UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA Y SISTEMAS

TESIS

"Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018"

Presentado por:

Jessica Noralina Huallpa Laguna

Para optar el Título de Ingeniero Informático y Sistemas

Abancay, Perú

2020

Repositorio Institucional – UNAMBA - PERÚ

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA Y SISTEMAS

TESIS

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC, 2018"

Presentado por **Jessica Noralina Huallpa Laguna**, para optar el Título de:

INGENIERO INFORMÁTICO Y SISTEMAS

Sustentado y aprobado el 12 de febrero de 2021 ante el jurado evaluador:

Presidente: *Dr. Erech Ordoñez Ramos*

Primer Miembro: *Ing. Ebert Gómez Aiquipa*

Segundo Miembro: *Dr. Lintol Contreras Salas*

Asesor : *Mag. Mario Aquino Cruz*

Repositorio Institucional – UNAMBA - PERÚ

Agradecimiento

Agradezco a mis padres Natividad y Domingo por estar ahí conmigo apoyándome constantemente y motivándome para la culminación de la tesis.

Agradezco a mis hermanos Carlos, Maribel, Antonio y Américo por estar siempre ahí a pesar de la distancia y circunstancias. Los amo.

De igual manera mis agradecimientos a la Universidad nacional Micaela Bastidas de Apurímac, a toda la Escuela Académico profesional de Ingeniería Informática y Sistemas, a mis profesores quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente quiero expresar mi más grande y sincero agradecimiento al Ing. Mario Aquino Cruz, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de esta tesis.

Repositorio Institucional – UNAMBA - PERÚ

Dedicatoria

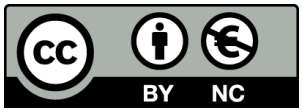
Esta tesis está dedicado principalmente a mis padres ya que con su esfuerzo y sacrificio diario pudieron sacarme adelante a pesar de las dificultades que hemos enfrentado día a día, demostrándome su incondicional apoyo y amor infinito. A mi abuelita Juana que desde el cielo recibo sus bendiciones.

Repositorio Institucional – UNAMBA - PERÚ

“Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018

Ingeniería Informática, Industria Y Sociedad

Esta publicación está bajo una Licencia Creative Commons



Repositorio Institucional – UNAMBA - PERÚ

ÍNDICE

Repositorio Institucional – UNAMBA - PERÚ

Repositorio Institucional – UNAMBA - PERÚ

Repositorio Institucional – UNAMBA - PERÚ

ÍNDICE DE TABLAS

Repositorio Institucional – UNAMBA - PERÚ

ÍNDICE DE FIGURAS

Repositorio Institucional – UNAMBA - PERÚ

INTRODUCCIÓN

Actualmente las tecnologías de información van evolucionando a pasos agigantados, permitiendo minimizar el tiempo de procesamiento de los procesos tecnológicos de las organizaciones. Los sistemas de información cada vez se diseñan con mayores propósitos estratégicos que operacionales, ayudando a la toma de decisiones a través de la información que se obtiene y permitiendo su almacenamiento en diferentes dispositivos de seguridad.

Por lo que implica que las organizaciones brinden una mayor importancia a la seguridad de la información, ya que así como evoluciona la tecnología también se evidencia el crecimiento de ataques informáticos por lo que pueden causar daños al software del sistema o al hardware. Este tipo de vulnerabilidades y amenazas suelen causar daños en la infraestructura física o en la información de varias formas, que van desde la más simples como desconectar el computador de la electricidad mientras se está trabajando, hasta las más complejas como el uso de software malicioso o el uso de los virus informáticos.

Es por ello que el presente trabajo de tesis titulado " Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018" tiene por finalidad implementar el SGSI siguiendo los lineamientos de la norma ISO/IEC 27001:2013, consiguiendo así garantizar la confidencialidad, integridad y disponibilidad de la información de la Dirección de Tecnologías de Información. El trabajo de tesis se encuentra dividido en cinco capítulos, los cuales se detallan a continuación:

CAPÍTULO I: describe el plan de investigación, indicando la descripción del problema, enunciado del problema y justificación.

CAPÍTULO II: describe los objetivos, la hipótesis y la operacionalización de variables.

CAPÍTULO III: describe el marco teórico referencial a emplearse en el presente trabajo, indicando los antecedentes y conceptos e información necesaria para facilitar su realización.

CAPÍTULO IV: describe la metodología, indicando tipo y nivel de investigación, diseño de investigación, población y muestra, técnicas e instrumentos y análisis estadístico.

CAPÍTULO V: describe todo sobre los resultados y discusión.

CAPÍTULO VI: describe todo sobre las conclusiones y recomendaciones.

Repositorio Institucional – UNAMBA - PERÚ

RESUMEN

La presente tesis tuvo como objetivo principal contribuir a mejorar el nivel de la seguridad de la información en la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac implementando el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013. La Dirección de Tecnologías de Información de la UNAMBA es la encargada de administrar las tecnologías y la información por lo que también tiene el deber de salvaguardar los activos informáticos que se encuentran bajo su responsabilidad, pero no cuenta con ningún plan, norma ni directiva que le permita resguardar la información de una manera correcta, es por ello que se propuso la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, esta norma nos permite el aseguramiento de la confidencialidad, disponibilidad e integridad de la información, así como de los sistemas que manejan. En la presente tesis la metodología empleada fue de tipo de investigación aplicada, con un nivel de investigación explicativo y diseño de investigación pre experimental. La metodología para el diseño del Sistema de Gestión de Seguridad de la Información, se utilizó el método Deming PDCA (Plan, Do, Check, Act), la cual consiste en la identificación de los activos informáticos y a partir de ello realizar el análisis y gestión de riesgos para luego establecer acciones de respuesta (controles) para mitigar los riesgos a los que se encuentran expuestos, realizar las políticas de seguridad de información y así también el sistema de gestión de Incidentes SOPORTETICK para poder controlar y mejorar la seguridad de la información de la Dirección de Tecnologías de Información. Para la realización de análisis y gestión de riesgos se usó la metodología MAGERIT III. Como resultados del trabajo de investigación, se obtuvo que el nivel de riesgos de seguridad antes de la implementación de los controles era de un 86.15% para luego obtener 11.15% por lo que se indica que hubo una disminución de 75%. Así mismo se indica que hubo un incremento de los controles de seguridad ya que antes de realizar el plan de tratamiento de riesgos se obtuvo solo 18(15.78%) controles pero luego se incrementó a 65(57.01%) controles lo que representa un aumento de 41.23%. Además hubo una mejora en el nivel de capacitación en temas de seguridad de la información en los usuarios de la DTI ya que antes de la implementación del SGSI solo el 48% de los encuestados tenían conocimiento sobre seguridad de información pero luego ascendió a un 95%.

Palabras clave: ISO/IEC 27001, ISO/IEC 27002, Sistema de Gestión de Seguridad de Información (SGSI).

Repositorio Institucional – UNAMBA - PERÚ

ABSTRACT

The main objective of this thesis was to contribute to improve the level of information security in the Information Technology Department of the Universidad Nacional Micaela Bastidas de Apurímac by implementing the Information Security Management System based on the ISO/IEC 27001:2013 standard.

The Directorate of Information Technology of the UNAMBA is responsible for managing technology and information so it also has the duty to safeguard the computer assets that are under its responsibility, but does not have any plan, standard or directive that allows you to safeguard the information in a proper manner, which is why we proposed the implementation of an information security management system based on ISO / IEC 27001:2013, this standard allows us to ensure the confidentiality, availability and integrity of information, as well as the systems they handle. In this thesis the methodology used was applied research, with a level of explanatory research and pre-experimental research design. The methodology for the design of the Information Security Management System, was used the Deming PDCA method (Plan, Do, Check, Act), which consists of the identification of the computer assets and from it to carry out the analysis and management of risks to then establish response actions (controls) to mitigate the risks to which they are exposed, to carry out the policies of information security and thus also the system of management of Incidents SOPORTETICK to be able to control and to improve the security of the information of the Direction of Technologies of Information. The MAGERIT III methodology was used to carry out risk analysis and management.

