UNIVERSIDAD PRIVADA ANTENOR ORREGO

ESCUELA DE POSTGRADO

FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT.

TESIS

PARA OBTENER EL GRADO DE MAESTRO EN GERENCIA EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.

AUTOR:

Jara Arenas, Jorge Antonio

ASESOR:

Sagástegui Chigne, Teobaldo Hernán

Fecha de sustentación: 2019-09-20

Trujillo - Perú

2019

DEDICATORIA

A nuestro divino señor que nos guía
por el camino del amor y el respeto
a nuestros seres queridos como
parte de su enseñanza.

A mi hija Nicole Alessandra
que es el tesoro más preciado que
me llena de alegría hasta en los momentos
más difíciles.

A mis padres Máximo y Aguedita
aunque no les tengo físicamente a mi
lado siempre vivirán y estarán en mi corazón.

AGRADECIMIENTOS

El presente trabajo de investigación no hubiera sido posible sin la ayuda valiosa y para quien va mi agradecimiento especial: A un excelente maestro y asesor Dr. Teobaldo Hernán Sagástegui Chigne por orientarme y apoyarme con sus conocimientos y consejos necesarios para la culminación de la presente tesis.

A mi novia que me apoyo con su espíritu de perseverancia en este proceso.

RESUMEN

La presente investigación titulada "FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT", desarrolla un Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT en su versión piloto - Servicios de Matrícula, Notas y Asignaturas -.

El Framework propuesto hace posible la implementación de manera gradual de los controles de seguridad. Esto en el contexto de la Universidad Pública que requiere de mayor flexibilidad en aspectos que atañen a la alta dirección como la formalización de una estructura orgánica responsable de gestionar la Seguridad de la Información. Considerando esto, se decidió implementar el uso del Framework en una versión piloto. En esta primera ejecución se implementó el software de Gestión de Incidentes de Seguridad de la Información, lo cual permitió elevar el nivel de cumplimiento a 72 % del dominio 16: "Gestión de Incidentes en la Seguridad de la Información".

Se cumplió con el objetivo de diseñar y desarrollar un Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT en su versión piloto y se recomienda incorporarlo formalmente a la institución para seguir avanzando en la madurez de la cultura institucional de seguridad de la información.

Propiciando la fiabilidad del marco de trabajo, Se desarrolló un prototipo de soporte al Framework de seguridad de la información, el cual consta de 11 historias de usuario y 13 clases que permitirán registrar las fases y actividades del Framework. En la documentación se describen las historias y se diseñaron pantallas que facilitaran el desarrollo de la aplicación.

Por el Br. Jorge Antonio Jara Arenas

Palabras clave: *Framework de seguridad de la información, Proceso Académico, Seguridad de la Información*

ABSTRACT

The present research entitled "FRAMEWORK OF INFORMATION SECURITY BASED ON THE CONTROLS OF ISO 27002 FOR THE ACADEMIC PROCESS OF THE UNT", development an Information Security Framework based on the controls of the ISO 27002 of Information Security Management for the UNT academic processes in its pilot version – Services of Enrollment, Notes and Subjects –.

The proposed Framework makes possible the gradual implementation of security controls. This in the context of the Public University that requires greater flexibility in aspects that concern senior management as the formalization of an organizational structure responsible for managing Information Security. Considering this, it was decided to implement the use of the Framework in a pilot version. In this first execution, the Information Security Incident Management software was implemented, which allowed raising the level of compliance to 72% of domain 16: "Incident Management in Information Security".

The objective of designing and developing an Information Security Framework based on the controls of ISO 27002 for Information Security Management for the UNT academic processes in its pilot version was complied with and it is recommended to formally incorporate it into the institution to continue advancing in the maturity of the institutional culture of information security.

Enabling the reliability of the framework, a prototype was developed to support the Information Security Framework, which consists of 11 user stories and 13 classes that will record the phases and activities of the Framework. In the documentation the stories are described and screens were designed to facilitate the development of the application.

By Br. Jorge Antonio Jara Arenas

Keywords: *Information security framework, Academic Process, Information Security*

ÍNDICE

DEDICATORIA **2**

AGRADECIMIENTOS **3**

RESUMEN **4**

ABSTRACT **5**

ÍNDICE **6**

ÍNDICE DE FIGURAS **10**

ÍNDICE DE TABLAS **12**

CAPÍTULO I: INTRODUCCIÓN **14**

1.1. FOCALIZACIÓN DEL PROYECTO **14**
1.2. EL PROBLEMA **15**
1.3. ENUNCIADO DEL PROBLEMA **18**
1.4. ALCANCE **18**
1.5. JUSTIFICACIÓN **19**
1.5.1. JUSTIFICACIÓN ACADÉMICA **19**
1.5.2. JUSTIFICACIÓN TECNOLÓGICA **19**
1.6. VIABILIDAD **19**
1.7. APORTE **20**
1.8. HIPÓTESIS **20**
1.9. OBJETIVOS **20**
1.9.1. OBJETIVO GENERAL **20**
1.9.2. OBJETIVOS ESPECÍFICOS **20**

CAPÍTULO II: MARCO TEÓRICO **23**

2.1. ANTECEDENTES **23**
2.2. MARCO TEÓRICO **29**
2.2.1. SEGURIDAD DE LA INFORMACIÓN **29**
2.2.2. POLÍTICAS DE SEGURIDAD **33**
2.2.3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) **33**
2.2.4. ISO 27001 ..... **35**
2.2.5. ISO 27002 ..... **37**

2.2.6. GESTIÓN ACADÉMICA **41**
2.3. MARCO CONCEPTUAL **41**
2.3.1. LA MATRIZ DE FORTALEZAS, OPORTUNIDADES, DEBILIDADES, Y AMENAZAS (FODA) **41**
2.3.2. CICLO PDCA **43**
2.3.3. GESTIÓN DE RIESGOS **45**
2.3.4. INFORMACIÓN *48*
CAPÍTULO III: MATERIAL Y MÉTODOS **50**
3.1. MATERIAL Y PROCEDIMIENTO: **50**
3.1.1. MATERIAL **50**
3.1.2. PROCEDIMIENTOS **50**
3.1.2.1. DISEÑO DE TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN **50**
3.1.2.2. TÉCNICAS E INSTRUMENTOS **51**
3.1.2.2.1. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS *51*
3.1.2.2.2. TÉCNICAS E INSTRUMENTOS DE PROCESAMIENTO Y ANÁLISIS DE DATOS ... **52**
3.1.3. METODOLOGÍA **53**
VARIABLES Y OPERATIVIZACIÓN DE VARIABLES **53**
CAPÍTULO IV: RESULTADOS **56**
4.1. OBJETIVO 1: HACER UN ANÁLISIS DEL ENTORNO TANTO INTERNO COMO EXTERNO DE LA UNT USANDO LA MATRIZ FODA PARA DETERMINAR LAS FORTALEZAS, DEBILIDADES, OPORTUNIDADES Y AMENAZAS, RELEVANDO LO QUE CORRESPONDE A LOS PROCESOS ACADÉMICOS QUE SE RELACIONAN CON LA GESTIÓN DE LA INFORMACIÓN Y SON SUSCEPTIBLES DE DESTRUCCIÓN, SABOTAJE, FRAUDE, VIOLACIÓN DE LA PRIVACIDAD, INTRUSISMO, ETC. **56**
4.2. OBJETIVO 2: EVALUAR LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA ISO 27002 DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA INFORMACIÓN DE LOS PROCESOS ACADÉMICOS DE LA UNT EN SU VERSIÓN PILOTO - SERVICIOS DE MATRÍCULA, NOTAS Y ASIGNATURAS..... **63**
4.3. OBJETIVO 3: DISEÑAR EL NUEVO FRAMEWORK DE GESTIÓN DE LA INFORMACIÓN DE LOS PROCESOS ACADÉMICOS DE LA UNT BASADO EN LOS CONTROLES DE LA ISO 27002 DE GESTIÓN. **66**

4.4. OBJETIVO 4: DESARROLLAR UN PROTOTIPO DE SOPORTE AL FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS ACADÉMICOS DE LA UNT 69

4.4.1. MARCO DE TRABAJO SCRUMBAN 69

4.4.1.1. REQUERIMIENTOS 69

4.4.1.2. VISIÓN 70

4.4.1.3. HISTORIAS DE USUARIO Y FIREWORK 70

4.4.1.4. BACKLOG DEL PRODUCTO 81

4.4.1.5. SPRINT BACKLOG 81

4.4.1.6. TABLERO SCRUMBAN 82

4.4.2. ARQUITECTURA 83

4.4.2.1. DIAGRAMA DE CASOS DE USO 83

4.4.2.2. DIAGRAMA DE CLASES 84

4.4.2.3. DIAGRAMA DE COMPONENTES VISTA GENERAL 85

4.4.2.4. ARQUITECTURA RELEASE 01: SEGURIDAD DEL SISTEMA 86

4.4.2.5. ARQUITECTURA RELEASE 02: GESTIÓN DEL FRAMEWORK DE SEGURIDAD 87

4.5. OBJETIVO 5: HACER LAS PRUEBAS DE FUNCIONALIDADES EN LA VERSIÓN PILOTO DEL PROCESO ACADÉMICO - SERVICIOS DE MATRÍCULA, NOTAS Y ASIGNATURAS – PARA LAS MEDICIONES PERTINENTES. 89

CAPÍTULO V: DISCUSIÓN 95

5.1. ANÁLISIS DE LOS RESULTADOS 95

EN LOS RESULTADOS SE HAN IDENTIFICADO ESTRATEGIAS QUE TIENEN UNA ALTA RELACIÓN CON LA SEGURIDAD DE LA INFORMACIÓN Y, POR LO TANTO, PUEDEN SER SUSCEPTIBLES DE EVENTOS NO DESEADOS COMO DESTRUCCIÓN, SABOTAJE, FRAUDE, VIOLACIÓN DE LA PRIVACIDAD, INTRUSISMO, ETC. 95

5.2. CONTRASTACIÓN DE LA HIPÓTESIS 98

CONCLUSIONES 102

RECOMENDACIONES 103

REFERENCIAS BIBLIOGRÁFICAS 104

ANEXOS 108

ANEXO1: CUESTIONARIO APLICADO AL RESPONSABLE DE TI 109

ANEXO2: CUESTIONARIO APLICADO A LOS RESPONSABLES DE LOS SERVICIOS DEL PROCESO ACADÉMICO 111
ANEXO3: SOLICITUDES PARA EJECUTAR LA SENSIBILIZACIÓN DEL SOFTWARE DE GESTIÓN DE INCIDENTES 113
ANEXO4: CRONOGRAMA DE SENSIBILIZACIÓN DEL SOFTWARE DE GESTIÓN DE INCIDENTES AL PERSONAL DE LOS SERVICIOS DEL PROCESO ACADÉMICO 116
ANEXO5: SENSIBILIZACIÓN DEL SOFTWARE DE GESTIÓN DE INCIDENTES AL PERSONAL DE LOS SERVICIOS DEL PROCESO ACADÉMICO 117
ANEXO6: ACTAS DE SENSIBILIZACIÓN EN EL SOFTWARE DE GESTIÓN DE INCIDENTES AL PERSONAL DE LOS SERVICIOS DEL PROCESO ACADÉMICO 119
ANEXO7: ORGANIGRAMA DE LA UNIVERSIDAD NACIONAL DE TRUJILLO..... 123

ÍNDICE DE FIGURAS

FIGURA 1: ÁMBITO DE LA ESPECIALIDAD DE SISTEMAS DE INFORMACIÓN……14
FIGURA 2: MODELO ACTUAL Y EVOLUTIVO DE LA SEGURIDAD DE LA INFORMACIÓN 30
FIGURA 3: PRINCIPIOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN 31
FIGURA 4: ESTRUCTURA DE LA NORMA ISO 27001. 36
FIGURA 5: NORMA ISO 27002 38
FIGURA 6: MATRIZ FODA 42
FIGURA 7: CICLO PDCA 44
FIGURA 8: ACTIVO, AMENAZA, VULNERABILIDAD E IMPACTO 45
FIGURA 9: FASES DE IDENTIFICACIÓN DE RIESGOS 47
FIGURA 10: GRADO DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA ISO 27002 PARA EL SERVICIO DE MATRÍCULA. 63
FIGURA 11: GRADO DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA ISO 27002 PARA EL SERVICIO DE NOTAS 64
FIGURA 12: GRADO DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA ISO 27002 PARA EL SERVICIO DE GESTIÓN DE ASIGNATURAS. 65
FIGURA 13: MARCO DE TRABAJO BASADO EN LOS CONTROLES DE LA ISO 27002..... 67
FIGURA 14: REGISTRAR DATOS DE EMPRESA EVALUADA. 71
FIGURA 15: REGISTRAR USUARIOS DEL SISTEMA. 72
FIGURA 16: ADMINISTRAR ACCESOS DEL SISTEMA. 73
FIGURA 17: REGISTRAR LA FASE PLANIFICAR..... 74
FIGURA 18: REGISTRAR LA FASE HACER. 76
FIGURA 19: REGISTRAR LA FASE VERIFICAR. 78
FIGURA 20: REGISTRAR LA FASE ACTUAR. 80
FIGURA 21: TABLERO SCRUMBAN..... 82
FIGURA 22: DIAGRAMA DE CASOS DE USO. 83
FIGURA 23: DIAGRAMA DE CLASES..... 84
FIGURA 24: DIAGRAMA DE COMPONENTES VISTA GENERAL. 85
FIGURA 25: ARQUITECTURA RELEASE 01: SEGURIDAD DEL SISTEMA..... 86
FIGURA 26: ARQUITECTURA RELEASE 02: GESTIÓN DEL FRAMEWORK DE SEGURIDAD... 87
FIGURA 27: SOFTWARE DE GESTIÓN DE INCIDENTES. 88
FIGURA 28: PANEL DE ACCESO AL SOFTWARE DE GESTIÓN DE INCIDENTES..... 88
FIGURA 29: LISTA DE USUARIOS DEL SOFTWARE DE GESTIÓN DE INCIDENTES..... 89

FIGURA 30: RESULTADOS DE PRUEBA NO PARAMÉTRICA. 100

ÍNDICE DE TABLAS

TABLA 1: GRADO DE CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA ISO 27002 PARA LOS SERVICIOS DE MATRÍCULA, NOTAS Y ASIGNATURAS. 65
TABLA 2: DESCRIPCIÓN DE ACTIVIDADES DEL MARCO DE TRABAJO BASADO EN LOS CONTROLES DE LA ISO 27002 DE GESTIÓN. 67
TABLA 3: INCIDENTES REGISTRADOS EN EL PROTOTIPO EN UN PERÍODO DE 30 DÍAS. 89
TABLA 4: ANÁLISIS DE ESTRATEGIAS ASOCIADAS A LA SEGURIDAD DE LA INFORMACIÓN. 95
TABLA 5: GRADO DE CUMPLIMIENTO RESUMEN DE LOS CONTROLES DE LA NORMA ISO 27002. 96
TABLA 6: INCIDENTES REGISTRADOS POR EL SOFTWARE DE GESTIÓN DE INCIDENTES EN LA VERSIÓN PILOTO. 98
TABLA 7: NIVEL DE CUMPLIMIENTO ANTES (AI) Y DESPUÉS DE LA IMPLANTACIÓN (DI) DEL FRAMEWORK. 99

CAPÍTULO I

INTRODUCCIÓN

"La educación es el arma más poderosa que puedes usar para cambiar el mundo"

Nelson Mandela.

CAPÍTULO I: INTRODUCCIÓN

1.1. FOCALIZACIÓN DEL PROYECTO

ACM (2006) publicó un informe que describe las cinco sub-disciplinas informáticas: Ingeniería Informática, Ciencias de la Computación, Sistemas de información, Tecnología de información e Ingeniería de software.

(ACM/IEEE, 2017) describe la disciplina de tecnología de la información como la integración, desarrollo y administración de tecnologías informáticas seguras que cumplan con las necesidades comerciales de la organización y en consecuenta los sistemas informáticos deben funcionar de manera adecuada considerando como base uno de los cinco pilares claves como es la seguridad de la información, con el objetivo de hacer frente a las amenazas que pueden generar un daño en las organizaciones.

En este sentido y considerando la naturaleza de la presente tesis de investigación, se concluye que la tesis esta focalizada en la disciplina de Tecnologías de Información haciendo enfasis en la seguridad de sistemas de información en organizaciones indistintamente, como se muestra en la Figura 1.

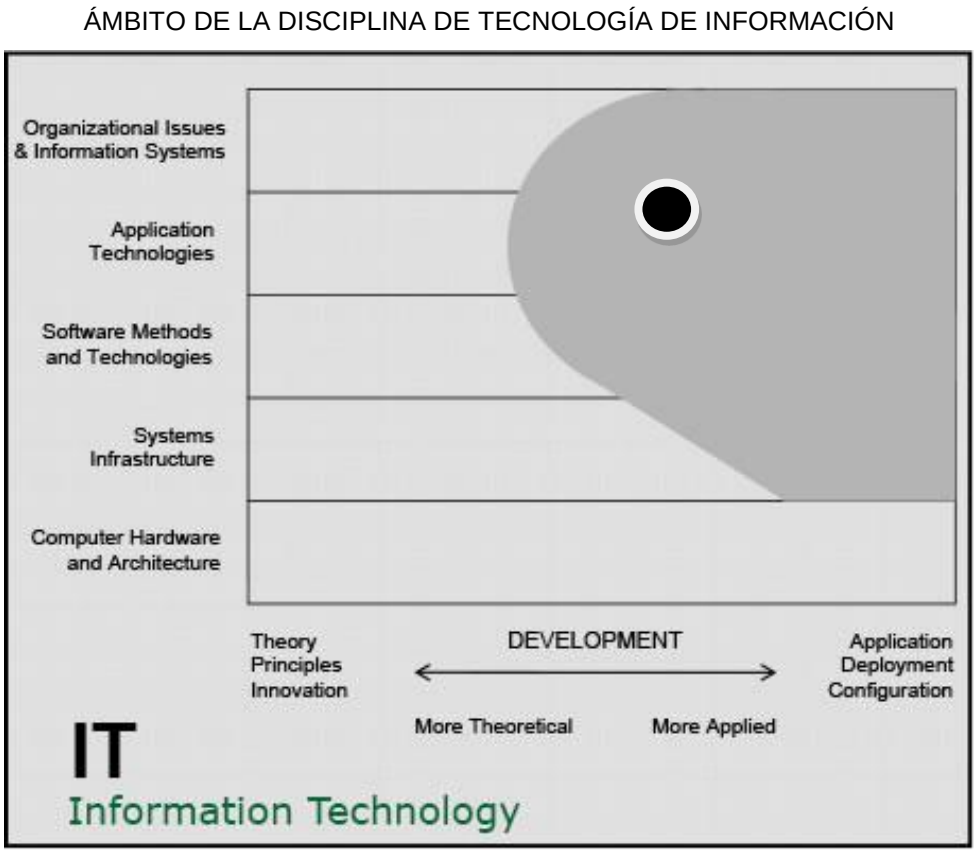


Figura 1: Ámbito de la especialidad de Tecnología de Información. Fuente: (ACM, 2006)

1.2. EL PROBLEMA

Durante los últimos años, en cualquier organización, las tecnologías digitales han cambiado el modo de interacción con los sistemas de información. Por ejemplo, la conexión de productos o servicios a Internet, permite procesar, almacenar o compartir información de estos, de manera inmediata y global. Dentro de este contexto, se ha llegado a considerar la seguridad de los sistemas de información como un componente clave cada vez más necesario en el desarrollo económico de una organización (Areitio , 2008).

Acosta (2018) presenta en su informe de resultados de la 20 Encuesta Global de Seguridad de Información 2017-2018 que solo el 4% de las organizaciones a nivel global y 3% en el Perú se sienten seguras de haber considerado completamente las implicancias de seguridad de la información en su estrategia actual y que el 43% de las empresas a nivel global no cuentan con estrategias o planes de comunicación para recuperarse de un ataque cibernético. Los dispositivos de interconexión, la innovación de los procesos y la transformación digital, están cada día más presentes y con ello han aparecido nuevas amenazas de seguridad de información. Por lo tanto, las empresas deben desarrollar nuevas estrategias para poder enfrentar a las crecientes amenazas cibernéticas. Las organizaciones están cada vez más interconectadas con la implementación de nuevas tecnologías que generan ventajas competitivas, pero al mismo tiempo riesgos en toda la cadena de valor. Las organizaciones deben considerar la seguridad de la información como un componente principal de la estrategia y cultura empresarial para permitir que toda la organización pueda comprender las amenazas que enfrentan para poder mitigar los riesgos. Las amenazas pueden extenderse desde interrupciones del sistema hasta fuga de información en todos los niveles generando un gran impacto en la organización.

Para Pwc (2018), la mayoría de las organizaciones buscan tecnologías emergentes para desarrollar nuevos servicios o productos, pero no están considerando de forma proactiva las estrategias de seguridad frente a nuevas amenazas de ciberseguridad que podrían poner en riesgo estos sistemas una vez que se implementan. La estrategia de gestión de riesgos de una empresa debe basarse en una clara comprensión de las amenazas cibernéticas a las que se enfrenta la organización y un conocimiento de qué

activos importantes requieren la mayor protección. Debe haber un marco de trabajo de riesgo coherente.

En enero del 2016 la Presidencia del Consejo de Ministros emitió la Resolución Ministerial 004-2016-PCM, en la que aprueba el Uso Obligatorio de Norma Técnica Peruana: "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a edición", en todas las entidades integrantes del Sistema Nacional de Informática.

La fundación de la Universidad Nacional de Trujillo se remonta al inicio de nuestra Época Republicana. Fue el General Simón Bolívar, el Libertador de América, quien expide en su cuartel general de Huamachuco el Decreto de Fundación el 10 de Mayo de 1824. Influenció mucho en ello, el entonces Secretario General de la Nación, el Tribuno don José Faustino Sánchez Carrión (Universidad Nacional de Trujillo, 2019b).

El primer Rector fue Don Carlos Pedemonte y Talavera y su instalación ocurre el 12 de Octubre de 1831 en ceremonia realizada en la capilla interior del Colegio Seminario de San Carlos y San Marcelo prestando el juramento respectivo el Dr. Pedro José Soto y Velarde, Vicerrector encargado del Rectorado en ausencia del titular, el Doctor Tomás Dieguez de Florencia, entonces Senador de la República (Universidad Nacional de Trujillo, 2019b).

El organigrama que rige a la Universidad Nacional de Trujillo, fue aprobado según resolución del Consejo Universitario N° 0208-2016/UNT de fecha 28 de Marzo del 2016(ver Anexo 7). La resolución lleva la firma del Rector Doctor Orlando Moises Gonzales Nieves. De acuerdo a este instrumnto de gestión, se establece que el órgano jerarquico máximo es la Asamblea Universitaria.

Para la SUNEDU, la universidad ha venido impulsando el aseguramiento de la calidad del servicio educativo a través de la mejora continua de sus procesos académicos y administrativos. A esto se suma una adecuada gestión que le ha permitido obtener importantes beneficios de las transferencias presupuestales otorgadas por el Ministerio de Educación, en el marco de sus compromisos de gestión (Superintendencia Nacional de Educación Superior Universitaria, 2018).

Como parte del proceso de autoevaluación y ordenamiento de la Universidad, impulsado por el licenciamiento, la UNT decidió mantener en su oferta académica 233 programas (45 de pregrado, 86 maestrías 26 doctorados y 76 segundas especialidades) (Superintendencia Nacional de Educación Superior Universitaria, 2018).

La UNT cuenta con 44 líneas de investigación priorizadas, proyectos de investigación financiados con fondos del Canon Minero, y reglamentos que establecen los procedimientos para determinar el financiamiento y presupuesto de los proyectos de investigación, así como para la promoción, convocatoria y evaluación de proyectos de investigación (Superintendencia Nacional de Educación Superior Universitaria, 2018).

La Universidad Nacional de Trujillo, agrupa la oferta de sus carreras en los grupos "A" y "B" (Universidad Nacional de Trujillo, 2019a).

GRUPO "A"

Medicina	Ciencias Biológicas	Informática
Estomatología	Microbiología y Parasitología	Ing. Química
Farmacia y Bioquímica	Pesquería	Ing. Ambiental
Enfermería	Matemáticas	Ing. Industrial
Zootecnia	Física	Ing. Mecánica
Agronomía	Estadística	Ing. Minas
Ing. Metalúrgica	Ing. Agrícola	Ing. Agroindustrial
Ing. de Sistemas	Ing. Mecatrónica	Ing. de Materiales
Ing.Civil	Arquitectura y Urbanismo	

GRUPO "B"

Administración	Economía	Contabilidad y Finanzas
Arqueología	Antropología	Turismo
Trabajo Social	Historia	Derecho y Ciencias Políticas
Ciencia Política y Gobernabilidad	Ciencias de la Comunicación	Educación Inicial
Educación Primaria		
Educación Secundaria:	ED.Sec.:Ciencias Matemáticas	ED.Sec.:Filosofía-Psicología y CC. Sociales
	ED.Sec.:Historia y Geografía.	ED.Sec.:Lengua y Literatura
	Ed.Sec.: Idiomas	

La Universidad Nacional de Trujillo en el marco de su gestión académica establece los procesos de Admisión, Matrícula, Graduación y Titulación. Estos procesos contienen datos importantes y confidenciales como: registro de postulantes, registro de ingresantes y estudiantes, registro de notas y asistencias, así como expedientes de graduación y titulación de estudiantes de pregrado, segunda especialidad profesional y posgrado. Por ejemplo, el ingreso de notas y asistencias es realizado por el docente en cualquier momento, debido a que no existe procedimientos ni controles establecidos por avance silábico ni por fechas de ingreso. Asimismo, este registro puede ser accedido utilizando los servicios de internet por el programador y el personal de Registro Técnico quienes pueden modificar las notas sin autorización alguna. Ademas, no se realiza un seguimiento de las actividades realizadas con respecto al ingreso de notas, ni se cuenta con registro de cambio de notas ni oficio que autorice los cambios.

En este contexto, la Universidad Nacional de Trujillo carece de una política de seguridad de la información, de procedimientos implementados o controles para el adecuado manejo de los datos. Existe la probabilidad de que se produzcan incidentes o acciones ilícitas como: interrupción de servicios, violación de la privacidad, o alteración de datos, que comprometan la integridad, disponibilidad y confiabilidad de los datos almacenados a través de sus sistemas de información, no garantizando a los estudiantes, en la mejor medida posible, de servicios protegidos frente a la pérdida o alteración no autorizada de su información.

