y egresados por ocurrencia de desastres naturales	N
36	Pérdida del equipo de cómputo e información digital por ocurrencia de desastres naturales	N
37	Pérdida de las comunicaciones para reportes a la Senescyt o entidades externas por daños en los sistemas de comunicación por ocurrencia de desastres naturales	N
38	Pérdida de información en el equipo de cómputo de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte por fallos del fluido eléctrico	A,N
39	Desactivación de los Tags de acceso magnético por fallos del fluido eléctrico	A, I, N
40	Retrasos en el proceso de generación de certificados académicos / actas consolidadas de titulación por fallos del fluido eléctrico	N
41	Daño en archivos físicos, tesis física o digital o equipos de cómputo e información digital por fuego provocado	I
42	Afectación física en el personal de la Unidad de Titulación por fuego provocado y ausencia de planes de contingencia y/o rutas adecuadas de evacuación	I
43	Deterioro de expedientes de estudiantes y egresados, así como tesis físicas debido a corrosión provocada por humedad	N
44	Incumplimiento en reportes de graduados a Senescyt y otros organismos de control por fallos en dispositivos que permiten acceso al servicio de Internet	A
45	Intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus	A,I
46	Divulgación de información académica de estudiantes en proceso de titulación por medio de prácticas inadecuadas de desecho de información	A,I
47	Divulgación de información de estudiantes en proceso de titulación por falta de políticas y mecanismos para la adecuada disposición de desechos	A,I
48	Fallos en el funcionamiento del equipo de cómputo de la Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte por instalación de software pirata, ocasionado por falta de políticas de gestión con proveedores y personal del ITSS	A, I
49	Exposición de las contraseñas de acceso a instalaciones y a equipos de cómputo y sistemas operativos por falta de medidas de prevención, uso adecuado y preservación de las mismas	A,I
50	Demoras en el restablecimiento de servicios de consulta o gestión de procesos de titulación por fallos relacionados a extracción/restablecimiento de copias de seguridad	A,I

Fuente: Elaboración propia basada en ISO 27005 (Instituto Ecuatoriano de Normalización, 2012)

5.3.5. Asignación de valor de probabilidad de riesgo

Esta actividad implica el desarrollo de un componente de tipo teórico cubierto en el numeral 4.3.5.

5.3.6. Valoración del impacto potencial

Esta actividad implica el desarrollo de un componente de tipo teórico cubierto en el numeral 4.3.6.

5.3.7. Cálculo de la vulnerabilidad inherente

La base teórica y fórmulas que corresponden a esta fase fueron abordadas en el numeral 4.3.7. A continuación se presentan los resultados del cálculo de vulnerabilidad inherente en la Tabla 34.

Tabla 34: Matriz de Cálculo de Vulnerabilidad Inherente de los Activos de Información de la Unidad de Titulación del ITSS

N°	Escenario de riesgo		Impacto				Vulnerabilidad inherente			
		P	Ic	Ii	Id	Itotal	VIc	VIi	VId	VIt
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	1	3	3	3	9	33%	33%	33%	33%
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	1	3	3	3	9	33%	33%	33%	33%
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	1	3	3	3	9	33%	33%	33%	33%
4	Afectación legal por pérdida de anillados o empastados de las tesis	2	3	3	3	9	67%	67%	67%	67%
5	Afectación legal por pérdida de actas consolidadas de titulación	1	3	3	3	9	33%	33%	33%	33%
6	Afectación legal por pérdida de bancos de preguntas de los exámenes complexivos	1	3	3	3	9	33%	33%	33%	33%
7	Afectación legal por acceso no autorizado a cuentas de docentes del sistema SAO-P	2	3	3	3	9	67%	67%	67%	67%
8	Acceso a información confidencial de los estudiantes empleando contraseñas débiles generadas por default al momento de matricular a estudiantes	1	1	1	1	3	11%	11%	11%	11%
9	Afectación legal por alteración de calificaciones de estudiantes en el sistema SAO-P por acceso no autorizado a cuentas de docentes	1	3	3	3	9	33%	33%	33%	33%
10	Alteración de información de estudiantes o docentes en el sistema SAO-P por acceso no autorizado a cuentas de administrador	2	3	3	3	9	67%	67%	67%	67%
11	Acceso no autorizado al área de secretaría académica sede Sur por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	3	3	3	3	9	100%	100%	100%	100%
12	Acceso no autorizado a las área de coordinación de carrera por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	3	3	3	3	9	100%	100%	100%	100%
13	Acceso no autorizado a los anaqueles en vicerrectorado (sede sur) por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo	2	3	3	3	9	67%	67%	67%	67%
14	Acceso no autorizado a anaqueles de la sala de lectura (sede sur) por daño en candados o falta de mecanismos de control de acceso físico a estudiantes fuera del horario de clases	3	3	3	3	9	100%	100%	100%	100%

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad inherente			
			Ic	Ii	Id	Itotal	VIc	VIi	VId	VIt
15	Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	3	3	3	3	9	100%	100%	100%	100%
16	Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	2	3	3	3	9	67%	67%	67%	67%
17	Acceso no autorizado a información de calificaciones de defensas de tesis/temas de tesis por ausencia de políticas de manejo confidencial de registro académico	1	2	2	2	6	22%	22%	22%	22%
18	Acceso no autorizado a exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	1	2	2	2	6	22%	22%	22%	22%
19	Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	2	1	1	1	3	22%	22%	22%	22%
20	Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico	2	1	1	1	3	22%	22%	22%	22%
21	Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur	1	3	3	3	9	33%	33%	33%	33%
22	Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	1	3	3	3	9	33%	33%	33%	33%
23	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	3	2	2	2	6	67%	67%	67%	67%
24	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	3	2	2	2	6	67%	67%	67%	67%
25	Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo	2	1	1	1	3	22%	22%	22%	22%
26	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por falta de mantenimiento preventivo programado	2	1	1	1	3	22%	22%	22%	22%
27	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	2	1	1	1	3	22%	22%	22%	22%
28	Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	3	2	2	2	6	67%	67%	67%	67%
29	Demora en la atención de usuarios por demoras en el proceso de ingreso de calificaciones de exámenes complexivos o de los trabajos teóricos (tesis)	2	1	1	1	3	22%	22%	22%	22%
30	Desatención de los equipos de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios destinados a atención al público por parte de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte	3	1	1	1	3	33%	33%	33%	33%
31	Entrega de papel membretado institucional a personal no autorizado por parte de Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte	1	3	3	3	9	33%	33%	33%	33%
32	Fallos o demoras en atención al público por afectación de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte	2	1	1	1	3	22%	22%	22%	22%
33	Afectación por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte a causa de uso inadecuado de los recurso por parte de personal a cargo	2	1	1	1	3	22%	22%	22%	22%

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad inherente			
			Ic	Ii	Id	Itotal	VIc	VIi	VId	VIt
34	Afectación de las comunicaciones por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte que afecta los drivers de las respectivas tarjetas de red	2	1	1	1	3	22%	22%	22%	22%
35	Pérdida de carpetas físicas de estudiantes y egresados por ocurrencia de desastres naturales	1	3	3	3	9	33%	33%	33%	33%
36	Pérdida del equipo de cómputo e información digital por ocurrencia de desastres naturales	1	2	2	2	6	22%	22%	22%	22%
37	Pérdida de las comunicaciones para reportes a la Senescyt o entidades externas por daños en los sistemas de comunicación por ocurrencia de desastres naturales	1	1	1	1	3	11%	11%	11%	11%
38	Pérdida de información en el equipo de cómputo de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte por fallos del fluido eléctrico	3	1	1	1	3	33%	33%	33%	33%
39	Desactivación de los Tags de acceso magnético por fallos del fluido eléctrico	2	3	3	3	9	67%	67%	67%	67%
40	Retrasos en el proceso de generación de certificados académicos / actas consolidadas de titulación por fallos del fluido eléctrico	2	2	2	2	6	44%	44%	44%	44%
41	Daño en archivos físicos, tesis física o digital o equipos de cómputo e información digital por fuego provocado	1	3	3	3	9	33%	33%	33%	33%
42	Afectación física en el personal de la Unidad de Titulación por fuego provocado y ausencia de planes de contingencia y/o rutas adecuadas de evacuación	1	3	3	3	9	33%	33%	33%	33%
43	Deterioro de expedientes de estudiantes y egresados, así como tesis físicas debido a corrosión provocada por humedad	2	2	2	2	6	44%	44%	44%	44%
44	Incumplimiento en reportes de graduados a Senescyt y otros organismos de control por fallos en dispositivos que permiten acceso al servicio de Internet	2	1	1	1	3	22%	22%	22%	22%
45	Intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus	1	2	2	2	6	22%	22%	22%	22%
46	Divulgación de información académica de estudiantes en proceso de titulación por medio de prácticas inadecuadas de desecho de información	2	2	2	2	6	44%	44%	44%	44%
47	Divulgación de información de estudiantes en proceso de titulación por falta de políticas y mecanismos para la adecuada disposición de desechos	2	2	2	2	6	44%	44%	44%	44%
48	Fallos en el funcionamiento del equipo de cómputo de la Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte por instalación de software pirata, ocasionado por falta de políticas de gestión con proveedores y personal del ITSS	3	1	1	1	3	33%	33%	33%	33%
49	Exposición de las contraseñas de acceso a instalaciones y a equipos de cómputo y sistemas operativos por falta de medidas de prevención, uso adecuado y preservación de las mismas	3	3	3	3	9	100%	100%	100%	100%
50	Demoras en el restablecimiento de servicios de consulta o gestión de procesos de titulación por fallos relacionados a extracción/restablecimiento de copias de seguridad	2	2	2	2	6	44%	44%	44%	44%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

5.3.8. Establecimiento de criterios de aceptación de riesgo

Este paso implica el desarrollo de un componente de tipo teórico, el cual ha sido cubierto en el numeral 4.3.8 donde se indica que los riesgos se clasifican por su vulnerabilidad en inaceptables, tolerables y aceptables donde a los primeros se los presenta con color rojo, a los segundos con amarillo y a los terceros con verde.

5.3.9. Creación de mapas de temperatura de vulnerabilidad inherente

En este paso se presentan los mapas de temperatura de vulnerabilidad inherente para la confidencialidad de la información, para la integridad y para la disponibilidad, así como también se muestra la matriz de vulnerabilidad inherente consolidada total. El procedimiento seguido para su elaboración fue abordado en el numeral 4.3.9.

En la tabla 35 se presenta la matriz de clasificación inherente correspondiente a la confidencialidad de la información; en la 36, la que corresponde a la integridad; en la 37, aquella que corresponde a la disponibilidad; para finalmente, en la tabla 38 presentar la matriz de vulnerabilidad inherente total.

Tabla 35: Matriz de vulnerabilidad inherente para confidencialidad de la información en la Unidad de Titulación del ITSS

CONFIDENCIALIDAD				
PROBABILIDAD	3	30,38,48	23,24,28	11,12,14,15,49
	2	19,20,25,26,27, 29,32,33,34,44	40,43,46,47,50	4,7,10,13,16,39
	1	8,37	17,18,36,45	1,2,3,5,6,9,21,2 2,31,35,41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La tabla anterior arroja el primer resultado: se logra detectar que los riesgos con calificación de vulnerabilidad inaceptable para la confidencialidad de la información son : el número 11, acceso no autorizado a secretaría académica sur por falta de mecanismos de control de acceso físico o falta de control en la atención al público; 12, acceso no autorizado a las áreas de coordinación de carrera, por las mismas falencias que aquejan al riesgo 11; accesos no autorizados a áreas de anaqueles en la sala de lectura en la sede sur y en la Unidad de Bienestar Estudiantil sede norte -riesgos 14 y 15,

respectivamente-; y el riesgo número 49, relativo a la exposición de contraseñas de acceso a instalaciones y equipos de cómputo por falta de medidas de prevención. Son estos riesgos los que precisan de atención prioritaria en las estrategias de aseguramiento de la confidencialidad de la información.

Tabla 36: Matriz de vulnerabilidad inherente para integridad de la información en la Unidad de Titulación del ITSS

INTEGRIDAD				
PROBABILIDAD	3	30,38,48	23,24,28	11,12,14,15,49
	2	19,20,25,26,27, 29,32,33,34,44	40,43,46,47,50	4,7,10,13,16, 39
	1	8,37	17,18,36,45	1, 2,3,5, 6, 9,21,22,31,35,4 1,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La Tabla 36 evidencia que los riesgos cuya sensibilidad es máxima y catalogado como inaceptable también lo son para la integridad de la información y deberán priorizarse en una estrategia de tratamiento de riesgo.

Tabla 37: Matriz de vulnerabilidad inherente para disponibilidad de la información en la Unidad de Titulación ITSS

DISPONIBILIDAD				
PROBABILIDAD	3	30,38,48	23,24,28,	11,12,14,15,49
	2	19,20,25,26,27, 29,32,33,34,44	40,43,46,47,50	4,7, 10,13,16,39
	1	8,37,	17,18,36,45	1,2,3,5,6,9,21,22 ,31,35,41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Al igual que en las dos tablas anteriores los riesgos que representan los puntos más débiles de seguridad también lo son para la disponibilidad de la información.

Tabla 38: Matriz consolidada de vulnerabilidad inherente de la información de la Unidad de Titulación ITSS

VULNERABILIDAD INHERENTE										
PROBABILIDAD	3			30,38,48			23,24,28			11,12,14,15,49
	2			19,20,25,26,27,29,32,33,34,44			40,43,46,47,50			4,7,10,13,16,39
	1			8,37			17,18,36,45			1,2,3,5,6,9,21,22,31,35,41,42
		1	2	3	4	5	6	7	8	9
		IMPACTO								

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Como resultado de evaluación preliminar se puede afirmar, luego de observar los resultados presentados en las cuatro matrices anteriores, que es prioritario para la Unidad de Titulación el aseguramiento del Control de Acceso Físico a los siguientes lugares: Secretaría Académica de la Sede Sur, Coordinaciones de Carrera Sur y Norte, Sala de Lectura Sur y Unidad de Bienestar Estudiantil Norte, así como, también es de suma importancia establecer estrategias de atención al público más seguras. Adicionalmente la matriz consolidada de vulnerabilidad inherente presenta que el riesgo de

exposición de las contraseñas de acceso a instalaciones y equipos es otro escenario de riesgo por asegurar, que requiere la máxima atención de las autoridades.