As a result of the research work, the level of security risks before the implementation of the controls was 86. 15% and then 11. 15%, indicating a decrease of 75%. It is also indicated that there was an increase in security controls, since before the risk treatment plan was carried out, only 18 (15. 78%) controls were obtained, but then this increased to 65 (57. 01%) controls, which represents an increase of 41. 23%. In addition, there was an improvement in the level of training on information security issues among ITD users as before the implementation of the ISMS only 48% of respondents had information security knowledge but then it rose to 95%.

Keywords: ISO / IEC 27001, ISO / IEC 27002, Information Security Management System (ISMS).

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

Las organizaciones ya sean públicas o privadas, pequeñas o grandes generan todo tipo de información de suma importancia para ellas. Esta información en la mayoría de los casos, son almacenadas en diferentes medios tanto como físicos o electrónicos por lo que se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionajes, virus informáticos, ataques de intrusión y denegación de servicios así mismo se incluye los sabotajes, vandalismos, incendios o inundaciones.

Por lo que la seguridad de la información se logra con la implementación de un conjunto de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

En el Perú la cultura organizacional en el ámbito de seguridad de información no es abundante, y mucho menos en el caso de las universidades, es por ello que tampoco toman en cuenta aspectos administrativos como la modelación de sus procesos lo cual es de suma importancia para la realización de sus actividades, ya que al tratarse de actividades laborales que realizan siempre, no lo ven como algo que pueda servirles, presentándose situaciones en las que dejan pasar los años y no logran evolucionar en ese aspecto.

Actualmente la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional Micaela Bastidas de Apurímac es la encargada de administrar las tecnologías y la información, a través de la Web e Intranet, analiza y desarrolla software y sistemas de información e implementa redes y conectividad, orientados a dar soporte a la tecno estructura de la UNAMBA, presta además servicio de soporte técnico a los usuarios; de esta manera la DTI se encarga de dar cumplimiento a las funciones establecidas en el Reglamento de Organización y Funciones vigente. La DTI no cuenta con un SGSI por lo que se presenta problemas relacionados a la seguridad de la información tales como: perdida de activos de información, desorden en la DTI debido a que frecuentemente personal administrativo, docentes y alumnos solicitan soporte de manera personal ya que no se cuenta con un control de incidencias; no se cuenta con licencia de antivirus por lo que las PC’s de personal

Repositorio Institucional – UNAMBA - PERÚ

administrativo y laboratorios de las diferentes escuelas académicos profesionales se encuentran infectadas de virus y eso no permite el normal desarrollo de sus actividades, internet deficiente ya que cualquiera puede conectarse a la red lo que provoca lentitud en el funcionamiento de los sistemas informáticos de la UNAMBA ; falta de un manual de procesos (MAPRO) por lo que genera desorden y descoordinación entre el personal al momento de realizar una actividad, tarea o procedimiento ; no se cuenta con un acuerdo de confidencialidad para el practicante pre profesional nuevo en la DTI lo que podría provocar que algún personal enfurecido revele información confidencial; falta de capacitación y formación en temas de seguridad de la información del personal administrativo, docentes y alumnos.

De continuar con esta situación, se verían afectados las instalaciones físicas, el hardware, los sistemas de información y la información contenida en ellos; lo que perturbaría el normal desarrollo de las actividades dentro de la universidad.

Por lo expuesto anteriormente se propone la implementación de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013, el cual permitirá proteger los activos de información y la información que se manejen dentro del flujo de los procesos más importantes.

1.2 Enunciado del Problema

1.2.1 Problema general

¿En qué medida la implementación del SGSI basado en la norma ISO/IEC 27001:2013, contribuye en mejorar el nivel de seguridad de la información de la Dirección de Tecnologías de Información de la UNAMBA?

1.2.2 Problemas específicos

- ¿En qué medida se disminuye los niveles de riesgos de seguridad en la Dirección de Tecnologías de Información de la UNAMBA?
- ¿En qué medida se incrementa los Controles de Seguridad en la Dirección de Tecnologías de Información de la UNAMBA?
- ¿En qué medida se mejora el nivel de capacitación y formación en temas de seguridad de la información en los usuarios de Dirección de Tecnologías de Información de la UNAMBA?

Repositorio Institucional – UNAMBA - PERÚ

1.2.3 Justificación de la investigación

El Sistema de Gestión de Seguridad de Información que se implementó en la presente tesis, protege y salvaguarda la confidencialidad, integridad y disponibilidad de los activos de información de la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac frente a amenazas y riesgos que puedan ponerlas en peligro.

La tesis beneficia a todos los administradores y/o usuarios que hacen uso de los servicios informáticos y de la información que brinda la Dirección de Tecnologías de Información, puesto que tienen un control apropiado de las incidencias presentadas así mismo tienen mayor formación y conocimientos en cuanto al uso de la información y equipos.

Asimismo en vista que se aprobó el uso obligatorio de la 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 (1).

Si bien es cierto que la Universidad Nacional Micaela Bastidas de Apurímac no pertenece directamente al Sistema Nacional de Informática, el Ministerio de Educación y la Superintendencia Nacional de Educación si pertenecen y la UNAMBA está bajo la jurisdicción de ellas e indirectamente esta norma va dirigida a todas las universidades.

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO II

OBJETIVOS E HIPÓTESIS

2.1 Objetivos de la investigación

2.2.1 Objetivo general

Contribuir a mejorar el nivel de la seguridad de la información en la Dirección de Tecnologías de Información de la UNAMBA implementando el SGSI basado en la norma ISO/IEC 27001:2013

2.2.2 Objetivos específicos

- Disminuir los niveles de riesgos de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.
- Incrementar los controles de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.
- Mejorar el nivel de capacitación y formación en temas de seguridad de la información en los usuarios de la Dirección de Tecnologías de Información de la UNAMBA.

2.2 Hipótesis de la investigación

2.2.3 Hipótesis general

La implementación del SGSI basado en la norma ISO/IEC 27001:2013 mejora la seguridad de información en la Dirección de Tecnologías de la Información de la UNAMBA.

2.2.4 Hipótesis específicas

- La implementación del SGSI disminuye los niveles de riesgos de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.
- La implementación del SGSI incrementa los controles de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.
- La implementación del SGSI mejora el nivel de capacitación y formación de los usuarios de la Dirección de Tecnologías de Información de la UNAMBA en temas de seguridad de la información.

Repositorio Institucional – UNAMBA - PERÚ

2.3 Operacionalización de variables

La Operacionalización de variables es como se muestra en la tabla 1.

Tabla 1.*Operacionalización de variables*

VARIABLES	DIMENSIÓN	INDICADOR	ÍNDICES
Independiente **Sistema de gestión de seguridad de la información: "**es la parte del sistema de gestión de la entidad, basado en un enfoque de riesgos del negocio, para establecer, implementar, operar, monitorear, mantener y mejorar la seguridad de la información" (2).	Metodología PDCA – PHVA - Mejora continua - Ciclo Deming	*Según fase Planear	a) Si b) No
		*Según fase hacer	a) Si b) No
		*Según fase verificar	a) Si b) No
		*Según fase actuar	a) Si b) No
Dependiente **Seguridad de Información: "**es la protección de la información contra una amplia gama de amenazas respecto a minimizar daños, oportunidades del negocio, retorno de la inversión, continuidad del negocio y cultura ética" (3).	Riesgos	*Nivel de Riesgos	a) 5 b) 10 c) 50 d)70 e) 100
	Controles	*Controles aplicados	a) Si b) No
	Capacitación y formación en temas de seguridad de la información	*Nivel de capacitación y formación en temas de seguridad de la información	a) Si b) No

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO III
MARCO TEÓRICO REFERENCIAL