1.3. ENUNCIADO DEL PROBLEMA

¿Cómo influye un Framework de seguridad de la información en el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002?

1.4. ALCANCE

La presente tesis tiene como alcance la Gestión de Seguridad de la Información en la gestión de los procesos académicos de la UNT (servicios de Matrícula, Notas y Asignaturas). Es en este contexto que se propone desarrollar el Framework de Seguridad de la información.

1.5. JUSTIFICACIÓN

1.5.1. Justificación Académica

Este proyecto permite estudiar una variedad de términos relacionados a la seguridad de la información como son las amenazas tanto físicas como lógicas que van desde el acceso hasta la destrucción de datos y la manera de controlarlas a través de la gestión de riesgos. Así mismo permite describir y analizar la importancia de las normas de seguridad de la información como un marco de trabajo que permite asegurar la continuidad de las operaciones. Además, se describen los objetivos principales de la seguridad de la información: integridad, confidencialidad y la disponibilidad como parte de la protección de los activos de información.

1.5.2. Justificación Tecnológica

Este proyecto permite definir un marco de trabajo de seguridad de la información en las instituciones académicas, manteniendo las funciones claramente definidas mediante los roles establecidos para cada dueño de los procesos, las políticas de seguridad, los procedimientos y la correcta aplicación de controles de incidencias de seguridad, de tal manera que se pueda gestionar y garantizar que todos los activos estén debidamente protegidos dentro de la organización para asegurar el desarrollo y sostenibilidad de sus operaciones.

1.6. VIABILIDAD

El presente proyecto reúne aspectos de predisposición, condiciones técnicas y operativas, y facilidad al acceso de la información, siendo esto un factor muy importante para el cumplimiento de objetivos; Sin embargo, cabe resaltar que el universo a estudiar es amplio, por lo que se focalizarán ciertas actividades académico-administrativas dentro de la gestión universitaria.

En la presente investigación se contó con recursos humanos, financieros, materiales y de tiempo, acceso a la información y conocimientos; entre otros recursos que fueron necesarios para desarrollar la tesis.

1.7. APORTE

La presente investigación es un aporte de innovación, muy relevante, en la gestión, auditoría y seguridad de los sistemas de información que se aplicarán en las Universidades para la gestión académica de las mismas, basadas en el estándar internacional ISO 27002 de seguridad de la información. Este es un factor que ha sido muy descuidado en casi todas las Universidades del país, según el estudio arrojado por la 20 Encuesta Global de Seguridad de Información 2017-2018 (sólo un porcentaje inferior al 3% tiene políticas y controles de seguridad de información en la gestión académica) Por ello, se pretende empezar con un plan piloto en la Universidad Nacional de Trujillo y luego extender este a todas las Universidades del País.

1.8. HIPÓTESIS

H1: Un Framework de seguridad de la información incrementa el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002 en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.

1.9. OBJETIVOS

1.9.1. OBJETIVO GENERAL

Diseñar y desarrollar un Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas -

1.9.2. OBJETIVOS ESPECÍFICOS

- Hacer un análisis del entorno tanto interno como externo de la UNT usando la matriz FODA para determinar las fortalezas, debilidades, oportunidades y amenazas, relevando lo que corresponde a los procesos académicos que se relacionan con la gestión de la información y son susceptibles de destrucción, sabotaje, fraude, violación de la privacidad, intrusismo, etc.

- Evaluar la implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.
- Diseñar el nuevo Framework de gestión de la información de los procesos académicos de la UNT basado en los controles de la ISO 27002 de Gestión.
- Desarrollar un prototipo de soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT.
- Hacer las pruebas de funcionalidades en la versión piloto del proceso académico - servicios de Matrícula, Notas y Asignaturas – para las mediciones pertinentes.

CAPÍTULO II

MARCO TEÓRICO

"Comienza haciendo lo que es necesario, después lo que es posible y de repente estarás haciendo lo imposible"

San Agustín.

CAPÍTULO II: MARCO TEÓRICO

En este capítulo se presenta el estado del conocimiento de la investigación tanto en el ámbito nacional como internacional. Se referencian trabajos de investigación que aportan a la investigación y se define tanto teórica como científicamente los principales términos utilizados en la investigación.

2.1. Antecedentes

En este acápite presentamos los contenidos de tesis de investigación relacionado a la presente tesis que estoy desarrollando:

Según Vital (2019), en su tesis titulada "Seguridad de la información: estrategia de gestión basada en marcos de referencia de control y seguridad para las organizaciones en México", presenta y describe una propuesta de estrategia para la implementación de la seguridad de la información para el mejoramiento en los procesos de confidencialidad, integridad y disponibilidad de la información en una organización. El estudio concluye definiendo a la seguridad de la información no como un asunto propiamente tecnológico; considera como factores preponderantes a la infraestructura, los procesos de manejo y resguardo, así como la concientización del factor humano que va desde los altos directivos hasta los niveles operativos de la organización. El aporte de la investigación está en el conjunto de marcos y normas de referencia propuestos tanto de control, análisis de riesgos y de seguridad de la información y que en su conjunto conforman la estrategia para la implementación de la seguridad de la información.

Sarkkinen (2017), en su tesis titulada "Security Management systems for global high technology corporation, case Wärtsilä corporation", describe un plan de implementación de cómo el sistema de gestión de seguridad debería ser construido y define qué tipos de organización de seguridad serían adecuados para apoyar en la implementación, para lo cual utilizó métodos cualitativos como un caso de estudio para resolver el problema de la investigación. Su estudio concluyó que no existe una organización adecuada con soporte de la alta dirección, recursos y responsabilidad operativa para administrar la seguridad en la medida en que la organización lo necesite, llegando a establecer un modelo organizacional de tres etapas para la

implementación efectiva de los sistemas de gestión: la primera como organización de seguridad de área global para crear, establecer y mantener el Framework para los sistemas de administración de seguridad, con el fin de brindar apoyo en la implementación real del sistema de administración de seguridad para la organización; la segunda, función centralizada de gestión de riesgos que se centra en garantizar la cooperación y la alineación en la gestión de riesgos y seguridad y crearía el vínculo necesario entre las diferentes funciones de apoyo para el proceso de gestión de riesgos; la tercera, como información y organización de seguridad cibernética como rol de apoyo en la prestación de asistencia en seguridad de la información administrativa, como la capacitación, la comunicación y el conocimiento diario de la seguridad de la información de los empleados. El principal aporte al trabajo de investigación es que el modelo organizacional establecido puede aplicarse en corporaciones u organizaciones similares como soporte para la implementación y administración efectiva de los sistemas de gestión de seguridad.

Puga (2017), en su tesis titulada "Propuesta de un modelo de gestión para mejorar la capacidad de gestión de la seguridad de la información de una institución financiera del sector público", propone un modelo de gestión para mejorar la capacidad de gestión de la seguridad de la información de una Institución Financiera del Sector Público, que contribuya al cumplimiento de los objetivos estratégicos de la Institución, a través de la adopción de tres prácticas y estándares específicos (COBIT 5, ITIL v3,ISO 27001:2013), los que están siendo ampliamente adoptados a nivel global y que deben ser implementadas en base al Esquema Gubernamental de Seguridad de la Información (EGSI). Su estudio concluyó determinando la falta de concienciación y conocimiento en temas de seguridad de la información por parte de todos los funcionarios de la institución. En este sentido la Institución Financiera requiere contar con una Política de Seguridad, implementar un programa de culturización y concientización en Seguridad de la Información, establecer un proceso de gestión de incidentes y realizar de manera periódica el análisis y evaluación de riesgos.

Mohamed (2016), en su tesis titulada "An information security cultural Framework", propone un Framework de seguridad de la información que incluya controles de gestión de riesgos y el efecto de la cultura en el comportamiento de los empleados

con respecto a la seguridad de la información. Para medir el efecto de la cultura en la seguridad de la información utilizó el modelo cultural de Hofstede, llegando a la conclusión que la cultura de seguridad de la información está influenciada por la cultura nacional. Determinó que una cultura de seguridad de la información con los valores de conocimiento y conciencia puede minimizar los incidentes causados por los empleados, debido a que la mayoría de los incidentes de seguridad se generan debido a que no cumplen con las políticas y procedimientos de la organización. Asimismo, estableció que muchas organizaciones implementaron medidas técnicas de seguridad, pero descuidan el efecto que el comportamiento humano tiene en los sistemas de información. El principal aporte al trabajo de investigación es que las organizaciones puedan mejorar el nivel de seguridad de los servicios de información, así como el cumplimiento de los empleados con las políticas de seguridad utilizando como guía el Framework de seguridad de la información como un mecanismo coherente que relaciona a las personas y las medidas técnicas.

Pino (2014), en su tesis titulada "Marco de referencia para la implementación de un esquema gubernamental de seguridad de la información (EGSI), basado en la Norma Técnica Ecuatoriana INEN ISO/IEC 27001:2010 y en concordancia con el acuerdo 166", establece la necesidad de aplicar normas y procedimientos para mitigar los riesgos asociados a confidencialidad, integridad y disponibilidad de la información. El marco de referencia no solo se limita al diseño e implementación sino también a las actividades básicas a cubrirse con la finalidad de operar, mantener, evaluar y mejorar el Esquema Gubernamental de Seguridad de la Información para las empresas públicas del Ecuador. La investigación arriba a dos conclusiones fundamentales: La primera establece que la implementación del Esquema Gubernamental de Seguridad de la información puede ser considerada como un paso previo a la implementación de un Sistema de Gestión de Seguridad de la Información con todos los requisitos de la Norma ISO /IEC 27001; la segunda se relaciona a la necesidad de cambio cultural y organizacional por parte del personal de la organización quienes deben regir sus acciones bajo un esquema de monitoreo y mejora continua. El principal aporte al trabajo es la propuesta de un marco de referencia de seguridad de la información aplicable a las empresas públicas del Ecuador, el cual no solo considera aspectos técnicos sino también aquellos relacionados con la cultura organizacional de sus miembros, que consta de tres fases:

Diagnóstico y Planificación, Implementación y Evaluación y Mejora, el mismo que se desarrolló en base a los requerimientos de la norma ISO 27001:2013 y el modelo de mejora continua PDCA, cuya implementación mejorará la gestión de la calidad y fiabilidad de la información.

Sullca (2018), en su tesis titulada "Propuesta de un Marco de Seguridad de la Información en la Nube Publica para la SUNAT: Caso Sistema de Cuenta Única del Contribuyente", elabora un Marco de Seguridad de la Información para la Nube Publica de SUNAT aplicado al Sistema de Cuenta Única del Contribuyente. El estudio concluye que las políticas de Seguridad con las que cuenta actualmente la SUNAT no cubren los aspectos respecto al establecimiento de controles de seguridad de la información para sistemas que se construyan sobre la Nube Publica; no existe una "solución única" para agregarle la seguridad de la información a los Sistemas Informáticos que se construyan sobre la Nube Publica. Se debe analizar cada Sistema por Separado y agregarle los controles de seguridad de acuerdo con los requerimientos del proyecto y los lineamientos que establezcan las políticas de seguridad de la SUNAT. El aporte de esta investigación es la propuesta de un marco de seguridad de la información adecuado que le permitirá a la SUNAT cubrir la brecha en lo que respecta a seguridad de la información para la Nube Publica. En estos aspectos que constituyen esta brecha, se identifican también aspectos legales y regulatorios que por su naturaleza jurídica escapan al alcance del presente trabajo de investigación.

Huamán (2017), en su tesis titulada "Plan de comunicaciones en Seguridad de la Información para el personal administrativo de la Pontificia Universidad Católica del Perú", Construye las bases para la cultura de seguridad de la información en el personal administrativo de la PUCP a través de concientización del problema, las buenas prácticas en el uso y manejo de la tecnología (entrenamiento) y mediante sus comportamientos (educación) para garantizar la protección y resguardo de la información de la Universidad. El estudio concluye que el personal administrativo conoce y maneja, en un 50% más, los conceptos básicos en seguridad de la información; un 72% más de los colaboradores reconoce los canales de comunicación interna que debe seguir un administrativo PUCP en caso ocurriese un incidente de seguridad de la información; Un 37% más del personal administrativo conoce y

adopta un conjunto de buenas prácticas para el personal administrativo, segmentando según las funciones y actividades que realiza. El presente proyecto de comunicación permitió tener las bases para construir la cultura de seguridad de la información en el personal administrativo de la Universidad mediante un enfoque que se concentró en mayor medida en las fases Concientización y Entrenamiento del modelo NIST 108.

Atalaya (2016), en su tesis titulada "Propuesta de un sistema de seguridad de la información para la oficina de admisión y registro académico de la universidad privada Antonio Guillermo Urrelo, 2016", diagnostica las condiciones de seguridad de la información y formula una propuesta para el Departamento de Admisión y registro Académico (DARA) de la Universidad Privada Antonio Guillermo Urrelo - 2016. Las conclusiones a la que se arriba en esta investigación son: se encontraron una serie de riesgos asociados a los activos de información a los que es necesario prestarles la importancia debida; los procesos más importantes que se dan en el DARA, son los que sirvieron; La identificación de los activos de información, se ha podido realizar de una manera ordenada, al cumplir los lineamentos de las normas base que fueron empleados en el presente trabajo de base para identificar los activos de información y Como universidad, disponer que este SGSI se convierta en un marco común de gestión de la seguridad, con el fin de asegurar la integridad, disponibilidad y la confidencialidad de los datos pertenecientes a la institución. El aporte de esta investigación está en la identificación de los activos del DARA y los riesgos que podrían afectar la continuidad de los procesos. Sugiere, además, la implementación inmediata del SGSI.

Mercado (2016), en su tesis titulada "Modelo de gestión de seguridad de la información para el E-Gobierno", elabora un modelo de gestión de seguridad de la información para el gobierno electrónico en las entidades públicas. La investigación concluye con la elaboración de un modelo a partir de la revisión de 11 modelos de seguridad de la información tomando los aspectos más relevantes; también se definió una estructura organizacional con funciones definidas que contempla los procesos estratégicos, fundamentales y de soporte, la cual permite gestionar la seguridad de la información y garantizar una mejor experiencia al cliente cuando requiera interactuar con los procesos o servicios de la organización. El aporte de esta investigación es la elaboración de un modelo que consta de 04 fases que brindan servicio de gobierno

electrónico donde se explica los pasos a seguir, desde la planeación de la seguridad hasta su revisión y mejora del sistema de seguridad de la información implementado. La propuesta de modelo se orienta a los procesos que brindan servicios de gobierno electrónico, lo cual a través de una estructura organizacional y funciones permite implementar y gestionar la seguridad de la información de acuerdo a las fases establecidas y nivel de madurez requerido, mediante la actualización, mejora o desarrollo de documentos y controles; asimismo permite el monitoreo del nivel de seguridad a través de la revisión de los indicadores y métricas establecidas.

Seclén (2016), en su tesis titulada "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001", analiza las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI, así como también investiga las estrategias y metodologías que vienen aplicando las entidades públicas que ya han completado su ejecución, los beneficios obtenidos de haberlo realizado en sus instituciones y la importancia de fomentar la capacitación y especialización en seguridad de la información, para lograr dichos objetivos, utilizó un método basado en la Teoría Fundamentada que le permitió construir teorías, conceptos e hipótesis partiendo directamente de los datos y no de los supuestos a priori. Su estudio concluyó en ocho categorías que representan los factores que afectan la implementación del SGSI en las entidades públicas, distribuidos en tres niveles: la primera, a nivel estratégico, se debe impulsar una política estratégica de estado que conlleve a formalizar funcionalmente el cargo de Oficial de Seguridad de Información para realizar un seguimiento de la ejecución del avance de la implementación del SGSI en las entidades públicas; la segunda, a nivel operativo, establece llevar a cabo una gestión eficiente de la seguridad de la información con el apoyo institucional de la alta dirección, realizar una adecuada organización del SGSI y la aplicación efectiva de la normatividad en seguridad de información; la tercera, a nivel técnico, establece contar con un presupuesto nacional para la seguridad de la información, así como la especialización técnica de profesionales en SGSI como prioridad nacional. El principal aporte al trabajo de investigación es que las entidades públicas del estado cuenten con información organizada y estructurada que sirva de apoyo para la implementación de las políticas y el control de riesgos de seguridad de la información como medidas de mejora en la

gestión de sus procesos de negocio, de tal manera que les permita encontrar un punto de equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización.

2.2. Marco teórico

2.2.1. Seguridad de la información

La seguridad de la información se mantiene implementando un conjunto de controles a través de la aplicación de políticas, procesos, programas de capacitación, procedimientos, estructuras organizacionales, concientización, y funciones de software y hardware. Se necesitan implementar, monitorear, revisar y mejorar estos controles en la medida de lo posible para asegurar que se cumplan los objetivos comerciales y de seguridad como soporte a la continuidad del negocio (ISO/IEC 27002, 2005).

Según Cano (2014), La seguridad de la información debe adaptarse a los nuevos retos que emergen de la dinámica del entorno empresarial y necesita transformarse para mantener una ventaja competitiva. No es conveniente seguir utilizando los controles tradicionales sino más bien es mejor focalizar nuevas medidas que aseguren la información en una era móvil, abierta, con proveedores y completamente social. En este contexto, se advierte que la transformación en la gerencia y gestión de la seguridad de la información supone tener un conocimiento profundo de su modelo actual y apuntar hacia un modelo evolutivo que guarde relación con los retos que impone la sociedad actual, como se muestra en la figura 2.

Modelo actual y evolutivo de la seguridad de la información	
Modelo actual de la seguridad de la información	**Modelo evolutivo de la seguridad de la información**
Basado en mitigación del riesgo (reducción de riesgo)	Basado en gestión del riesgo (aceptación de umbral de riesgo)
Orientado a los activos de información críticos	Orientado al funcionamiento confiable de procesos críticos
Fundado en el aseguramiento del perímetro tecnológico definido	Fundado en el cambio de comportamiento de las personas frente a la información
Basado en procedimientos y guías de seguridad y control	Basado en reglas y acuerdos de uso fundados en los impactos
Soportado en acciones preventivas y sancionatorias	Soportado en acciones de monitoreo activo y de pronóstico

Figura 2: Modelo actual y evolutivo de la seguridad de la información. Fuente: (Cano, 2014)

En consecuencia, **¿Que es la seguridad de la información?**

Se define como la protección de la información incluyendo los sistemas y el hardware que se utilizan en el almacenamiento y transmisión de la información frente a una variedad de amenazas (de acceso, divulgación, interrupción, modificación o destrucción no autorizados) para poder asegurar las operaciones de continuidad del negocio, maximizar el retorno de las inversiones y mitigar los riesgos.

Y ¿Por qué es importante la seguridad de la información?

La seguridad de la información es muy importante tanto en empresas públicas como privadas porque la información y las redes de soporte que utilizan son activos importantes que les permiten asegurar la continuidad de las operaciones del negocio y que frente al intercambio de información a través de medios locales como remotos incrementan la dificultad de obtener un adecuado control de acceso. Por consiguiente, los usos de estos medios tecnológicos desencadenan diferentes amenazas de seguridad como sabotaje, espionaje, inundación, denegación de servicio, robo de información que pueden generar un impacto negativo en la organización.

La mayor parte de los sistemas de información no han sido desarrollados para ser seguros. La seguridad que se puede establecer por medios técnicos es

insuficiente, y debería ser apoyada por la gestión y los procedimientos adecuados. Para identificar los controles a implementar se requiere de una planeación rigurosa y para gestionar la seguridad de la información se requiere la participación de diferentes actores como gerentes, empleaos, proveedores y clientes. (ISO/IEC 27002, 2005)

Según Gómez (2011), define la seguridad de la información como la preservación de los siguientes principios básicos:

Figura 3: Principios básicos de seguridad de la información. Fuente (Gómez, 2011)

a. Disponibilidad:

Es un pilar importante para garantizar que los usuarios autorizados tengan acceso a la información cuando lo requieran. La disponibilidad de la información protege al sistema contra determinadas amenazas como la denegación de servicio (inundar o saturar al sistema con más mensajes de los que se pueden procesar, impidiendo los accesos autorizados) e intentos deliberados de acceder o utilizar los datos que pueden generar implicaciones serias. En este contexto, es necesario diseñar un sistema lo suficientemente robusto frente a estas amenazas ya sean intencionadas o por desastres naturales para garantizar la continuidad de las operaciones de una organización. Por ejemplo ¿Qué sucede si sus clientes no pueden iniciar sesión en sus sistemas para el proceso de matrícula?

b. Integridad:

Se encarga de garantizar que la información esté libre de alteraciones y errores desde la creación. Ello puede realizarse mediante la transmisión, a través de sistemas informáticos, sobre una infraestructura de red. De esta manera, se puede verificar si se han agregado o borrado datos de un mensaje o archivos durante su almacenamiento, procesamiento o comunicación sobre una red informática. Cabe mencionar que la modificación no autorizada de la información se presenta por -debilidades del sistema, por usuarios internos de la organización malintencionados o por errores.

Según Gelbstein (2011) menciona como un ejemplo de ataque a la integridad de datos: "el gusano informático Stuxnet, que fue descubierto en el año 2010, el cual alteró el funcionamiento de un proceso industrial, ya que fue diseñado con la finalidad de dañar equipos físicos y modificar las indicaciones de los operadores a cargo de la supervisión, para impedir, de este modo, que se identificara cualquier anomalía en los equipos".

c. Confidencialidad:

Garantiza que la información solo podrá ser accedida o leída únicamente por usuarios o sistemas autorizados. Con esta función de seguridad se pretende preservar los datos almacenados en un host, (dispositivos de copias de respaldo) o, mientras están en tránsito, a través de redes de comunicaciones. Ejemplos de vulnerabilidades de confiabilidad son la divulgación de información de historias clínicas de los pacientes de un hospital o el acceso no autorizado de estudiantes a información como el registro de notas y asistencias. En este sentido, es un requisito de la confiabilidad mantener el acceso autorizado, protegiendo la información de propiedad y la privacidad personal de tal manera que no se divulgue a personas no autorizadas.

2.2.2. Políticas de seguridad

Se define como un conjunto de reglas, medidas, procedimientos y prácticas que regulan la manera como una organización previene, protege, distribuye y maneja la información. Así mismo la política de seguridad proporciona los cimientos para establecer y delimitar responsabilidades específicas. Indica lo que está permitido o no en el área de seguridad durante la operación de los sistemas de informáticos, con el objetivo de brindar protección a los recursos técnicos y de información. En este contexto, es un documento de alto nivel que describe las directivas de seguridad de la información (Nieles, Dempsey, & Pillitteri, 2017).

2.2.3. Sistema de Gestión de Seguridad de la información (SGSI)

Un sistema de Gestión de Seguridad de la información, es un marco de Políticas y procedimientos que incluye todos los controles legales, físicos y técnicos que intervienen en los procesos de gestión del riesgo de la información de una organización (PECB, 2016).

Causas de una inadecuada gestión de la seguridad de la información

Las principales causas de una inadecuada gestión de la seguridad, se pueden resumir en (Merino & Cañizares, 2014):

- Errores humanos.
- Acciones mal intencionadas.
- Falta de control.
- Fallo de los sistemas.
- Carencia de formación y concienciación
- Incidentes externos
- Incumplimiento legal

Consecuencias de una inadecuada gestión de la seguridad de la información

La inadecuada gestión de la seguridad de la información, puede tener las siguientes consecuencias (Merino & Cañizares, 2014):

- Pérdida documental.
- Pérdida de confidencialidad.

- Indisponibilidad de la información.
- Alto tiempo de recuperación.
- Baja productividad.
- Aumento de los costes.
- Disminución del nivel de servicio.
- Pérdida reputacional.
- Pérdida de oportunidades de negocio.
- Pérdida de clientes

Ventajas de implementar un Sistema de Gestión de Seguridad de la Información

La mejora en la seguridad de la información, se verá reflejada en las siguientes ventajas que se describen a continuación (Merino & Cañizares, 2014):

- Reducción de riesgos

  Esto se consigue realizando un análisis de riesgos, y elaborando un conjunto de planes de acción derivado del mismo, que contemplará la implementación de un conjunto de salvaguardas, lo que reducirá los riesgos hasta el nivel asumible por la Organización, este proceso estará alineado a los objetivos de negocio de esta.

- Aumento del retorno sobre la inversión (ROSI)

  La implantación de un SGSI permite una optimización de recursos y un incremento de la eficacia y eficiencia en el empleo de los mismos, lo que supone una mejora en el retorno de la inversión. Además de que la toma de decisiones podrá estar basada en prioridades y datos cuantitativos, no solo cualitativos, lo que permite gestionar mejor la inversión en seguridad, evitándose gastos innecesarios, inesperados, y sobredimensionados.

- Aumenta la madurez en la Gestión de la seguridad

  La implementación de un SGSI transforma la seguridad en una actividad de gestión, como cualquier otro proceso de la Organización. Este concepto es importante dado que la seguridad deja de ser un conjunto de actividades técnicas organizadas, para transformarse en un proceso con un ciclo de vida metódico y controlado.

- Cumplimiento Legal

  Durante la implementación de un SGSI se evalúa el cumplimiento la legislación vigente y se verifica la adecuación y el cumplimiento. Por lo tanto, se crea un marco legal en evaluación continua.

- Generación de valor y factor diferenciador

  Es un importante factor diferenciador con la competencia, por las ventajas derivadas de la mejora de la imagen y de otras ventajas competitivas en el mercado.

2.2.4. ISO 27001

Esta norma de seguridad de la información define los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Esta Norma Internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para satisfacer los requisitos propios de seguridad de la información de la organización. Establecen conjunto de requisitos para seleccionar controles de seguridad a la medida de las necesidades de cada organización, basado en las mejores prácticas de la industria (PECB, 2016).
Una organización puede ser certificada en ISO 27001; para ello debe cumplir con todos los términos definidos en las cláusulas 4 a 10 de la norma. También debe definir, en la declaración de aplicabilidad, los controles aplicables y justificar la inaplicabilidad de los controles del Anexo A.