5.3.10. Identificación de controles existentes

El siguiente paso de esta metodología tiene que ver con la identificación de Controles de Seguridad de la Información existentes en la Unidad de Titulación del ITSS, como se presentó en el numeral 4.3.10 cuyos resultados presentan en la tabla 39.

Tabla 39: Controles de Seguridad de la Información existentes en la Unidad de Titulación ITSS

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur, Bienestar Estudiantil Norte y computadores de coordinadores de carrera
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
4	Afectación legal por pérdida de anillados o empastados de las tesis	A.11.1.1	1. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.2	2. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
5	Afectación legal por pérdida de actas consolidadas de titulación	A.11.1.1	1. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.2	2. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
6	Afectación legal por pérdida de bancos de preguntas de los exámenes complexivos	A.11.1.2 A.11.1.3	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.5.1.1 A.9.4.3	3. Protección con contraseñas de los equipos de secretaría sede sur, Bienestar Estudiantil Norte y computadores de coordinadores de carrera
7	Afectación legal por acceso no autorizado a cuentas de docentes del sistema SAO-P	A.9.4.3	1. El acceso al sistema de notas del ITSS SAO-P está protegido por contraseña, misma que es gestionada por el usuario
8	Acceso a información confidencial de los estudiantes empleando contraseñas débiles generadas por default al momento de matricular a estudiantes	A.9.4.3	1. El acceso al sistema de notas del ITSS SAO-P está protegido por contraseña, misma que es gestionada por el usuario
9	Afectación legal por alteración de calificaciones de estudiantes en el sistema SAO-P por acceso no autorizado a cuentas de docentes	A.9.4.3	1. El acceso al sistema de notas del ITSS SAO-P está protegido por contraseña, misma que es gestionada por el usuario
10	Alteración de información de estudiantes o docentes en el sistema SAO-P por acceso no autorizado a cuentas de administrador	A.9.4.3	1. El acceso al sistema de notas del ITSS SAO-P está protegido por contraseña, misma que es gestionada por el usuario
11	Acceso no autorizado al área de secretaría académica sede Sur por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
12	Acceso no autorizado a las área de coordinación de carrera por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
13	Acceso no autorizado a los anaqueles en vicerrectorado (sede sur) por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
14	Acceso no autorizado a anaqueles de la sala de lectura (sede sur) por daño en candados o falta de mecanismos de control de acceso físico a estudiantes fuera del horario de clases	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
15	Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
16	Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas protegidas con rejas para prevenir accesos físicos no autorizados
17	Acceso no autorizado a información de calificaciones de defensas de tesis/temas de tesis por ausencia de políticas de manejo confidencial de registro académico	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur y computadores de coordinadores de carrera
18	Acceso no autorizado a exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur y computadores de coordinadores de carrera
19	Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur y computadores de coordinadores de carrera

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
21	Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de computador de secretaría sede sur
22	Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.7.3.1	4. Las responsabilidades de seguridad de la información están especificadas en el acuerdo de confidencialidad firmado al inicio de labores del funcionario, mismo que sigue vigente hasta dos años después de dada por finalizada la vinculación
23	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
24	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
25	Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo	A.12.1.1 A.12.1.2	1. Los procesos del sistema de gestión de calificaciones SAO-P y repositorio físico están documentados. El control de cambios se cumple por disposiciones de rectorado
26	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por falta de mantenimiento preventivo programado	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A11.2.4	2. Los equipos de cómputo cuentan con mantenimiento preventivo coordinado por la unidad de TIC
27	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A11.2.4	2. Reportes respecto al desempeño de los equipos de cómputo son enviados vía correo electrónico institucional a personal de TIC en ambas sedes
		A12.1.2	3. Se controlan los cambios en sistemas de procesamiento de información a través de disposiciones de rectorado

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
20	Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de los equipos de secretaría sede sur y computadores de coordinadores de carrera
21	Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.5.1.1 A.9.4.3	4. Protección con contraseñas de computador de secretaría sede sur
22	Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
		A.7.3.1	4. Las responsabilidades de seguridad de la información están especificadas en el acuerdo de confidencialidad firmado al inicio de labores del funcionario, mismo que sigue vigente hasta dos años después de dada por finalizada la vinculación
23	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
24	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A.11.1.1	2. Control de acceso perimetral a mediante muros y cerramientos
		A.11.1.3	3. Ventanas y puertas protegidas con rejas para prevenir accesos físicos no autorizados
25	Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo	A.12.1.1 A.12.1.2	1. Los procesos del sistema de gestión de calificaciones SAO-P y repositorio físico están documentados. El control de cambios se cumple por disposiciones de rectorado

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
26	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por falta de mantenimiento preventivo programado	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A11.2.4	2. Los equipos de cómputo cuentan con mantenimiento preventivo coordinado por la unidad de TIC
27	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	A.11.1.2	1. Control de acceso de particulares mediante guardias de seguridad y tags de acceso magnético
		A11.2.4	2. Reportes respecto al desempeño de los equipos de cómputo son enviados vía correo electrónico institucional a personal de TIC en ambas sedes
		A12.1.2	3. Se controlan los cambios en sistemas de procesamiento de información a través de disposiciones de rectorado
28	Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	A.15.2.2	1. TIC gestiona con el proveedor cambios en el suministro de servicios
29	Demora en la atención de usuarios por demoras en el proceso de ingreso de calificaciones de exámenes complexivos o de los trabajos teóricos (tesis)	A.15.2.2	1. TIC gestiona con el proveedor cambios en el suministro de servicios
30	Desatención de los equipos de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios destinados a atención al público por parte de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte		
31	Entrega de papel membretado institucional a personal no autorizado por parte de Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte		
32	Fallos o demoras en atención al público por afectación de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte		
33	Afectación por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte a causa de uso inadecuado de los recurso por parte de personal a cargo	A.12.2.1	1. Los equipos cuentan con programas antivirus sin licencia
34	Afectación de las comunicaciones por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte que afecta los drivers de las respectivas tarjetas de red	A.12.2.1	1. Los equipos cuentan con programas antivirus sin licencia

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
35	Pérdida de carpetas físicas de estudiantes y egresados por ocurrencia de desastres naturales		
36	Pérdida del equipo de cómputo e información digital por ocurrencia de desastres naturales		
37	Pérdida de las comunicaciones para reportes a la Senescyt o entidades externas por daños en los sistemas de comunicación por ocurrencia de desastres naturales		
38	Pérdida de información en el equipo de cómputo de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte por fallos del fluido eléctrico		
39	Desactivación de los Tags de acceso magnético por fallos del fluido eléctrico		
40	Retrasos en el proceso de generación de certificados académicos / actas consolidadas de titulación por fallos del fluido eléctrico		
41	Daño en archivos físicos, tesis física o digital o equipos de cómputo e información digital por fuego provocado		
42	Afectación física en el personal de la Unidad de Titulación por fuego provocado y ausencia de planes de contingencia y/o rutas adecuadas de evacuación		
43	Deterioro de expedientes de estudiantes y egresados, así como tesis físicas debido a corrosión provocada por humedad		
44	Incumplimiento en reportes de graduados a Senescyt y otros organismos de control por fallos en dispositivos que permiten acceso al servicio de Internet		
45	Intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus	A.12.2.1	1. Parcialmente. Los equipos cuentan con programas antivirus sin licencia
46	Divulgación de información académica de estudiantes en proceso de titulación por medio de prácticas inadecuadas de desecho de información		
47	Divulgación de información de estudiantes en proceso de titulación por falta de políticas y mecanismos para la adecuada disposición de desechos		

N° riesgo	Escenario de riesgo	Código ISO 27002 del control	Control Actual
48	Fallos en el funcionamiento del equipo de cómputo de la Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte por instalación de software pirata, ocasionado por falta de políticas de gestión con proveedores y personal del ITSS		
49	Exposición de las contraseñas de acceso a instalaciones y a equipos de cómputo y sistemas operativos por falta de medidas de prevención, uso adecuado y preservación de las mismas	A.9.4.3	1. Está gestionado para accesos a correo electrónico institucional, acceso a SAO-P por el proveedor
50	Demoras en el restablecimiento de servicios de consulta o gestión de procesos de titulación por fallos relacionados a extracción/restablecimiento de copias de seguridad		

Fuente: Elaboración propia

5.3.11. Cálculo de la vulnerabilidad residual

La base teórica y fórmulas que corresponden a esta actividad fueron abordadas en el numeral 4.3.11. A continuación se presentan los resultados en la Tabla 40.

Tabla 40: Matriz de Cálculo de Vulnerabilidad Residual en la Unidad de Titulación ITSS

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad residual			
			IRc	IRi	IRd	IRtotal	VRc	VRi	VRd	VRt
1	Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes	1	3	3	3	9	33%	33%	33%	33%
2	Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación	1	3	3	3	9	33%	33%	33%	33%
3	Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis	1	3	3	3	9	33%	33%	33%	33%
4	Afectación legal por pérdida de anillados o empastados de las tesis	2	3	2	1	6	67%	44%	22%	44%
5	Afectación legal por pérdida de actas consolidadas de titulación	1	3	1	1	5	33%	11%	11%	19%
6	Afectación legal por pérdida de bancos de preguntas de los exámenes complexivos	1	3	3	3	9	33%	33%	33%	33%
7	Afectación legal por acceso no autorizado a cuentas de docentes del sistema SAO-P	1	3	3	2	8	33%	33%	22%	30%
8	Acceso a información confidencial de los estudiantes empleando contraseñas débiles generadas por default al momento de matricular a estudiantes	1	1	1	1	3	11%	11%	11%	11%
9	Afectación legal por alteración de calificaciones de estudiantes en el sistema SAO-P por acceso no autorizado a cuentas de docentes	1	3	3	3	9	33%	33%	33%	33%
10	Alteración de información de estudiantes o docentes en el sistema SAO-P por acceso no autorizado a cuentas de administrador	1	1	1	1	3	11%	11%	11%	11%
11	Acceso no autorizado al área de secretaría académica sede Sur por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	3	3	2	2	7	100%	67%	67%	78%
12	Acceso no autorizado a las área de coordinación de carrera por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	3	3	2	2	7	100%	67%	67%	78%
13	Acceso no autorizado a los anaqueles en vicerrectorado (sede sur) por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo	1	3	3	3	9	33%	33%	33%	33%
14	Acceso no autorizado a anaqueles de la sala de lectura (sede sur) por daño en candados o falta de mecanismos de control de acceso físico a estudiantes fuera del horario de clases	2	3	3	3	9	67%	67%	67%	67%
15	Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	2	1	1	1	3	22%	22%	22%	22%

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad residual			
			IRc	IRi	IRd	IRtotal	VRc	VRi	VRd	VRt
16	Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público	1	3	3	3	9	33%	33%	33%	33%
17	Acceso no autorizado a información de calificaciones de defensas de tesis/temas de tesis por ausencia de políticas de manejo confidencial de registro académico	1	2	2	2	6	22%	22%	22%	22%
18	Acceso no autorizado a exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	1	2	2	2	6	22%	22%	22%	22%
19	Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	1	1	1	1	3	11%	11%	11%	11%
20	Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico	1	1	1	1	3	11%	11%	11%	11%
21	Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur	1	3	3	3	9	33%	33%	33%	33%
22	Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	1	1	1	1	3	11%	11%	11%	11%
23	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	3	2	2	2	6	67%	67%	67%	67%
24	Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	3	2	2	2	6	67%	67%	67%	67%
25	Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo	2	1	1	1	3	22%	22%	22%	22%
26	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por falta de mantenimiento preventivo programado	2	1	1	1	3	22%	22%	22%	22%
27	Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	2	1	1	1	3	22%	22%	22%	22%
28	Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	3	1	1	1	3	33%	33%	33%	33%
29	Demora en la atención de usuarios por demoras en el proceso de ingreso de calificaciones de exámenes complexivos o de los trabajos teóricos (tesis)	2	1	1	1	3	22%	22%	22%	22%
30	Desatención de los equipos de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios destinados a atención al público por parte de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte	3	1	1	1	3	33%	33%	33%	33%
31	Entrega de papel membretado institucional a personal no autorizado por parte de Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte	1	3	3	3	9	33%	33%	33%	33%

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad residual			
			IRc	IRi	IRd	IRtotal	VRc	VRi	VRd	VRt
32	Fallos o demoras en atención al público por afectación de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte	2	1	1	1	3	22%	22%	22%	22%
33	Afectación por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte a causa de uso inadecuado de los recurso por parte de personal a cargo	2	1	1	1	3	22%	22%	22%	22%
34	Afectación de las comunicaciones por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte que afecta los drivers de las respectivas tarjetas de red	2	1	1	1	3	22%	22%	22%	22%
35	Pérdida de carpetas físicas de estudiantes y egresados por ocurrencia de desastres naturales	1	3	3	3	9	33%	33%	33%	33%
36	Pérdida del equipo de cómputo e información digital por ocurrencia de desastres naturales	1	2	2	2	6	22%	22%	22%	22%
37	Pérdida de las comunicaciones para reportes a la Senescyt o entidades externas por daños en los sistemas de comunicación por ocurrencia de desastres naturales	1	1	1	1	3	11%	11%	11%	11%
38	Pérdida de información en el equipo de cómputo de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte por fallos del fluido eléctrico	3	1	1	1	3	33%	33%	33%	33%
39	Desactivación de los Tags de acceso magnético por fallos del fluido eléctrico	2	3	3	3	9	67%	67%	67%	67%
40	Retrasos en el proceso de generación de certificados académicos / actas consolidadas de titulación por fallos del fluido eléctrico	2	2	2	2	6	44%	44%	44%	44%
41	Daño en archivos físicos, tesis física o digital o equipos de cómputo e información digital por fuego provocado	1	3	3	3	9	33%	33%	33%	33%
42	Afectación física en el personal de la Unidad de Titulación por fuego provocado y ausencia de planes de contingencia y/o rutas adecuadas de evacuación	1	3	3	3	9	33%	33%	33%	33%
43	Deterioro de expedientes de estudiantes y egresados, así como tesis físicas debido a corrosión provocada por humedad	2	2	2	2	6	44%	44%	44%	44%
44	Incumplimiento en reportes de graduados a Senescyt y otros organismos de control por fallos en dispositivos que permiten acceso al servicio de Internet	2	1	1	1	3	22%	22%	22%	22%
45	Intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus	1	2	2	2	6	22%	22%	22%	22%
46	Divulgación de información académica de estudiantes en proceso de titulación por medio de prácticas inadecuadas de desecho de información	2	2	2	2	6	44%	44%	44%	44%
47	Divulgación de información de estudiantes en proceso de titulación por falta de políticas y mecanismos para la adecuada disposición de desechos	2	2	2	2	6	44%	44%	44%	44%

N°	Escenario de riesgo	P	Impacto				Vulnerabilidad residual			
			IRc	IRi	IRd	IRtotal	VRc	VRi	VRd	VRt
48	Fallos en el funcionamiento del equipo de cómputo de la Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte por instalación de software pirata, ocasionado por falta de políticas de gestión con proveedores y personal del ITSS	3	1	1	1	3	33%	33%	33%	33%
49	Exposición de las contraseñas de acceso a instalaciones y a equipos de cómputo y sistemas operativos por falta de medidas de prevención, uso adecuado y preservación de las mismas	3	3	3	3	9	100%	100%	100%	100%
50	Demoras en el restablecimiento de servicios de consulta o gestión de procesos de titulación por fallos relacionados a extracción/restablecimiento de copias de seguridad	2	2	2	2	6	44%	44%	44%	44%

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

5.3.12. Creación de mapas de temperatura de vulnerabilidad residual

En este paso se elaboran las matrices de vulnerabilidad residual para la confidencialidad de la información, la integridad y la disponibilidad, así como la matriz de vulnerabilidad inherente consolidada total. La descripción del proceso así como las fórmulas utilizadas en su cálculo fueron presentadas en el numeral 4.3.12.