3.1 Antecedentes

A Nivel Internacional

- En la tesis titulado "Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de Córdova", Universidad Nacional Abierta y a Distancia; este proyecto de tesis tiene como objetivo general: "Diseñar un Sistema de Gestión de la Seguridad de Información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 para la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba". Así mismo se utilizó la metodología de PDCA considerando solo las 2 primeras fases de la metodología que vienen a ser Planear y Hacer, la documentación realizada de acuerdo a la norma ISO 27001:2013 fueron las siguientes: "Soporte y Aprobación por la Dirección, Alcance del Sistema de Gestión de la Seguridad de la Información, Objetivos de Control y Controles de Seguridad, Políticas de Seguridad de la Información, Análisis de Riesgos, Evaluación de Riesgos y el Reporte de Evaluación de Riesgos, Declaración de Aplicabilidad y Plan de Tratamiento de Riesgos, Plan de Continuidad del Negocio". Finalmente se concluye que el "Sistema de Gestión de Seguridad de Información basado en la norma ISO 27001:2013 permitió conocer el estado actual de los dominios objetivos y controles de seguridad mediante un análisis diferencial, se pudo clasificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos, donde se pudo identificar los activos más críticos y que requieren de mayor atención y controles de seguridad dado el alto impacto que tienen en la prestación de servicios y funcionamiento óptimo de los procesos de la institución" (4).
- En la tesis titulado "Sistema de Gestión de la Seguridad de Información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de informática y Telecomunicaciones de la Universidad de Nariño", Universidad de Nariño; este proyecto de tesis tiene como objetivo general: "Mejorar la gestión de la seguridad de la información mediante la aplicación del proceso de análisis de riesgos y la verificación de control de seguridad que permita estructurar un Sistema de Gestión de Seguridad de Información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de informática y Telecomunicaciones de

Repositorio Institucional – UNAMBA - PERÚ

la Universidad de Nariño". Así mismo se utilizó la metodología PDCA para el SGSI y MAGERIT para el análisis y gestión de riesgos. Finalmente se concluye que el Sistema de Gestión de Seguridad de Información logra un alto nivel de calidad en los procesos de seguridad de la información (5).

A Nivel Nacional

- En la tesis titulado "Sistema de Gestión para mejorar la seguridad de la información en la institución servicios industriales de la marina", Universidad Nacional del Santa; este proyecto de tesis tiene como objetivo general: "Mejorar la Seguridad de la Información en la Institución de Servicios Industriales de la Marina". Así mismo formula como hipótesis: "El Sistema de Gestión mejora la Seguridad de la Información en la Institución de Servicios Industriales de la Marina". El tipo de la investigación es aplicada, el nivel es descriptiva y utiliza un diseño de investigación de Series cronológicas de un solo grupo. Finalmente se concluye que el Sistema de Gestión mejoró en 58% la Seguridad de la Información en la Institución de Servicios Industriales de la Marina, a través de la implementación de los procesos del Sistema de Gestión de Seguridad de la Información (6).
- En la tesis titulado "Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo", Universidad Católica Santo Toribio de Mogrovejo; este proyecto de tesis tiene como objetivo: "Contribuir a mejorar el nivel de seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo". Así mismo formula como hipótesis: "Con una Guía de Implementación de la Seguridad de la Información basado en la Norma ISO/IEC 27001, se apoyará en la mejora de la Seguridad en las Aplicaciones Informáticas de la comisaria del Norte –Chiclayo". El tipo de investigación es tecnológica aplicada. Finalmente se concluye que con la Guía de Implementación, "se logró incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma" (7).
- En la tesis titulado "Diseño de un sistema de gestión de seguridad de la información para un instituto educativo", Pontificia Universidad Católica del Perú; este proyecto tiene como objetivo general: "Diseñar un Sistema de Gestión de Seguridad de Información

Repositorio Institucional – UNAMBA - PERÚ

(SGSI) basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios el COBIT". Así mismo utiliza la metodología PDCA. Finalmente se concluye que se logró toda la documentación requerida por la norma ISO/IEC 27001 eso quiere decir que se cumplió con el objetivo general que es el de diseño de un sistema de gestión de seguridad de la información para un instituto educativo (8).

- En la tesis titulado "Estándar internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG", Universidad Nacional Pedro Ruiz Gallo; este proyecto de tesis tiene como objetivo general: Aplicar el Estándar Internacional ISO 27001 para la Gestión de Seguridad de la Información en el proceso de Soporte de TI en la Oficina Central de Informática de la UNPRG. Asimismo formula como hipótesis: Si se aplica el Estándar Internacional ISO 27001 mejora de manera eficaz y eficiente la Gestión de Seguridad de la Información en la Oficina Central de Informática de la Universidad Nacional Pedro Ruiz Gallo. El tipo de investigación es Tecnológica-Formal y la metodología usada es PDCA. Finalmente se concluye que Con el Sistema de Gestión de Seguridad de la Información en el Proceso de Soporte de TI de la Oficina Central de informática - UNPRG, el nivel de riesgo se logra disminuir en promedio de 6 a 4.4, lo que significa un 26.67%. El cual se logra después de haber aplicado la metodología de análisis y evaluación de riesgos, finalizando con la implementación de los controles de la ISO 27001 (9).

A nivel Local

Después de haber revisado fuentes bibliográficas y tesis de la localidad de la ciudad de Abancay en las diferentes universidades, no se encontró trabajo de investigación parecido o relacionado al presente.

Repositorio Institucional – UNAMBA - PERÚ

3.2 Marco teórico

3.2.1 Sistema de Gestión de Seguridad de Información

"Según la Oficina Nacional de Gobierno Electrónico e Informática- ONGEI, un SGSI (Sistema de Gestión de Seguridad de la Información) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr objetivos de negocio de la misma manera el análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, contribuye a la exitosa implementación de un SGSI". El Sistema de Gestión de la Seguridad de la Información (SGSI) en las empresas ayuda a establecer estas políticas, procedimientos y controles en relación a los objetivos de negocio de la organización (10).

El Sistema de Gestión de la Seguridad de la Información (SGSI) sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de ciclo Deming, que consiste en Panificar-Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés PDCA (Plan-DO-Check-Act) (similar a la más extendida y reconocida norma ISO 9001) (11).

3.2.2 Seguridad de Información

"La seguridad de la información, consiste en la preservación de su Confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran" (12).

Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** "la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados".
- **Integridad:** "mantenimiento de la exactitud y completitud de la información y sus métodos de proceso"**.**
- **Disponibilidad:** "acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran".

Repositorio Institucional – UNAMBA - PERÚ

La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas. Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades y para contrarrestar estos riesgos se implementan controles y se realiza concientización en el personal en temas de seguridad de la información (12).

3.2.3 Estándar Internacional ISO/IEC 27001

La norma/estándar UNE ISO/IEC 27001 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información (13).

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias, mientras que las secciones 4 a 10 cuentan con documentación a realizar.

Sección 0 (Introducción): "explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión".

Sección 1 (Alcance): "explica que esta norma es aplicable a cualquier tipo de organización".

Sección 2 (Referencias normativas): "hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones".

Sección 3 (Términos y definiciones): "de nuevo, hacen referencia a la norma ISO/IEC 27000".

Repositorio Institucional – UNAMBA - PERÚ

Sección 4 (Contexto de la organización): "esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI".

Sección 5 (Liderazgo): "esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información".

Sección 6 (Planificación): "esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información".

Sección 7 (Apoyo): "esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros".

Sección 8 (Funcionamiento): "esta sección es parte de la fase de Hacer del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información".

Sección 9 (Evaluación del desempeño): "esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección".

Sección 10 (Mejora): "esta sección forma parte de la fase de Actuar del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua".

Anexo A: "este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones" (secciones A.5 a A.18).

Documentos entregables en base a la norma ISO/IEC 27001:2013:

- **Alcance del Sistema de Gestión de Seguridad de la Información:** "ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia

Repositorio Institucional – UNAMBA - PERÚ

del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas)".

- **Política y Objetivos de Seguridad de información:** "documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información".
- **Informe de Análisis y evaluación de riesgos:** "estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización".
- **Plan de tratamiento de riesgos:** "documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc".
- **Declaración de Aplicabilidad:** "(SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones".

Figura 1. Estructura de la norma ISO 27001

Repositorio Institucional – UNAMBA - PERÚ

3.2.4 Metodología PDCA

¿Qué es el ciclo PDCA?