Figura 4: Estructura de la norma ISO 27001. Fuente: (PECB, 2016)

ISO 27001, clausula 0.1: Generalidades

Esta Norma Internacional ha sido preparada para proveer requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de un sistema de seguridad de la información es una decisión estratégica de una Organización. El diseño y la implementación del SGSI de una Organización dependen de las necesidades y objetivos de cada organización, así como de sus requisitos de seguridad, sus procesos utilizados, y el tamaño y estructura de la Organización. Es previsible que todos estos factores cambien con el tiempo.

El sistema de gestión de seguridad de la información mantiene la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da la confianza a las partes interesadas de que los riesgos son manejados adecuadamente.
Es importante que el sistema de seguridad de la Información sea parte de, y esté integrado con, los procesos de la estructura de gestión en general de la organización, que la seguridad de la información sea considerada en el diseño de los procesos, los sistemas de información y controles. Es de esperar que la

aplicación de un sistema de gestión de seguridad de la información será escalada de acuerdo con las necesidades de la Organización.

2.2.5. ISO 27002

Esta norma es una Guía para el código de prácticas para los controles de la seguridad de la información.

Esta norma internacional proporciona una lista de los objetivos y controles de seguridad generalmente practicados en la industria. En particular las cláusulas 5 a 18 prestan un asesoramiento específico y una guía para la aplicación de las mejores prácticas para apoyar los controles especificados en el Anexo A de la norma ISO 27001 (Cláusula A.5 a A.18) (PECB, 2016).

ISO 27002, clausula 1: Ámbito de aplicación

Esta Norma Internacional proporciona las pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluyendo la selección, la ejecución y la gestión de controles, teniendo en cuenta el entorno(s) de riesgos para la seguridad de la información de la organización.

Esta Norma Internacional está designada a ser utilizada por las organizaciones que intentan:

a) Seleccionar controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001;
b) Aplicar controles de seguridad de la información comúnmente aceptados;
c) Desarrollar sus propias directrices de gestión de la seguridad de la información.

Estándares de seguridad de la información según ISO 27002

Es un código de buenas prácticas para la gestión de la seguridad de la información que establece los objetivos de control y controles frente a los entornos de riesgo que está expuesta una organización. Esta norma consta de 14 dominios como se muestra en la figura 5. (ISO27000, 2012)

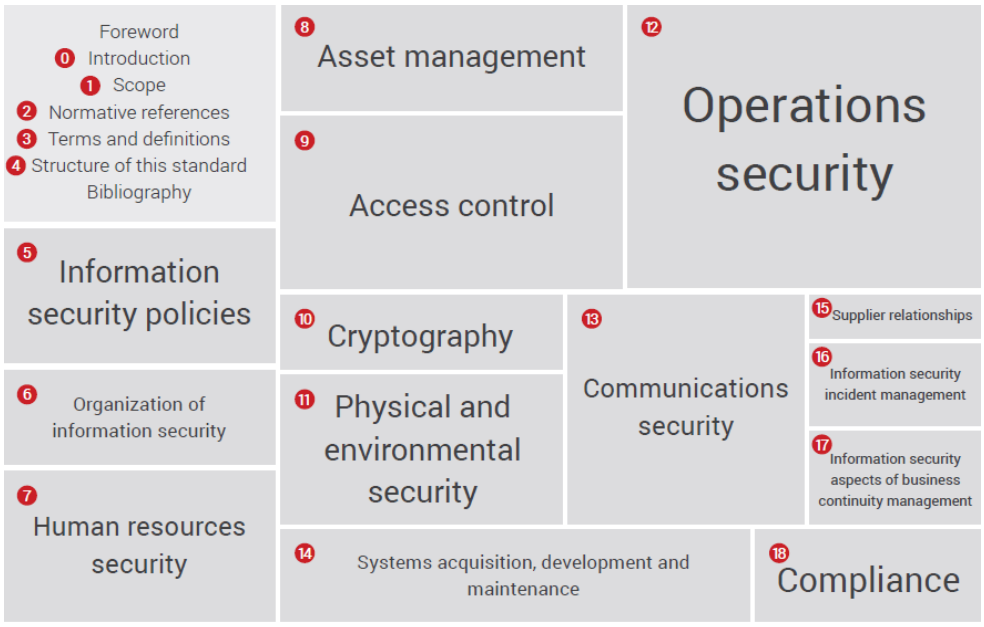


Figura 5: Norma ISO 27002. Fuente: (PECB, 2016)

A continuación, se describe cada dominio de la Norma ISO 27002:

a. Políticas de seguridad

Una política es un documento que proporciona una guía e instrucción dentro de la empresa establecida por la dirección de la organización. Cubre aspectos relacionados en el contexto en el que opera una organización, suele contener la definición de la seguridad de la información, el establecimiento de responsabilidades de manera clara, así mismo, considera los fines y objetivos alcanzadas a través de estrategias propuestas por la organización. Además, se ocupa de mantener el documento de la política, los requisitos aplicables, así como de reportar los incidentes que se consideren sospechosas en relación a la seguridad.

b. Aspectos organizativos de la seguridad de la información

En este dominio se establece la estructura de gestión de la seguridad de la información. Se encarga de la aprobación de las políticas de seguridad, la asignación de funciones y responsabilidades de seguridad y del control de acceso a datos de la organización por actores externos como terceras partes, que puede generar un riesgo si el acceso se da en el contexto de una incorrecta administración de la seguridad.

c. Seguridad ligada a los recursos humanos

El presente dominio tiene como objetivo de concientizar a los empleados de manera permanente, independientemente de su actividad, acerca de las amenazas existentes que pueden afectar el desarrollo de sus actividades debido a errores involuntarios y deliberadas, ejecución de actos ilícitos como robo, fraude y uso inadecuado de las instalaciones, considerándose la aplicación de posibles sanciones en caso de incumplimiento. Para ello se debe establecer de manera adecuada las responsabilidades e incluirlas en los acuerdos previamente aceptados y mediante la sensibilización lograr que los empleados informen los incidentes de seguridad por los medios de comunicación adecuados.

d. Gestión de activos

Se encarga de la clasificación y protección de los activos de la organización, con el objetivo de establecer como debe ser tratada y protegida los activos como son: el hardware, software y la información.

e. Control de accesos

Se encarga de controlar el acceso no autorizado a los sistemas de información mediante métodos de autenticación a las aplicaciones informáticas requiriéndoles el uso de contraseñas, así como la protección del equipamiento y estos procedimientos deben estar claramente establecidas y comunicadas para un correcto control con respecto a su cumplimiento.

f. Cifrado

El presente dominio utiliza sistemas y técnicas de encriptación para asegurar la información en relación al análisis de riesgo realizado con el objetivo de preservar la integridad y confidencialidad de la información.

g. Seguridad física y ambiental

Tiene como objetivo establecer áreas seguras mediante la implementación de controles de protección de las instalaciones para mantener las operaciones del negocio contra accesos físicos no autorizados, mitigando

de esta manera los riesgos que pueden generan los daños a la continuidad del negocio.

h. Seguridad en la operativa

Trata de evaluar la existencia de los procedimientos de operaciones ante los cambios previstos a sistemas y equipamiento con el fin de verificar su adecuada implementación, asignando para ello las respectivas responsabilidades y los medios técnicos necesarios.

Se debe monitorear las necesidades con respecto a la capacidad de las operaciones de los sistemas para evitar potenciales amenazas que interrumpan a los servicios de los usuarios y establecer controles para la protección contra código malicioso.

i. Seguridad en las telecomunicaciones

Tiene como objetivo la seguridad de las redes de la organización, protegiendo el flujo de datos dentro de la empresa o fuera de ella, como parte de intercambio de información entre organizaciones basadas en una política formal de intercambio, cumpliendo la legislación correspondiente.

j. Adquisición, desarrollo y mantenimiento de los sistemas de información

Establece que en la adquisición y desarrollo de los sistemas de información se debe asegurar que cuenten con los controles de seguridad, así como la validación de datos. Se debe establecer y documentar los procedimientos que se ejecutaran durante el ciclo de vida de los programas desarrollados o de terceros.

k. Relación con suministradores

Este dominio tiene como objetivo de establecer e implementar los mecanismos necesarios para asegurar que los servicios sean entregados para satisfacer todas las necesidades acordados con terceras personas.

l. Gestión de incidentes

Tiene como objetivo asegurar que los eventos de seguridad de la información y las debilidades vinculadas a los sistemas de información sean reportados por los canales adecuados de tal manera que se lleven a cabo las acciones correctivas en el momento adecuado para prevenir incidentes similares que se puedan presentar.

m. Gestión de la continuidad de negocio

Tiene como objetivo el diseño, la implementación y la preservación de planes de contingencia para asegurar que los procesos del negocio se pueden restaurar lo antes posible frente a una falla de cualquier tipo.

n. Cumplimiento

El objetivo es que la organización deba cumplir con las normas y leyes con el fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de no cumplir sus obligaciones.

2.2.6. Gestión Académica

Viza (2017) manifiesta que "la Gestión Académica es el conjunto de actividades y estratégicas guiadas por procedimientos y técnicas adecuadas para facilitar que las instituciones educativas públicas logren sus metas, objetivos y fines académicos"

Proceso que forma parte de toda la trama de la institucionalidad de la universidad. En él se concentran los saberes y prácticas institucionalizadas, que se conforman en torno a ciertos temas, problemáticas recurrentes y emergentes que involucran a los actores, principalmente a estudiantes y docentes (Ticona, 2014).

2.3. Marco conceptual

2.3.1. La matriz de Fortalezas, Oportunidades, Debilidades, y Amenazas (FODA)

D’Alessio (2015) atribuye la creación de este instrumento a Weihrich (1982), como una herramienta de análisis situacional. Exige un concienzudo pensamiento para generar estrategias en los cuatro cuadrantes de la matriz, estos son los de: fortalezas y oportunidades (FO), debilidades y oportunidades (DO), fortalezas y amenazas (FA), y debilidades y amenazas (DA). Desarrollar un serio y concienzudo análisis del entorno, de la competencia, y del entorno ayudará mucho a generar las estrategias de los cuatro cuadrantes Esta matriz es una de las más interesantes por las cualidades intuitivas que exige a los analistas, y es posiblemente la más importante y conocida (D’Alessio, 2015).

VISIÓN - MISIÓN - VALORES		
Análisis interno / Análisis externo	**FORTALEZAS-F** Liste las fortalezas 1. 2. 3. 4.	**DEBILIDADES-D** Liste las debilidades 1. 2. 3.
OPORTUNIDADES-O Liste las oportunidades 1. 2. 3. 4.	**ESTRATEGIAS FO** Use las fortalezas para sacar ventaja de las oportunidades **Explote Maxi-Maxi**	**ESTRATEGIAS DO** Mejore las debilidades para sacar ventaja de las oportunidades **Busque Mini-Maxi**
AMENAZAS-A Liste las amenazas 1. 2. 3.	**ESTRATEGIAS FA** Use fortalezas para neutralizar las amenazas **Confronte Maxi-Mini**	**ESTRATEGIAS DA** Mejore las debilidades y evite las amenazas **Evite Mini-Mini**

Figura 6: Matriz FODA. Fuente: (D’Alessio, 2015)

El proceso que se realiza en esos cuatro cuadrantes es el de emparejamiento (matching) para generar y registrar las estrategias en la matriz; para lo cual se requiere realizar los siguientes pasos:

a. Estrategias FO - Explotar

Empareje las fortalezas internas con las oportunidades externas. Genere las estrategias usando las fortalezas internas de la organización que puedan sacar ventaja de las oportunidades externas (Explotar). Registre las estrategias resultantes en el cuadrante FO con la notación que revela la lógica que las sustenta (Ej.: F1, F2 con O2, O3).

b. Estrategias DO - Buscar

Empareje las debilidades internas con las oportunidades externas. Genere las estrategias mejorando las debilidades internas para sacar ventaja de las oportunidades externas (Buscar). Registre las estrategias resultantes en el cuadrante DO con la notación que revela la lógica que las sustenta (Ej.: D1, D3 con O1, O4).

c. Estrategias FA - Confrontar

Empareje las fortalezas internas con las amenazas externas. Genere las estrategias usando las fortalezas de la organización para evitar o reducir el impacto de las amenazas externas (Confrontar). Registre las estrategias resultantes en el cuadrante FA con la notación que revela la lógica que las sustenta (Ej.: F3, F4 con A1).

d. Estrategias DA - Evitar

Empareje las debilidades internas con las amenazas externas. Genere las estrategias considerando acciones defensivas con el fin de reducir las debilidades internas evitando las amenazas del entorno (Evitar). Registre las estrategias resultantes en el cuadrante DA con la notación que revela la lógica que las sustenta (Ej.: D2 con A3).

2.3.2. Ciclo PDCA

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Comprobar, Actuar).

También conocido como "Círculo de Deming"**,** es una estrategia de mejora continua de la calidad en cuatro fases. Se basa en un concepto ideado por Walter A. Shewhart (Merino & Cañizares, 2014).

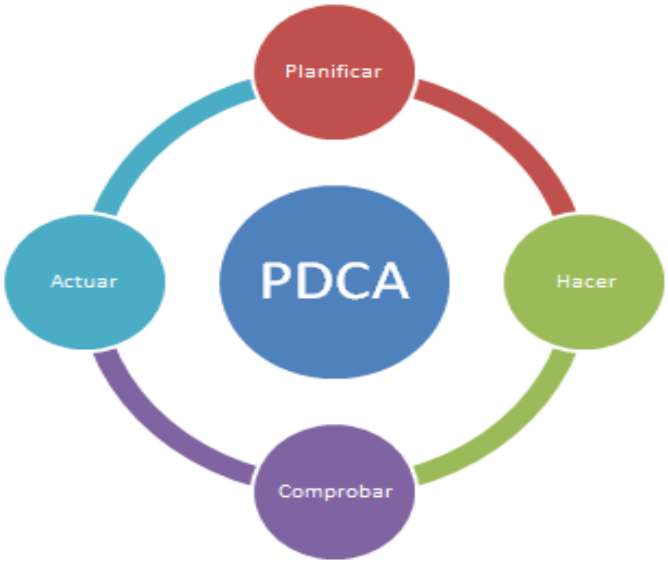


Figura 7: Ciclo PDCA. Fuente (Merino & Cañizares, 2014)

A continuación, se describen las fases de este ciclo de mejora continua, nombre con el que también se le conoce al ciclo PDCA:

PLANIFICAR

- Identificar el proceso que se quiere mejorar.
- Recopilar datos para profundizar el conocimiento del proceso.
- Analizar e interpretar los datos.
- Establecer los objetivos de mejora.
- Detallar las especificaciones de los resultados esperados.
- Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones.

HACER

- Ejecutar los procesos definidos en el paso anterior.
- Documentar las acciones realizadas.

COMPROBAR

- Pasado un período de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora especificada.
- Documentar las conclusiones.

ACTUAR

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.
- Aplicar nuevas mejoras si se han detectado errores en el paso anterior.
- Documentar el proceso

2.3.3. Gestión de riesgos

Actividades para identificar y controlar las amenazas, la ocurrencia de un evento y el impacto potencial una vez materializado tal evento. Además, se encarga de cuantificar la probabilidad de que ocurran amenazas y consecuentemente definir el nivel de aceptación del riesgo dentro de una organización, tomando en cuenta el impacto potencial de un evento o incidencia no deseado.

En la gestión de riesgos es importante la comprensión de los siguientes conceptos como se muestra en la Figura:

Figura 8: Activo, amenaza, vulnerabilidad e impacto. Fuente: (INCIBE, 2015)

Amenaza:

Puede causar incidentes desfavorables y cuando se materializa puede provocar daños sobre los activos de la organización generando la indisponibilidad o pérdida de la información. Una amenaza puede presentarse

desde las áreas internas de una organización o mediante el acceso desde redes externas no autorizadas.

Vulnerabilidad:

Puede entenderse como las debilidades en el sistema que pueden provocar que una amenaza se materialice y cause daños en lo activos de una organización. Por ejemplo, una inadecuada configuración de los sistemas podría ser aprovechado para cualquier ataque de intrusión.

Probabilidad:

Es la posibilidad de ocurrencia de un suceso que está relacionado con la amenaza.

Impacto:

Es la consecuencia de la materialización de una amenaza como los daños producidos sobre un activo.

La gestión de riesgos incluye dos grandes tareas:

a. **Análisis de riesgo:**

   Se entiende como un estudio que permite identificar el nivel de riesgo de los activos claves que brindan soporte a los procesos de una organización y las amenazas que puede vulnerar los objetivos principales de la seguridad de la información como: integridad, disponibilidad o confidencialidad. En ese sentido, con el fin de obtener los riesgos a los que está expuesta la organización, se deben realizar las siguientes fases:

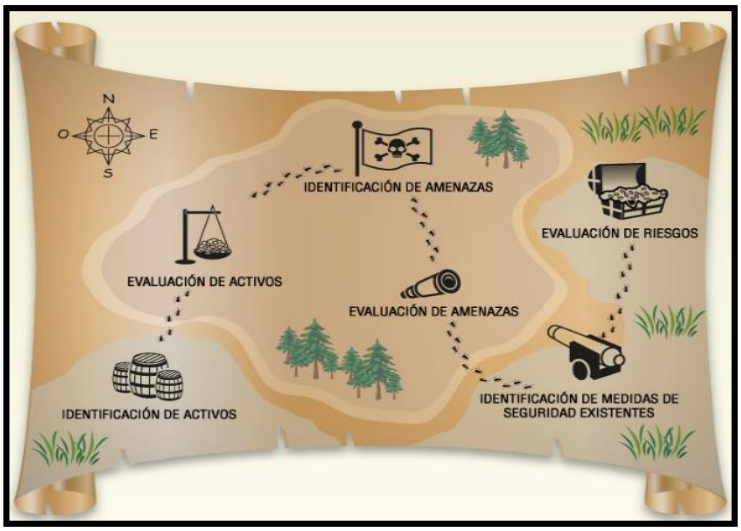


Figura 9: Fases de identificación de riesgos. Fuente: (INCIBE, 2015)

- **Identificación de activos:** Es la identificación de los recursos relacionados con los sistemas de información que dan soporte a los procesos de negocio, como el personal, los equipos, aplicaciones, proveedores, etc.
- **Evaluación de activos:** Consiste en la valoración cualitativa o cuantitativa de los activos críticos de la organización. Se considera objetivos como la integridad, disponibilidad o confiabilidad para la valoración.
- **Identificación de amenazas:** Se lleva a cabo la identificación de las principales amenazas que pueden afectar a los activos, como el robo de información.
- **Evaluación de amenazas:** En esta fase se asigna la probabilidad de impacto de las amenazas sobre los activos.
- **Identificación de medidas de seguridad existentes:** Es la identificación de las medidas de seguridad que reducen la probabilidad o el impacto de las amenazas existentes.
- **Evaluación de riesgos:** Se obtienen los riesgos residuales a los que la empresa está actualmente expuesta.

b. Tratamiento de los riesgos:

Es el proceso de encontrar las medidas apropiadas para modificar el riesgo. En ese sentido, para el tratamiento de riesgos se plantea las siguientes opciones de mitigación: (INCIBE, 2015)

- ✓ Eliminar el riesgo
- ✓ Reducir el riesgo
- ✓ Compartir o transferir el riesgo
- ✓ Aceptar el riesgo

2.3.4. Información

Es un activo principal para el negocio de cualquier organización y representa toda comunicación o conocimiento. Brinda datos, definidos en cualquier formato digital (imagen, base de datos) o material (escritos en un papel). Es decir, puede estar contenida en cualquier medio, ya sea audiovisual, magnético u otro y puede ser compartida electrónicamente utilizando aplicativos sobre redes informáticas, no obstante, debido a esta creciente interconectividad, la información está expuesta a una variedad de amenazas y vulnerabilidades que pueden comprometer la continuidad del negocio (Secretaría de Gobierno Digital, 2017).

CAPÍTULO III

MATERIAL Y MÉTODO

"La verdadera sabiduría está en reconocer la propia ignorancia"

Sócrates.

CAPÍTULO III: MATERIAL Y MÉTODOS

En este capítulo se define la población que es objeto de estudio y la muestra que fue observada y descrita en la investigación. Se identifica el nivel y el diseño de la investigación. También se explican las técnicas de recolección utilizados para la obtención de los resultados. Finalmente se muestran y describen las técnicas estadísticas utilizadas para el análisis de los datos procesados.

3.1. MATERIAL Y PROCEDIMIENTO:

3.1.1. MATERIAL

Población

La población está constituida por todos los procesos institucionales de la Universidad Nacional de Trujillo.

Muestra

La muestra está constituida por los procesos académicos de la Universidad Nacional de Trujillo.

Unidad de análisis

El proceso académico constituido por los servicios de Matrícula, Notas y Asignaturas que son prestados por los procesos académicos de la Universidad Nacional de Trujillo.

3.1.2. PROCEDIMIENTOS

3.1.2.1. DISEÑO DE TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Se realizará un análisis comparativo de un nuevo tipo de Framework de seguridad y su influencia sobre los procesos institucionales de la Universidad Nacional de Trujillo, considerando un diseño pre experimental de tipo transversal, debido a que solo se tomó en cuenta un dominio de la Norma ISO 27002, el cual se evaluó en dos

momentos dados, “pre” (evaluación situacional) y “post” (luego de implementar el nuevo Framework).

$$G \quad O_1 \quad x \quad O_2$$

Donde:

G: Único grupo.

O_1: Análisis situacional de proceso académico.

O_2: Análisis a posteriori de proceso académico, con el Framework propuesto

- **Modelo:** Analítico

3.1.2.2. TÉCNICAS E INSTRUMENTOS

3.1.2.2.1. Técnicas e Instrumentos de Recolección de datos

Técnicas:

- Encuestas

  Para caracterizar el objeto de estudio, establecer el análisis situacional que permita proponer el Framework propuesto en la tesis.

- Observación

  Para recoger información directa de la realidad con respecto al objeto de estudio en la Universidad Nacional de Trujillo.

- Análisis FODA

  Para realizar el análisis situacional de la Universidad Nacional de Trujillo, respecto a la seguridad de la Información.

Instrumentos

- Encuesta de verificación de controles ISO 27002 en los servicios de Matrícula, Notas y Asignaturas
- Hoja de Requisitos del aplicativo virtual de soporte al Framework de seguridad
- Ficha de evaluación de confirmación de requisitos del aplicativo virtual de soporte al Framework de seguridad después de la implementación.
- Matriz FODA
- Cuestionario de percepción del aplicativo virtual de soporte al Framework de seguridad de la información

3.1.2.2.2. Técnicas e Instrumentos de Procesamiento y análisis de datos

Se tuvo en cuenta para la presente investigación aspectos de análisis estadístico de tipo descriptivo: teniendo en cuenta tablas de resumen, medidas descriptivas y de tipo inferencial, además de gráficos radiales para verificar el grado de cumplimiento de los controles de la ISO 27002. Para poder realizar la contrastación de hipótesis estadística, se propone la prueba no paramétrica "U de Mann-Whitney", y así evaluar la existencia significativa de mejora o no entre la implementación del nuevo Framework y la eficiencia que se puede tener en los procesos de gestión institucional de la Universidad Nacional de Trujillo. Todos estos procedimientos se realizaron apoyándose en software estadístico: IBM SPSS Statistics 22.0, y herramientas ofimáticas: Microsoft Excel.

3.1.3. METODOLOGÍA

A continuación, se describe la metodología seguida, la cual se trabajó siguiendo los siguientes pasos:

- Análisis del entorno interno y externo de la Universidad Nacional de Trujillo, relevando aspectos que corresponden a los procesos académicos y su relación con la gestión de la seguridad de la información.
- Evaluación de la implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.
- Desarrollar un prototipo de soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT.
- Hacer las pruebas funcionales en la versión piloto del proceso académico - servicios de Matrícula, Notas y Asignaturas – para las mediciones pertinentes.
- Obtención de resultados
- Discusión de resultados
- Elaboración de conclusiones y recomendaciones.

Variables y operativización de variables

VI: Framework de seguridad de la información.

VD: Gestión de la información en los procesos académicos.

Variables	Definición Conceptual	Indicadores	Tipo	Técnicas	Instrumentos
V. Independiente: Framework de seguridad de la información	Sistema organizado por un conjunto de especificaciones de seguridad de la información basado en el ISO 27002 para sistemas de gestión académica de la UNT en su versión piloto. Esta soportado por un Prototipo Informático del Sistema	Controles de seguridad de la información - ISO 27002.	Cuantitativa	Encuesta	Encuesta
		Funcionalidad de Prototipo	Cuantitativa	Observación	Aplicativo Virtual - App
		Número de Actividades	Cuantitativa	Observación	Tabla resumen de actividades del Framework
V. Dependiente: Gestión de la información en los procesos académicos.	Cubre la gestión de la información acerca de los procesos académicos que se dan en la UNT. En el caso específico se hará sobre la muestra del piloto.	Análisis del entorno: interno y externo y su relación con la Gestión de la información en los procesos académicos de la Universidad Nacional de Trujillo.	Cualitativo	Análisis FODA	Matriz FODA
		Disponibilidad	Cualitativo	Encuesta	Cuestionario
		Eficacia de Control	Cuantitativa	Observación	Aplicativo Virtual - App

CAPÍTULO IV

RESULTADOS

"El que aprende y aprende y no practica lo que sabe, es como el que ara y ara y no siembra"

Platón.

CAPÍTULO IV: RESULTADOS

A continuación, se describe el análisis de cada uno de los objetivos específicos propuestos en esta investigación.

4.1. Objetivo 1: Hacer un análisis del entorno tanto interno como externo de la UNT usando la matriz FODA para determinar las fortalezas, debilidades, oportunidades y amenazas, relevando lo que corresponde a los procesos académicos que se relacionan con la gestión de la información y son susceptibles de destrucción, sabotaje, fraude, violación de la privacidad, intrusismo, etc.

Se realizó un análisis del entorno tanto interno como externo de la UNT usando la matriz FODA para determinar las fortalezas, debilidades, oportunidades y amenazas, para determinar las que se relacionan con la Gestión de la seguridad de la información en el proceso académico.

FORTALEZAS

F1: Licenciamiento institucional por parte de la SUNEDU

F2: Certificación del proceso de admisión con la norma de Calidad ISO 9001

F3: Ubicarse entre las 15 primeras universidades respecto a investigaciones indexadas a nivel nacional

F4: Cuenta con centros productivos como CEPUNT, CIDUNT, RAFAEL NARVAEZ, ESCUELA DE POSTGRADO, COMEDOR UNIVERSITARIO, CESTUNT.