En la tabla 41 se presenta la matriz de clasificación residual que corresponde a la confidencialidad; en la 42, la que corresponde a integridad; en la 43, aquella que corresponde a la disponibilidad; para finalmente, en la tabla 44 reportar los valores de vulnerabilidad inherente total.

Tabla 41: Matriz de vulnerabilidad residual para la confidencialidad en la Unidad de Titulación ITSS

CONFIDENCIALIDAD				
PROBABILIDAD	3	28,30,38, 48	23,24	11, 12,49
	2	15,25,26,27,29,32 ,33,34,44	40,43,46,47, 50	4,14,39
	1	8,10, 19,20,22,37	17,18,36,45	1,2, 3,5,6,7,9,13,16, 21,31,35,41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La tabla 41 muestra que a pesar de la existencia de controles de seguridad de la información, tres riesgos con calificación inaceptable persisten, lo cual representa un indicativo de la vulnerabilidad a la confidencialidad que representan. Dichos riesgos son: el número 11, acceso no autorizado a secretaría académica sur por falta de mecanismos de control de acceso físico o falta de control en la atención al público; 12, acceso no autorizado a las áreas de coordinación de carrera, por las mismas falencias que aquejan al riesgo 11; y el riesgo número 49, relativo a la exposición de contraseñas de acceso a instalaciones y equipos de cómputo por falta de medidas de prevención. Son estos riesgos los que precisan de atención prioritaria en las estrategias de aseguramiento de la confidencialidad de la información.

Tabla 42: Matriz de vulnerabilidad residual para la integridad en la Unidad de Titulación ITSS

INTEGRIDAD				
PROBABILIDAD	3	28,30,38,48	11,12,23,24	49
	2	15,25,26,27,29,32, 33,34,44	4,40,43,46,47, 50	14,39
	1	5,8,10,19,20,22,37	17,18,36,45	1,2,3,6, 7,9,13,16,21,31,35, 41,42
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La tabla 42 indica que existe un riesgo de vulnerabilidad residual máxima para la integridad de la información, el número 49, que a pesar de los controles existentes persiste y por ello se lo cataloga como inaceptable y se recomienda su priorización al momento de implementar estrategias de tratamiento de riesgo.

Tabla 43: Matriz de vulnerabilidad residual para la disponibilidad en la Unidad de Titulación ITSS

DISPONIBILIDAD				
PROBABILIDAD	3	28,30,38,48	11,12,23,,24	49
	2	4,15,25,26,27,29,32, 33,34,44	40,43,46,47,50	14,39
	1	5,8,10,19,20,22,37	7,17,18,36,45	1,2,3,6,9,13,16,21,31 ,35,41,42,
		1	2	3
		IMPACTO		

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La tabla 43 presenta que el riesgo número 49 tiene también una calificación inaceptable de vulnerabilidad residual para la disponibilidad de la información, por lo que se recomienda su priorización al momento de implementar estrategias de tratamiento de riesgo.

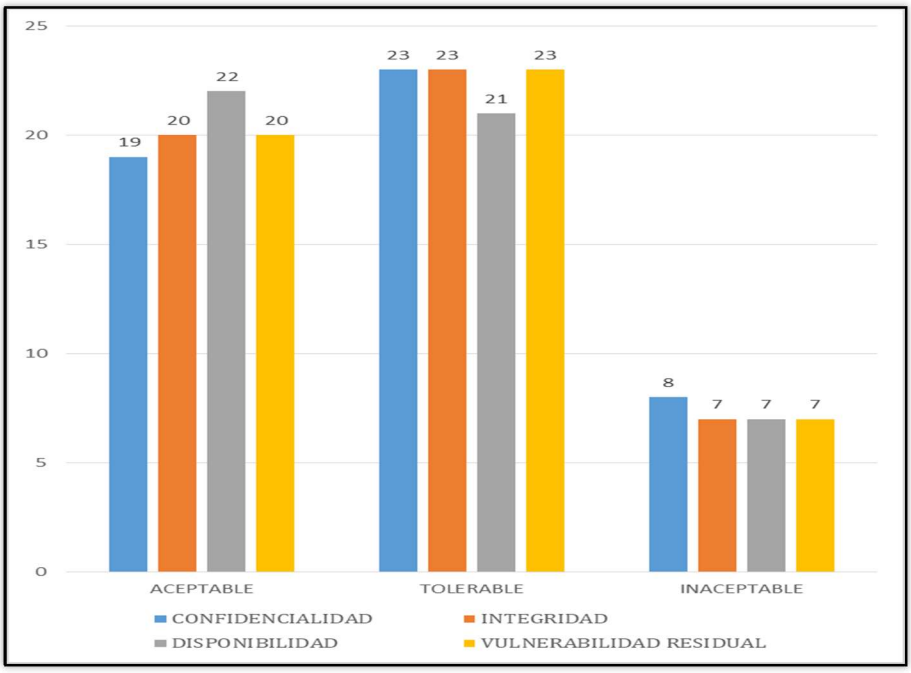
Tabla 44: Matriz de vulnerabilidad residual de la información de la Unidad de Titulación ITSS

VULNERABILIDAD RESIDUAL										
PROBABILIDAD	3			28,30,38,48			23,24	11,12		49
	2			15,25,26,27 ,29,32,33,3 4,44			4,40,43,46, 47,50			14,39
	1			8,10,19,20, 22,37		5	17,18,36,45		7	1,2,3,6,9,13, 16,21,31,35 ,41,42
		1	2	3	4	5	6	7	8	9
		IMPACTO								

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

La Tabla 44 presenta al riesgo número 49, exposición de contraseñas de acceso a instalaciones y a equipos de cómputo, como el primero a ser considerado al momento de implementar una estrategia de mitigación de riesgos.

Figura 10: Cantidad de riesgos por criterio y por aceptabilidad en análisis de vulnerabilidad residual



Fuente: Elaboración propia

La Figura 10 presenta el resumen de la cantidad de riesgos dentro del análisis de vulnerabilidad residual, clasificados por criterio de seguridad -confidencialidad, integridad, disponibilidad-, y agrupados por criterio de aceptabilidad.

5.4. Definición del Plan de Tratamiento de Riesgos

La Definición del Plan de Tratamiento de Riesgos como tal implica una explicación teórica que fue abordada en el numeral 4.4 en el anterior capítulo. Su implementación se presenta en el numeral 5.6 en este capítulo.

5.5. Aceptación del Riesgo

La Aceptación del Riesgo fue explicada en el numeral 4.4 del anterior capítulo. En dicho numeral se menciona la realización del Plan de Tratamiento para Riesgos Aceptables y Tolerables, cuyo diseño se realizó y se presenta en el Apéndice D.

5.6. Implementación del Plan de Tratamiento de Riesgos

Esta actividad da cumplimiento a la Fase de Implementación del Proceso de Gestión de Riesgos de Seguridad de la Información –Ver Figura 8, Alineamiento del Proceso de SGSI y del Proceso de Gestión

de Riesgos de Seguridad de la Información-. Este paso, descrito en el numeral 5.4, donde se presentó el Diseño del Plan de tratamiento de riesgos implementado en la Unidad de Titulación del ITS Sucre, abarca estrategias, actividades, responsables y plazos, direccionados a la administración de cada escenario de riesgo clasificado con vulnerabilidad residual inaceptable. Las razones de considerar únicamente a estos riesgos para el plan de tratamiento fueron mencionadas en el numeral 4.5, Aceptación de Riesgo. El resultado de la Implementación del Plan de Tratamiento de Riesgos mencionado se presenta en la Tabla 45.

Tabla 45: Resultado de la Implementación del Plan de Tratamiento de Riesgos

Escenario de riesgo	Plan de tratamiento de riesgos				
	Estrategia	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
11.Acceso no autorizado al área de secretaría académica sede Sur por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 14.Acceso no autorizado a anaqueles de la sala de lectura (sede sur) por daño en candados o falta de mecanismos de control de acceso físico a estudiantes fuera del horario de clases 23. Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público	Concienciar al personal de la Unidad de Titulación sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Establecer procedimientos para gestión segura de contraseñas para acceso a infraestructura, equipos de cómputo, sistemas de información y documentarlos	Definir una normativa para gestión de contraseñas	TIC	1/3/2018	1/4/2018
	Implementar políticas institucionales para el acceso físico de estudiantes, docentes, funcionarios del ITSS a instalaciones	Definir una normativa referente al uso obligatorio del carné institucional	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
		Establecer y ejecutar un cronograma para la carnetización de estudiantes, docentes y funcionarios	TIC con rector/ vicerrector	1/3/2018	1/5/2018
		Comunicar a personal de seguridad, estudiantes, docentes y funcionarios sobre la obligatoriedad del uso del carné para su control en ingresos/salidas de personas a instalaciones	Infraestructura	2/5/2018	9/5/2018
	Revisar/actualizar la política de acceso de personal externo al ITSS	Establecer una política de control de acceso al ITSS que contemple los permisos de acceso de exfuncionarios	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
	Identificar la información crítica almacenada en las áreas de Secretaría Sede Sur y Bienestar Estudiantil Sede Norte y determinar, implementar y dar seguimiento a mecanismos que impidan el intento de hurto	Caracterizar la información crítica	Titulación	1/3/2018	1/4/2018
		Establecer políticas para el uso de llaves físicas o magnéticas de acceso a las instalaciones	Titulación con Secretaría Sur y Bienestar Norte	1/3/2018	1/4/2018
		Establecer políticas sobre acceso restringido de personal a las áreas de secretaría sur y bienestar norte en horarios de atención al público	Titulación con Secretaría Sur y Bienestar Norte	1/3/2018	1/4/2018
	Establecer políticas para la gestión adecuada de dispositivos móviles en las áreas de Secretaría Sur, Bienestar Estudiantil Norte, Coordinaciones de carrera	Chequear y actualizar las disposiciones sobre el manejo de dispositivos móviles en áreas sensibles	Rector/ vicerrector	1/3/2018	1/4/2018
	Establecer directrices tendientes a garantizar que la información de estudiantes y docentes no es accesible a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad para equipos de cómputo desatendidos	TIC	1/3/2018	1/4/2018
		Definir protocolos de escritorios limpios/ pantallas limpias	TIC	1/3/2018	1/4/2018

Escenario de riesgo	Plan de tratamiento de riesgos				
	Estrategia	Actividad	Responsable	Fecha inicio	Fecha final
12. Acceso no autorizado a las área de coordinación de carrera por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 24. Hurto de dispositivos de almacenamiento y procesamiento del área de coordinación de carrera por falta de controles de acceso y al área en horarios de atención al público	Concienciar al personal de Coordinación de Carreras sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Identificar la información crítica almacenada en las áreas de cada una de las Coordinaciones de Carrera y determinar, implementar y dar seguimiento a mecanismos que impidan el intento de hurto	Caracterizar la información crítica	Cada Coordinación de Carrera	1/3/2018	1/4/2018
		Establecer políticas para el uso de llaves físicas o magnéticas de acceso a las instalaciones	Cada Coordinación de Carrera	1/3/2018	1/4/2018
		Establecer políticas sobre acceso restringido de personal a las áreas de secretaría sur y bienestar norte en horarios de atención al público	Cada Coordinación de Carrera	1/3/2018	1/4/2018
	Implementar políticas institucionales para el acceso físico de estudiantes, docentes, funcionarios del ITSS a instalaciones	Definir una normativa referente al uso obligatorio del carné institucional	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
		Establecer y ejecutar un cronograma para la carnetización de estudiantes, docentes y funcionarios	TIC con rector /vicerrector	1/3/2018	1/5/2018
		Comunicar a personal de seguridad, estudiantes, docentes y funcionarios sobre la obligatoriedad del uso del carné para su control en ingresos/salidas de personas a instalaciones	Infraestructura	2/5/2018	9/5/2018
	Revisar/actualizar la política de acceso de personal externo al ITSS	Establecer una política de control de acceso al ITSS que contemple los permisos de acceso de exfuncionarios	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
39. Desactivación de los Tags de acceso magnético por fallos del fluido eléctrico	Establecer mecanismos que protejan a los dispositivos de subidas de voltaje y/o fallos en suministro de energía eléctrica Establecer procedimientos de copia de seguridad	Incluir un plan de adquisiones de UPS, planta eléctrica y plan de mantenimiento de tendido eléctrico Definir protocolos de copia de seguridad	TIC, Coordinación de carrera de Electricidad y Gestión de Riesgos TIC	1/3/2018	31/12/2018
49. Exposición de las contraseñas de acceso a instalaciones y a equipos de cómputo y sistemas operativos por falta de medidas de prevención, uso adecuado y preservación de las mismas	Concienciar al personal de la Unidad de Titulación, Secretaría Sur, Bienestar Estudiantil Norte sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Establecer procedimientos para gestión segura de contraseñas para acceso a infraestructura, equipos de cómputo, sistemas de información y documentarlos	Definir una normativa para gestión de contraseñas	TIC	1/3/2018	1/4/2018

Fuente: Elaboración propia basada en (Benavides Sepúlveda & Blandón Jaramillo, 2017)

5.7. Monitoreo Continuo de Riesgos

Actividad descrita en el numeral 4.7 y actualmente en estado de ejecución.