"El nombre del Ciclo PDCA (o Ciclo PHVA) viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". También es conocido como Ciclo de mejora continua o Círculo de Deming, por ser Edwards Deming su autor. Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales). El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones" (14).

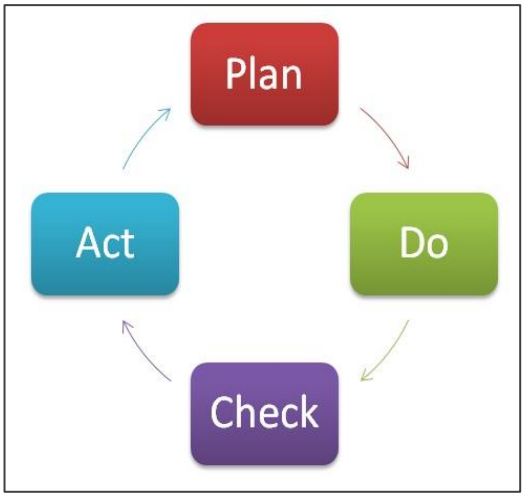


*Figura 2.*Ciclo PDCA- Plan, Do, Check, Act.

¿Cómo implantar el ciclo PDCA?

Las cuatro etapas que componen el ciclo son las siguientes:

- **Planificar (Plan):** "Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc".

Repositorio Institucional – UNAMBA - PERÚ

- **Hacer (Do):** “Se realizan los cambios para implantar la mejor propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala”.
- **Verificar (Check):** “Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados”.
- **Actuar (Act):** “Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar”.

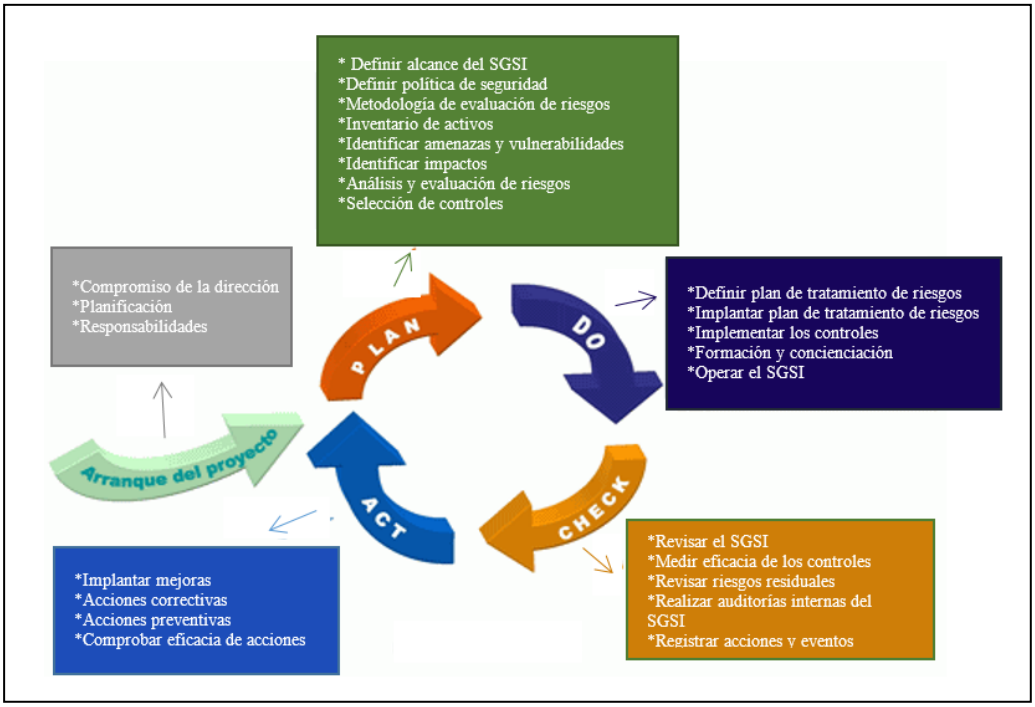


Figura 3. Estructura Ciclo Deming y pasos de SGSI

Repositorio Institucional – UNAMBA - PERÚ

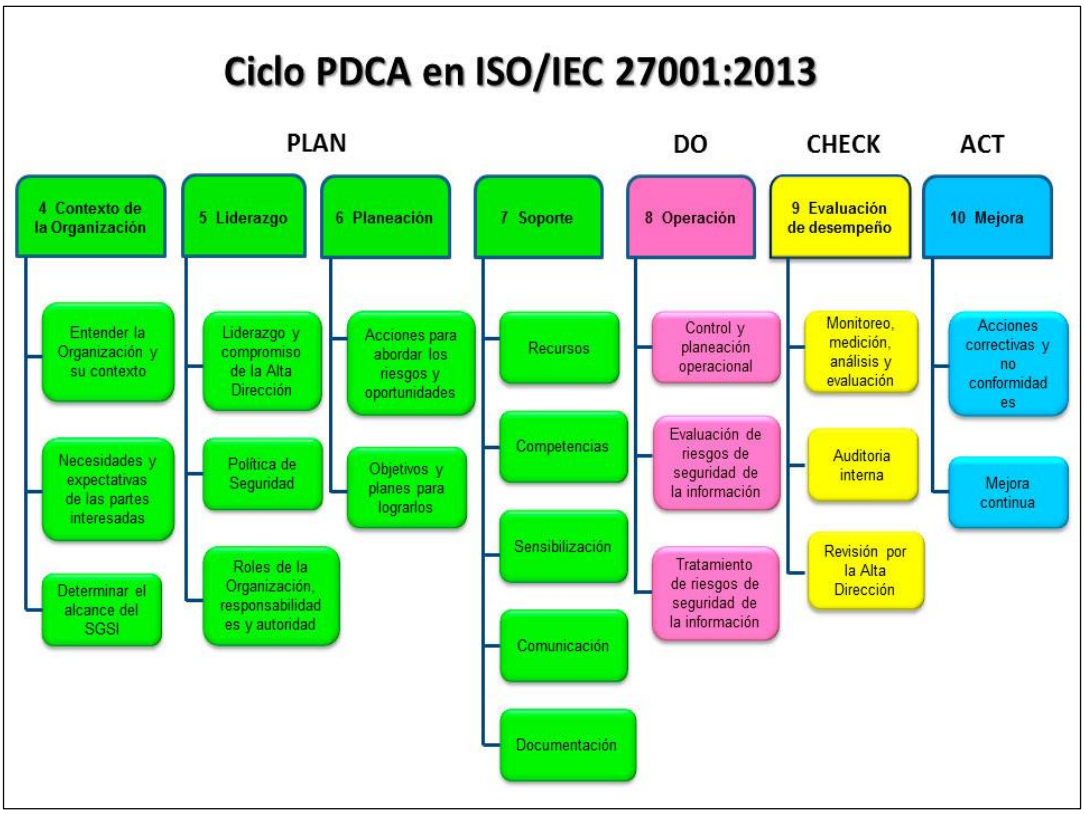


Figura 4. Estructura del estándar ISO/IEC 27001:2013 y PDCA

3.2.5 Metodología de Análisis y Gestión de Riesgos de los sistemas de información (MAGERIT)

Según la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (15).

El análisis de riesgo es un elemento imprescindible en la implementación del Sistema de Gestión de Seguridad de la Información para el Servicio de Soporte de TI, además de ser un requerimiento de la ISO 27001, permitiendo identificar los riesgos que deben ser gestionados de manera más inmediata. El modelo de administración de riesgos de seguridad de información consta de un proceso continuo de 4 fases principales que permite medir y manejar los riesgos de seguridad de información en un nivel aceptable. La presente metodología está basado Magerit v3.0, y en el estándar ISO 27001:2013 (15).