F5: Bajo coste de matrícula por semestre

F6: Brinda Educación Profesional gratuita y de reconocida calidad.

F7: Alto prestigio institucional por la competitividad profesional de los egresados

F8: Examen de admisión riguroso y competitivo

F9: Estudiantes de pregrado con alto nivel académico

F10: Servicios de asistencia social para los estudiantes

F11: Amplia expansión territorial de la Ciudad Universitaria

F12: Plana docente con amplia experiencia profesional.

OPORTUNIDADES:

O1: Llegada a la región de empresas e instituciones de especialización profesional con las cuales se pueden suscribir nuevos convenios

O2: Acceso a financiamiento del canon minero

O3: Acceso a pasarelas de pago como VISA para pagos masivos

O4: Posibilidad de apertura de nuevas carreras profesionales debido al alto nivel de demanda de servicios universitarios

O5: Posibilidad de apertura de nuevas sedes a nivel nacional debido al alto nivel de demanda de servicios universitarios

O6: Becas por parte del Estado para alumnos de bajos recursos económicos

O7: Demanda de estudios de Post-Grado.

DEBILIDADES:

D1: Devolución del canon minero por falta de capacidad de administración

D2: Huelgas administrativas, de docentes y alumnos

D3: Falta e incumplimiento de protocolos de seguridad

D4: Algunas escuelas cuentan con infraestructura e implementos obsoletos.

D5: Insuficiente cobertura de internet en toda la infraestructura de la UNT

D6: Falta de acreditación en algunas carreras

D7: Lentitud en los procesos administrativos

D8: Falta de un sistema de seguimiento y evaluación del desempeño de los estudiantes, egresados de las carreras profesionales y de postgrado

D10: La presencia de partidos políticos dentro de la Universidad impide el trabajo unificado

D11: Los sistemas informáticos de la Universidad no cuentan con una Arquitectura de Información de calidad.

AMENAZAS:

A1: Ingreso y/o apertura de nuevas sedes de universidades privadas en la región

A2: Fenómenos naturales que impidan el desarrollo de las actividades universitarias

A3: Está situada en una zona insegura para los administrativos y estudiantes de la institución.

A4: Robos de equipos y daño a la infraestructura de la institución

A5: Posibilidad de que el estado peruano valide estudios profesionales de inmigrantes sudamericanos

A6: Huelgas y conflictos que afecten el cronograma académico

A7: Posibilidad que el SUNEDU puede quitar el licenciamiento a la Universidad

A8: Posible reducción del financiamiento asignado a las universidades en el Presupuesto General de la República

A9: Creciente oferta de educación a distancia y semipresencial de instituciones educativas externas

A10: Creciente presencia de universidades privadas de diversos niveles de calidad

A11: Inestabilidad política en el país

A12. Mejor remuneración ofrecida a los docentes en las universidades privadas

Con la lista de componentes FODA, se procedió a organizarlos en la matriz FODA

Análisis externo Análisis Interno	OPORTUNIDADES	AMENAZAS
	O1: Llegada a la región de empresas e instituciones de especialización profesional con las cuales se pueden suscribir nuevos convenios. O2: Acceso a financiamiento del canon minero. O3: Acceso a pasarelas de pago como VISA para pagos masivos. O4: Posibilidad de apertura de nuevas carreras profesionales debido al alto nivel de demanda de servicios universitarios. O5: Posibilidad de apertura de nuevas sedes a nivel nacional debido al alto nivel de demanda de servicios universitarios. O6: Becas por parte del Estado para alumnos de bajos recursos económicos. O7: Demanda de estudios de Post-Grado.	A1: Ingreso y/o apertura de nuevas sedes de universidades privadas en la región. A2: Fenómenos naturales que impidan el desarrollo de las actividades universitarias. A3: Situada en una zona insegura para los administrativos y estudiantes de la institución. A4: Robos de equipos y daño a la infraestructura de la institución. A5: Posibilidad de que el estado peruano valide estudios profesionales de inmigrantes sudamericanos. A6: Huelgas y conflictos que afecten el cronograma académico. A7: Posibilidad que el SUNEDU puede quitar el licenciamiento a la Universidad. A8: Posible reducción del financiamiento asignado a las universidades en el Presupuesto General de la República. A9: Creciente oferta de educación a distancia y semipresencial de instituciones educativas externas. A10: Creciente presencia de universidades privadas de diversos niveles de calidad. A11: Inestabilidad política en el país. A12. Mejor remuneración ofrecida a los docentes en las universidades privadas.

FORTALEZAS	FO	FA
F1: Licenciamiento institucional por parte de la SUNEDU. F2: Certificación del proceso de admisión con la norma de Calidad ISO 9001. F3: Ubicarse entre las 15 primeras universidades respecto a investigaciones indexadas a nivel nacional. F4: Cuenta con centros productivos como CEPUNT, CIDUNT, RAFAEL NARVAEZ, ESCUELA DE POSTGRADO, COMEDOR UNIVERSITARIO, CESTUNT. F5: Bajo coste de matrícula por semestre. F6: Brinda Educación Profesional gratuita y de reconocida calidad. F7: Alto prestigio institucional por la competitividad profesional de los egresados. F8: Examen de admisión riguroso y competitivo. F9: Estudiantes de pregrado con alto nivel académico. F10: Servicios de asistencia social para los estudiantes. F11: Amplia expansión territorial de la Ciudad Universitaria. F12: Plana docente con amplia experiencia profesional.	FO1. Implementar cursos virtuales donde los docentes interactúen con los alumnos para fortalecer el aprendizaje académico. FO2. Realización de actividades o proyectos innovadores que resalten el conocimiento de los alumnos. FO3. Crear sitio web de información sobre los beneficios que el canon minero proporciona. FO4. Ampliar los servicios de pregrado y posgrado. FO5. Potenciar los trabajos de investigación de los estudiantes para la acreditación de escuelas profesionales. FO6. Promover herramientas tecnológicas, infraestructura, experiencia y compromiso del plantel docente para formar profesionales capaces de satisfacer y asumir retos según la demanda del mercado laboral.	FA1. Brindar información a la población acerca de las ventajas y oportunidades económicas que brinda la universidad respecto a las demás universidades privadas locales. FA2. Aprovechar el prestigio para gestionar la firma de convenios con empresas locales y nacionales. FA3. Organizar concursos de proyectos de investigación e invitar a empresarios, con el fin de que se reconozca el talento de los estudiantes. FA4. Capacitar a los docentes en la utilización de herramientas tecnológicas para la impartición de materias vía web.

DEBILIDADES	DO	DA
D1: Devolución del canon minero por falta de capacidad de administración. D2: Huelgas administrativas, de docentes y alumnos. D3: Falta e incumplimiento de protocolos de seguridad. D4: Algunas escuelas cuentan con infraestructura e implementos obsoletos. D5: Insuficiente cobertura de internet en toda la infraestructura de la UNT. D6: Falta de acreditación en algunas carreras. D7: Lentitud en los procesos administrativos. D8: Falta de un sistema de seguimiento y evaluación del desempeño de los estudiantes, egresados de las carreras profesionales y de postgrado D10: La presencia de partidos políticos dentro de la Universidad impiden el trabajo unificado. D11: Los sistemas informáticos de la Universidad no cuentan con una Arquitectura de Información de calidad	DO1. Creación de un centro especializado de cursos adicionales que permita a estudiantes y docentes especializarse o recibir conocimiento de su línea profesional. DO2. Implementar un cronograma anual para realización de evaluaciones de docentes. DO3. Implementar un sistema que haga el seguimiento correspondiente de nuestros egresados. DO4. Coordinar visitas periódicas por parte de la SUNEDU para fiscalizar la correcta asignación de los recursos presupuestales. DO5. Creación de un sistema bibliotecario virtual para los estudiantes (pregrado y postgrado) y docentes.	DA1. Incentivar al desarrollo de proyectos de investigación, a través de concursos premiados con becas estudiantiles. DA2. Implementar nuevas ofertas de cursos para tener mayor alumnado en postgrado. DA3. Planificar la adquisición de herramientas tecnológicas para brindar una mejor oferta educativa

Planteadas las estrategias, se puede identificar aquellas que tienen una **alta relación con la seguridad de la información y** que pueden ser susceptibles de eventos no deseados como destrucción, sabotaje, fraude, violación de la privacidad, intrusismo, etc. Esto se resume a continuación:

Estrategias FO
FO1. Implementar cursos virtuales donde los docentes interactúen con los alumnos para fortalecer el aprendizaje académico. FO3. Crear sitio web de información sobre los beneficios que el canon minero proporciona.
Estrategias FA
FA2. Aprovechar el prestigio para gestionar la firma de convenios con empresas locales y nacionales. FA3. Organizar concursos de proyectos de investigación e invitar a empresarios, con el fin de que se reconozca el talento de los estudiantes. FA4. Capacitar a los docentes en la utilización de herramientas tecnológicas para la impartición de materias vía web.
Estrategias DO
DO2. Implementar un cronograma anual para realización de evaluaciones de docentes. DO3. Implementar un sistema que haga el seguimiento correspondiente de nuestros egresados.
Estrategias DA
DA1. Incentivar al desarrollo de proyectos de investigación, a través de concursos premiados con becas estudiantiles. DA2. Implementar nuevas ofertas de cursos para tener mayor alumnado en postgrado. DA3. Planificar la adquisición de herramientas tecnológicas para brindar una mejor oferta educativa.

Es importante precisar que las estrategias identificadas se relacionan con la oferta educativa de la universidad y por ende con sus procesos académicos.

4.2. Objetivo 2: Evaluar la implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.

Se evaluó la implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de los procesos académicos de la UNT (servicios de Matrícula, Notas y Asignaturas). Para el desarrollo de este objetivo, se aplicó el instrumento de recolección de datos (Encuesta).

En lo que refiere al servicio de matrícula se ha podido identificar niveles de cumplimiento del 21% respecto a los controles de los dominios planteados por la Norma ISO 27002. Destacan la implementación de los controles 11. Seguridad Física y Ambiental; 15. Relaciones con Suministradores; y 17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.

En este servicio, existen dominios que no tienen controles establecidos. Estos dominios corresponden a los siguientes: 5. Políticas de Seguridad; 6. Aspectos Organizativos de la Seguridad de la Información; y 8. Gestión de Activos. Los controles restantes tienen un grado de implementación parcial. Lo descrito se muestra en la Figura 10.

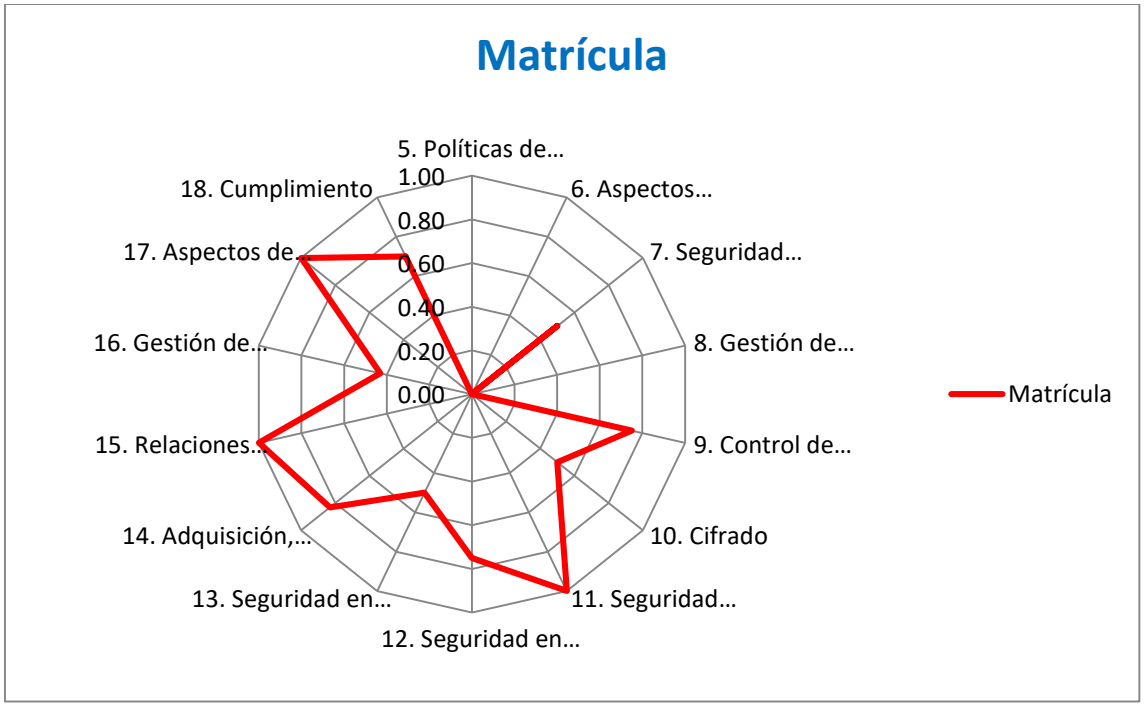


Figura 10: Grado de cumplimiento de los controles de la Norma ISO 27002 para el servicio de Matrícula.

En lo que refiere al servicio de notas se ha podido identificar niveles de cumplimiento del 36% respecto a los controles de los dominios planteados por la Norma ISO 27002. Destacan la implementación de los controles 8. Gestión de Activos; 9. Control de Accesos; 11. Seguridad Física y Ambiental; 14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información; y 15. Relaciones con Suministradores.

En este servicio, existen dominios que no tienen controles establecidos. Los dominios referidos son: 5. Políticas de Seguridad; 6. Aspectos Organizativos de la Seguridad de la Información; 7. Seguridad Ligada a los Recursos Humanos; 17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio; y 18. Cumplimiento. Los controles restantes tienen un grado de implementación parcial. Lo descrito se muestra en la Figura 11.

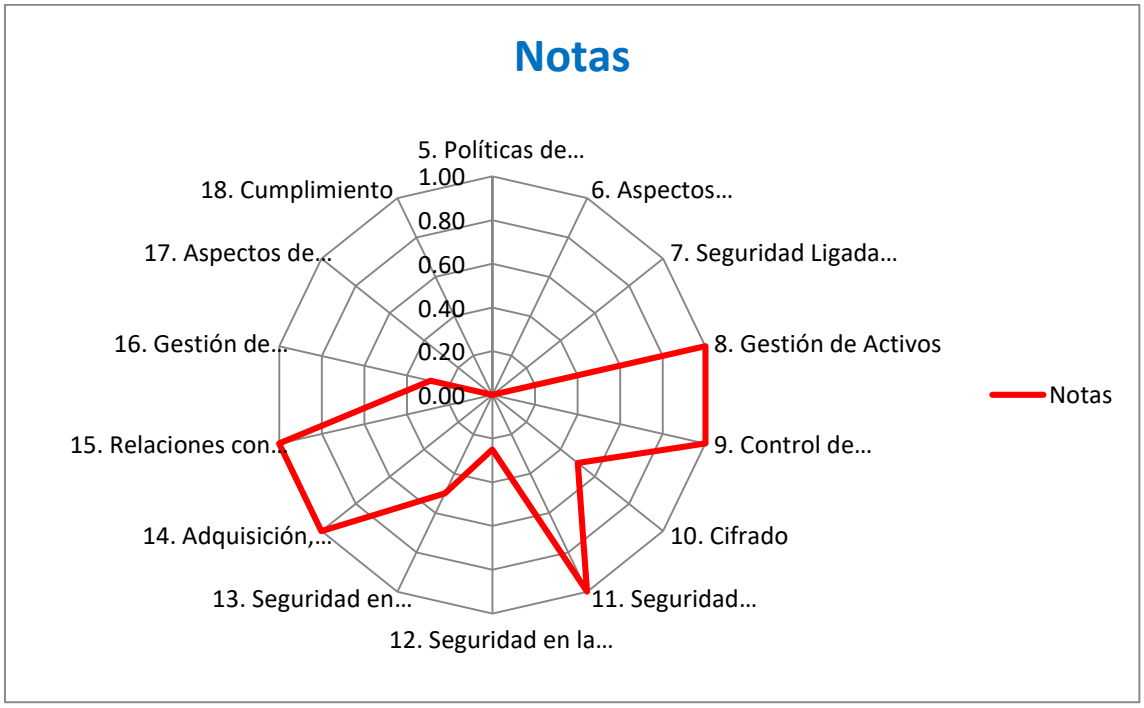


Figura 11: Grado de cumplimiento de los controles de la Norma ISO 27002 para el servicio de Notas.

En lo que refiere al servicio de gestión de asignaturas se ha podido identificar niveles de cumplimiento del 43% respecto a los controles de los dominios planteados por la Norma ISO 27002. Es este servicio el que presenta mayor nivel de cumplimiento respecto a los controles de seguridad de la información. Los dominios que destacan por su implementación son: 5. Políticas de Seguridad; 6. Aspectos Organizativos de

la Seguridad de la Información; 8. Gestión de Activos; 9. Control de Accesos; 11. Seguridad Física y Ambiental; y 15. Relaciones con Suministradores.

En este servicio, existen dominios que no tienen controles establecidos. Los dominios referidos son: 7. Seguridad Ligada a los Recursos Humanos; y 18. Cumplimiento. Los controles restantes tienen un grado de implementación parcial. Lo descrito se muestra en la Figura 12.

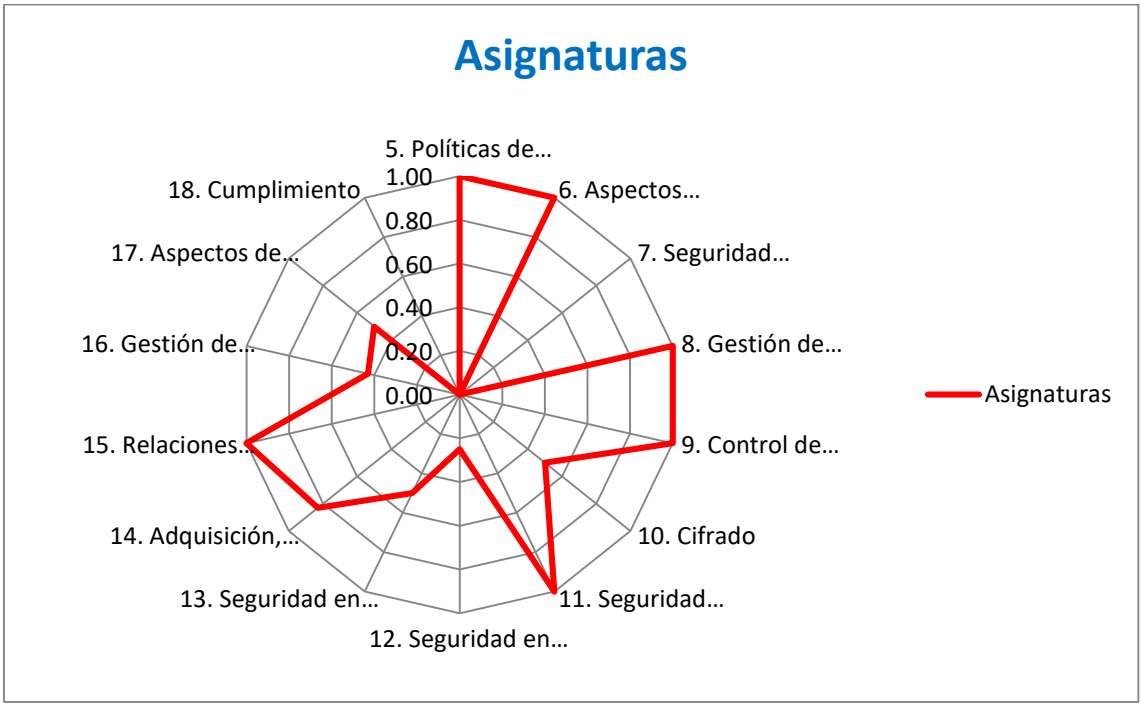


Figura 12: Grado de cumplimiento de los controles de la Norma ISO 27002 para el servicio de Gestión de Asignaturas.

En la Tabla 1, se visualiza el grado de implementación de los controles de los servicios de matrícula, notas y gestión de asignaturas. Como se describió en párrafos anteriores, el servicio con mayor grado de implementación de controles de seguridad es el servicio de gestión de asignaturas.

Tabla 1: Grado de cumplimiento de los controles de la Norma ISO 27002 para los servicios de Matrícula, Notas y Asignaturas.

Dominio	Matrícula	Notas	Asignaturas
5. Políticas de Seguridad	0.00	0.00	1.00
6. Aspectos Organizativos de la Seguridad de la Información	0.00	0.00	1.00

Dominio	Matrícula	Notas	Asignaturas
7. Seguridad Ligada a los Recursos Humanos	0.50	0.00	0.00
8. Gestión de Activos	0.00	1.00	1.00
9. Control de Accesos	0.75	1.00	1.00
10. Cifrado	0.50	0.50	0.50
11. Seguridad Física y Ambiental	1.00	1.00	1.00
12. Seguridad en la Operativa	0.75	0.25	0.25
13. Seguridad en las Telecomunicaciones	0.50	0.50	0.50
14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	0.83	1.00	0.83
15. Relaciones con Suministradores	1.00	1.00	1.00
16. Gestión de Incidentes en la Seguridad de la Información	0.43	0.29	0.43
17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	1.00	0.00	0.50
18. Cumplimiento	0.70	0.00	0.00
Grado de Cumplimiento	0.21	0.36	0.43

Este análisis inicial, permitirá establecer la situación futura deseada en el ámbito de la seguridad de la información para los servicios académicos de la Universidad Nacional de Trujillo.

4.3. Objetivo 3: Diseñar el nuevo Framework de gestión de la información de los procesos académicos de la UNT basado en los controles de la ISO 27002 de Gestión.

Se diseñó el nuevo Framework de gestión de la información de los procesos académicos de la UNT basado en los controles de la ISO 27002 de Gestión.

Para realizar la propuesta de marco de trabajo, se tuvo en cuenta el análisis interno y externo, así como el nivel de implementación de los controles de la ISO 27002. Es importante reiterar que las acciones que se plantean, se organizan considerando el enfoque de mejora continua (PDCA).

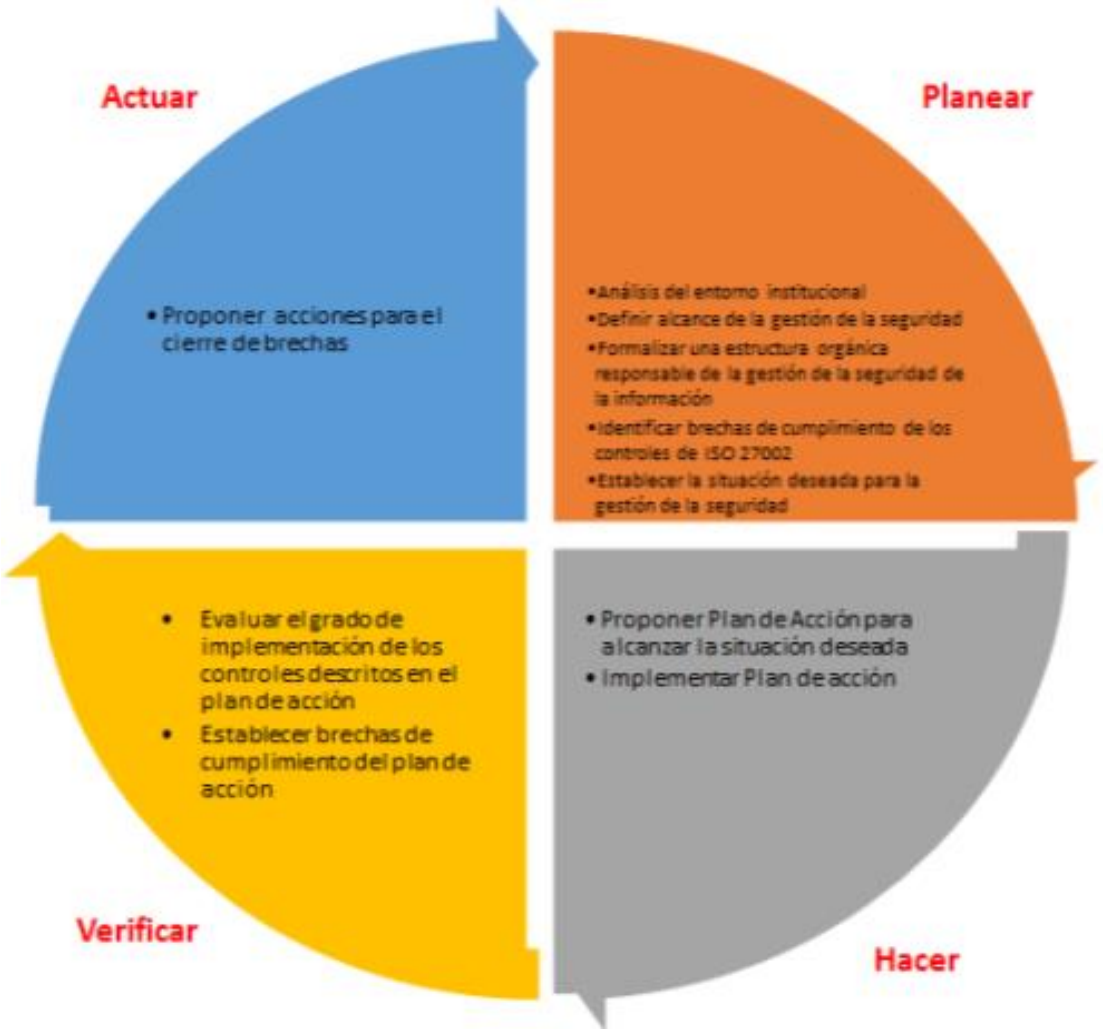


Figura 13: Marco de trabajo basado en los controles de la ISO 27002.

La descripción de las actividades propuestas para el marco de trabajo se describe en la siguiente tabla:

Tabla 2: Descripción de actividades del marco de trabajo basado en los controles de la ISO 27002 de Gestión.

Fase	Actividad	Descripción
Planear	Análisis del entorno institucional	Es la actividad por la cual la Universidad Nacional de Trujillo debe identificar los aspectos positivos y negativos del entorno, de tal forma que pueda establecer el impacto en la gestión de la seguridad de la información institucional, considerando las fortalezas y debilidades.