5.8. Mejora Continua del Proceso de Gestión de Riesgos de Seguridad de la Información

Actividad descrita en el numeral 4.8 y actualmente en estado de ejecución. Está planificada una nueva iteración del Proceso de Gestión de Riesgos de Seguridad de la Información para el 1/1/2019, a menos que, como se indicó en el numeral 4.8, haya cambios significativos tanto en los riesgos como en sus factores detectados en la Unidad de Titulación del ITS Sucre.

5.9. Comunicación y Consulta

Actividad descrita en el numeral 4.7 y actualmente en estado de ejecución.

Validación de la metodología implementada

Se vuelve a correr el modelo de Diagnóstico de SGSI presentado en el numeral 4.1 e implementado en 5.1 una vez implementada la Metodología de Gestión de Riesgos de Información en el Instituto Tecnológico Superior Sucre y se obtienen los siguientes resultados:

Tabla 46: Resumen de resultados del diagnóstico final de Logro 1

RESUMEN DEL DIAGNÓSTICO FINAL EN EL LOGRO 1 EN EL ITSS (SOBRE 30%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
3 a 15	**Cumple satisfactoriamente**	**3**	**4,6%**	Propósito de Seguridad de Información
3 a 15	**Cumple parcialmente**	**6**	**4,6%**	
3 a 15	No cumple	4	0	
1	**Cumple satisfactoriamente**	**1**	**5,0%**	Autodiagnóstico de S.I.
1	Cumple parcialmente	0	0	
1	No cumple	0	0	
2	**Cumple satisfactoriamente**	**1**	**5,0%**	Creación plan inicial de proyecto
2	Cumple parcialmente	0	0	
2	No cumple	0	0	
TOTAL			**19,2%**	

Fuente: Elaboración propia

Al volver a testear la Definición de Marco de Seguridad y Privacidad de Información, Logro 1, se observan cambios:

1) En la primera pregunta que tiene una ponderación de 5% ahora se tiene cumplimiento satisfactorio, es decir, subió 5 puntos porcentuales al contarse con Autodiagnóstico de Seguridad; $\frac{1*5\%}{1}$ = **5%**

2) En la segunda pregunta que también tiene ponderación de 5%, se obtuvo cumplimiento satisfactorio, al obtener conformidad en la pregunta relativa a la Creación de Plan de Trabajo de Seguridad, es decir, incrementó 5%; $\frac{1*5\%}{1}$ = **5%**

3) En las 13 preguntas relativas al Propósito de Seguridad de Información que antes se tenía únicamente tres respuestas en cumplimiento parcial, ahora tiene 3 respuestas en cumplimiento satisfactorio, lo que da 4,6% de incremento y 3 respuestas adicionales en cumplimiento parcial, total 6, que incrementan el nivel de conformidad en otro 4.6%.

$\frac{3*20\%}{13} + \frac{6*10\%}{13}$ = **4,616% + 4,616% = 9,23 %** que se redondea en 9,2%

Total en Logro 1 se alcanza un nivel de conformidad de 19,2% cuando antes únicamente se contaba con 2,3%. El nivel de seguridad de la información ha incrementado **16.9 %**

En cuanto al Diagnóstico de la Implementación del Plan de Seguridad, Logro 2, la implementación de controles será evaluada al finalizar esta iteración del Proceso de Gestión de Riesgos de SI el 1/1/19, así que se mantiene sin cambios.

Tabla 47: Resumen de resultados del diagnóstico final de Logro 2

RESUMEN DEL DIAGNÓSTICO FINAL DE IMPLEMENTACIÓN DEL LOGRO 2 EN EL ITSS (SOBRE 40%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
1 a 114	Cumple satisfactoriamente	0	0	114 controles de seguridad de información desde A5.1.1 hasta A18.2.3
1 a 114	Cumple parcialmente	39	8,2%	
1 a 114	No cumple	56	0	
1 a 114	No aplica	19	10,0%	
Número de controles que aplican		95		
TOTAL			8,2%	

Fuente: Elaboración propia

A continuación la matriz correspondiente a evaluación final de Logro 3.

Tabla 48: Resumen de resultados del diagnóstico final de Logro 3

RESUMEN DEL DIAGNÓSTICO FINAL DE LOGRO 3 EN EL ITSS (SOBRE 30%)				
PREGUNTAS	**VALORACION**	**TOTAL**	**PESO**	**DETALLES**
1 a 6	Cumple satisfactoriamente	**1**	**2,5%**	Monitoreo (Verificar)
1 a 6	Cumple parcialmente	**3**	**3,8%**	
1 a 6	No cumple	2	0,0%	
7 a 12	Cumple satisfactoriamente	0	0,0%	Mejora Continua (Actuar)
7 a 12	Cumple parcialmente	4	5,0%	
7 a 12	No cumple	2	0,0%	
TOTAL			**11,3%**	

Fuente: Elaboración propia

Al volver a testear la Procesos de Monitoreo y Mejora Continua, Logro 3, se observan cambios:

1) En las 6 primeras preguntas, relativas al subproceso de monitoreo que tiene una ponderación de 15% para cumplimiento satisfactorio, ahora se tiene 1 respuesta, es decir, subió 2,5 puntos porcentuales; en cuanto a preguntas con cumplimiento parcial, valoradas en 7,5% para cumplimiento parcial, se tienen ahora 3 respuestas, es decir, subió 3,8%. En Diagnóstico Inicial este ítem obtuvo 0% de conformidad.

$\frac{1*15\%}{6} + \frac{3*7,5\%}{6} =$ **2,5%** + **3,8%** = 6,3% de conformidad por Monitoreo

2) En las 6 preguntas restantes, relativas al subproceso de mejora continua incrementa de 2 a 4 las respuestas de cumplimiento parcial, valoradas con 7,5%; lo que se refleja un crecimiento del 2,5% de conformidad al 5%.

$\frac{4*7,5\%}{6} =$ **5%** de conformidad por Mejora Continua

Por lo tanto, al volver a testear Logro 3, se obtuvo: **6,3% + 5% = 11,3%**

Lo cual representa un incremento de 8,8% respecto al estado inicial de Seguridad.

En total se tiene los siguientes valores finales de seguridad de información respecto a SGSI:

Tabla 49: Resumen consolidado de resultados del Diagnóstico Final de Seguridad

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	19,2%
LOGRO2	HACER	40%	8,2%
LOGRO3	VERIFICAR	15%	6,3%
	ACTUAR	15%	5,0%
	TOTAL	100%	38,7%

Fuente: Elaboración propia

Interpretando resultados de la Tabla 49 se incrementa el nivel de conformidad de SGSI de 13% obtenido en el análisis inicial hasta el 38,7%, es decir, hay un aumento de 25,7%. Las matrices de diagnóstico final que han sufrido modificación se muestran en el Apéndice E.

Capítulo 6

Conclusiones y Recomendaciones

6.1. Conclusiones

Se diagnosticó la situación inicial de la seguridad de la información al interior del ITS Sucre y se determinó cumplimientos de 2,3% sobre un total de 30% por existencia de un Marco de Seguridad de la Información; de 8,2% sobre un total de 40% por cumplimiento en la Implementación de un Plan de Seguridad de la Información; y, de 2,5% sobre el 30% por cumplimiento de Procesos de Monitoreo y Mejora Continua del Plan de Seguridad de la Información; totalizando 13%,

Se contribuyó en la Institución de Educación Superior, IES, antes mencionada, con el desarrollo de una Metodología de Gestión de Riesgos de Seguridad de la Información, misma que es fruto de la adaptación de un Modelo de Sistema de Gestión de Seguridad de la Información desarrollado en Colombia de acuerdo a las normas internacionales ISO/IEC 27001 y 27002; y su alineación con el Proceso de Gestión de Riesgos de Seguridad de la Información especificado en la norma ISO/IEC 27005. Dicha metodología comprende procesos como Análisis y Evaluación de riesgos, así como también Definición e Implementación del Plan de Tratamiento de Riesgos.

Se determinó, como resultado de los procesos de Análisis y Evaluación, que el mayor riesgo para los activos de información de la Unidad de Titulación del ITS Sucre -dependencia donde se autorizó la implementación de la Metodología- es la exposición de contraseñas de acceso físico y lógico a Secretaría Académica y Vicerrectorado en el Campus Sur y de acceso físico a la Unidad de Bienestar Estudiantil en el Campus Norte.

Se informó a las partes involucradas -autoridades, coordinadores de Talento Humano y Jurídico, coordinadores de Carreras tanto de la Sede Norte como de la Sede Sur, funcionarios y coordinador de la Unidad de Titulación- sobre los avances en las fases de Análisis y Evaluación a medida que estas se lograban; así como también sobre el diseño y la asignación de actividades que en la ejecución del Plan de Tratamiento de Riesgos de Información les corresponde, previa a su puesta en práctica.

Se ejecuta el Plan de Tratamiento de Riesgos para la Unidad de Titulación del ITSS dando cumplimiento así a la implementación de la metodología desarrollada en este trabajo de titulación.

Dicha ejecución se la viene haciendo desde primeros días del mes de marzo de 2018 sobre aquellos riesgos cuyo valor de vulnerabilidad residual es mayor o iguales al 50%, es decir aquellos catalogados con criterio de inaceptables.

Se realizó, una vez puesto en ejecución el Plan de Tratamiento de Riesgos mencionado, un nuevo diagnóstico de seguridad de la información, determinándose los siguientes valores: por Definición del Marco de Seguridad,19,2% sobre 30%; por el valor de Implementación del Plan de Seguridad se mantiene en 8,2% sobre el 40%, hasta terminar esta iteración del Proceso Gestión de Riesgos de Seguridad de la Información; y 11,3% sobre 30% por Procesos de Monitoreo y Mejora Continua; totalizando un valor de 38%, lo cual refleja una subida en el valor ponderado de la seguridad de la información del 25% respecto al resultado obtenido en el diagnóstico inicial.

6.2. Recomendaciones

Dar cumplimiento a las actividades planificadas dentro del Plan de Tratamiento de Riesgos de la Información para la Unidad de Titulación del ITSS, para su ejecución en lo que resta de este año para de esa manera, poder contar con una memoria técnica y modelo a seguir, al darse una nueva iteración del Proceso de Gestión de Riesgos.

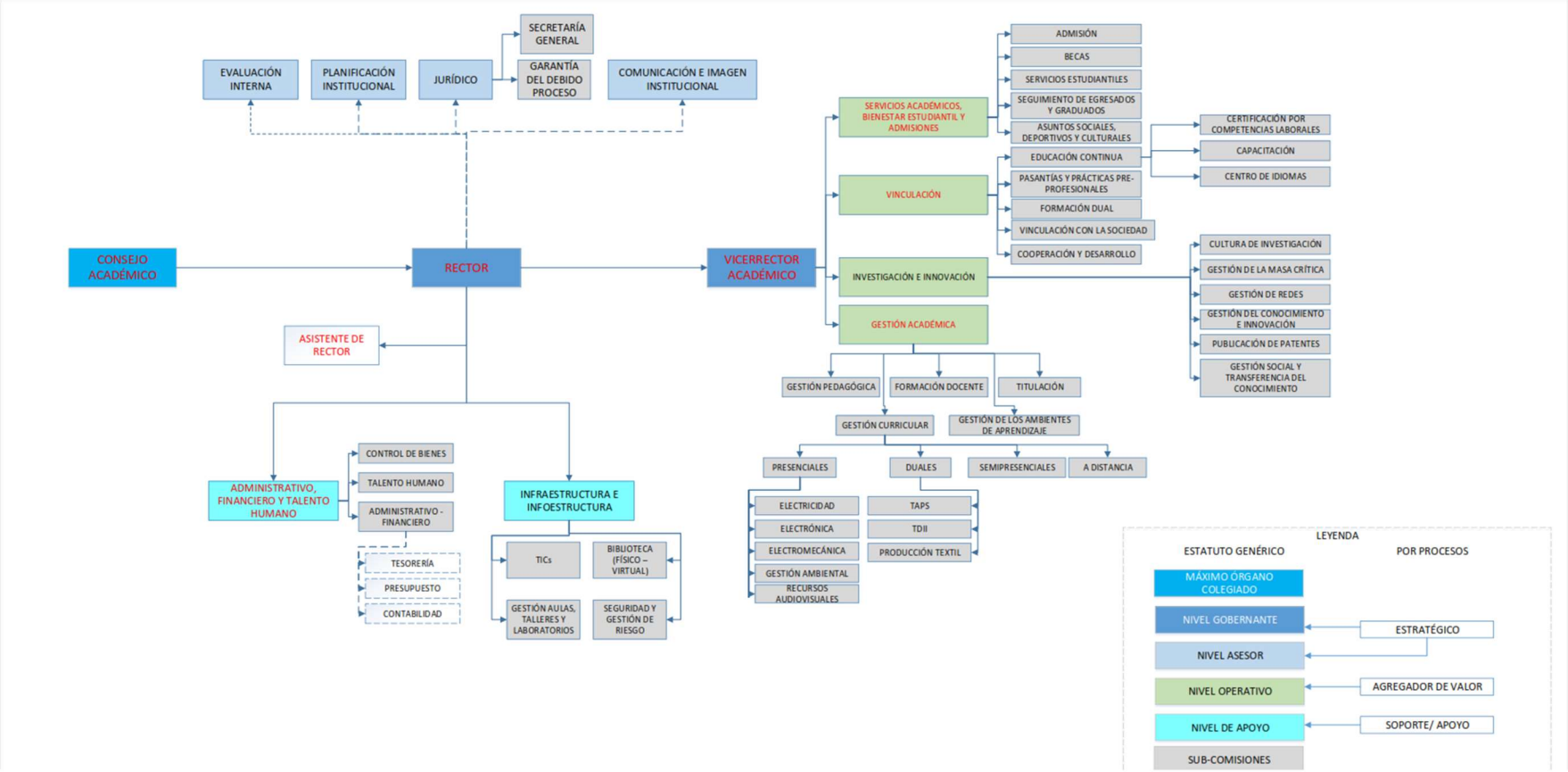
Continuar con la implementación de la metodología adaptada para gestión de riesgos en las restantes dependencias administrativas del ITS Sucre, así como la creación del SGSI institucional.