Repositorio Institucional – UNAMBA - PERÚ

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

- Inventario de Activos de Información
- Análisis del Riesgo
- Evaluación del Riesgo
- Tratamiento del Riesgo

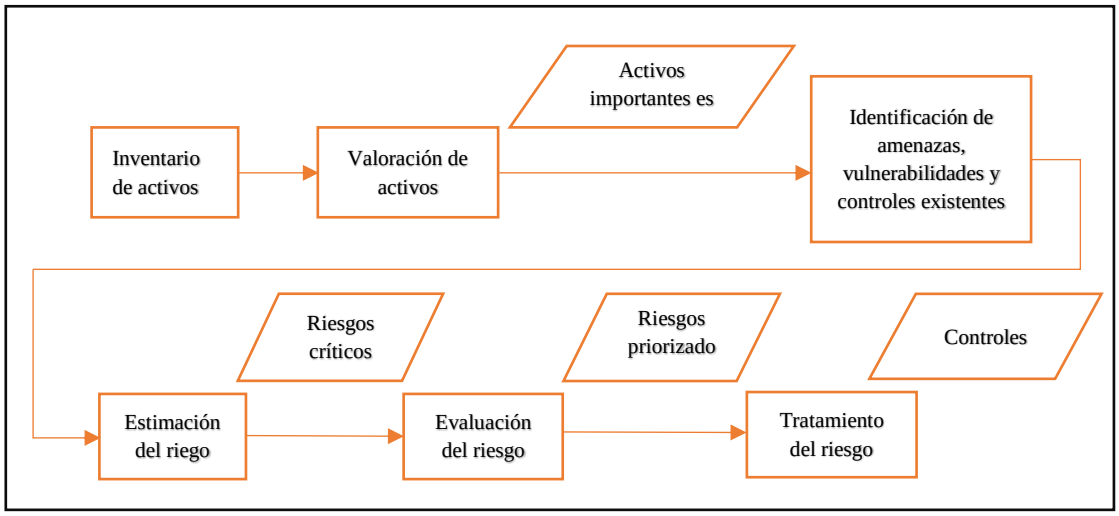


Figura 5. Metodología del Análisis, Evaluación y Tratamiento del Riesgo

Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Repositorio Institucional – UNAMBA - PERÚ

3.2.6 Dirección de Tecnologías de Información

La Dirección de Tecnologías de la Información, es la encargada de administrar las tecnologías y la información de la Universidad, a través de la Web e Intranet, analiza y desarrolla software y sistemas de información e implementa redes y conectividad, orientados a dar soporte a la tecno estructura de la UNAMBA, presta además servicio de soporte técnico a los usuarios. (16)

Funciones de la Dirección de Tecnología de Información:

- Analizar, desarrollar y evaluar sistemas de información, y proyectos informáticos requeridos por la universidad y administrar la operatividad de los mismos.
- Establecer conectividad del servicio de Red Local – LAN / Internet, Wireless, requerida por la Universidad.
- Proporcionar soporte tecnológico para asegurar la operatividad continua de los equipos de cómputo y comunicaciones (Red Local –LAN / Internet, Wireless).
- Evaluar, proponer e implementar nuevas tecnologías como soluciones para la optimización de los procesos administrativos y gestión universitaria.
- Promover y apoyar la capacitación a docentes y personal administrativo en el manejo de los sistemas de información y manejo de recursos informáticos.
- Elaborar planes, políticas, normas, reglamentos, directivas y estándares para el desarrollo y uso de recursos informáticos (hardware y software), redes y conectividad en la Universidad.

Áreas de la Dirección de Tecnologías de Información

- **Área de Gestión de Proyectos:** es la encargada de analizar, diseñar, programar sistemas de información requeridas por la universidad, con documentación y manuales aplicativos, conforme a normas y estándares establecidos.
- **El área de red corporativa:** es la encargada de administrar y establecer la conectividad del servicio de Red local - LAN / Internet, wíreless de la universidad.
- **El área de soporte técnico y mantenimiento:** es la encargada de proporcionar soporte tecnológico, asegurando la operatividad de las tecnologías de información y comunicación, y haciendo conocer el correcto funcionamiento de los equipos, sistemas en uso. Elabora planes de contingencia ante posibles interrupciones del servicio.

Repositorio Institucional – UNAMBA - PERÚ

3.3 Marco conceptual

- **Activo:** Algo que tenga valor para lo organización (17).
- **Ataque:** Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo (17).
- **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización (17).
- **Activo de información:** Datos o información que se almacena en cualquier tipo de medio y que es considerada como sensitiva o crítica (17).
- **Información:** Comprende los datos y conocimientos que se usan en la toma de decisiones.
- **Control:** Medida que modifica un riesgo (17).
- **Confidencialidad:** Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados (17).
- **Disponibilidad:** Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada (17).
- **Integridad:** Propiedad de la exactitud y la integridad (17).
- **Política:** Dirección general y formal expresada por la gerencia.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas (17).
- **Riesgo:** Es la posibilidad de sufrir daños o pérdidas (17).
- **Impacto:** Impresión o efecto intenso producido en una persona por una acción o suceso.
- **Sistema de información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información (17).
- **PDCA - PHVA:** Es la abreviatura de Plan (Planear), Do (Hacer), Check (Verificar), Act (Actuar).
- **SGSI:** Es la abreviatura de Sistema de Gestión de Seguridad de Información.
- **ISO:** Es la abreviatura de varios vocablos en inglés que hace referencia a la International Organization for Standardization, que traduce al español Organización Internacional de Estandarización.
- **IEC:** Abreviatura de International Electrotechnical Commission, se traduce en español en Comisión Electrotécnica Internacional.

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO IV

METODOLOGÍA

4.1 Tipo y nivel de investigación

4.1.1 Tipo de investigación

El tipo de investigación es Aplicada, en razón que se hará el estudio bajo conocimientos de teorías, leyes de investigación básica y gestión de seguridad de la información.

4.1.2 Nivel de investigación

El nivel de estudio es Explicativo, porque se evaluará el efecto de la variable independiente sobre la variable dependiente y probar hipótesis.

4.2 Diseño de la investigación

El diseño de la investigación es pre experimental de pre- test y post-test, con un solo grupo.

El esquema es el siguiente:

G O1 X O2

Dónde:

G: Grupo de Investigación

O1: Pre test/ observación

X: Aplicación de SGSI

O2: Post test/ observación

4.3 Población y muestra

4.3.1 Población

"Población es el total de los individuos o elementos a quienes se refiere la investigación, es decir, todos los elementos que vamos a estudiar, por ello también se le llama universo" (18).

La población de estudio para el objetivo específico 1 y objetivo específico 2 es el proceso de análisis y Gestión de riesgos que está conformado por:

Tabla 2. *Población de Objetivo específico 1 y 2*

PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS	CANTIDAD
Amenazas	4
Activos	21
Controles	114
Riesgos	21

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ

La población de estudio para el objetivo 3 es todo el personal administrativo que son usuarios beneficiarios de las diferentes dependencias de la universidad.

Tabla 3. *Población de objetivo específico 3*

AREA	**CANTIDAD**
Rectorado, Oficina de imagen institucional, Oficina de secretaria general, etc.	22
Vicerrectorado Académico, Dirección de Servicios Académicos, Dirección de Bienestar Universitario, etc.	18
Vicerrectorado de Investigación, Dirección General de Institutos, unidades y Centros de Investigación, etc.	12
Dirección General de Administración, Oficina de Tesorería, Dirección de recursos humanos, etc.	19
Escuela de Postgrado	3
Dirección de escuelas académicos profesionales, decanatura, etc.	26
Total	**100**

Fuente: RR. HH

4.3.2 Muestra

La muestra "es una parte representativa de una población cuyas características deben producirse en ella lo más exactamente posible" (19).

En el muestreo no probabilístico, “la selección de un elemento de la población que va a formar parte de la muestra se basa hasta cierto punto en el criterio del investigador o entrevistar de campo” (20).

La muestra seleccionada para el objetivo específico 1 y objetivo específico 2 está conformada de la siguiente manera:

Tabla 4. *Muestra de Objetivo específico 1 y 2*

PROCESO DE ANÁLISIS Y GESTIÓN DE RIESGOS	**CANTIDAD**
Controles	114
Riesgos	13

Fuente: Elaboración propia

La presente tesis se realizó con un procedimiento de muestreo no probabilístico por conveniencia puesto que solo se entrevistó y encuestó a los responsables de áreas y/o oficinas con mayor relevancia y manejo de información de la universidad.