Fase	Actividad	Descripción
	Definir alcance de la gestión de la seguridad	La Universidad Nacional de Trujillo debe establecer los límites y la aplicabilidad de los controles que permitan ir construyendo de manera progresiva un Sistema de Gestión de la Seguridad de la Información.
	Formalizar una estructura orgánica responsable de la gestión de la seguridad de la información	La institución universitaria debe establecer una unidad orgánica que pueda operativizar la política de la seguridad de la información. A esta unidad, se le debe dotar de unidad y responsabilidad.
	Identificar brechas de cumplimiento de los controles de ISO 27002	La estructura orgánica responsable de la seguridad de la información en la Universidad, debe establecer el grado de implementación de los controles de la ISO 27002.
	Establecer la situación deseada para la gestión de la seguridad	En esta actividad se va a establecer la situación deseada a la que espera llegar la Universidad en términos de implementación de los controles de la ISO 27002.
Hacer	Proponer Plan de Acción para alcanzar la situación deseada	Se debe realizar esta actividad de tal forma que se establezcan los pasos a seguir para poder alcanzar la situación deseada. Se deben indicar los plazos y los recursos requeridos para desplegar el plan de acción generado.
	Implementar Plan de acción	El plan de acción debe desplegarse considerando las partes interesadas identificadas. Corresponde a la unidad responsable de la seguridad de la información velar por el cumplimiento de las acciones descritas en el plan.

Fase	Actividad	Descripción
Verificar	Evaluar el grado de implementación de los controles descritos en el plan de acción	Esta actividad permite establecer el grado de implementación de los controles de la norma ISO 27002 propuestos en el plan de acción. Corresponde a la unidad responsable de la seguridad de la información preparar esta información y comunicarla a las partes interesadas.
	Establecer brechas de cumplimiento del plan de acción	Las acciones de monitoreo, van a permitir establecer el grado de ejecución del plan y por ende las acciones no ejecutadas o ejecutadas de manera parcial. Es importante que se indague en las razones que no permitieron la ejecución y también el impacto que tiene el incumplimiento en términos de la seguridad de la información.
Actuar	Proponer acciones para el cierre de brechas del plan de acción	Se deben proponer actividades que permitan completar las acciones no ejecutadas en el plan de acción considerando lecciones aprendidas derivadas de las actividades de monitoreo.

4.4. Objetivo 4: Desarrollar un prototipo de soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT.

Se desarrolló un prototipo titulado: “Sistema WEB para el soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT”.

4.4.1. Marco de trabajo scrumban

4.4.1.1. Requerimientos

1. Registrar los datos de identificación de la empresa a ser evaluada.
2. Registrar el proceso a gestionar.
3. Registrar bitácora de dominios de seguridad
4. Registrar fases y actividades de cada fase.

5. Registrar análisis preliminar
6. Registrar iteraciones
7. Registrar objetivo y asignar dominios
8. Registrar plan de acción
9. Registrar implementación de plan de acción
10. Registrar evaluación y calcular el grado de implementación
11. Registrar brechas de cumplimiento
12. Registrar acciones para el cierre de brechas
13. Administrar el acceso del sistema
14. Se debe permitir subidas masivas de información
15. Contener un repositorio de documentos para permitir la subida de documentos escaneados correspondientes a las políticas, procesos y procedimientos firmadas y aprobadas por la alta dirección y el responsable de seguridad.
16. Se debe permitir exportar datos a Excel para ser analizados más fácilmente.

4.4.1.2. Visión

Desarrollar una herramienta web para el soporte en la implementación del framework de seguridad de la información basado en los controles de la ISO 27002 de gestión de seguridad de la información para los procesos académicos de la UNT.

4.4.1.3. Historias de usuario y firework

HU001: Registrar empresa evaluada

Como Oficial de seguridad de la información se requiere almacenar los datos de la empresa a ser evaluada para tener la identificación de la empresa.

Criterios de aceptación

- Caja de texto obligatorio para ingresar los nombres de la empresa y acepte 150 caracteres.
- Caja de texto obligatorio para ingresar la dirección de la empresa y acepte 150 caracteres.

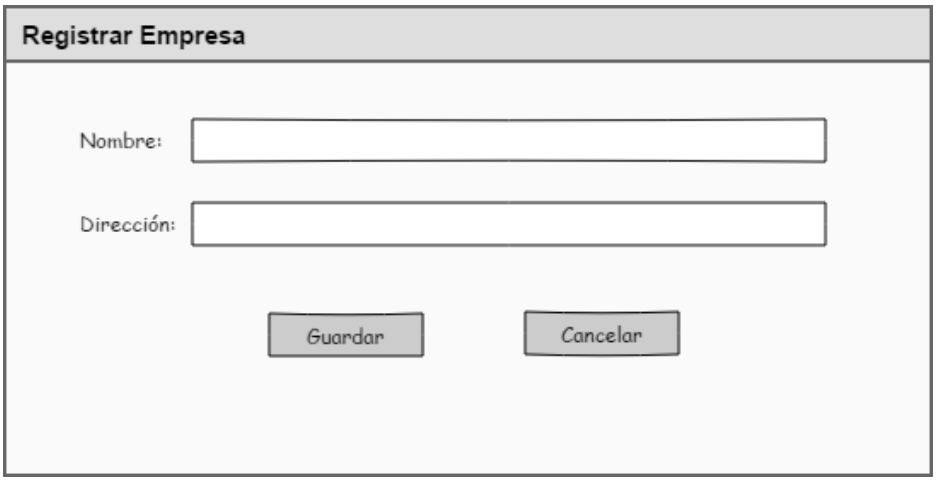


Figura 14: Registrar datos de empresa evaluada.

HU002: Crear usuarios del sistema

Como Oficial de seguridad de la información se requiere tener una opción para crear usuarios del sistema para garantizar la confidencialidad de la información que se maneja en el sistema.

Criterios de aceptación

- Caja de texto obligatorio para ingresar los nombres del usuario y acepte 150 caracteres.
- Caja de texto obligatorio para ingresar los apellidos del usuario y acepte 150 caracteres.
- Caja de texto obligatorio para ingresar el nombre de usuario que servirá para identificarlo en el sistema y acepte 15 caracteres alfanuméricos.
- Caja de texto obligatorio enmascarada para la clave de acceso al sistema y acepte máximo 50 caracteres alfanuméricos y caracteres especiales.
- Debe considerarse un botón para guardar los datos ingresados del usuario
- Debe considerarse un botón para cancelar la operación permitiendo que se limpien las cajas de texto.

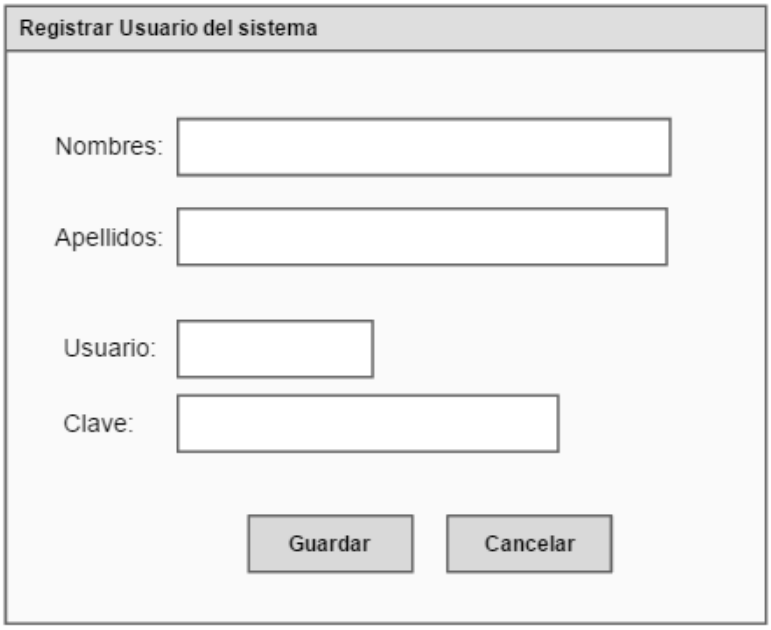


Figura 15: Registrar usuarios del sistema.

HU003: Administrar accesos del sistema

Como Oficial de seguridad de la información se requiere tener una opción para otorgar o denegar accesos de los usuarios a las opciones del sistema de tal forma que se haga uso adecuado de la información.

Criterios de aceptación

- Listar los usuarios registrados del sistema activos.
- A seleccionar el usuario se mostrarán en una grilla todas las opciones del sistema con una caja de ckeck a la izquierda donde se marcará las opciones a las que tiene acceso al sistema, a la derecha se habilitará un scroll para deslizarse por el listado de la grilla.
- Debe considerarse un botón para guardar las opciones marcadas por usuario
- Debe considerarse un botón para cancelar la operación permitiendo que se seleccione nuevamente el usuario.

Figura 16: Administrar accesos del sistema.

HU004: Registrar estudio preliminar

Como Oficial de seguridad de la información se requiere registrar el análisis preliminar de la fase de planificar del framework de seguridad para almacenar la evidencia inicial que sirve para la evaluación.

Criterios de aceptación

- Debe haber una caja de texto mixtilínea que permita redactar el análisis de estudio preliminar
- Debe permitir subir documentos adjuntos.

HU005: Registrar iteración del proceso

Como Oficial de seguridad de la información se requiere establecer el código que identifique la iteración, así como, su fecha de inicio, fecha fin para identificar la ejecución del framework de seguridad

Criterios de aceptación

- Debe haber una caja de texto obligatoria que acepte solo caracteres alfanuméricos y guiones
- Debe contener dos campos formateados para contener fechas, uno para la fecha de inicio y otro para la fecha de fin.

HU006: Registrar dominios asociados al objetivo

Como Oficial de seguridad de la información se requiere registrar el objetivo del proceso, así como asignar los dominios que cubre la evaluación para completar la fase de planificación

Criterios de aceptación

- Mostrar una lista de dominios de los cuales se marcarán los que se asocian a la evaluación.

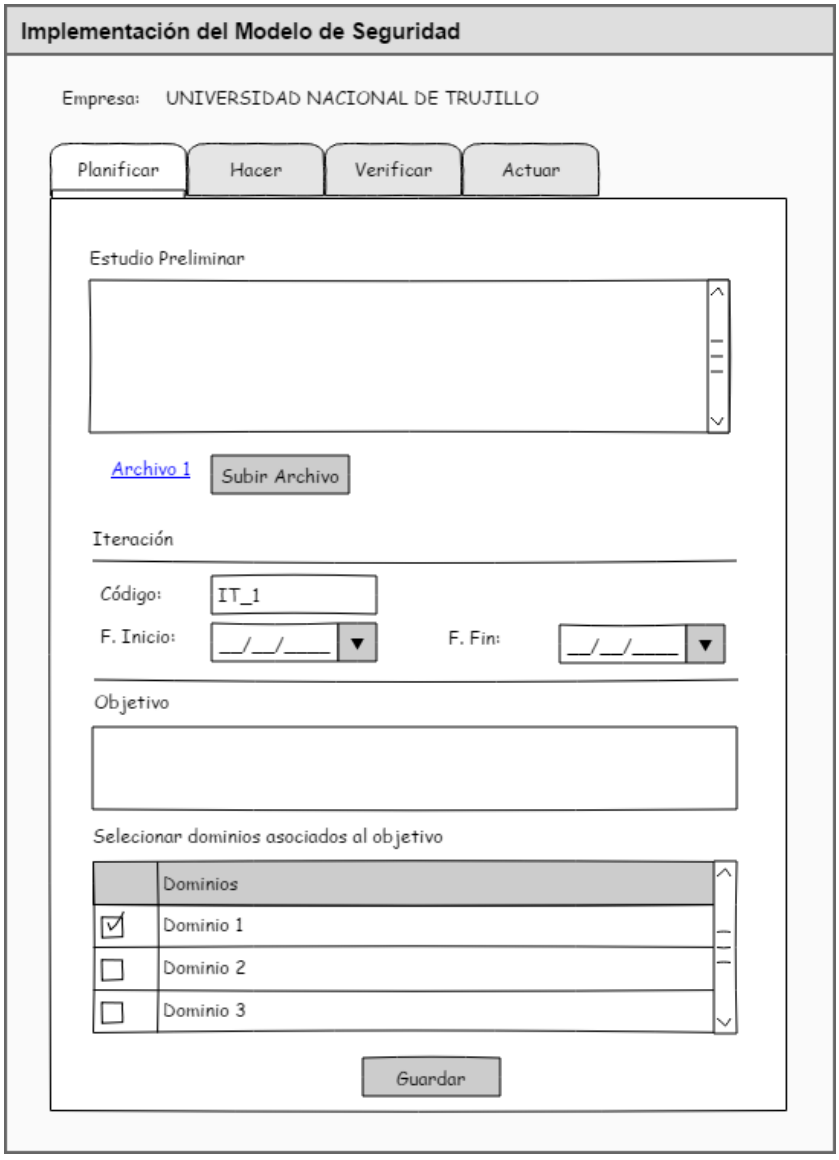


Figura 17: Registrar la fase Planificar.

HU007: Registrar Plan de acción

Como Oficial de seguridad de la información se requiere registrar el plan de acción como inicio de la fase de Hacer para almacenar la evidencia necesaria para la evaluación

Criterios de aceptación

- Mostrar el objetivo registrado.
- Mostrar la lista de dominios registrados.
- Según el dominio seleccionado se mostrará una grilla con los planes de acción asociados al dominio, si se desea agregar un plan de acción se debe abrir una ventana para agregar el detalle del plan de acción y se retornará a la pantalla origen. Si se desea eliminar un plan de acción se seleccionará de la grilla y se procederá a través de un botón de eliminación.

HU008: Registrar evidencias de seguimiento de Plan de acción

Como Oficial de seguridad de la información se requiere elaborar matriz de plan de acción y guardar las evidencias del seguimiento del plan de acción para guardar las evidencias que permita la evaluación

Criterios de aceptación

- Por cada plan de acción se podrá subir un documento de sustento el mismo que puede eliminarse y volverse a agregar.

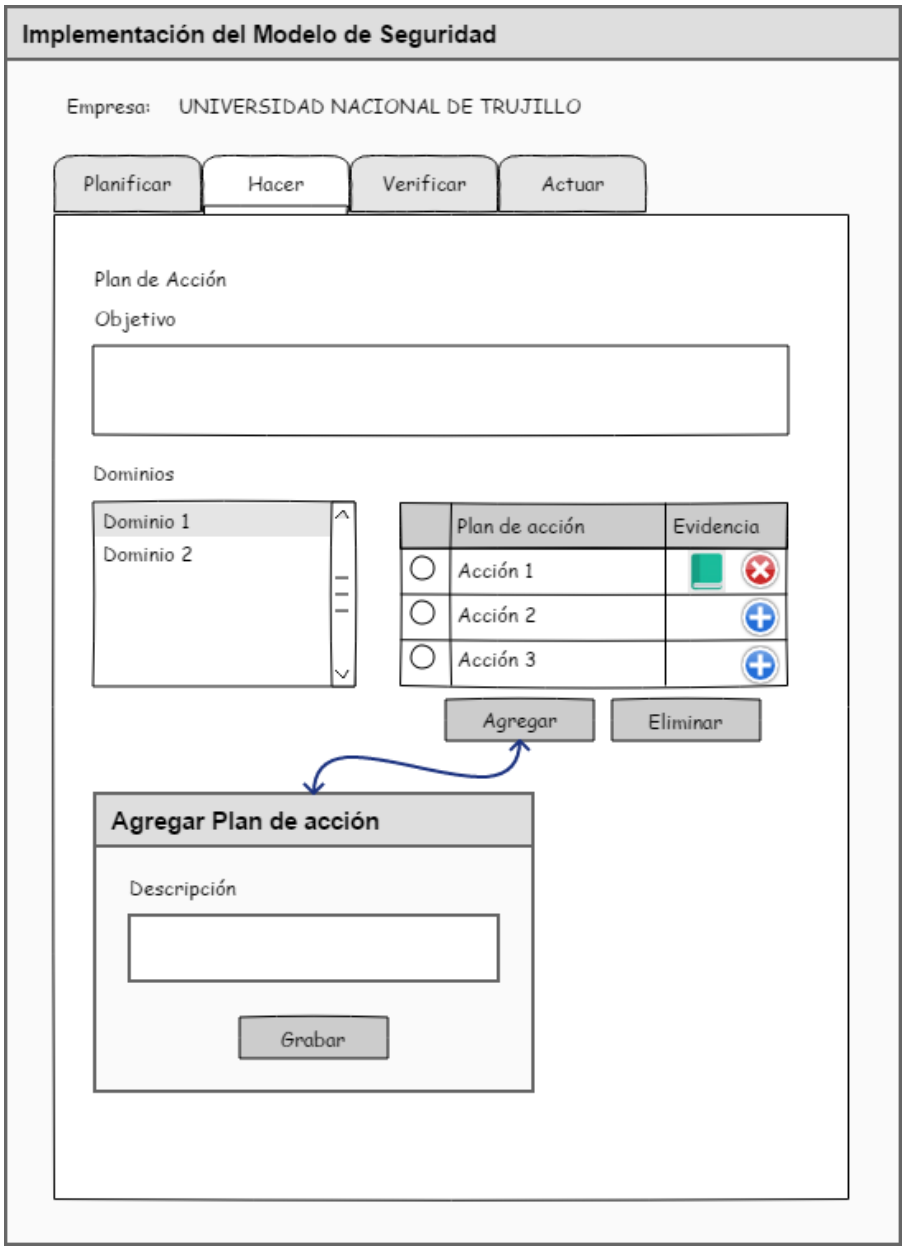


Figura 18: Registrar la fase Hacer.

HU009: Registrar evaluación de plan de acción y calcular el grado de implementación

Como Oficial de seguridad de la información se requiere registrar la evaluación según la matriz del plan de acción y calcular el grado de implementación para establecer las brechas de cumplimiento

Criterios de aceptación

- Se visualizará el objetivo registrado.

- Se mostrará una matriz con los dominios registrados y sus planes de acción. Por cada plan de acción se podrá marcar si es conforme su evaluación presentada como evidencia.
- Se mostrará el cálculo en porcentaje del valor obtenido de grado de cumplimiento cuyo valor es calculado dividiendo el número de planes de acciones marcados como conformes entre el número total de planes de acción registrados y multiplicados por 100.

HU010: Registrar Brechas de cumplimiento

Como Oficial de seguridad de la información se requiere registrar las brechas de cumplimiento para finalizar la fase de verificar

Criterios de aceptación

- Se visualizará el objetivo registrado.
- Se mostrará una matriz con los dominios registrados y sus planes de acción. Por cada plan de acción se podrá marcar si es conforme su evaluación presentada como evidencia.
- Se mostrará el cálculo en porcentaje del valor obtenido de grado de cumplimiento.
- Se mostrará una caja de texto para ingresar una anotación sobre las brechas de cumplimiento.
- Se mostrará un botón para adjuntar el documento sustentatorio de esta anotación.

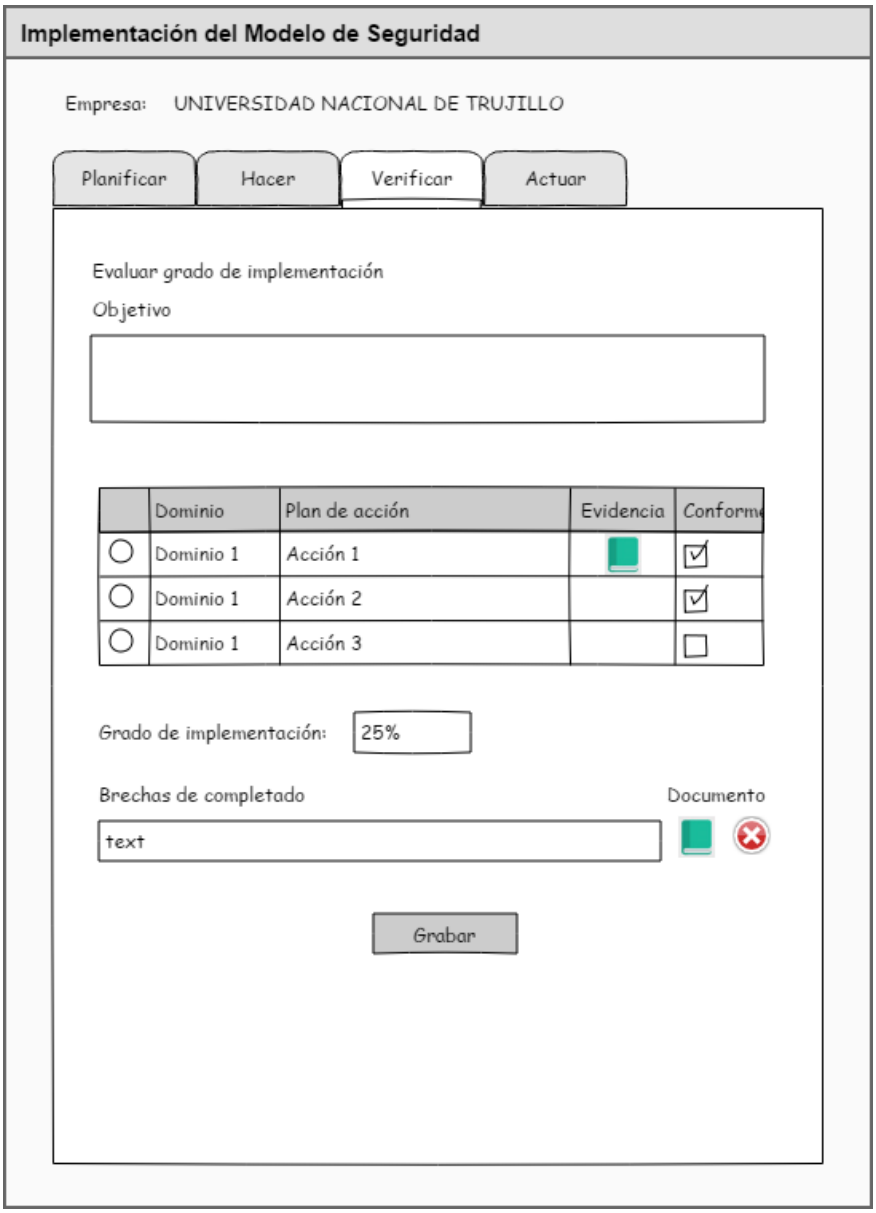


Figura 19: Registrar la fase Verificar.

HU011: Registrar cierre de brechas

Como Oficial de seguridad de la información se requiere almacenar documentos de acciones de cierre de brechas para cumplir con la fase de actuar

Criterios de aceptación

- Se visualizará el objetivo registrado.
- Se mostrará una matriz con los dominios registrados y sus planes de acción. Por cada plan de acción se podrá marcar si es conforme su evaluación presentada como evidencia.

- Se mostrará el cálculo en porcentaje del valor obtenido de grado de cumplimiento.
- Se mostrará la anotación sobre las brechas de cumplimiento y su documento sustentatorio.
- Se mostrará una caja de texto para ingresar una anotación sobre las brechas de cierre.
- Se mostrará un botón para adjuntar el documento sustentatorio de esta anotación.

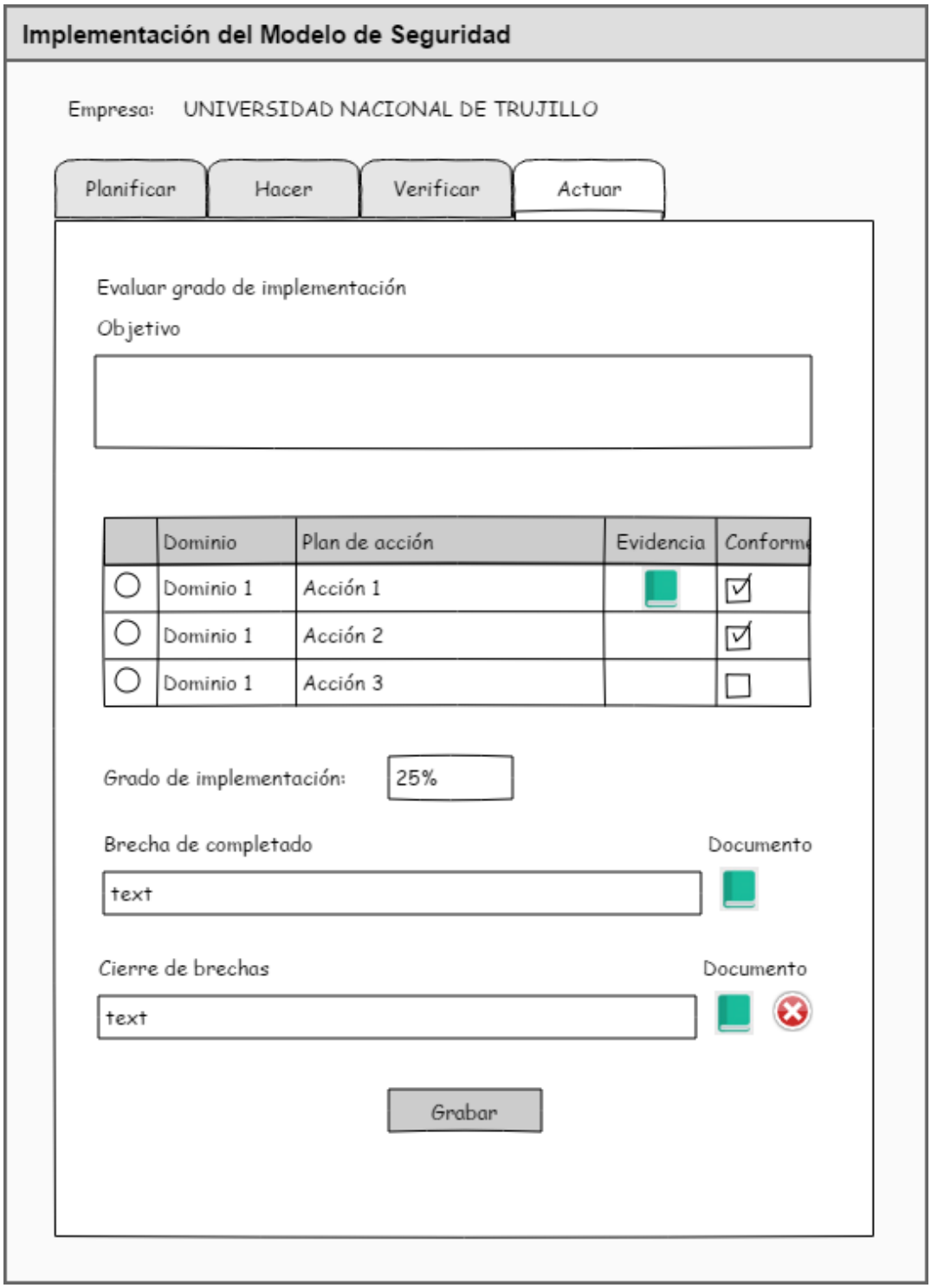


Figura 20: Registrar la fase Actuar.