Crear al interior del ITS Sucre la Comisión de Gestión de Riesgos de Seguridad de la Información, con la finalidad de disponer de un ente administrativo acorde a las especificaciones provistas tanto en la norma ISO/IEC 27005 como en el Esquema Gubernamental para la Seguridad de la Información, EGSI, vigente en el país.

Incentivar el uso de la metodología presentada en este trabajo de titulación en otras instituciones educativas del país, dentro de procesos de gestión de riesgos de seguridad de la información puntuales o como partes integrantes de SGSI como una guía a seguir que permita de una manera práctica a dichos centros de estudios, precautelar la seguridad y privacidad de la información que producen, procesan y custodian.

Apéndice A

Organigrama estructural del Instituto Tecnológico Superior Sucre



Fuente: Comisión de Planificación ITSS

Apéndice B

Diagnóstico Inicial del Sistema de Gestión de Seguridad de la Información SGSI en el ITSS

DIAGNÓSTICO SGSI LOGRO 1: DEFINICIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)

Por favor, conteste la siguiente encuesta.

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2014 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple al 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2014) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información)?	No cumple		Diligenciar autodiagnostico de seguridad de la informacion.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	No cumple		Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	No cumple		Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	Cumple parcialmente	Actas de reuniones de la comisión de las TIC, evidencia digital en posesión del coordinador	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Plan de trabajo con rectorado, en actas que reposan en rectorado del ITSS	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	No cumple		Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Cómite de Seguridad de la Información?	Cumple parcialmente	Se ha designado a la persona responsable de salvaguardar la seguriadad de la información en el ITSS en acta respectiva aprobada por Consejo Académico Superior	Definir mediante acto administrativo el comite de seguridad de la informacion que describa las responsabilidades de los integrantes, reuniones entre otros.
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	No cumple		Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.
9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple		Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple		Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	No cumple		Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	No cumple		Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2014.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	No cumple		Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	No cumple		Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple		Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente

Fuente: NTE-INEN-ISO-IEC 27001:2014

DIAGNOSTICO SGSI LOGRO 2: IMPLEMENTACION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (40%)

Por favor, conteste la siguiente encuesta.

Estado	Significado
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	¿Existe un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes?	No cumple	
A5.1.2	Revisión de las políticas para la seguridad de la información.	¿ Existen revisiones de las políticas para seguridad de la información a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas?	No cumple	
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	¿Están definidas y asignadas todas las responsabilidades de la seguridad de la información?	Cumple parcialmente	Existe un documento que designa a las personas que cumplen roles específicos de SI, hay seguimiento pero no se sigue un estándar
A6.1.2	Separación de deberes	¿Están segregados las tareas y áreas de responsabilidad que pudieran entrar en conflicto para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización?	Cumple parcialmente	Existe roles definidos para el control de los sistemas de gestión,
A6.1.3	Contacto con las autoridades	¿Se mantiene contacto apropiado con las autoridades pertinentes?	Cumple parcialmente	Actas de reuniones que reposan en
A6.1.4	Contacto con grupos de interés especial	¿Se mantiene un contacto apropiado con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad?	No cumple	
A6.1.5	Seguridad de la información en la gestión de proyectos.	¿Se toma en cuenta a la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto?	No cumple	

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A6.2	Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A6.2.1	Política para dispositivos móviles	¿Se han adoptado una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles?	No cumple	
A6.2.2	Teletrabajo	¿Están implentadas una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo?	No cumple	
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A7.1	Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A7.1.1	Selección	¿La investigación de los antecedentes de todos los candidatos a un empleo se llevan a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y son proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos?	Cumple parcialmente	Se pide certificado de no tener impedimento de ejercer cargo público, se pide los aportes patronales que tiene en el IESS y a través de ellos se da seguimiento, los certificados de trabajo, la cédula, la papeleta
A7.1.2	Términos y condiciones del empleo	¿Los acuerdos contractuales con empleados y contratistas, contemplan responsabilidades y las de la organización en cuanto a la seguridad de la información?	Cumple parcialmente	Se hace firmar un convenio de confidencialidad que reposa en la base digital y en los archivos princales de la Senescyt
A7.2	Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A7.2.1	Responsabilidades de la dirección	¿La dirección exige a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización?	No cumple	
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	¿Todos los empleados de la organización, y en donde sea pertinente, los contratistas, han recibido capacitación y formación en la toma de conciencia de la seguridad de la información, y así como actualizaciones regulares sobre las políticas y procedimientos de la organización, según sea pertinentes para la función del trabajo que cumplen?	No cumple	No hay capacitación al respecto
A7.2.3	Proceso disciplinario	¿Se cuenta con un proceso disciplinario formal el cual haya sido comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?	No cumple	

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A7.3	Terminación y cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A7.3.1	Terminación o cambio de responsabilidades de empleo	¿Las responsabilidades y los deberes de seguridad de la información que deben seguir válidos después de la terminación o cambio de contrato han sido definidos, comunicados al empleado o contratista y se hacen cumplir?	Cumple parcialmente	Está especificado en el acuerdo de confidencialidad, donde se especifica su vigencia por dos años posteriores a la terminación del contrato
A8	**GESTION DE ACTIVOS**			
A8.1	Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A8.1.1	Inventario de activos	¿Están identificados los activos asociados con la información y las instalaciones de procesamiento de información, existe y se mantiene un inventario de dichos activos?	Cumple parcialmente	Existe el inventario pero no dentro de un sistema de gestión de seguridad de la información, debido a que el instituto está en un proceso de transición
A8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario tienen un propietario	Cumple parcialmente	Debido al proceso de transición los bienes pertenecen al Secap, sede Norte y el MinEduc, sede Sur.
A8.1.3	Uso aceptable de los activos	Se identifican, documentan e implementan reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información	No cumple	
A8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas devuelven todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo	Cumple parcialmente	Se lleva el control a través de actas
A8.2	Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A8.2.1	Clasificación de la información	¿Está clasificada la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada?	No cumple	
A8.2.2	Etiquetado de la información	¿Se desarrolla e implementa un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización?	No cumple	
A8.2.3	Manejo de activos	¿Se desarrollan e implementan procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización?	No cumple	
A8.3	Manejo de medios			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A8.3.1	Gestión de medio removibles	¿Se implementan procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización?	No cumple	
A8.3.2	Disposición de los medios	¿Se dispone en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales?	No cumple	No hay políticas
A8.3.3	Transferencia de medios físicos	¿Los medios que contienen información están protegidos contra acceso no autorizado, uso indebido o corrupción durante el transporte?	No cumple	Los equipos son propiedad de los docentes

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A9	**CONTROL DE ACCESO**			
A9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A9.1.1	Política de control de acceso	¿Se ha establecido, documenta y revisa una política de control de acceso con base en los requisitos del negocio y de seguridad de la información?	No cumple	No hay políticas
A9.1.2	Acceso a redes y a servicios en red	¿Solo se permite acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	Cumple parcialmente	Mediante usuario y mac address para identificar la dirección física de los usuarios se valida el acceso
A9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A9.2.1	Registro y cancelación del registro de usuarios	¿Está implementado un proceso formal de registro y baja de usuarios, para posibilitar la asignación de los derechos de acceso?	No aplica	No hay servidores en la institución
A9.2.2	Suministro de acceso de usuarios	¿Se tiene implementado un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios?	No aplica	No hay servidores en la institución
A9.2.3	Gestión de derechos de acceso privilegiado	¿Se restringe y controla la asignación y uso de derechos de acceso privilegiado?	No aplica	No hay servidores en la institución
A9.2.4	Gestión de información de autenticación secreta de usuarios	¿La asignación de la información de autentificación secreta está controlada por medio de un proceso de gestión formal?	No aplica	No hay servidores en la institución
A9.2.5	Revisión de los derechos de acceso de usuarios	¿Los propietarios de los activos chequean los derechos de acceso de los usuarios, a intervalos regulares?	No cumple	No hay políticas
A9.2.6	Retiro o ajuste de los derechos de acceso	¿Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información son removidos al terminar su empleo, contrato o acuerdo, o se ajustan cuando se hacen cambios?	Cumple parcialmente	A nivel de plataformas específicas con las que cuenta la institución se regulan estos ítems, por ejemplo correo, sistema de notas SAO-P, acceso a parqueaderos
A9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A9.3.1	Uso de información de autenticación secreta	¿Se exige a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta?	No cumple	No se cumple porque el usuario es responsable de su información, no hay normativas que regulen esto

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A9.4.1	Restricción de acceso a la información	¿El acceso a la información y a las funciones de los sistemas de las aplicaciones se restringen de acuerdo con la política de control de acceso?	Cumple parcialmente	Se tiene control en las plataformas que dispone la institución, el administrador (coordinador TIC) asigna los roles
A9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, ¿el acceso a sistemas y aplicaciones se controla mediante un proceso de ingreso seguro?	No cumple	Solo es contraseña y nada más
A9.4.3	Sistema de gestión de contraseñas	¿Los sistemas de gestión de contraseñas son interactivos y aseguran la calidad de las contraseñas?	Cumple parcialmente	A nivel de plataformas específicas con las que cuenta la institución se regulan estos ítems, por ejemplo correo institucional, sistema de notas SAO-P
A9.4.4	Uso de programas utilitarios privilegiados	¿Se restringe y controla estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones?	No aplica	No hay sistemas de gestión
A9.4.5	Control de acceso a códigos fuente de programas	¿Está restringido el acceso a los códigos fuente de los programas?	Cumple parcialmente	El sistema de gestión de notas SAO-P es responsabilidad de una empresa externa
A10	**CRIPTOGRAFIA**			
A10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A10.1.1	Política sobre el uso de controles criptográficos	¿Existe una política desarrollada e implementada sobre el uso de controles criptográficos para la protección de la información ?	No cumple	No hay normativa
A10.1.2	Gestión de llaves	¿Está desarrollada e implementada una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida?	No cumple	No existe un sistema de gestión propio
A11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	¿Se han definido y usan perímetros de seguridad, y son usados para proteger áreas que contienen información sensible o critica, e instalaciones de manejo de información?	Cumple parcialmente	Existe acceso controlado a instalaciones en la sede sur mediante tarjetas magnéticas y claves de acceso, además de existir servicio de guardianía en ambas sedes verificado

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.2	Controles de acceso físicos	¿Se protege a las áreas seguras mediante controles de entrada apropiados para así asegurar que solamente se permite el acceso a personal autorizado?	Cumple parcialmente	Existe acceso controlado a instalaciones en la sede sur mediante tarjetas magnéticas y claves de acceso, además de existir servicio de guardianía en ambas sedes verificado
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	¿Está diseñada y se aplica seguridad física a oficinas, recintos e instalaciones?	Cumple parcialmente	Existe acceso controlado a instalaciones en la sede sur mediante tarjetas magnéticas y claves de acceso, además de existir servicio de guardianía en ambas sedes verificado
A11.1.4	Protección contra amenazas externas y ambientales.	¿Está diseñada y se aplica protección física contra desastres naturales, ataques maliciosos o accidentes?	No cumple	
A11.1.5	Trabajo en áreas seguras.	¿Se han diseñado y aplican procedimientos para trabajo en áreas seguras?	No cumple	
A11.1.6	Áreas de carga, despacho y acceso público	¿Se controlan los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado?	No cumple	
A11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A11.2.1	Ubicación y protección de los equipos	¿Los equipos están ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado?	Cumple parcialmente	Existe acceso controlado a instalaciones en la sede sur mediante tarjetas magnéticas y claves de acceso, además de existir servicio de guardianía en ambas sedes verificado
A11.2.2	Servicios de suministro	¿ Están protegidos los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro?	No cumple	No existen UPS ni generadores de emergencia
A11.2.3	Seguridad en el cableado.	¿El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería está protegido contra interceptación, interferencia o daño?	No cumple	No existe un cableado estructurado
A11.2.4	Mantenimiento de los equipos.	¿Los equipos reciben mantenimiento adecuado para asegurar su disponibilidad e integridad continuas?	Cumple parcialmente	Ya se realizó un mantenimiento a los laboratorios de cómputo