Repositorio Institucional – UNAMBA - PERÚ

Tabla 5. *Muestra de Objetivo específico 3*

	ÁREA	**CANTIDAD**
Rectorado	Rectorado, Oficina de imagen institucional, Oficina de secretaria general, etc.	06
Vicerrectorado Académico	Vicerrectorado Académico, Dirección de Servicios Académicos, Dirección de Bienestar Universitario, etc.	01
Vicerrectorado de Investigación	Vicerrectorado de Investigación, Dirección General de Institutos, unidades y Centros de Investigación, etc.	01
Dirección General de Administración	Oficina de Tesorería, Dirección de recursos humanos, etc.	04
Escuela de Postgrado	Escuela de Postgrado	01
Facultades	Dirección de escuelas académicos profesionales, decanatura, etc.	07
Total		**20**

Fuente: Elaboración propia

4.4 Técnica e instrumentos

4.4.1 Técnica

Las técnicas de recolección de datos utilizados son las siguientes:

- **Observación:** Esta técnica permite observar la realidad problemática de la DTI, antes y después de la aplicación de la ISO 27001.
- **Encuestas:** Es una técnica que al igual que la observación está destinada para recopilar los datos necesarios para realizar la investigación.
- **Entrevista:** Consiste en una conversación personal que el entrevistador establece con los sujetos investigados, con el propósito de obtener los datos necesarios para realizar la investigación.

4.4.2 Instrumentos

Los instrumentos facilitan a las técnicas el proceso de recolección de los datos. Los instrumentos empleados en la investigación son los siguientes:

- Cuaderno de observación
- Checklist
- Cuestionarios
- Guía de entrevista cerrada
- Cámara Fotográfica

Repositorio Institucional – UNAMBA - PERÚ

4.5 Análisis estadístico

Para el análisis estadístico del trabajo de investigación se utilizó:

- La prueba de T-Student se utilizó para la validación de la hipótesis de la investigación con un nivel de confianza de 95%, con la finalidad de evaluar si los resultados obtenidos de la investigación el pre y post prueba se aceptan significativamente.
- IBM SPSS 25 para realizar la contratación de la hipótesis
- Excel 2013 para tablas y gráficos estadísticos que permitan analizar y visualizar los resultados que se obtengan de los cuestionarios.

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO V
RESULTADOS Y DISCUSIONES

5.1 Análisis de resultados

5.1.1 Objetivo General: *"Contribuir a mejorar el nivel de la seguridad de la información en la DTI de la UNAMBA implementando el SGSI basado en la norma ISO/IEC 27001:2013"*

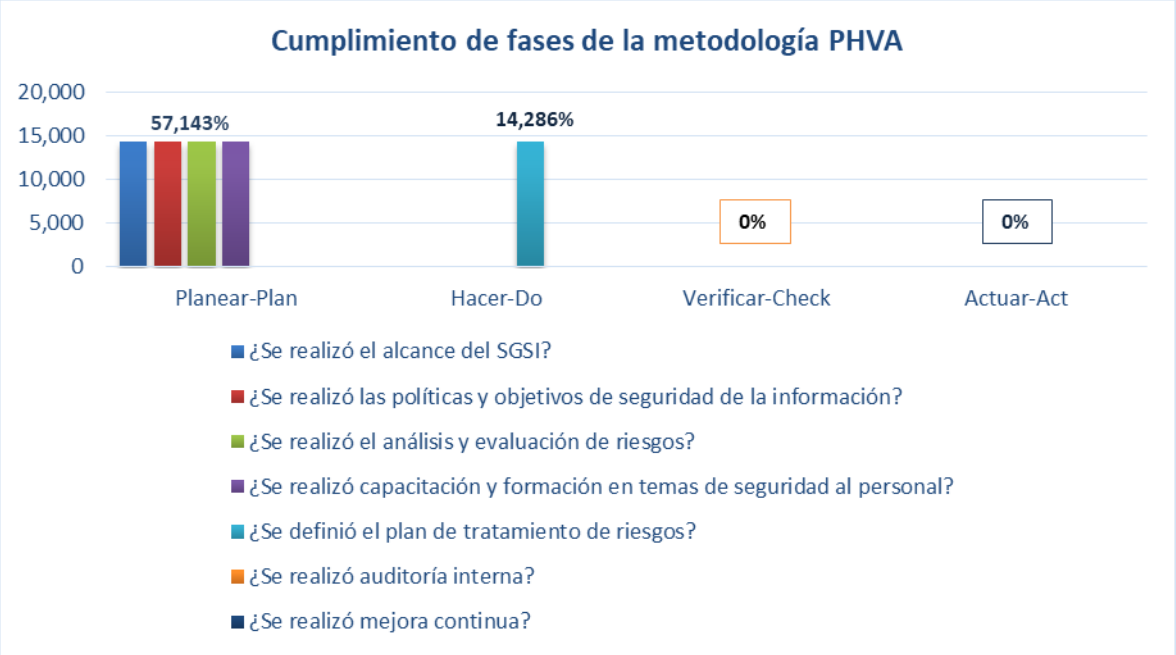


Figura 6. Checklist de metodología PHVA

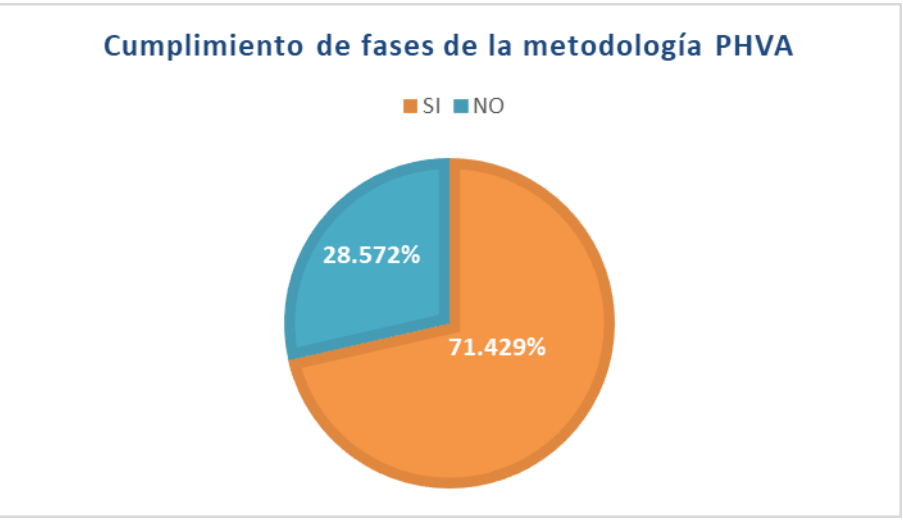


Figura 7. Checklist genera de metodología PHVA

Repositorio Institucional – UNAMBA - PERÚ

Interpretación:

Para verificar que la implementación del SGSI basado en la norma ISO/IEC 27001:2013 ha contribuido en mejorar el nivel de seguridad de la información en la DTI de la UNAMBA se realizó un checklist con el listado de las actividades a realizar según la metodología PHVA (planear, hacer, verificar y actuar), ver anexo 5.

El checklist cuenta con 4 fases; en la fase Planear se tiene 4 actividades relevantes, en la fase Hacer, Verificar y Actuar se tiene 1 actividad en cada una de ellas, lo indicado se observa en la figura número 6. Cada actividad realizada tiene el valor de 14,286% y actividad no realizada tiene la puntuación de 0%.

Se observa en la figura número 7 que después de haber realizado el cheklist se obtiene la respuesta "SI" en un 71.429% y la respuesta "No" en un 28.572% lo que nos lleva a decir que se cumplió la mayoría de actividades que solicita cada fase de la metodología PHVA; así mismo cabe indicar que solo se ha considerado las 2 primeras fases ya que es ahí donde se realiza todos los documentos que solicita el ISO 27001:2013.