4.4.1.4. Backlog del producto

HISTORIA DE USUARIO	VALOR DE NEGOCIO	PUNTOS
HU001: Registrar empresa evaluada	10	2
HU002: Crear usuarios del sistema	10	2
HU003: Administrar accesos del sistema	10	2
HU004: Registrar estudio preliminar	70	8
HU005: Registrar iteración del proceso	60	8
HU006: Registrar dominios asociados al objetivo	70	8
HU007: Registrar Plan de acción	70	10
HU008: Registrar evidencias de seguimiento de Plan de acción	80	10
HU009: Registrar evaluación de plan de acción y calcular el grado de implementación	70	10
HU010: Registrar Brechas de cumplimiento	80	8
HU011: Registrar cierre de brechas	40	8

4.4.1.5. Sprint backlog

Release 1 - Seguridad del sistema		
Prioridad	**Historia de Usuario**	**Estimación**
Sprint 1 - Velocidad 18		
1	HU002: Crear usuarios del sistema	5
2	HU003: Administrar Accesos del sistema	13

Release 2 - Gestión del Framework de seguridad		
Prioridad	**Historia de Usuario**	**Estimación**
Sprint 2 - Velocidad 18		
3	HU001: Registrar empresa evaluada	5
4	HU005: Registrar iteración del proceso	5
5	HU004: Registrar estudio preliminar	8
Sprint 3 - Velocidad 18		
6	HU006: Registrar dominios asociados al objetivo	5
7	HU007: Registrar Plan de acción	13
Sprint 4 - Velocidad 18		
8	HU008: Registrar evidencias de seguimiento de Plan de acción	13
9	HU010: Registrar Brechas de cumplimiento	5
Sprint 5 - Velocidad 18		
10	HU009: Registrar evaluación de plan de acción y calcular el grado de implementación	13
11	HU011: Registrar cierre de brechas	5

4.4.1.6. Tablero scrumban

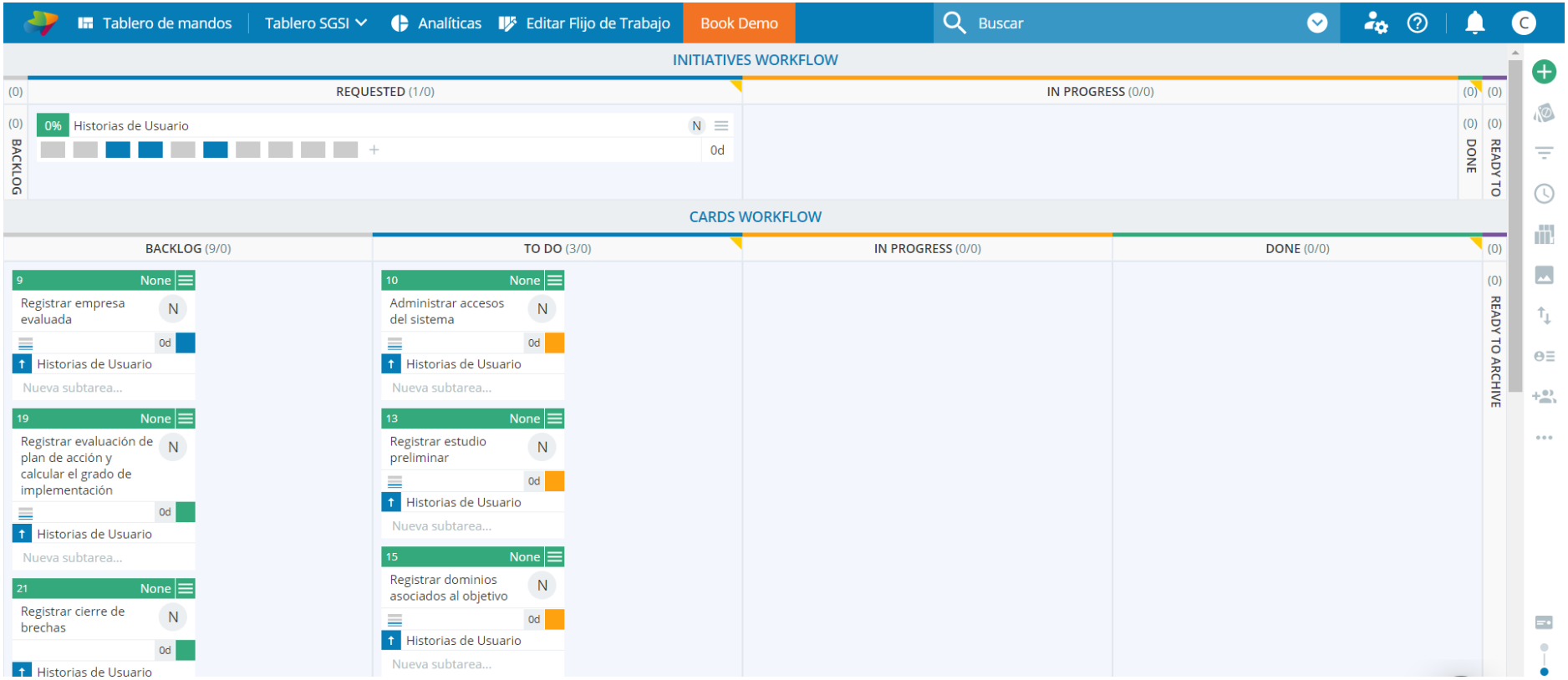


Figura 21: Tablero scrumban.

4.4.2. ARQUITECTURA

4.4.2.1. Diagrama de casos de uso

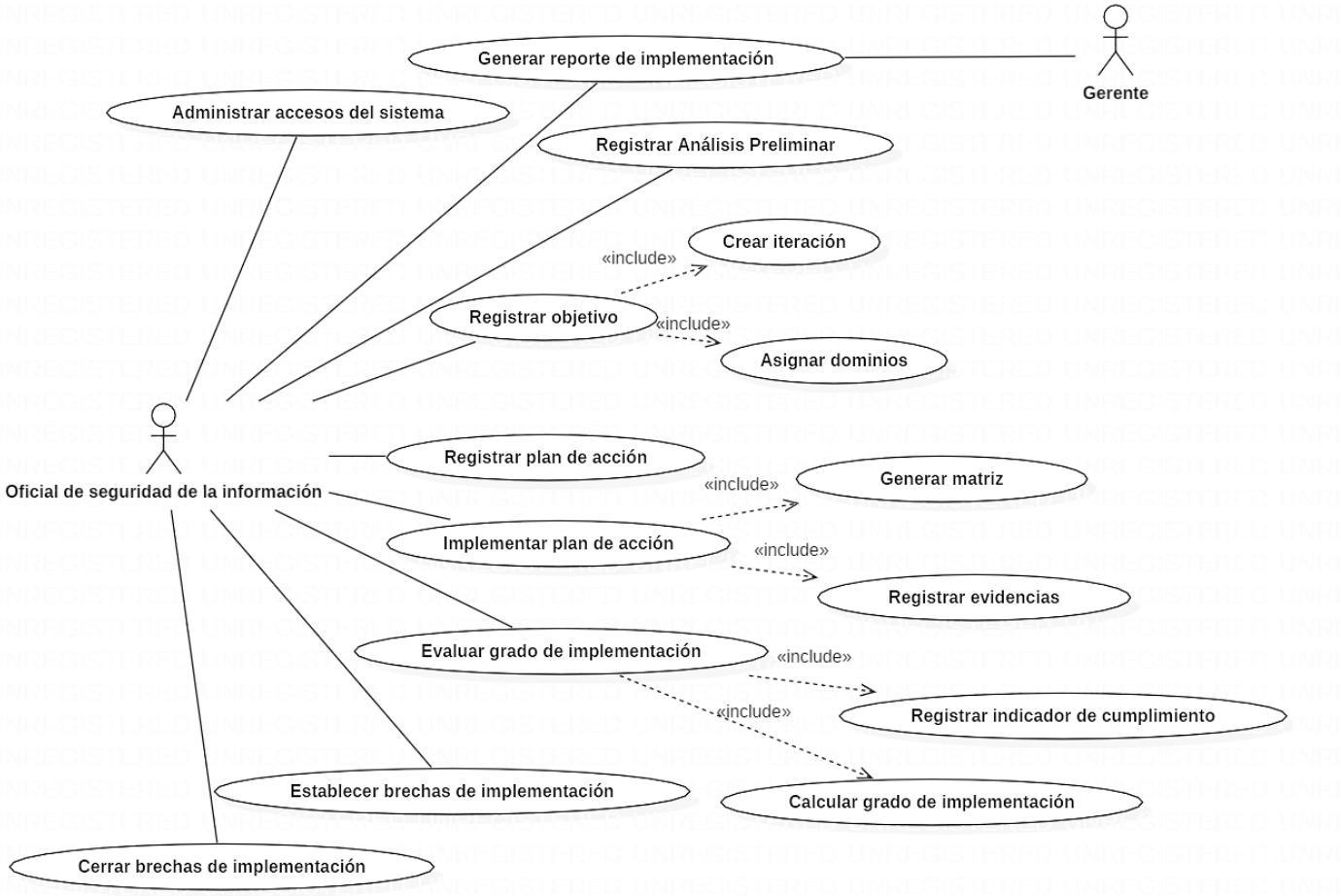


Figura 22: Diagrama de casos de uso.

4.4.2.2. Diagrama de Clases

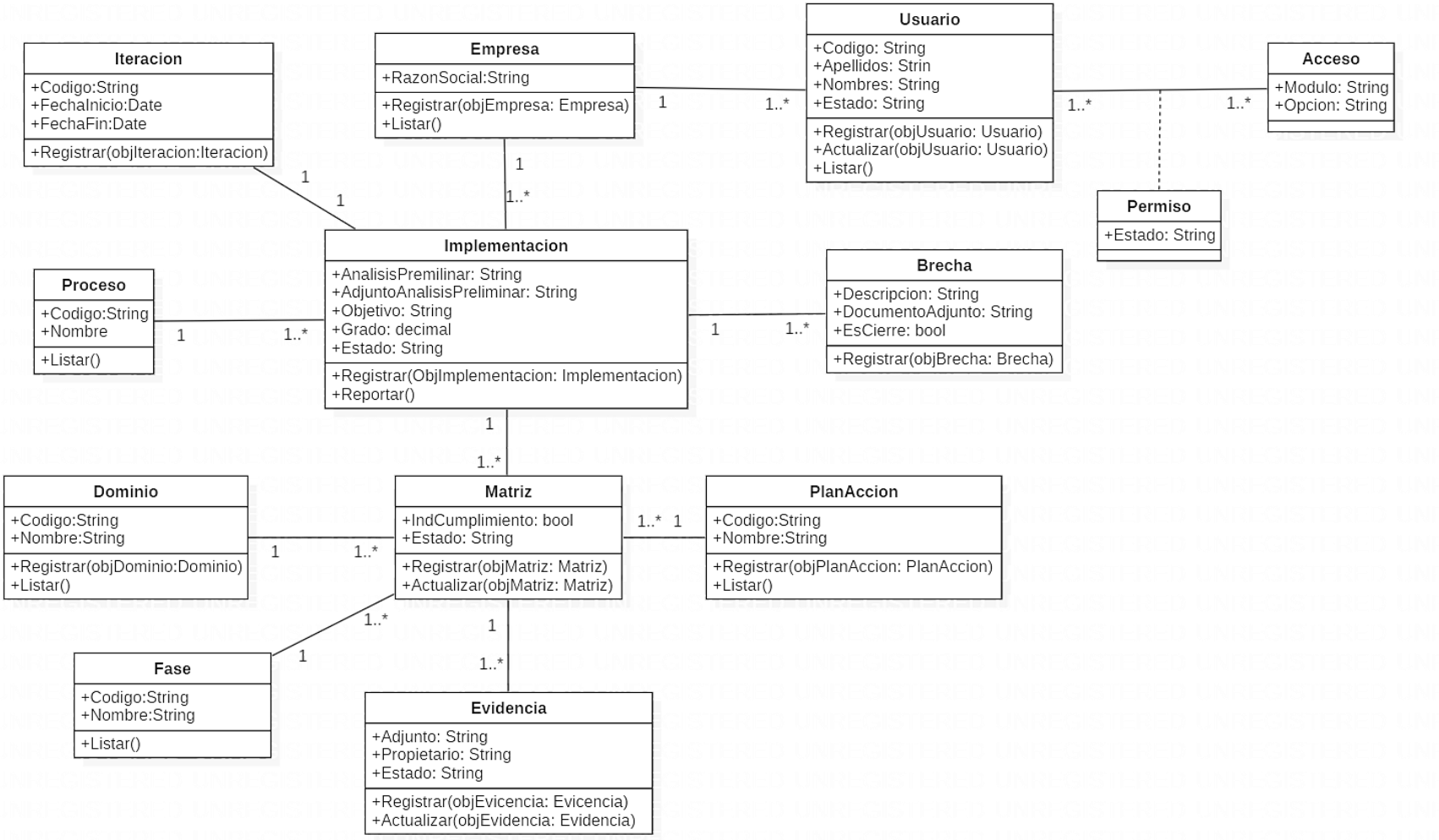


Figura 23: Diagrama de clases.

4.4.2.3. Diagrama de componentes Vista general

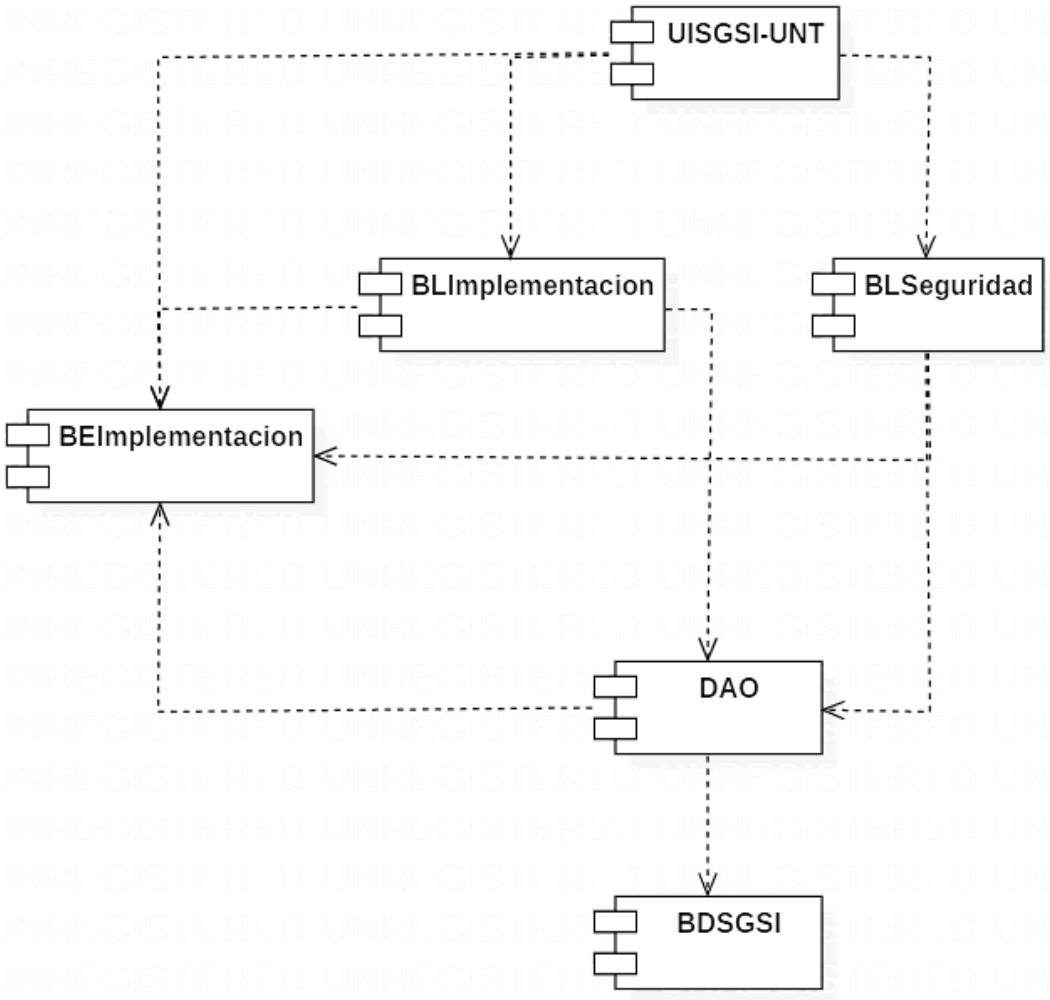


Figura 24: Diagrama de componentes Vista general.

4.4.2.4. Arquitectura Release 01: Seguridad del Sistema

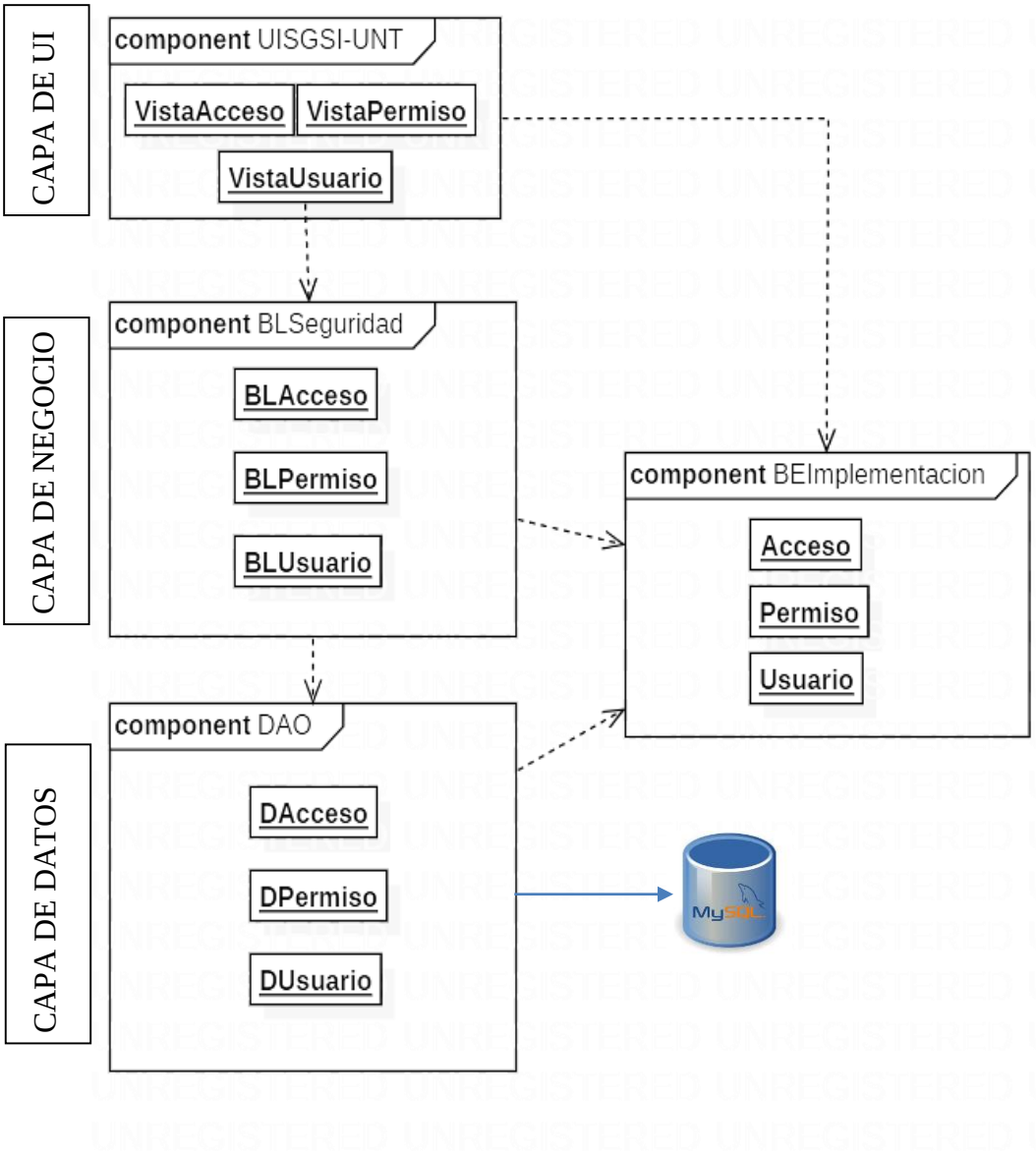


Figura 25: Arquitectura Release 01: Seguridad del Sistema.

4.4.2.5. Arquitectura Release 02: Gestión del Framework de Seguridad

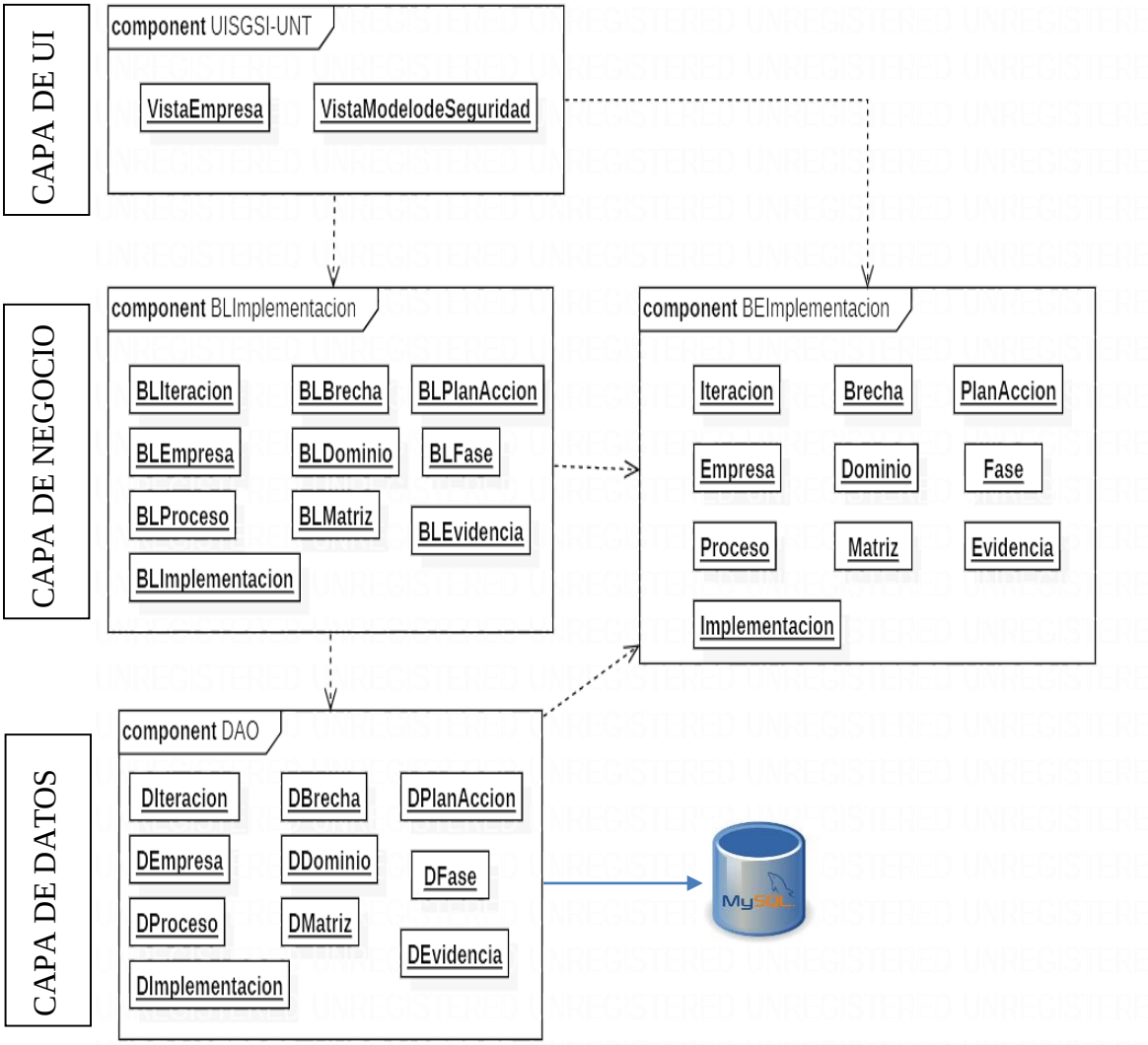


Figura 26: Arquitectura Release 02: Gestión del Framework de Seguridad.

Para poder registrar la evidencia de la primera iteración que considera el dominio de Gestión de Incidentes en la Seguridad de la Información se utilizó un software que permitió hacer pruebas en un entorno piloto.