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A11.2.5	Retiro de activos	¿Los equipos, información o software no se retiran de su sitio sin autorización previa?	Cumple parcialmente	Los equipos propiedad del instituto se retiran bajo autorización del coordinador de TIC
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	¿Se aplican medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones?	No aplica	No existen equipos de la institución que se movilicen externamente
A11.2.7	Disposición segura o reutilización de equipos	¿Se verifican todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización?	Cumple parcialmente	Valida el coordinador de TIC antes de entregar a otro usuario
A11.2.8	Equipos de usuario desatendido	¿Los usuarios se aseguran de que a los equipos desatendidos se les da protección apropiada?	No aplica	Son equipos de los docentes, no de la institución
A11.2.9	Política de escritorio limpio y pantalla limpia	¿Se ha adoptado una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información?	Cumple parcialmente	No todos los usuarios aseguran la información
A12	**SEGURIDAD DE LAS OPERACIONES**			
A12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Los procedimientos de operación documentan y ponen a disposición de todos los usuarios que los necesiten	Cumple parcialmente	El sistema de gestión de notas SAO-P y repositorio físico (UBE) tienen sus procedimientos documentados y los siguen los usuarios
A12.1.2	Gestión de cambios	Se controlan los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información	Cumple parcialmente	Se cumple a través de las disposiciones de la autoridad
A12.1.3	Gestión de capacidad	¿Para asegurar el desempeño requerido del sistema se da seguimiento al uso de los recursos, se realizan ajustes, y se hacen proyecciones de los requisitos sobre la capacidad futura?	No cumple	Se ajusta en función de los requerimientos institucionales cuando estos se presentan pero no se hacen proyecciones
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Están separados los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No aplica	No existe software propietario de la institución ni se desarrolla aplicaciones

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
A12.2.1	Controles contra códigos maliciosos	Están implementados controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para protegerse contra códigos maliciosos	Cumple parcialmente	Se tiene control en los laboratorios de informática con el sistema de congelamiento de equipos
A12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				
A12.3.1	Respaldo de la información	¿Se realizan copias de respaldo de la información, del software e imágenes de los sistemas, y son puestas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada?	Cumple parcialmente	El proveedor realiza respaldos mensuales de la base de datos de los estudiantes de la institución
A12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A12.4.1	Registro de eventos	Se elaboran, conservan y revisan regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	No cumple	No hay un sistema de control de eventos
A12.4.2	Protección de la información de registro	¿Las instalaciones y la información de registro están protegidas contra alteración y acceso no autorizado?	Cumple parcialmente	Está implementado sistemas de autenticación en función de la plataforma que se usa . Y se tiene gestionado el acceso físico por control magnético en la sede sur
A12.4.3	Registros del administrador y del operador	¿Las actividades del administrador y del operador del sistema se registran, y los registros se protegen y revisan con regularidad?	Cumple parcialmente	Dependemos de un proveedor externo, que sí implementa este tipo de registro
A12.4.4	Sincronización de relojes	¿Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad están sincronizados con una única fuente de referencia de tiempo?	No cumple	No hay servidores en la institución
A12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A12.5.1	Instalación de software en sistemas operativos	¿Están implementados procedimientos para controlar la instalación de software en sistemas operativos?	Cumple parcialmente	Están implementados procedimientos mediante software instalado en los laboratorios de informática

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A12.6.1	Gestión de las vulnerabilidades técnicas	¿Se obtiene oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usan; evalúa la exposición de la organización a estas vulnerabilidades, y toma las medidas apropiadas para tratar el riesgo asociado?	No cumple	
A12.6.2	Restricciones sobre la instalación de software	¿Se establece e implementa reglas para la instalación de software por parte de los usuarios?	Cumple parcialmente	Están implementados procedimientos mediante software instalado en los laboratorios de informática
A12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A12.7.1	Controles de auditorías de sistemas de información	¿Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos están planificados y se acuerdan cuidadosamente para minimizar las interrupciones en los procesos del negocio?	No cumple	No hay sistemas de gestión propios
A13	**SEGURIDAD DE LAS COMUNICACIONES**			
A13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A13.1.1	Controles de redes	Las redes se gestionan y controlan para proteger la información en sistemas y aplicaciones	No cumple	
A13.1.2	Seguridad de los servicios de red	Se identifican los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, y se incluyen en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente	No cumple	Se está a expensas del proveedor
A13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información son segregados en las redes.	No cumple	No hay servidores en la institución
A13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A13.2.1	Políticas y procedimientos de transferencia de	Se cuenta con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación	Cumple parcialmente	La parte administrativa cumple esto mediante plataforma quipux
A13.2.2	Acuerdos sobre transferencia de información	Los acuerdos consideran la transferencia segura de información del negocio entre la organización y las partes externas.	No cumple	No sabemos
A13.2.3	Mensajería Electronica	Se protege adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente	Se cumple mediante las políticas de seguridad de la información de gmail
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Se identifican, revisan regularmente y documentan los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información	No cumple	

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A14.1	Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información están incluidos en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes	No aplica	Todo está concesionado a empresas externas
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas está protegida de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No aplica	
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones está protegida para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	No aplica	
A14.2	Seguridad en los procesos de Desarrollo y de Soporte			
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Se establecen y aplican reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización	No aplica	No se desarrollan sistemas en la institución
A.14.2.2	Procedimientos de control de cambios en	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se controlan mediante el uso de procedimientos formales de control de cambios	No aplica	Se hace externamente en el sistema arrendado
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se revisan las aplicaciones críticas del negocio, y se las pone a prueba para asegurar que no hay impacto adverso en las operaciones o seguridad de la organización	Cumple parcialmente	Se planifica con el proveedor externo
A.14.2.4	Restricciones en los cambios a los paquetes de software	¿Existen restricciones a las modificaciones en los paquetes de software, que se limitan solamente a los cambios necesarios, y todos los cambios están estrictamente controlados?	Cumple parcialmente	Todo está en función de las facilidades que brinda el proveedor
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Se establecen, documentan y mantienen principios para la construcción de sistemas seguros, que son aplicados a cualquier actividad de implementación de sistemas de información.	No aplica	No se desarrollan sistemas en la institución
A.14.2.6	Ambiente de desarrollo seguro	¿Esta organización establece y protege adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprenden todo el ciclo de vida de desarrollo de sistemas?	No aplica	No se desarrollan sistemas en la institución
A.14.2.7	Desarrollo contratado externamente	¿La organización supervisa y hace seguimiento de la actividad de desarrollo de sistemas contratados externamente?	Cumple parcialmente	Solo es por medio del coordinador de TIC
A.14.2.8	Pruebas de seguridad de sistemas	¿Durante el desarrollo llevan a cabo pruebas de funcionalidad de la seguridad?	No aplica	No se desarrollan sistemas en la institución
A.14.2.9	Prueba de aceptación de sistemas	¿Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se han establecido programas de prueba para aceptación y criterios de aceptación relacionados?	No aplica	No se desarrollan sistemas en la institución
A14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Los datos de prueba se seleccionan, protegen y controlan cuidadosamente.	No aplica	No se desarrollan sistemas en la institución

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A15	**RELACIONES CON LOS PROVEEDORES**			
A15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se acuerdan con estos y están debidamente documentados.	No cumple	No se tiene una normativa con el proveedor
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con	Están establecidos y acordados todos los requisitos de seguridad de la información pertinentes con cada proveedor que tiene acceso, procesa, almacena, comunica o suministra componentes de infraestructura de TI para la información de la organización.	Cumple parcialmente	A través del contrato con el proveedor
A15.1.3	Cadena de suministro de tecnología de información y comunicación	¿Se contempla en los acuerdos con proveedores requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación?	Cumple parcialmente	En base a las políticas del proveedor
A15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	¿Esta organización hace seguimiento, revisa y audita con regularidad la prestación de servicios de los proveedores?	Cumple parcialmente	Se valida backups mensuales de la información y servicios por parte del coordinador de TI
A15.2.2	Gestión del cambio en los servicios de los proveedores	¿Se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos?	Cumple parcialmente	Gestiona el coordinador de TI el cambio de servidores y sus prestaciones
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A16.1.1	Responsabilidades y procedimientos	¿Están establecidas las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	No cumple	
A16.1.2	Reporte de eventos de seguridad de la información	¿Los eventos de seguridad de la información se informan debidamente a través de los canales de gestión apropiados, tan pronto como es posible?	No cumple	
A16.1.3	Reporte de debilidades de seguridad de la información	¿Se exige a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios?	No cumple	
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	¿Los eventos de seguridad de la información son sometidos a evaluación y se decide si se los clasifica como incidentes de seguridad de la información?	No cumple	
A16.1.5	Respuesta a incidentes de seguridad de la información	¿Se da respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados?	No cumple	

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	¿El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se utiliza para reducir la posibilidad o el impacto de incidentes futuros?	No cumple	No existe infraestructura propia para este proceso
A16.1.7	Recolección de evidencia	¿La organización define y aplica procedimientos para la identificación, recolección, adquisición y preservación de información que puede servir como evidencia?	No cumple	
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**			
A17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A17.1.1	Planificación de la continuidad de la seguridad de la información	Esta organización ha determinado sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	No cumple	
A17.1.2	Implementación de la continuidad de la seguridad de la información	Esta organización establecido, documentado, implementado y mantenido procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	No cumple	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Esta organización verifica a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.	No cumple	
A17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de	Las instalaciones de procesamiento de información se han implementado con redundancia suficiente para cumplir los requisitos de disponibilidad.	No aplica	No disponemos de enlaces backup ni servidores
A18	**CUMPLIMIENTO**			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A18.1.1	Identificación de la legislación aplicable.	¿Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, son identificados y documentados explícitamente y mantenidos actualizados para cada sistema de información y para la organización?	No cumple	
A18.1.2	Derechos propiedad intelectual (DPI)	¿Se implementan procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados?	No cumple	
A18.1.3	Protección de registros	¿Los registros gozan de protección contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de	No cumple	

ANEXO A NTE INEN-ISO/IEC 27001:2014			ESTADO	EVIDENCIA
A18	**CUMPLIMIENTO**			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A18.1.4	Privacidad y protección de información de datos personales	¿Cuando es aplicable, se asegura la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes?	No cumple	
A18.1.5	Reglamentación de controles criptográficos.	¿Se deberían usan controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes?	No cumple	
A18.2	Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A18.2.1	Revisión independiente de la seguridad de la información	¿El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) son revisados independientemente a intervalos planificados o cuando ocurren cambios significativos?	No cumple	
A18.2.2	Cumplimiento con las políticas y normas de seguridad	¿Los directivos revisan con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad?	No cumple	No existe una normativa
A18.2.3	Revisión del cumplimiento técnico	¿Los sistemas de información se revisan periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información?	No cumple	

Fuente: NTE-INEN-ISO-IEC 27001:2014

AUTODIAGNÓSTICO SGSI LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30 %)

Por favor, conteste la siguiente encuesta de acuerdo con el instructivo.

Estado	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO27001 versión 2014 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. cumple 100%.
Cumple parcialmente	Lo que la norma requiere (ISO27001 versión 2014) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó pero no se gestiona.
No cumple	No existe y/o no se está haciendo.

VERIFICAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de laInformación.?	No cumple	No existe un SGSI	Se debe tener en cuenta que se desea medir, cuando, quien realizará la mediciónу cuando se analizaran los resultados.
2	La entidad ha realizado auditorias internas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Se deben programar auditorias en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la Información.
3	La entidad cuenta con programas de auditorias aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	No existe un SGSI	Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periodicas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	No cumple	No existe un SGSI	
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	No existe un SGSI	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluacion de las no conformidades y acciones correctivas. Esta revisión debe incluir las decisiones relacionadas con las oportunidades de mejora

ACTUAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoria?	Cumple parcialmente	A petición de la Senescyt que es nuestro órgano regulador externo se hacen los correctivos necesarios	Se deben tomar acciones para eliminar las causas de las no conformidades, para que no vuelvan a ocurrir.
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	No cumple	No existe un SGSI	Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	La entidad revisa la eficiacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	Cumple parcialmente	A petición de las autoridades se hacen los correctivos necesarios	Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información despues de las acciones tomadas?	No cumple	No existe un SGSI	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	No cumple	No existe un SGSI	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: NTE-INEN-ISO-IEC 27001:2014

Fuente: Adaptación de (Alta Consejería Distrital de TIC, 2015)

Apéndice C

Certificado de Definición del Contexto de la Gestión de Riesgos de Seguridad de la Información

INSTITUTO TECNOLÓGICO SUPERIOR SUCRE

Quito, 08 de diciembre del 2017

CERTIFICADO

Certifico, que dentro del Proyecto de Investigación "Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre", luego de mantener varias reuniones de trabajo este proyecto se declaró como una necesidad Institucional.

Por lo tanto, se solicitó al Ing. Flavio López Vasco, que la implementación de dicha investigación se efectúe sobre los procesos que maneja la Unidad de Titulación del plantel, tanto en el Campus Norte como en el Campus Sur.

Atentamente,

Fabián Cobos Alvarado
Vicerrector Académico

"liderando la formación tecnológica"

Dirección Teodoro Gómez S14 – 72 y Joaquín Gutiérrez – San Bartolo Telfs : 2910-513
Web: www.tecnologicosucre.edu.ec * mail: secretaria@tecnologicosucre.edu.ec
Its_sucre@hotmail.com Quito - Ecuador

INSTITUTO TECNOLÓGICO SUPERIOR SUCRE

Quito, 25 de julio de 2018

Oficio N° 168-REC-ITS SUCRE-2017

DE: PhD. Santiago Illescas
PARA: Ing. Flavio López
ASUNTO: Carta de aceptación "desarrollo del trabajo de titulación en el ITS Sucre"

Presente.-

El Ing. Flavio López, con cédula de identidad 1712353596, docente del Instituto Tecnológico Superior Sucre, con fecha 15 de diciembre de 2017, presentó el tema de proyecto "IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE INFORMACIÓN BASADA EN LAS NORMAS ISO/IEC 27001 Y 27002 EN EL INSTITUTO TECNOLÓGICO SUPERIOR SUCRE", previa a la obtención del título de cuarto nivel "Maestría en Gerencia Informática" de la Pontificia Universidad Católica del Ecuador Sede Ambato.

Una vez revisado el proyecto y con los antecedentes mencionados **SE ACEPTÓ Y SE AUTORIZÓ** el desarrollo de la implementación del proyecto mencionado en el ITS Sucre en la unidad de Titulación.

Particular que pongo en su conocimiento para los fines pertinentes.