5.1.2 Objetivo específico 1: *"Disminuir los niveles de riesgos de seguridad en la DTI de la UNAMBA"*

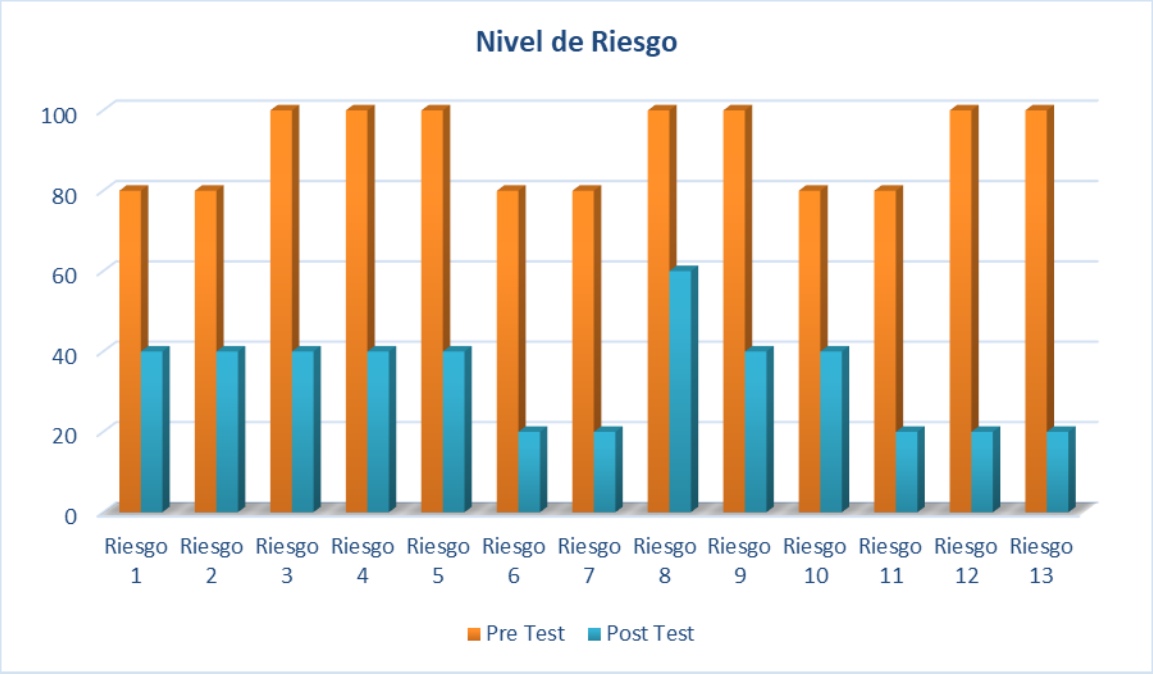


Figura 8. Comparación de nivel de riesgo pre test y post test

Tabla 6. *Riesgos- Muy Altos y Altos*

N° Riesgo	Código de riesgo	Activo
Riesgo 1	R_D_CR	Copias de respaldo
Riesgo 2	R_ S_WWW	Página web
Riesgo 3	R_ SW_EST	Software Estándar
Riesgo 4	R_ SW_BDS	Gestores de base de datos
Riesgo 5	R_ HW_HOS	Servidores
Riesgo 6	R_ HW_ROU	Router
Riesgo 7	R_ HW_SWH	Switch
Riesgo 8	R_ COM_INT	Internet
Riesgo 9	R_ COM_LAN	Red de Área Local
Riesgo 10	R_ L_SIT	Dirección de Tecnologías de Información
Riesgo 11	R_ P_ADM	Administrador de sistemas
Riesgo 12	R_ P_COM	Administrador de comunicación
Riesgo 13	R_ P_DBA	Administrador de Base de datos

Fuente: Elaboración propia

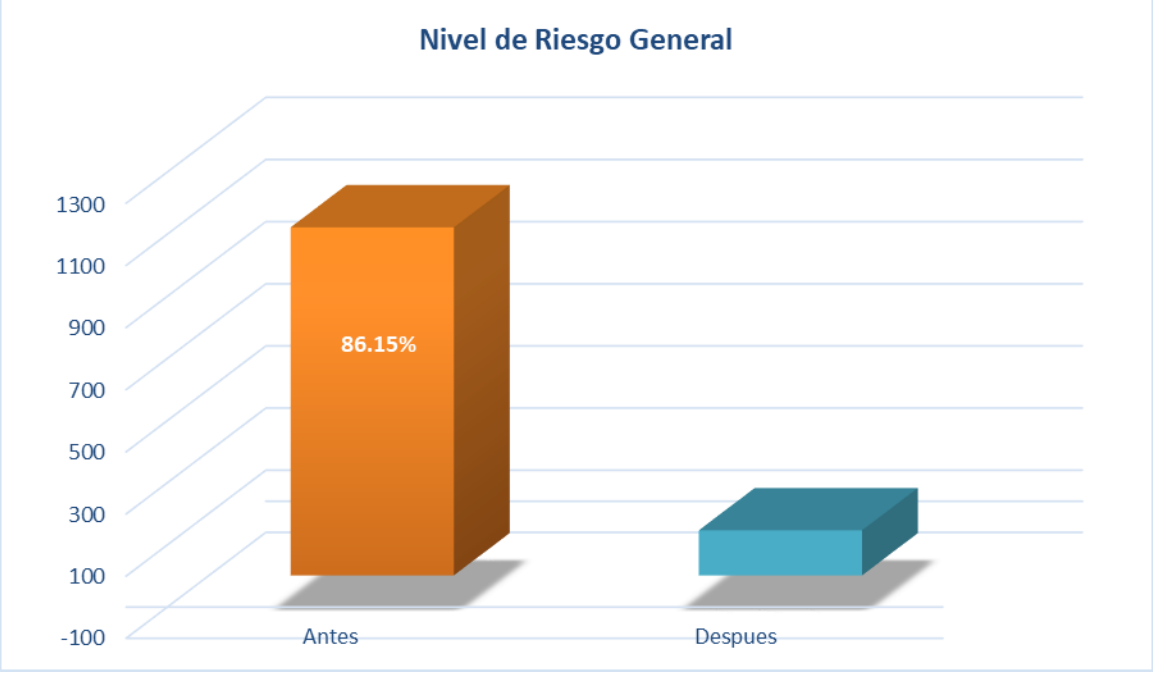


Figura 9. Comparación general de nivel de riesgo pre test y post test

Repositorio Institucional – UNAMBA - PERÚ

Interpretación:

Para verificar que efectivamente hubo una disminución de riesgos a los que se encontraban expuestos los activos de la información en la Dirección de Tecnologías de Información, se ha realizado el análisis y evaluación de riesgos de todos los activos, para medir se ha considerado los 13 riesgos con impacto Muy Alto (100) y Alto (70), por lo que se ha realizado un análisis del antes y después de la identificación de los controles, ver anexo 13 y 15.

Se observa en la figura número 8 que antes de la implementación de los controles, los 13 riesgos son de impacto Muy Alto (100) y Alto (70), pero después el nivel de riesgos baja a un nivel más aceptable como Medios, Bajos y Muy Bajos, así mismo en la comparación general de la figura número 9 se reitera lo dicho anteriormente ya que hay una disminución de 75%. Esto nos permite afirmar y comprobar que efectivamente se logró con el objetivo de disminuir los niveles de riesgos de seguridad en la DTI de la Universidad Nacional Micaela Bastidas de Apurímac.