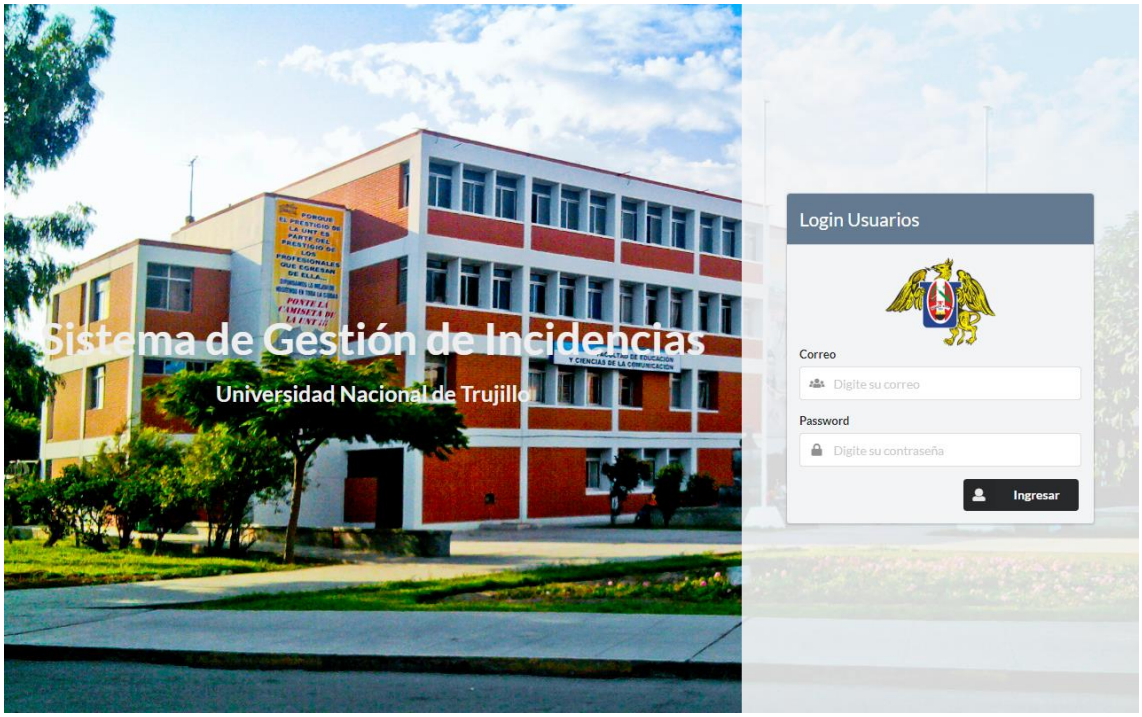


Figura 27: Software de Gestión de Incidentes.

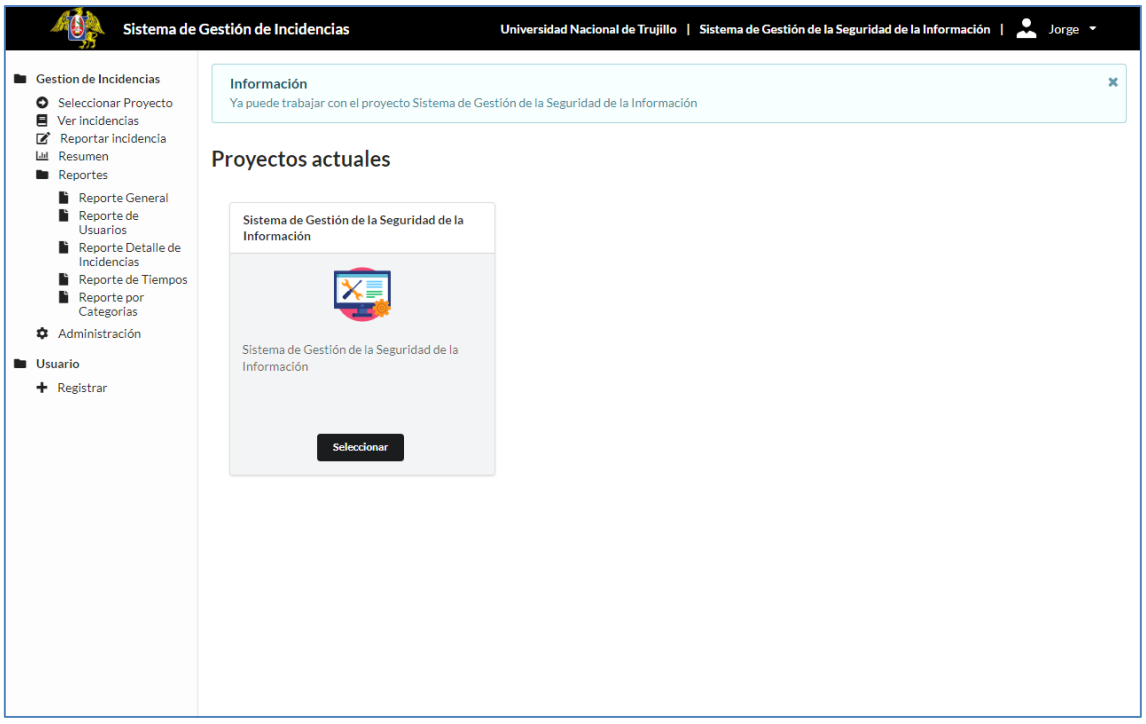


Figura 28: Panel de acceso al software de Gestión de Incidentes.

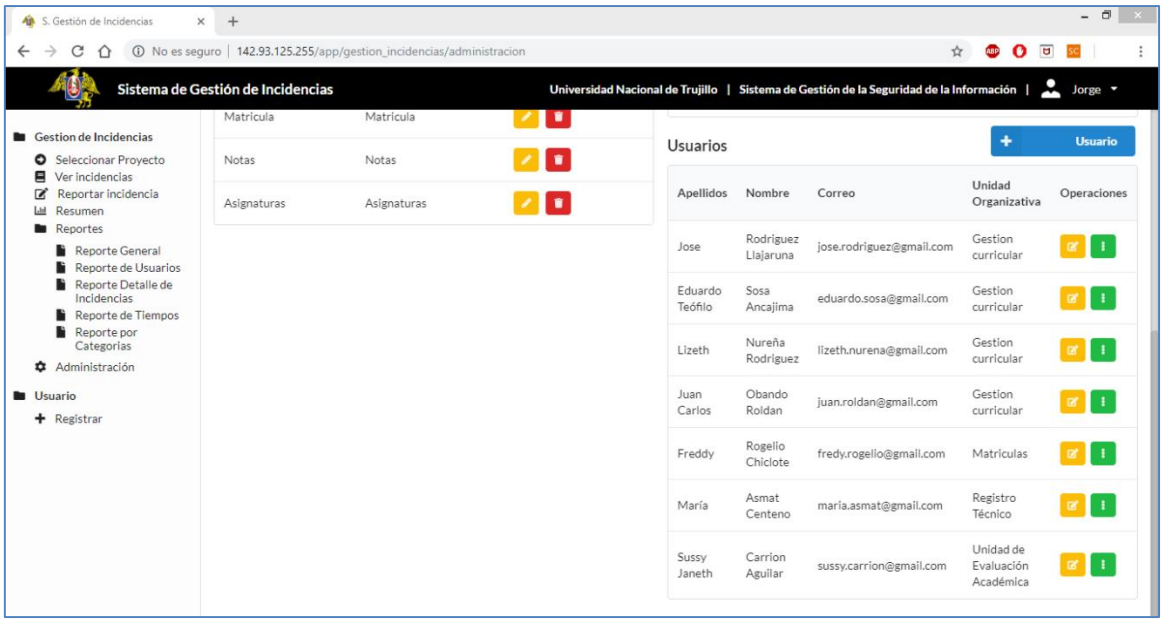


Figura 29: Lista de usuarios del software de Gestión de Incidentes.

4.5. Objetivo 5: Hacer las pruebas de funcionalidades en la versión piloto del proceso académico - servicios de Matrícula, Notas y Asignaturas – para las mediciones pertinentes.

Se hicieron las pruebas funcionales del proceso académico - servicios de Matrícula, Notas y Asignaturas – por un periodo de 30 días. Los resultados referidos al registro de incidentes de Seguridad de la información se muestran a continuación

Tabla 3: Incidentes registrados en el prototipo en un período de 30 días.

Categoría de incidentes / Servicio	Matrícula	Notas	Asignaturas	Total
Errores involuntarios	3	7	2	12
Denegación del servicio.	4	7	3	14
Modificación no autorizada.	1	0	0	1
Uso indebido de Activos de información	1	3	1	5
Uso Indebido de Software	0	1	0	1
Suplantación de Identidad	0	1	1	2
			Total	35

Implementar el procedimiento así como el software de Gestión de Incidentes de Seguridad de la Información, permite elevar el nivel de cumplimiento a 72 % del dominio analizado, siendo la principal restricción para un cumplimiento pleno la **implementación de la estructura orgánica,** responsable de la seguridad de la información así como la implementación de las instalaciones alternas que garanticen la continuidad de las operaciones en caso de eventos de desastre (inundaciones, incendios u otros) para los servicios de Matrículas, Notas y Asignaturas.

Respecto a la estructura orgánica, se recomienda formalizar la creación del Comité de Gestión de Seguridad de la Información y el puesto de Oficial de Seguridad de la Información. A continuación, el detalle de la propuesta:

- **Comité de Gestión de Seguridad de la Información**

  El comité de Gestión de Seguridad de la Información estará conformado por:

  - Rector
  - Director General de Administración
  - Gerente de Planificación y Desarrollo
  - Jefe de la Oficina de Asuntos Jurídicos
  - Director de Informática y Comunicaciones
  - Oficial de Seguridad de la Información (Puesto propuesto)

  Las siguientes son las principales funciones que asume el comité:

  - Al momento de su implementación el comité deberá definir un presidente y otros roles internos que se consideren necesarios, así como establecer la frecuencia de las reuniones y metodología de trabajo.
  - Formular y proponer las normas, controles, procedimientos y responsabilidades generales, asociados a la seguridad de la información.
  - Definir las estrategias de la institución con respecto a normas del Estado Peruano y estándares internacionales referidos a la seguridad de la información.
  - Velar por el cumplimiento y actualización de la Seguridad de la Información.
  - Proponer la revisión del cumplimiento de las políticas y buenas prácticas de Seguridad de la Información por entidades externas e independientes a la institución.

- Monitorear cambios significativos que pudieran variar los riesgos presentes en la Institución.
- Definir los lineamientos para implementar un Plan de Sensibilización de Seguridad de Información para el personal de la Universidad Nacional de Trujillo el cual comprenderá actividades de capacitación en coordinación con la Gerencia de Recursos Humanos, proponiendo su inclusión en el Plan anual de capacitaciones.
- Proponer que la seguridad de la información, en todos sus ámbitos, deba ser considerada como un ítem dentro de la evaluación periódica de desempeño del personal.
- Proponer el establecimiento de metas institucionales en materia de seguridad de la información, así como la periodicidad en que estas deben de lograrse dentro del planeamiento estratégico de la Entidad.
- Evaluar la necesidad de realizar auditorías de seguridad de la información y promover su ejecución en coordinación con las unidades orgánicas competentes.
- Proponer una metodología de evaluación y tratamiento de riesgos apropiados a la Seguridad de la Información y que correspondan a las actividades de la Universidad Nacional de Trujillo, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Determinar cuáles son las partes interesadas y sus necesidades con respecto a la Gestión de Seguridad de la Información en la Universidad Nacional de Trujillo
- Reportar de manera semestral, al Rector, el desempeño de la gestión de seguridad de la información.

- **Oficial de Seguridad de la Información:**

Persona designada por la Alta Dirección, que tendrá como principales responsabilidades las siguientes:

- Canalizar los riesgos tecnológicos en cada una de las unidades organizacionales de la Universidad.

- Coordinar activamente con los profesionales responsables de la seguridad de la información de las unidades orgánicas para definir controles y procedimientos que mitiguen los posibles riesgos que puedan afectar los procesos críticos de la Universidad.
- Monitorear y revisar la adecuada implementación de los controles y procedimientos de seguridad definidos como parte de la ejecución de los procesos críticos de la Universidad.
- Coordinar con la Gerencia de Planificación y Desarrollo que los aspectos de seguridad, sean considerados dentro del planeamiento institucional.
- Apoyar en la definición, implementación, validación y mantenimiento del Plan de Recuperación de Desastres de Sistemas, informando con la periodicidad que establezca el Comité de Gestión de Seguridad de la Información.
- Validar que los principales aspectos del Plan de Recuperación de Desastres de Sistemas sean probados cuando menos una vez al año, apoyando a las áreas involucradas en el planeamiento y supervisión de la ejecución de las pruebas.
- Verificar el cumplimiento y efectividad de las medidas de administración de riesgos relacionados a: seguridad lógica, seguridad física, seguridad del recurso humano, administración de operaciones, clasificación de seguridad y procedimientos de respaldo.
- Verificar que se mantengan las características de seguridad de la información definidas por el Comité de Gestión de Seguridad de la Información, cuando los procesos críticos sean objeto de una subcontratación; además de verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.
- Verificar y evaluar que la Dirección de Informática y Comunicaciones realice un inventario periódico de activos asociados a la tecnología de información según la clasificación del nivel de seguridad requeridos por dichos activos.
- Verificar que los cargos existentes en la organización tengan asociados perfiles de acceso acordes al principio “necesidad-de-conocer”, es decir,

el usuario sólo debe tener acceso a la información y recursos que necesita para completar o desarrollar las tareas que están asociadas al rol que el usuario tiene dentro de la Universidad.

- Verificar el cumplimiento y efectividad de los procedimientos de control y actualización de versiones y pases a producción.
- Verificar que el proceso para la aprobación de propuestas de desarrollo y/o adquisición de sistemas cuente con una descripción general de los riesgos identificados, requerimientos de seguridad y las acciones a tomar para controlar dichos riesgos.
- Garantizar la correcta implementación del Sistema de Seguridad de Información, definido para la Universidad

CAPÍTULO V

DISCUSIÓN

"El hombre más poderoso es aquel que es totalmente dueño de sí mismo"

Aristóteles.

CAPÍTULO V: DISCUSIÓN

En este capítulo se analizan e interpretan los resultados encontrados, enfatizando en aquellos que corresponden a aspectos importantes del estudio. Con los hallazgos, se identifica si los resultados concuerdan o disienten con los hallazgos de otros investigadores en el campo.

Para el presente estudio, se planteó la siguiente hipótesis: Un Framework de seguridad de la información incrementa el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002 en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.

5.1. Análisis de los resultados

En los resultados se han identificado estrategias que tienen una alta relación con la seguridad de la información y, por lo tanto, pueden ser susceptibles de eventos no deseados como destrucción, sabotaje, fraude, violación de la privacidad, intrusismo, etc.

Tabla 4: Análisis de estrategias asociadas a la seguridad de la información.

	Cantidad	**Porcentaje**
Estrategias Asociadas a la seguridad de la información	10	56%
Total Estrategias	18	100%

Este resultado se obtuvo utilizando la Matriz FODA confirmando lo que establece Rojas (2018) acerca de esta matriz, a la cual la considera como “una herramienta de análisis situacional”. Precisamente, se requirió establecer la necesidad de aplicar controles de seguridad de la información; por ello el análisis del entorno permitió confirmar que el direccionamiento estratégico que la Universidad Nacional de Trujillo establezca, puede ser susceptible de eventos no deseados como destrucción, sabotaje, fraude, violación de la privacidad, intrusismo.

Se evaluó el grado de implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de los procesos académicos de la UNT. El detalle de estos resultados, se encuentra en la Tabla 1: Grado de cumplimiento de los controles de la Norma ISO 27002 para los servicios de Matrícula, Notas y Asignaturas.

Se pudo identificar que aún hay brechas por cerrar en este ámbito, siendo el servicio de Matrícula el que presenta menor grado de cumplimiento (21%, ver Tabla 6). En este sentido, es una oportunidad para que las organizaciones puedan mejorar el nivel de seguridad de los servicios de información (Mohamed, 2016).

Tabla 5: Grado de cumplimiento Resumen de los controles de la Norma ISO 27002.

	Matrícula	**Notas**	**Asignaturas**
Grado de Cumplimiento	0.21	0.36	0.43

Vital (2019), Establece que se debe tener una estrategia para la implementación de la seguridad de la información para el mejoramiento en los procesos de confidencialidad, integridad y disponibilidad de la información en una organización. Coincidiendo con este concepto, se diseñó un Framework de gestión de la información de los procesos académicos de la UNT, de acuerdo a los controles de la ISO 27002 de Gestión. Este Framework se basa en el proceso de mejora continua de Deming (Planear, Hacer, Verificar y Actuar) y propone 10 actividades que deben desplegarse para mejorar los niveles de cumplimiento, aplicables a la Universidad y a instituciones universitarias del sector público.

De esa forma, se coincide con Sarkkinen (2017) que establece que el modelo organizacional establecido (Framework) puede aplicarse en corporaciones u organizaciones similares como soporte para la implementación y administración efectiva de los sistemas de gestión de seguridad.

Se desarrolló un prototipo de soporte al Framework de seguridad de la información, el cual consta de 11 historias de usuario y 13 clases que permitirán registrar las fases del marco de trabajo. Este objetivo se desarrolló teniendo en cuenta la necesidad que tienen los marcos de trabajo de contar con herramientas que hagan más fiable su aplicabilidad. Todo esto considerando a Seclén (2016), quien propone encontrar un punto de equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización.

En la investigación, se pudo obtener resultados en un dominio específico de la ISO 27002. El dominio en seleccionado fue el dominio 16: "Gestión de Incidentes en la Seguridad de la Información". En este dominio, se implementó un software de gestión de incidentes, lo cual permitió elevar el nivel de cumplimiento del dominio a 72 %. Avanzar en los otros controles se vislumbra como una tarea de mediano y largo plazo. En este sentido, se coincide con Seclén (2016), quien establece que se debe impulsar una política estratégica de estado que conlleve a formalizar funcionalmente el cargo de Oficial de Seguridad de Información para realizar un seguimiento de la ejecución del avance de la implementación del SGSI en las entidades públicas

Se hicieron las pruebas funcionales del proceso académico - servicios de Matrícula, Notas y Asignaturas – por un periodo de 30 días. Analizando los resultados se puede establecer que el 60% de los incidentes corresponden al factor humano (Ver Tabla 6). En este punto el estudio coincide con Mohamed (2016), quién estableció que muchas organizaciones implementan medidas técnicas de seguridad, pero descuidan el efecto que el comportamiento humano tiene en los sistemas de información. Es importante establecer que debe existir un equilibrio entre el factor tecnológico y humano por lo que se coincide con Huamán (2017), quién propone concientizar en buenas prácticas referidas al uso y manejo de la tecnología (entrenamiento) y mediante sus comportamientos (educación) para garantizar la protección y resguardo de la información de la Universidad.

Tabla 6: Incidentes registrados por el software de gestión de incidentes en la versión piloto.

Factor Asociado	Categoría de incidente / Servicio	Total	%
Humano	Errores involuntarios	12	60
	Modificación no autorizada.	1	
	Uso indebido de Activos de información	5	
	Uso Indebido de Software	1	
	Suplantación de Identidad	2	
Tecnológico	Denegación del servicio.	14	40
	Total	35	

De acuerdo a los resultados obtenidos, se establece que un Framework de seguridad de la información incrementa el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002 en la gestión de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas; habiéndose logrado el objetivo planteado en la investigación y por ende contrastar la hipótesis.

5.2. Contrastación de la Hipótesis

A continuación, se hará la contrastación de la hipótesis, haciendo uso de la metodología planteada y de los resultados encontrados, basados en las pruebas funcionales del proceso académico - servicios de Matrícula, Notas y Asignaturas – por un periodo de 30 días, con la aplicación del Framework de Seguridad de la Información basado en los controles de la ISO 27002.

- **Hipótesis Planteada**

  Un Framework de seguridad de la información incrementa el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002 en la gestión

de la información de los procesos académicos de la UNT en su versión piloto - servicios de Matrícula, Notas y Asignaturas.

Equivalentemente significa que:

El nivel de cumplimiento (de la Seguridad de Información) "Inicial" es MENOR al nivel de cumplimiento "Posterior" al de implementación (del Framework de Seguridad).

- **Hipótesis Nula:**

  Ho: Un Framework de seguridad de la información NO incrementa el nivel de cumplimiento de los controles propuestos por la Norma ISO 27002 en la gestión de la información.

  O que:

  El nivel de cumplimiento "Inicial" es MAYOR o IGUAL al nivel de cumplimiento "Posterior" al de implementación.

Así, y la Hipótesis alternativa:

H1: El nivel de cumplimiento "Inicial" es menor al "Posterior" de la implementación.

Nivel de significancia $\propto = 0.05$

Con los datos registrados de la Tabla 7 (Nivel de cumplimiento antes (AI) y después de la implantación (DI) del Framework), se procederá a la prueba de contrastación de hipótesis.

Tabla 7: Nivel de cumplimiento antes (AI) y después de la implantación (DI) del Framework.

Dominio	Matrícula		Notas		Asignaturas	
	AI	DI	AI	DI	AI	DI
16. Gestión de Incidentes en la Seguridad de la Información	0.43	0.72	0.29	0.72	0.43	0.72

Pruebas NPar

Prueba de Mann-Whitney

Rangos

	Grupos	N	Rango promedio	Suma de rangos
Medicion	Momento Pre	3	2,00	6,00
	Momento Post	3	5,00	15,00
	Total	6		

Estadísticos de prueba[a]

	Medicion
U de Mann-Whitney	,000
W de Wilcoxon	6,000
Z	-2,121
Sig. asintótica (bilateral)	**,034**
Significación exacta [2* (sig. unilateral)]	,100[b]

a. Variable de agrupación: Grupos

b. No corregido para empates.

Figura 30: Resultados de prueba no paramétrica.

Comentario:

Mediante la aplicación de la prueba no paramétrica "W. de Wilcoxon" y "U de Mann-Whitney" se evaluaron los valores medianos de los niveles de cumplimento en los dos momentos: "Antes" y "Después", y apreciamos que el "nivel de significancia bilateral" es 0.034 (menor a 0.05). Se rechaza Ho.

Podemos concluir que existe diferencia significativa en el momento "Antes" y "Después" (si hay cambios). Todo esto como consecuencia de la implementación del prototipo.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

"Haz sólo lo que amas y serás feliz, y el que hace lo que ama está benditamente condenado al éxito, que llegará cuando deba llegar, porque lo que debe ser, será; y llegará naturalmente"

Facundo Cabral.

Finalmente presentamos las conclusiones de la investigación **"FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT"** las cuales se basan en hallazgos redactados en el informe. También se incluyen las recomendaciones a ejecutar a partir de los resultados encontrados.

CONCLUSIONES

Se diseñó y desarrolló un Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información para los procesos académicos de la UNT en su versión piloto. Esto se vio reflejado en el desarrollo de los siguientes objetivos:

- Se realizó un análisis del entorno tanto interno como externo de la UNT usando la matriz FODA, logrando identificar 10 estrategias que se relacionan con la oferta educativa de la universidad, así como con sus procesos académicos y que tienen una alta relación con la seguridad de la información.
- Se evaluó el grado de implementación de políticas de seguridad de la información basadas en la ISO 27002 en la gestión de los procesos académicos de la UNT, obteniéndose los siguientes resultados: para los servicios de Matrícula, Notas y Asignaturas se identificaron un nivel de cumplimiento del 21%, 36% y 43% respectivamente. Siendo el servicio de Matrícula el que presenta menor grado de cumplimiento (21%).
- Se diseñó un Framework de gestión de la información de los procesos académicos de la UNT basado en los controles de la ISO 27002, que se basa en el proceso de mejora continua de Deming (Planear, Hacer, Verificar y Actuar) y propone 10 actividades que deben desplegarse para mejorar los niveles de cumplimiento, como se puede visualizar en la figura 13.
- Se desarrolló un prototipo de soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 para los procesos académicos de la UNT. El dominio en el que se centró el prototipo fue el dominio 16: "Gestión de Incidentes en la Seguridad de la Información". En este dominio, se implementó un software de gestión de incidentes, lo cual permitió elevar el nivel de cumplimiento del dominio a 72 %.

RECOMENDACIONES

- Se debe continuar analizando el entorno para evaluar los cambios que puedan existir en el ámbito de las fortalezas, debilidades, oportunidades y amenazas, que impacten en la seguridad de la información.
- Continuar evaluando el grado de implementación de políticas de seguridad de la información basadas en la ISO 27002 de Gestión de Seguridad de la Información en la gestión de los procesos académicos de la UNT de tal forma de elevar el grado de cumplimiento.
- Retroalimentar el Framework de gestión de la información propuesto de tal forma que se validen a plenitud las 10 actividades propuestas para el despliegue.
- Se recomienda formalizar la creación del Comité de Gestión de Seguridad de la Información y el puesto de Oficial de Seguridad de la Información para un cumplimiento pleno respecto a los controles de los dominios planteados por la Norma ISO 27002.
- Incorporar formalmente a la institución el prototipo de soporte al Framework de seguridad de la información basado en los controles de la ISO 27002 de Gestión de Seguridad de la Información y que este sea dotado por toda la institución.

REFERENCIAS BIBLIOGRÁFICAS

ACM/IEEE. (2017). *Information Technology Curricula 2017 IT2017 Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology A Report in the Computing Curricula Series Task Group on Information Technology Curricula Association for Computing Machinery (ACM) IEEE Computer Society (IEEE-CS)*. Retrieved from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf

ACM. (2006). Computing Curricula 2005: The Overview Report. In *ACM SIGCSE Bulletin* (Vol. 38). Retrieved from https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf

Acosta, J. (2018). *Recuperando la ciberseguridad: prepárese para enfrentar los ataques cibernéticos*. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-recuperando-la-ciberseguridad/$File/EY-recuperando-la-ciberseguridad.pdf

Areitio Bertolín, J. (2008). *Seguridad de la información : redes, informática y sistemas de información*. Madrid, España: Paraninfo.

Atalaya Vásquez, O. (2016). Propuesta de un sistema de seguridad de la información para la oficina de admisión y registro académico de la Universidad Privada Antonio Guillermo Urrelo, 2016 (Universidad Privada Antonio Guillermo Urrelo). Retrieved from http://repositorio.upagu.edu.pe/handle/UPAGU/96

Cano, J. (2014). *La función de seguridad de la información*. Retrieved from https://www.isaca.org/Journal/archives/2014/Volume-6/Documents/The-Information-Security-Function_joa_Spa_1114.pdf

D'Alessio Ipinza, F. (2015). *El proceso estratégico : un enfoque de gerencia* (3rd ed.). Lima, Perú: PEARSON.

Gelbstein, E. (2011). *La integridad de los datos*. Retrieved from https://www.isaca.org/Journal/Documents/11v6-Data-Integrity-Information-Securitys-Poor-Relation-spanish.pdf

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática*. Madrid, España: Alfaomega.