Atentamente,

PhD. Santiago Illescas Correa
RECTOR DEL ITS SUCRE

"liderando la formación tecnológica"

Campus Norte (Matriz): Av. 10 de Agosto N28-27 y Luis Vásquez Narváez
Telef.: 02 2547-350, E- mail: secretaria@tecnologicosucre.edu.ec
Campus Sur: Av. Teodoro Gómez de la Torre S14 - 72 y Joaquín Gutiérrez Telef.: 02 2915-513
Web: www.tecnologicosucre.edu.ec
Quito - Ecuador

Apéndice D

Plan de Tratamiento para Riesgos Aceptables y Tolerables Unidad de Titulación ITSS

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
1. Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes 2. Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación 3. Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis 4. Afectación legal por pérdida de anillados o empastados de las tesis 5. Afectación legal por pérdida de actas consolidadas de titulación 13. Acceso no autorizado a los anaqueles en vicerrectorado por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo 15. Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 16. Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 19. Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico 20. Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico 21. Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur. 22.Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	Concienciar al personal de la Unidad de Titulación sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Establecer procedimientos para gestión segura de contraseñas para acceso a infraestructura, equipos de cómputo, sistemas de información y documentarlos	Definir una normativa para gestión de contraseñas	TIC	1/3/2018	1/4/2018
	Implementar políticas institucionales para el acceso físico de estudiantes, docentes, funcionarios del ITSS a instalaciones	Definir una normativa referente al uso obligatorio del carné institucional	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
		Establecer y ejecutar un cronograma para la carnetización de estudiantes, docentes y funcionarios	TIC con rector/ vicerrector	1/3/2018	1/5/2018
		Comunicar a personal de seguridad, estudiantes, docentes y funcionarios sobre la obligatoriedad del uso del carné para su control en ingresos/salidas de personas a instalaciones	Infraestructura	2/5/2018	9/5/2018
	Revisar/actualizar la política de acceso de personal externo al ITSS	Establecer una política de control de acceso al ITSS que contemple los permisos de acceso de exfuncionarios	Jurídico y Consejo Directivo	1/3/2018	1/4/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	Actividad	Responsable	Fecha inicio	Fecha final
1. Afectación legal por pérdida mediante sustracción de las carpetas que contienen información académica de los estudiantes 2. Afectación legal por pérdida mediante sustracción de documentación del proceso de titulación 3. Afectación legal por pérdida mediante sustracción de los CD que contienen los archivos digitales de las tesis 4. Afectación legal por pérdida de anillados o empastados de las tesis 5. Afectación legal por pérdida de actas consolidadas de titulación 13. Acceso no autorizado a los anaqueles en vicerrectorado por falta de seguros o candados en los mismos o falta de mecanismos de control de acceso físico a personal externo 15. Acceso no autorizado al área de anaqueles en la Unidad de Bienestar Estudiantil sede Norte por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 16. Acceso no autorizado al computador de secretaría (sede sur) por falta de mecanismos de control de acceso físico a personal externo y/o falta de control en la atención al público 19. Acceso no autorizado a información de calificaciones de exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico 20. Acceso no autorizado a promedios para graduación por ausencia de políticas de manejo confidencial de registro académico 21. Acceso no autorizado a formatos institucionales para generación de actas consolidadas de titulación por falta de controles para el uso del computador de secretaría sede sur. 22.Acceso a información confidencial física o digital de estudiantes y egresados por parte de excolaboradores del ITSS por falta de controles para eliminación de usuarios y políticas de acceso a la plantas físicas de personal retirado de la institución	Identificar la información crítica almacenada en las áreas de Secretaría Sede Sur y Bienestar Estudiantil Sede Norte y determinar, implementar y dar seguimiento a mecanismos que impidan el intento de hurto	Caracterizar la información crítica	Titulación	1/3/2018	1/4/2018
		Establecer políticas para el uso de llaves físicas o magnéticas de acceso a las instalaciones	Titulación con Secretaría Sur y Bienestar Norte	1/3/2018	1/4/2018
		Establecer políticas sobre acceso restringido de personal a las áreas de secretaría sur y bienestar norte en horarios de atención al público	Titulación con Secretaría Sur y Bienestar Norte	1/3/2018	1/4/2018
	Establecer políticas para la gestión adecuada de dispositivos móviles en las áreas de Secretaría Sur, Bienestar Estudiantil Norte, Coordinaciones de carrera	Chequear y actualizar las disposiciones sobre el manejo de dispositivos móviles en áreas sensibles	Rector/ vicerrector	1/3/2018	1/4/2018
	Establecer directrices tendientes a garantizar que la información de estudiantes y docentes no es accesible a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad para equipos de cómputo desatendidos	TIC	1/3/2018	1/4/2018
		Definir protocolos de escritorios limpios/ pantallas limpias	TIC	1/3/2018	1/4/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
6 . Afectación legal por pérdida de bancos de preguntas de los exámenes complexivos 17. Acceso no autorizado a información de calificaciones de defensas de tesis/temas de tesis por ausencia de políticas de manejo confidencial de registro académico 18. Acceso no autorizado a exámenes complexivos por ausencia de políticas de manejo confidencial de registro académico	Concienciar al personal de Coordinación de Carreras sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Identificar la información crítica almacenada en las áreas de cada una de las Coordinaciones de Carrera y determinar, implementar y dar seguimiento a mecanismos que impidan el intento de hurto	Caracterizar la información crítica	Cada Coordinación de Carrera	1/3/2018	1/4/2018
		Establecer políticas para el uso de llaves físicas o magnéticas de acceso a las instalaciones	Cada Coordinación de Carrera	1/3/2018	1/4/2018
		Establecer políticas sobre acceso restringido de personal a las áreas de secretaría sur y bienestar norte en horarios de atención al público	Cada Coordinación de Carrera	1/3/2018	1/4/2018
	Implementar políticas institucionales para el acceso físico de estudiantes, docentes, funcionarios del ITSS a instalaciones	Definir una normativa referente al uso obligatorio del carné institucional	Jurídico y Consejo Directivo	1/3/2018	1/4/2018
		Establecer y ejecutar un cronograma para la carnetización de estudiantes, docentes y funcionarios	TIC con rector/vicerrector	1/3/2018	1/5/2018
		Comunicar a personal de seguridad, estudiantes, docentes y funcionarios sobre la obligatoriedad del uso del carné para su control en ingresos/salidas de personas a instalaciones	Infraestructura	2/5/2018	9/5/2018
	Revisar/actualizar la política de acceso de personal externo al ITSS	Establecer una política de control de acceso al ITSS que contemple los permisos de acceso de exfuncionarios	Jurídico y Consejo Directivo	1/3/2018	1/4/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
7. Afectación legal por acceso no autorizado a cuentas de docentes del sistema SAO-P 8. Acceso a información confidencial de los estudiantes empleando contraseñas débiles generadas por default al momento de matricular a estudiantes 9.Afectación legal por alteración de calificaciones de estudiantes en el sistema SAO-P por acceso no autorizado a cuentas de docentes 10. Alteración de información de estudiantes o docentes en el sistema SAO-P por acceso no autorizado a cuentas de administrador	Establecer procedimientos documentados para la gestión segura y actualización periódica de contraseñas para acceso al sistema SAO-P	Definir procedimientos de creación segura/actualización de contraseñas	TIC	1/3/2018	1/4/2018
	Concienciar a estudiantes y docentes sobre los procesos de creación/actualización de contraseñas seguras de acceso al sistema de notas SAO-P	Establecer un cronograma de capacitaciones sobre claves seguras para estudiantes y docentes	Jurídico y TIC	2/4/2018	1/10/2018
26. Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil campus norte por falta de mantenimiento preventivo programado 27. Avería en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por no reporte de incidencias por parte del personal a cargo	Establecer canales de comunicación efectiva para la detección y atención oportuna de incidentes presentados en los equipos de cómputo	Definir protocolos para la comunicación de incidentes que faciliten su trazabilidad	TIC	2/4/2018	1/10/2018
	Implementar medidas que garanticen el adecuado funcionamiento de los equipos de cómputo	Elaborar cronogramas de mantenimiento preventivo de los equipos de cómputo			
28. Demora en la atención de usuarios por problemas en el acceso al sistema SAO-P para emisión de récords académicos	Establecer/ revisar medidas que permitan garantizar el adecuado funcionamiento del Sistema de calificaciones SAO-P	Revisar el SLA o Acuerdo de nivel de servicio entre el proveedor del sistema SAO-P y el ITSS	Jurídico y TIC	1/3/2018	1/4/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	**Actividad**	**Responsable**	**Fecha inicio**	**Fecha final**
25. Fallos en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte por uso inadecuado del recurso por parte del personal a cargo 29. Demora en la atención de usuarios por demoras en el proceso de ingreso de calificaciones de exámenes complexivos o de los trabajos teóricos (tesis) 32. Fallos o demoras en atención al público por afectación de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte 33. Afectación por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte a causa de uso inadecuado de los recurso por parte de personal a cargo 34.Afectación de las comunicaciones por infección de software malicioso en el equipo de cómputo de Secretaría sede Sur/Bienestar Estudiantil sede Norte que afecta los drivers de las respectivas tarjetas de red 45. Intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus 48. Fallos en el funcionamiento del equipo de cómputo de la Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte por instalación de software pirata, ocasionado por falta de políticas de gestión con proveedores y personal del ITSS	Controlar la efectividad de los procesos de inducción	Establecer mecanismos que permitan verificar la efectividad de los procesos de inducción	Recursos humanos y TIC	1/3/2018	1/7/2018
	Definir mecanismos que faciliten el uso adecuado de los recursos tecnológicos	Implementar un plan anual de capacitación para el uso idóneo de los recursos tecnológicos	Recursos humanos, TIC y Unidad de Capacitación	1/3/2018	31/12/2018
	Establecer mecanismos para medir el desempeño de funcionarios	Definir las competencias laborales a ser adicionadas en la evaluación del desempeño relativo al tratamiento de la información	Recursos humanos y TIC	1/3/2018	31/12/2018
30. Desatención de los equipos de procesamiento de datos y archivo por citaciones a reuniones constantes en horarios destinados a atención al público por parte de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte	Establecer directrices tendientes a garantizar que la información de estudiantes y docentes no es accesible a simple vista por personal no autorizado en las zonas de atención al público	Definir protocolos de seguridad para equipos de cómputo desatendidos	TIC	1/3/2018	1/4/2018
		Definir protocolos de escritorios limpios/ pantallas limpias	TIC	1/3/2018	1/4/2018
31. Entrega de papel membretado institucional a personal no autorizado por parte de Secretaría Sede Sur/ Bienestar Estudiantil Sede Norte	Concienciar al staff de funcionarios sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	Actividad	Responsable	Fecha inicio	Fecha final
35. Pérdida de carpetas físicas de estudiantes y egresados por ocurrencia de desastres naturales	Elaboración de mecanismos de prevención y respuesta a desastres naturales Establecer procedimientos de copia de seguridad	Establecimiento de un plan de continuidad del negocio Definir protocolos de copia de seguridad	TIC y Comisión de Gestión de Riesgos	1/3/2018	31/12/2018
36. Pérdida del equipo de cómputo e información digital por ocurrencia de desastres naturales					
41. Daño en archivos físicos, tesis física o digital o equipos de cómputo e información digital por fuego provocado					
37. Pérdida de las comunicaciones para reportes a la Senescyt o entidades externas por daños en los sistemas de comunicación por ocurrencia de desastres naturales			TIC		
38. Pérdida de información en el equipo de cómputo de Secretaría Sede Sur/Bienestar Estudiantil Sede Norte por fallos del fluido eléctrico	Establecer mecanismos que protejan a los dispositivos de subidas de voltaje y/o fallos en suministro de energía eléctrica Establecer procedimientos de copia de seguridad	Incluir un plan de adquisiones de UPS, planta eléctrica y plan de mantenimiento de tendido eléctrico Definir protocolos de copia de seguridad	TIC, Coordinación de carrera de Electricidad y Gestión de Riesgos	1/3/2018	31/12/2018
40. Retrasos en el proceso de generación de certificados académicos / actas consolidadas de titulación por fallos del fluido eléctrico			TIC		
42. Afectación física en el personal de la Unidad de Titulación por fuego provocado y ausencia de planes de contingencia y/o rutas adecuadas de evacuación	Elaboración de mecanismos de prevención y respuesta a desastres naturales	Establecimiento de un plan de continuidad del negocio	TIC, Comisión de Titulación y Comisión de Gestión de Riesgos	1/3/2018	31/12/2018
43. Deterioro de expedientes de estudiantes y egresados, así como tesis físicas debido a corrosión provocada por humedad	Establecer mecanismos que protejan la información física y los dispositivos almacenados en vicerrectorado y sala de lectura sur y bienestar estudiantil norte de corrosión provocada por humedad	Incluir en el plan de adquisiones un plan de mantenimiento de infraestructura de las instalaciones involucradas	Rector/ vicerrector	1/3/2018	31/12/2018

Escenario de riesgo	Plan de tratamiento de riesgos para riesgos aceptables y tolerables				
	Estrategia	Actividad	Responsable	Fecha inicio	Fecha final
44. Incumplimiento en reportes de graduados a Senescyt y otros organismos de control por fallos en dispositivos que permiten acceso al servicio de Internet	Establecer/ revisar medidas que permitan garantizar el adecuado funcionamiento del servicio de internet	Revisar los contratos de prestación de servicios de conectividad entre los ISPs y el ITSS	Jurídico y TIC	1/3/2018	1/4/2018
46. Divulgación de información académica de estudiantes en proceso de titulación por medio de prácticas inadecuadas de desecho de información 47. Divulgación de información de estudiantes en proceso de titulación por falta de políticas y mecanismos para la adecuada disposición de desechos	Concienciar al personal de la Unidad de Titulación sobre la importancia de la preservación segura de la información	Establecer un cronograma de capacitaciones sobre protección de información para docentes	Recursos humanos y jurídico	1/3/2018	10/11/2018
	Establecer mecanismos que garanticen la adecuada disposición de residuos documentales	Incluir en el plan de adquisiones la compra de un triturador de papel	Rector/ vicerrector	1/3/2018	31/12/2018
	Establecer mecanismos que garanticen que la información desechada en medios físicos o digitales es tratada adecuadametne	Definir políticas para el tratamiento de desechos que pudieran poner en riesgo la información confidencial de los estudiantes del ITSS	TIC	1/3/2018	31/12/2018
50. Demoras en el restablecimiento de servicios de consulta o gestión de procesos de titulación por fallos relacionados a extracción/restablecimiento de copias de seguridad	Establecer protocolos para generar y probar copias de seguridad en las áreas involucradas con Titulación	Definir el protocolo para extracción y prueba de copias de seguridad, almacenamiento y ejecución	TIC	1/3/2018	31/12/2018
	Disponer de los medios de almacenamiento para copias de seguridad	Incluir en el plan de adquisiones los dispositivos necesarios para el almacenamiento de copias de seguridad	Rector/ vicerrector	1/3/2018	31/12/2018