Huamán Monzón, F. M. (2017). Plan de comunicaciones en seguridad de la información

para el personal administrativo de la Pontificia Universidad Católica del Perú (Pontificia Universidad Católica del Perú). Retrieved from http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/8358

INCIBE. (2015). *Gestión de riesgos*. Retrieved from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

ISO/IEC 27002. (2005). *Information technology-Security techniques-Code of practice for information security management*. Retrieved from http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27002.pdf

ISO27000. (2012). El portal de ISO 27001. Gestión de Seguridad de la Información. Retrieved August 20, 2018, from http://www.iso27000.es/iso27000.html

Mercado Rojas, J. E. (2016). Modelo de gestión de seguridad de la información para el E-Gobierno (Universidad Nacional Mayor de San Marcos). Retrieved from http://cybertesis.unmsm.edu.pe/handle/cybertesis/6414

Merino Bada, C., & Cañizares Sales, R. (2014). *Auditoría de sistemas de gestión de seguridad de la información (SGSI)*. Retrieved from https://www.amazon.es/Auditoría-sistemas-gestión-seguridad-información/dp/8415683979

Mohamed, S. (2016). *An information security cultural framework* (Delft University of Technology). Retrieved from https://repository.tudelft.nl/islandora/object/uuid:fa493c67-3a6a-49a3-80c5-2e612d54d8fe?collection=education

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An Introduction to Information Security*. https://doi.org/10.6028/NIST.SP.800-12r1

PECB. (2016). ISO/IEC 27002:2013 Information Technology - Security Techniques Code of Practice for Information Security Controls. Retrieved August 20, 2018, from https://pecb.com/whitepaper/isoiec-270022013-information-technology---security-techniques-code-of-practice-for-information-security-controls

Pino Vera, J. A. (2014). *Marco de referencia para la implementación de un esquema gubernamental de seguridad de la información (EGSI), basado en la norma técnica ecuatoriana inen iso/iec 27001:2010 y en concordancia con el acuerdo 166* (Quito: Universidad de las Américas, 2014). Retrieved from http://dspace.udla.edu.ec/handle/33000/3107

Puga Hermosa, C. del P. (2017). *Propuesta de un modelo de gestión para mejorar la capacidad de gestión de la seguridad de la información de una institución financiera del sector público* (Quito: Universidad de las Américas, 2017.). Retrieved from http://dspace.udla.edu.ec/handle/33000/8282

Pwc. (2018). Strengthening digital society against cyber shocks: PwC. Retrieved August 10, 2018, from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html

Rojas Valera, J. K. (2018). Propuesta de un plan estratégico para la empresa SYMI S.R.L. Cajamarca, periodo 2018-2021 (Universidad Privada del Norte). Retrieved from http://repositorio.upn.edu.pe/handle/11537/13784

Sarkkinen, P. (2017). *Security Management systems for global high technology corporation, case Wärtsilä corporation* (Laurea-ammattikorkeakoulu). Retrieved from https://www.theseus.fi/handle/10024/122148?show=full

Seclén Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001 (Universidad Nacional Mayor de San Marcos). Retrieved from http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884

Secretaría de Gobierno Digital. (2017). *Política nacional de ciberseguridad*. Retrieved from http://www.gobiernodigital.gob.pe/docs/Política_Nacional_de_Ciberseguridad.pdf

Sullca Recharte, N. (2018). Propuesta de un marco de seguridad de la información en la nube pública para la SUNAT: Caso Sistema de Cuenta Única del Contribuyente (Universidad Peruana de Ciencias Aplicadas (UPC)). Retrieved from https://repositorioacademico.upc.edu.pe/handle/10757/625625

Superintendencia Nacional de Educación Superior Universitaria. (2018). Prensa: Superintendencia Nacional de Educación Superior Universitaria. Retrieved May 1, 2019, from https://www.sunedu.gob.pe/sunedu-otorga-licencia-institucional-numero-53-universidad-nacional-de-trujillo/

Ticona Aguilar, E. (2014). Evaluación de la gestión académica y competencias docentes en la formación profesional desde la percepción de los estudiantes del décimo semestre de la facultad de educación - UNMSM - 2013 (Universidad Nacional Mayor de San Marcos). Retrieved from http://cybertesis.unmsm.edu.pe/handle/cybertesis/3987

Universidad Nacional de Trujillo. (2019a). Carreras Profesionales: Universidad Nacional de Trujillo. Retrieved May 1, 2019, from http://www.admisionunt.info/carreras.php

Universidad Nacional de Trujillo. (2019b). Historia: Universidad Nacional de Trujillo. Retrieved May 1, 2019, from https://www.unitru.edu.pe/index.php/universidad/organizacion/historia-de-la-unt

Vital Cedillo, O. (2019). *Seguridad de la Información: Estrategia de Gestión basada en Marcos de Referencia de Control y Seguridad para las Organizaciones en México* (Universidad Nacional Autónoma de México). Retrieved from http://oreon.dgbiblio.unam.mx/F/K9RN9HXN555TICYCBX6QP5RTE2BHM7VI4YYEMS6AE9QNQTTQQC-34480?func=find-acc&acc_sequence=003097587

Viza Astulli, J. J. (2017). Clima institucional y gestión académica en la Universidad Nacional Micaela Bastidas de Apurímac 2016 (Universidad Nacional de San Agustín de Arequipa). Retrieved from http://repositorio.unsa.edu.pe/handle/UNSA/4658?show=full

ANEXOS

Anexo1: Cuestionario aplicado al responsable de TI

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN.

Estamos investigando aspectos que se relacionan a la Seguridad de la Información en los procesos académicos de la Universidad Nacional de Trujillo. Su colaboración es muy importante para que podamos detectar los aspectos positivos y negativos del proceso y nos permitirá aportar medidas de mejora oportunas.

I.- DATOS DE LA INSTITUCIÓN

1. **Nombre de la Institución:**

……..…….……..……..….

2. **Nombres y Apellidos:**

……..…….……..……..….

3. **Cargo Desempeñado:**

……..…….……..……..….

PREGUNTAS	SI	NO	N/A	OBSERVACIONES
¿El proceso cuenta con una política de seguridad de la información, establecida y aprobada por la alta Dirección, que además de las actividades propias de la institución considera las leyes y marco regulatorio?				
¿La política de seguridad, se encuentra procedimentada en un instrumento de gestión institucional sobre el cual se rige el personal de la institución?				
¿Los empleados conocen y ponen en práctica la política de seguridad de la información establecida por la alta dirección?				
¿La política de seguridad incluye a personal de otras áreas o partes interesadas externas a la institución?				
¿Se tiene identificada la información clave que se genera en el proceso?				
Respecto a la información sensible, ¿se establecen de manera clara y apropiada los roles y responsabilidades del personal?				
¿Se limita al personal el acceso a la información sensible del proceso?				

¿Se establecen mecanismos que Impiden el acceso físico no autorizado, daño e interferencia a la información?				
¿Conoce la existencia de controles que previenen la perdida, daño o robo de la información?				
¿Conoce la existencia de controles que mitiguen la interrupción de las operaciones de la organización?				
¿La información que requiere o se genera en el proceso es gestionada utilizando Sistemas de Información?				
¿Los Sistemas de Información se han desarrollado, considerando los requisitos de su proceso?				
¿La información que generan los sistemas de información, pueden ser accedidos desde Internet o ambientes externos a la institución?				
¿Cómo comunica los incidentes que se relacionan a la Seguridad de la información?				
¿Para los incidentes de Seguridad de la información que se relacionan con las Tecnologías, conoce el área o personal a quien debe reportarlo?				
¿Los tiempos de resolución de incidentes de Seguridad de la información están establecidos?				
¿Se cuenta con equipos que garanticen la continuidad de las operaciones ante los cortes de fluido eléctrico?				
¿Se cuenta con instalaciones alternas que garanticen la continuidad de las operaciones en caso de eventos de desastre (inundaciones, incendios u otros)?				
¿Tiene conocimiento de la Ley de Protección de datos Personales?				
¿Ha sido sensibilizado en el conocimiento de la Ley de Protección de datos Personales?				

MUCHAS GRACIAS POR SU COLABORACIÓN.

Anexo2: Cuestionario aplicado a los responsables de los servicios del Proceso Académico

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN.

Estamos investigando aspectos que se relacionan a la Seguridad de la Información en los procesos académicos de la Universidad Nacional de Trujillo. Su colaboración es muy importante para que podamos detectar los aspectos positivos y negativos del proceso y nos permitirá aportar medidas de mejora oportunas.

I.- DATOS DE LA INSTITUCIÓN

1. **Nombre de la Institución:**

……..…….……..……..….

2. **Nombres y Apellidos:**

……..…….……..……..….

3. **Cargo Desempeñado:**

……..…….……..……..….

PREGUNTAS	**SI**	**NO**	**N/A**	**OBSERVACIONES**
¿Se establecen y administran los perfiles de acceso a la información?				
¿Se limita el acceso a las instalaciones de procesamiento de la información?				
¿Se establecen mecanismos de encriptación que aseguren la protección de la confidencialidad de la información?				
¿Se cuenta con controles que previenen la perdida, daño o robo de la información? Indicar cuales.				
¿Se cuenta con controles que mitiguen la interrupción de las operaciones de la organización? Indicar cuales				
¿Se cuenta con controles que aseguren la protección de la información en las redes?				

¿Se cuenta con controles que aseguren la protección de las instalaciones de los equipos de red?				
¿Se ha implementado buenas prácticas que soporten el ciclo de vida de los sistemas de Información?				
¿Se cuenta con un procedimiento de gestión de requisitos de acuerdo al ciclo de vida de los sistemas de Información?				
¿Se han implementado controles de seguridad para los sistemas de información que son accedidos desde internet o desde el exterior?				
¿Existen Proveedores TI con acceso a las instalaciones de procesamiento de la información?				
¿Se cuenta con un procedimiento de gestión de incidentes?				
¿Se cuenta con una estructura orgánica y personal asignado para la gestión de incidentes?				
¿Se cuenta con equipos que garanticen la continuidad de las operaciones ante los cortes de fluido eléctrico?				
¿Se cuenta con instalaciones alternas que garanticen la continuidad de las operaciones en caso de eventos de desastre (inundaciones, incendios u otros)?				
¿Se han establecido controles tendientes a lograr el cumplimiento de la Ley de Protección de datos Personales?				

MUCHAS GRACIAS POR SU COLABORACIÓN.

Anexo3: Solicitudes para ejecutar la sensibilización del software de Gestión de incidentes

SOLICITA: PERMISO PARA PRUEBA PILOTO EN EL PROCESO ACADEMICO

Lic. ANTOLIN PRIETO MURCIA
DIRECTOR DE LA OFICINA DE REGISTRO TECNICO

Yo Jorge Antonio Jara Arenas, con DNI: 18134686, a usted me presento y expongo:

Con el debido respeto solicito la autorización para hacer la prueba piloto como parte del desarrollo de mi tesis de maestría, titulada: **"FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT"** que, permitiría la gestión de seguridad de la información en los procesos académicos de la universidad, dicha prueba piloto no tendrá costo alguno para la universidad, ni cambios en su infraestructura tecnológica, debido a que el sistema informático estará en la nube. Adicionalmente se me autorice la posibilidad de realizar programas de capacitación a su personal para un buen uso de la información.
Por lo expuesto, solicito se me proporcione las fechas para realizar los programas de capacitación y la prueba piloto, según documento adjunto de cronograma de actividades.

Agradeciendo la atención a la presente.

Atentamente,

Trujillo, 08 de Febrero del 2019.

Firma
Nombre: Jorge Antonio Jara Arenas
D.N.I. Nº 18134686

Se adjunta:
- Cronograma de Actividades

UNIVERSIDAD NACIONAL DE TRUJILLO
FECHA: 11 FEB. 2019
FIRMA: HORA:

SOLICITA: PERMISO PARA PRUEBA PILOTO EN EL PROCESO ACADEMICO

Dra. ROSA MORENO
JEFA DE LA DIRECCION DE DESARROLLO ACADEMICO

Yo Jorge Antonio Jara Arenas, con DNI: 18134686, a usted me presento y expongo:

Con el debido respeto solicito la autorización para hacer la prueba piloto como parte del desarrollo de mi tesis de maestría, titulada: **"FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT"** que, permitiría la gestión de seguridad de la información en los procesos académicos de la universidad, dicha prueba piloto no tendrá costo alguno para la universidad, ni cambios en su infraestructura tecnológica, debido a que el sistema informático estará en la nube. Adicionalmente se me autorice la posibilidad de realizar programas de capacitación a su personal para un buen uso de la información.
Por lo expuesto, solicito se me proporcione las fechas para realizar los programas de capacitación y la prueba piloto, según documento adjunto de cronograma de actividades.

Agradeciendo la atención a la presente.

Atentamente,

Trujillo, 08 de Febrero del 2019.

Firma
Nombre: Jorge Antonio Jara Arenas
D.N.I. N° 18134686

Se adjunta:
- Cronograma de Actividades

UNIVERSIDAD NACIONAL DE TRUJILLO
DIRECCION DE DESARROLLO ACADEMICO
12 FEB 2019
Registro #
Folios: 02 Firma:
Hora: 8:30

SOLICITA: PERMISO PARA PRUEBA PILOTO EN EL PROCESO ACADEMICO

Dra. HILDA JARA LEON
JEFA DE LA UNIDAD DE ESTUDIOS GENERALES

Yo Jorge Antonio Jara Arenas, con DNI. 18134686, a usted me presento y expongo:

Con el debido respeto solicito la autorización para hacer la prueba piloto como parte del desarrollo de mi tesis de maestría, titulada: "**FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT**" que, permitiría la gestión de seguridad de la información en los procesos académicos de la universidad, dicha prueba piloto no tendrá costo alguno para la universidad, ni cambios en su infraestructura tecnológica, debido a que el sistema informático estará en la nube. Adicionalmente se me autorice la posibilidad de realizar programas de capacitación a su personal para un buen uso de la información.
Por lo expuesto, solicito se me proporcione las fechas para realizar los programas de capacitación y la prueba piloto, según documento adjunto de cronograma de actividades.

Agradeciendo la atención a la presente.

Atentamente,

Trujillo, 08 de Febrero del 2019.

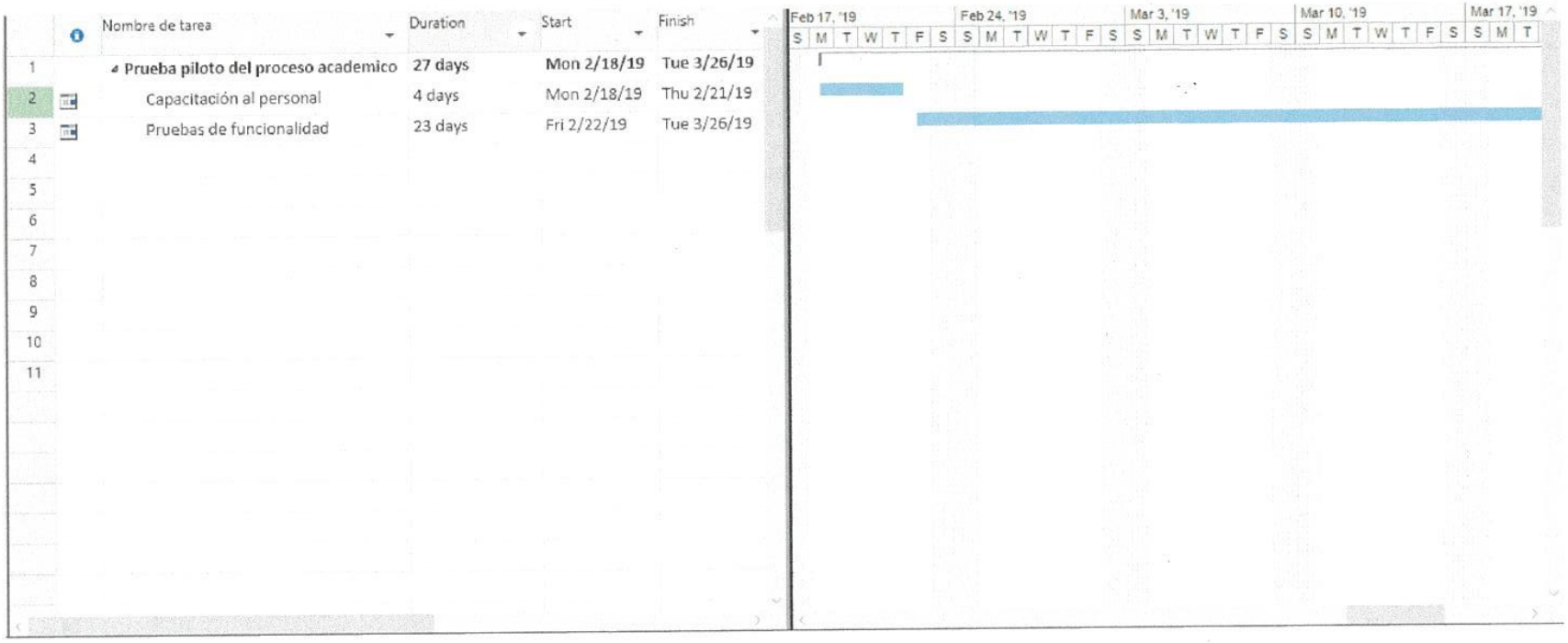
Firma
Nombre: Jorge Antonio Jara Arenas
D.N.I. N° 18134686

Se adjunta:
- Cronograma de Actividades

UNIVERSIDAD NACIONAL DE TRUJILLO
ESTUDIOS GENERALES
RECIBIDO
11 FEB. 2019
Folios: Firma:
Hora: 11:05 am

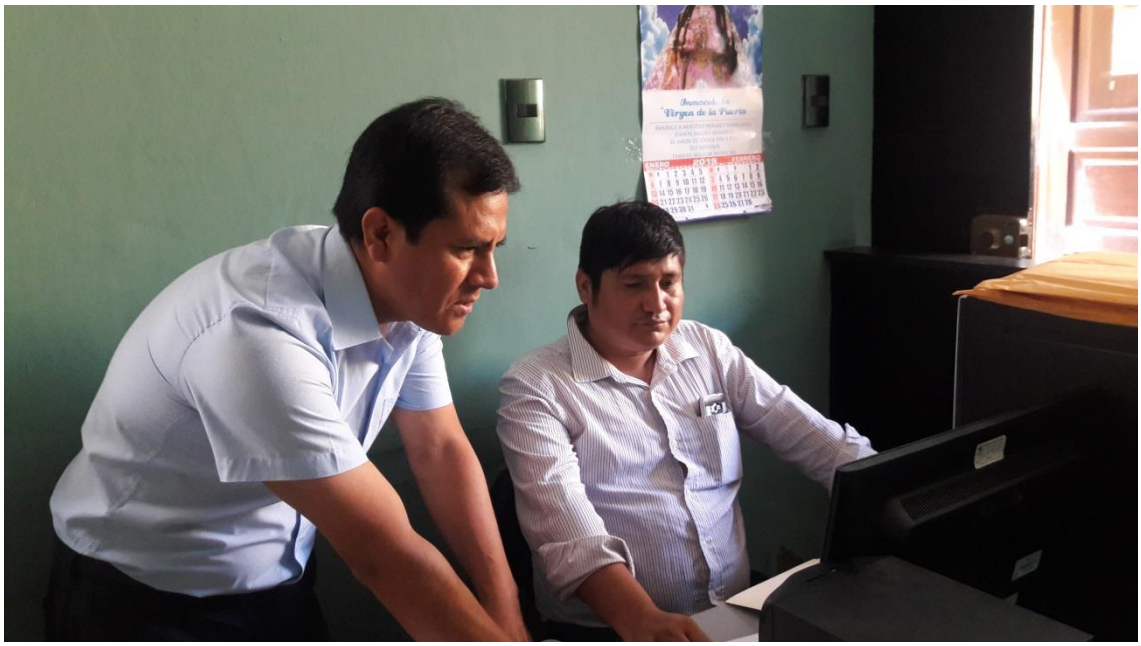
Anexo4: Cronograma de Sensibilización del software de Gestión de incidentes al personal de los servicios del Proceso Académico

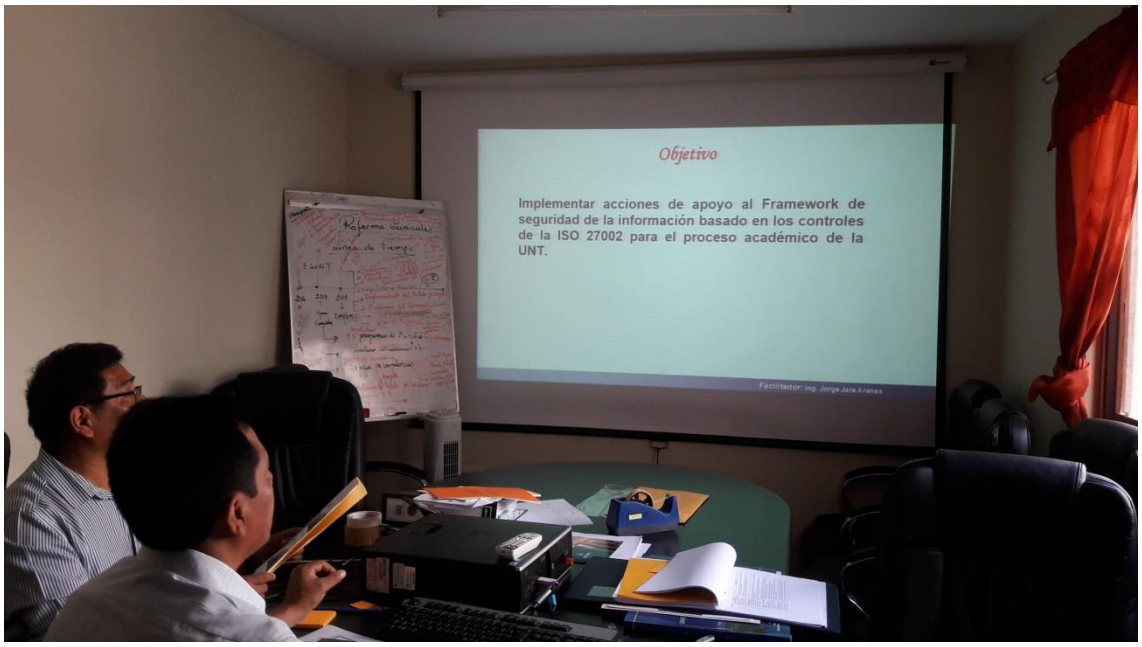
Cronograma de Actividades



	Nombre de tarea	Duration	Start	Finish
1	**Prueba piloto del proceso academico**	**27 days**	**Mon 2/18/19**	**Tue 3/26/19**
2	Capacitación al personal	4 days	Mon 2/18/19	Thu 2/21/19
3	Pruebas de funcionalidad	23 days	Fri 2/22/19	Tue 3/26/19
4				
5				
6				
7				
8				
9				
10				
11				

Anexo5: Sensibilización del software de Gestión de incidentes al personal de los servicios del Proceso Académico




Objetivo
Implementar acciones de apoyo al Framework de seguridad de la información basado en los controles de la ISO 27002 para el proceso académico de la UNT.
Facilitador: Ing. Jorge Jara Aranas

Anexo6: Actas de Sensibilización en el software de Gestión de incidentes al personal de los servicios del Proceso Académico

ACTA DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

FACILITADOR: ING. JORGE ANTONIO JARA ARENAS

ACTIVIDADES:

- Implementar acciones de apoyo al Framework de Seguridad de la Información basado en los controles de la ISO 27002 para el proceso académico de la UNT.
- Brindar los conocimientos sobre la Gestión de Seguridad de la Información al personal que interviene en los procesos académicos de la UNT.
- Establecer una cultura en relación a la disponibilidad, la integridad y la confiabilidad de la información para llegar a comprender la importancia del buen uso de la información.
- Ayudar a fortalecer el compromiso del personal de los procesos académicos con el Sistema de Gestión de Seguridad de la Información para la prevención y respuesta a incidentes de seguridad.

PARTICIPANTES:

APELLIDOS Y NOMBRES	CARGO	FIRMA
SOSA ANCAJIMA EDUARDO TEÓFILO	JEFE EVALUACIÓN ACADÉMICA	
RODRIGUEZ LLAJARUNA JOSE	JEFE DE GESTIÓN CURRICULAR	
Carrión Aguilar Sussy	Unidad de Informática	

FECHA: 25 / 02 / 2019

ACTA DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

APELLIDOS Y NOMBRES	CARGO	FIRMA
Zambrano Saavedra José Antonio	Técnico Administrativo	
Soplopuco Campos Gladys Antoni	Jefe Unid. Grados y Títulos	
Guillermo Díaz Marco Antonio Alvarado Malca Mario	Téc. Administrativa Tec. Adm. A	
Vasquez Rodriguez Susan Cristina Villanueva Flores Margot Cecilia	Tec. Admvo. Auxiliar	

FECHA: 21/ 02/ 2019

ACTA DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

FACILITADOR: ING. JORGE ANTONIO JARA ARENAS

ACTIVIDADES:

- Implementar acciones de apoyo al Framework de Seguridad de la Información basado en los controles de la ISO 27002 para el proceso académico de la UNT.
- Brindar los conocimientos sobre la Gestión de Seguridad de la Información al personal que interviene en los procesos académicos de la UNT.
- Establecer una cultura en relación a la disponibilidad, la integridad y la confiabilidad de la información para llegar a comprender la importancia del buen uso de la información.
- Ayudar a fortalecer el compromiso del personal de los procesos académicos con el Sistema de Gestión de Seguridad de la Información para la prevención y respuesta a incidentes de seguridad.

PARTICIPANTES:

APELLIDOS Y NOMBRES	CARGO	FIRMA
Chiclote Suelpres Freddy Rogelio	Profesional de Redes	

FECHA: 20 / 02 / 2019

ACTA DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

FACILITADOR: ING. JORGE ANTONIO JARA ARENAS

ACTIVIDADES:

- Implementar acciones de apoyo al Framework de Seguridad de la Información basado en los controles de la ISO 27002 para el proceso académico de la UNT.
- Brindar los conocimientos sobre la Gestión de Seguridad de la Información al personal que interviene en los procesos académicos de la UNT.
- Establecer una cultura en relación a la disponibilidad, la integridad y la confiabilidad de la información para llegar a comprender la importancia del buen uso de la información.
- Ayudar a fortalecer el compromiso del personal de los procesos académicos con el Sistema de Gestion de Seguridad de la Información para la prevención y respuesta a incidentes de seguridad.

PARTICIPANTES:

APELLIDOS Y NOMBRES	CARGO	FIRMA
Zavaleta Cedeño Oscar Alonso	Téc. de la Sección de Informática y Sistemas	
Rodriguez Gutierrez Rosa	Jefe(e) de la Unidad de Matricula	
Abanto Ramos Haydée Yolanda	Secretaria - DRT	
[illegible] Centeno María	Unidad de Notas y Certificados	

Anexo7: Organigrama de la Universidad Nacional de Trujillo