Fuente: Adaptación de (Benavides Sepúlveda & Blandón Jaramillo, 2017)

Apéndice E

Diagnóstico final una vez implementada la Gestión de Riesgos de Seguridad de la Información en el ITSS

DIAGNÓSTICO SGSI LOGRO 1: DEFINICIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)				
Por favor, conteste la siguiente encuesta de **acuerdo con el instructivo.**				
PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información]?	Cumple satisfactoriamente	La implementación de la metodología de gestión de riesgos de información da cumplimiento a este requerimiento	Diligenciar autodiagnostico de seguridad de la informacion.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	Cumple satisfactoriamente	El caso de estudio está pormenorizado en la investigación aplicada a la Unidad de Titulación del ITSS	Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple parcialmente	Acta de reunión y aprobación para inicio de proyecto SGSI	Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	Cumple parcialmente	Actas de reuniones de la comisión de las TIC, evidencia digital en posesión del coordinador	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Plan de trabajo con rectorado, en actas que reposan en rectorado del ITSS	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	La evaluación consta en el documento de investigación	Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Cómite de Seguridad de la Información?	Cumple parcialmente	Se ha designado a la persona responsable de salvaguardar la seguridad de la información en el ITSS en acta respectiva aprobada por Consejo Académico Superior (CAS)	Definir mediante acto administrativo el comite de seguridad de la informacion que describa las responsabilidades de los integrantes, reuniones entre otros.
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	Cumple satisfactoriamente	Consta en Acta signada por las autoridades, en una primera fase orientada a Gestión de Riesgos para posteriormente ir hacia SGSI	Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.

PLANEAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple		Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple		Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	Cumple satisfactoriamente	Consta en el documento de la Metodología de Gestión de Riesgos de Información, capítulos 4 y 5	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	Cumple satisfactoriamente	Consta en el documento de la Metodología de Gestión de Riesgos de Información, capítulos 4 y 5	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	Cumple parcialmente	Consta en el documento de la Metodología de Gestión de Riesgos de Información, capítulos 4 y 5	Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	No cumple	Se utiliza correo electrónico institucional	Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	Pendiente	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.
Fuente: NTE-INEN-ISO-IEC 27001:2014				

AUTODIAGNÓSTICO SGSI LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30 %)

Por favor, conteste la siguiente encuesta de acuerdo con el instructivo.

VERIFICAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de laInformación.?	Cumple satisfactoriamente	Consta en el documento de la Metodología de Gestión de Riesgos de Información, capítulos 4 y 5	Se debe tener en cuenta que se desea medir, cuando, quien realizará la medicióny cuando se analizaran los resultados.
2	La entidad ha realizado auditorias internas al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Se tiene un esquema de trabajo de monitoreo crítico continuo a la Gestión de Riesgos de Seguridad de la Información	Se deben programar auditorias en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la Información.
3	La entidad cuenta con programas de auditorias aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	Cumple parcialmente	Se tiene un esquema de trabajo de monitoreo crítico continuo a la Gestión de Riesgos de Seguridad de la Información	Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periodicas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe todavía un SGSI	Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	Cumple parcialmente	Se tiene un esquema de trabajo de monitoreo crítico continuo a la Gestión de Riesgos de Seguridad de la Información	
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	No existe todavía un SGSI	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluacion de las no conformidades y acciones correctivas. Esta

AUTODIAGNÓSTICO SGSI LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30 %)

Por favor, conteste la siguiente encuesta de acuerdo con el instructivo.

ACTUAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoria?	Cumple parcialmente	Se tiene implementado un Plan de tratamiento de riesgos donde se gestiona los riesgos de mayor importancia, incluyendo aquellos relacionados con no conformidades iniciales	Se deben tomar acciones para eliminar las causas de las no conformidades, para que no vuelvan a ocurrir.
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	Cumple parcialmente	Se tiene implementado un Plan de tratamiento de riesgos donde se gestiona los riesgos de mayor importancia, incluyendo aquellos relacionados con no conformidades iniciales	Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	La entidad revisa la eficiacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	Cumple parcialmente	El plan de tratamiento de riesgos está bajo supervisión de autoridades	Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información despues de las acciones tomadas?	No cumple	No existe un SGSI	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	No cumple	No existe un SGSI	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	No existe un SGSI, pero se hace mejora continua a Gestión de Riesgos	Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: NTE-INEN-ISO-IEC 27001:2014

Fuente: Adaptación de (Alta Consejería Distrital de TIC, 2015)

Referencias

Alta Consejería Distrital de TIC. (2015). Autodiagnóstico SGSI. Bogotá D.C., Colombia. Obtenido de http://ticbogota.gov.co/sites/default/files/documentos/AutodiagnosticoSGSI_v2_09072015.xls

Asamblea Nacional Constituyente. (2008). Constitución Política de la República del Ecuador. Montecristi: Registro Oficial.

Asamblea Nacional de la República del Ecuador. (2010). LOES, Ley Orgánica de Educación Superior. QUITO: Registro Oficial.

Benavides Sepúlveda, A. M., & Blandón Jaramillo, C. A. (2017). Modelo de Sistema de Gestión de Seguridad de la Información basado en la norma NTC ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna Universidad de la Ciudad de Pereira. Manizales, Colombia: Universidad Autónoma de Manizales.

Carnegie Mellon University, SEI (Software Engineering Institute). (2005). OCTAVE v2.0 (2a. ed.). Estados Unidos: Carnegie Mellon University. Obtenido de http://www.cert.org/resilience/products-services/octave/index.cfm

Da Silva Netto, A., & Pinheiro da Silveira, M. A. (22 de septiembre de 2007). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. Revista de Gestão da Tecnologia e Sistemas de Informação(No. 3), 375-397.

Espasa Calpe, S. (2005). Diccionario de la lengua española. Madrid: Espasa.

Federal Office for Information Security (BSI). (2005). IT-Grundschutz (2a. ed.). Berlin: BSI.

Freire Zapata, F. (2014). Implementación del modelo de gestión de la seguridad de la información aplicando ISO 27000 en la empresa Coka Tours, Ambato-Ecuador. Quito, Ecuador: Universidad Central del Ecuador.

Gutierrez Espinosa, M. (2013). Curso La seguridad aeroportuaria. Obtenido de https://es.slideshare.net/hymcupcakes/curso-la-seguridad-aeroportuaria

Hideo Ohtoshi, P. (2008). Análise comparativa de metodologias de gestao e de analise de riscos sob a ótica da norma NBR-ISO/IEC 27005. Brasilia: Universidade de Brasília.

INEN Servicio Ecuatoriano de Normalización. (2014). Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27001: 2014. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI)requisitos. Quito , Ecuador: Instituto Ecuatoriano de Normalización INEN.

INEN, Instituto Ecuatoriano de Normalización. (2014). Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27002: 2014. Tecnología de la información. Código de práctica para la gestión de la seguridad de la información. Quito: INEN, Instituto Ecuatoriano de Normalización.

Insight Consulting. (2003). CRAMM (CCTA Risk Analysis and Management Method) (5a. ed.). Reino Unido: British CCTA (Central Communication and Telecommunication Agency).

Instituto Ecuatoriano de Normalización. (2012). Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27005: 2012. Tecnología de la información. Gestión del riesgo de la seguridad de la información. Quito, Ecuador: INEN, Instituto Ecuatoriano de Normalización.

Instituto Tecnológico Superior Sucre. (2016). Plan Estratégico de Desarrollo Institucional (1era ed.). Quito: ITSS.

ISO /IEC . (2016). International Standard ISO /IEC 27000: 2016 - Information technology - Security techniques - Information security management systems - Overview and vocabulary (4a ed.). Geneva, Switzerland: ISO copyright office.

ISOTools. (19 de marzo de 2015). www.isotools.org. Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

ISOTools Excellence. (31 de enero de 2014). ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

ISOTools Excellence. (5 de enero de 2017). ISO 27005: ¿Cómo identificar los riesgos? Obtenido de http://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

ITS Sucre. (2017). ITS SUCRE MISION Y VISION. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/instituto/mision-y-vision

ITS Sucre. (2017). Programas académicos. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/

ITS Sucre. (2018). Técnico en Atención Primaria de Salud. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/duales/atencion-primaria-de-salud

ITS Sucre. (2018). Tecnología en Desarrollo Infantil Integral. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/duales/desarrollo-infantil-integral

ITS Sucre. (2018). Tecnología en Gestión Ambiental. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/tradicionales/gestion-ambiental

ITS Sucre. (2018). Tecnología en Producción y Realización Audiovisual. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/tradicionales/produccion-y-realizacion-audiovisual

ITS Sucre. (2018). Tecnología Superior en Electricidad. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/tradicionales/electricidad

ITS Sucre. (2018). Tecnología Superior en Electromecánica. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/tradicionales/electromecanica

ITS Sucre. (2018). Tecnología Superior en Electrónica. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/tradicionales/electronica

ITS Sucre. (2018). Tecnología Superior en Producción Textil. Obtenido de http://www.tecnologicosucre.edu.ec/web/index.php/en/programas-academicos/duales/produccion-textil

La República. (6 de abril de 2017). Correa acusa a hackers de EE.UU. de atacar web del Consejo Nacional Electoral. La República, pág. 1. Obtenido de http://www.larepublica.ec/blog/politica/2017/04/06/correa-hackers-ee-uu-atacar-web-cne/

Mantilla Guerra, A. R. (2009). Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001. Quito, Ecuador: Escuela Politécnica Nacional.

Ministerio de Administraciones Públicas. (2005). MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (2a. ed.). España: Ministerio de Administraciones Públicas. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WYjGGZe0nIU

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2016). Guía de Gestión de Riesgos (3ra ed.). Bogotá, Colombia: MinTIC.

Ministerio de Salud Pública, MSP. (12 de 06 de 2014). Política de seguridad de la información - Resguardo de contraseñas. Obtenido de http://instituciones.msp.gob.ec/somossalud/index.php/100-intranet/guia-del-usuario/572-politica-de-seguridad-de-la-informacion-resguardo-de-contrasenas

Ministerio de Tecnologías de la Información y las Comunicación, MinTIC. (29 de Julio de 2016). Modelo de Seguridad y Privacidad de la Información MSPI. Obtenido de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

National Institute for Standards and Technology (NIST). (2002). Risk Management Guide for Information Technology systems. Estados Unidos.

Oliveira, M. S. (2015). Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica, 6. Obtenido de http://periodicos.unifacef.com.br/index.php/resiget/article/download/1065/848

Ormella Meyer , C. (2014). Las nuevas versiones de las normas ISO 27001 e ISO 27002. Buenos Aires: Universidad del Museo Social Argentino. Obtenido de http://www.criptored.upm.es/guiateoria/gt_m327k.htm

Ortiz, S. (09 de enero de 2016). Hackers registraron 366 títulos universitarios en la Senescyt y entregaron 600 licencias de conducir. El Comercio. Obtenido de http://www.elcomercio.com/actualidad/hackers-registraron-titulos-universitarios-falsos.html

Ramírez Castro, A., & Ortiz Bayona, Z. (15 de Agosto de 2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56-66.

Rodríguez Gahona , G., & Villa Sánchez, P. (2014). Aplicación de metodologías de generación de política de gestión de riesgos en Seguridad de la Información como caso de estudio de una empresa de teleinformática en la ciudad de Bogotá D.C. Risaralda: Universidad Tecnológica de Pereira.

Romo , D., & Valarezo, J. (2012). Análisis e implementación de la norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil. Guayaquil: Universidad Politécnica Salesiana.

Secretaría Nacional de la Administración Pública. (2013). Esquema Gubernamental de la Seguridad de la Información EGSI (1era ed.). Quito, Ecuador: Registro Oficial.

Suárez Altamirano, V. (2017). Procedimiento metodológico para la implementación de un customer relationship management en el control de servicios educativos del Instituto Tecnológico Superior "Luis A. Martínez". Ambato: PUCESA.

Torres Bermúdez, A. (2010). Introducción a la seguridad informática. Bogotá.

Resumen Final

Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre.

Flavio Eduardo López Vasco

137 páginas

Proyecto dirigido por Ing. Javier Wilfrido Cóndor Cruz, Mtr.

El objetivo de esta investigación es implementar una metodología basada en las normas internacionales ISO/IEC 27001 y 27002 para la gestión de riesgos de información en el Instituto Tecnológico Superior "Sucre" [ITSS] de la ciudad de Quito, para dar cumplimiento al acuerdo N° 166 emitido por la Secretaría Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la Información. El proyecto se sustenta en la inexistencia de una Gestión de Riesgos de Seguridad de la Información, evidenciada a través de estrategias de seguridad de información ineficaces. El marco teórico analiza tanto normas de gestión de seguridad de la información como metodologías internacionales de gestión de riesgos de información. El proyecto es de intervención porque actúa materialmente de manera directa sobre un problema específico y la investigación es de tipo aplicada, cuasiexperimental, de nivel aplicativo, porque opera variables. El resultado del diagnóstico inicial de seguridad de la información en el ITSS, de 13% de conformidad respecto a ISO 27001, evidencia la poca importancia que recibía. Un procedimiento metodológico para la gestión de riesgos de información se adaptó y validó en el instituto, lo cual arrojó un nivel de conformidad de 38, 7%.

Este trabajo propone las bases para futuras iniciativas en seguridad de la información que puedan ser implementadas en otros institutos tecnológicos superiores.