5.1.3 Objetivo específico 2: *"Incrementar los controles de Seguridad en la DTI de la UNAMBA"*

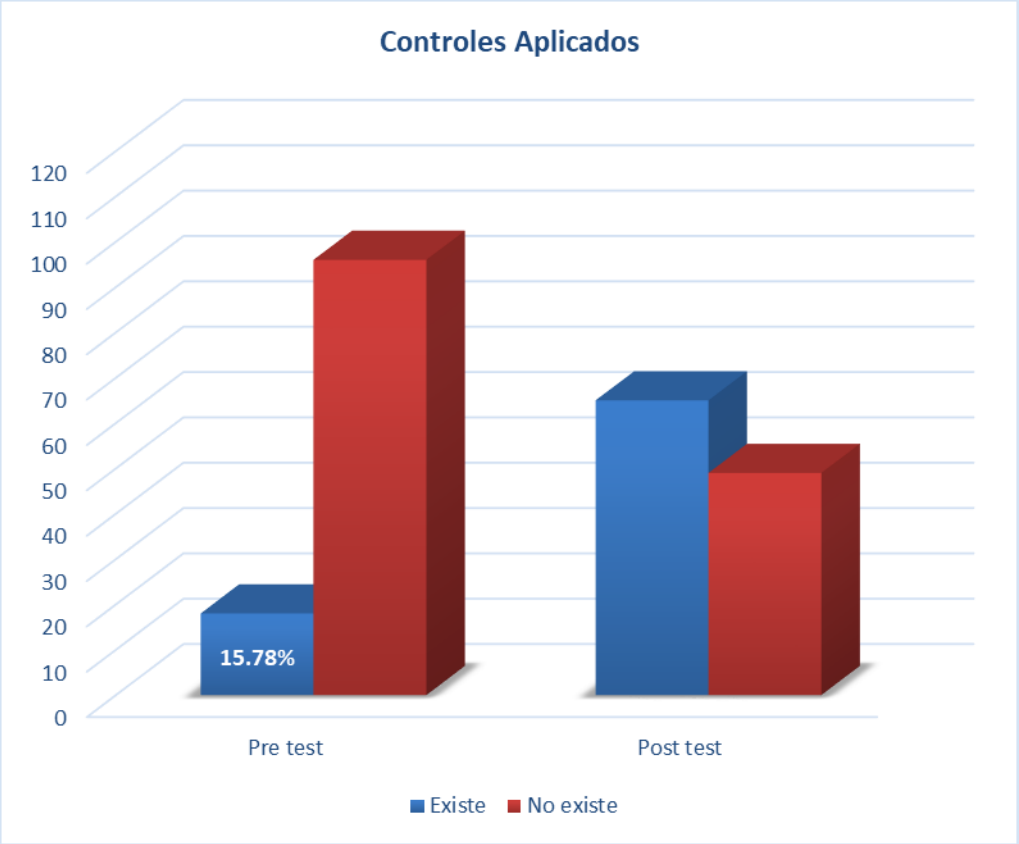


Figura 10. Comparación pre test y post test de nivel de controles de seguridad

Interpretación:

Para verificar el incremento de controles aplicados se ha realizado un checklist de los 114 controles, antes y después de la realización del plan de tratamientos de riesgos y declaración de aplicabilidad, cabe indicar que incrementar los controles de seguridad tiene mucha importancia ya que gracias a ellos nos permiten disminuir los riesgos a los que se encuentran expuestos los activos informáticos, ver anexo 6 para checklist de controles antes y después, anexo 14 declaración de aplicabilidad y anexo 15 para plan de tratamiento de riesgos.

En la figura número 10 se observa que los controles de seguridad se incrementan de 18 (15.78%) controles a 65 (57.01%) controles lo que representa 41.23% de incremento de controles y por consecuencia los controles inexistentes disminuyen.

5.1.4 Objetivo específico 3: *"Mejorar el nivel de capacitación y formación en temas de seguridad de la información en los usuarios de la DTI de la UNAMBA"*

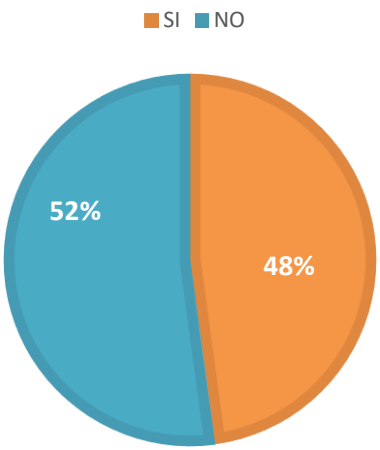
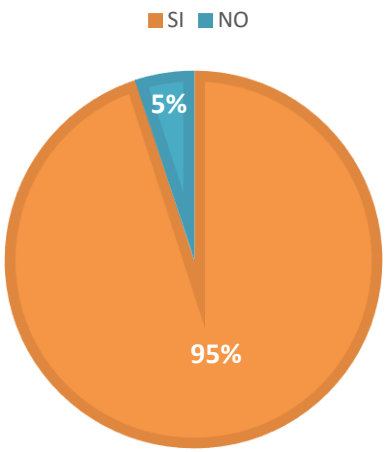
Nivel de capacitación y formación en temas de seguridad de información en los encuestados				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	67	48%	133	95%
No	73	52%	7	5%

Figura 11. Resultado de encuesta - análisis general

Repositorio Institucional – UNAMBA - PERÚ

Interpretación:

Para el cumplimiento de este objetivo se realizó una encuesta previa a la implementación del SGSI y posterior a esta, dicha encuesta consistía en 7 preguntas las cuales se verifica en el anexo 7 y los resultados detallados de cada pregunta verificar anexo 8 y 9.

En la figura anterior se puede observar que solo el 48% de los encuestados tienen conocimientos en temas de seguridad de la información pero después de haber realizado capacitaciones personales así mismo la entrega de volantes informativos en físico y por el correo institucional hubo una variación que ascendió a 95%.

5.2 Contrastación de hipótesis

5.2.1 Hipótesis estadísticas

Prueba de Hipótesis antes y después: La implementación del SGSI disminuirá los niveles de riesgos de seguridad en la DTI de la UNAMBA

μ_1: Test/encuesta antes de la implementación del SGSI basado en ISO 27001/2013

μ_2: Test/encuesta después de la implementación del SGSI basado en ISO 27001/2013

a) Hipótesis estadística

$$H_0 : \mu_1 = \mu_2$$
$$H_1 : \mu_1 > \mu_2$$

Dónde:

H_0: La implementación del SGSI no disminuye los niveles de riesgos de seguridad en la DTI de la UNAMBA

H_1: La implementación del SGSI disminuye los niveles de riesgos de seguridad en la DTI de la UNAMBA

b) Estadístico

Se utiliza la distribución T student puesto que se cuenta con n=13 riesgos con impacto Alto y Muy Alto

$$t_c = \frac{\bar{d}}{S_{\bar{d}}} \qquad \bar{d} = \frac{\sum d_i}{n} \qquad S_d = \sqrt{\frac{\sum (d_i - \bar{d})^2}{n-1}} \qquad S_{\bar{d}} = \frac{S_d}{\sqrt{n}}$$

Repositorio Institucional – UNAMBA - PERÚ

Dónde:

$\boldsymbol{x}$ = reporte de nivel de riesgo antes de implementación de controles

$\boldsymbol{y}$ = reporte de nivel de riesgo después de implementación de controles

$\boldsymbol{d_i}$ = Diferencia por cada par de reporte

$\boldsymbol{\bar{d}}$ = Media aritmética de las diferencias

$\boldsymbol{S_d}$ = Desviación estándar o típica de las diferencias

$\boldsymbol{S_{\bar{d}}}$ = Error estándar o típica de la media

$\boldsymbol{t_c}$ = t de student calculado

$\boldsymbol{n}$ = Tamaño de la muestra

A continuación se muestra la tabla de resultados de los cálculos de reportes de nivel de riesgo antes y después de la implementación de los controles.

Tabla 7. *Cálculos sobre nivel de riesgos antes y después de la implementación de controles*

N°	x	y	d_i = x− y	$d_i - \bar{d}$	$(d_i - \bar{d})^2$
1	70	10	60	-15	225
2	70	10	60	-15	225
3	100	10	90	15	225
4	100	10	90	15	225
5	100	10	90	15	225
6	70	5	65	-10	100
7	70	5	65	-10	100
8	100	50	50	-25	625
9	100	10	90	15	225
10	70	10	60	-15	225
11	70	5	65	-10	100
12	100	5	95	20	400
13	100	5	95	20	400
	Total=940	**Total=145**	**Total=975**	**Total=0**	**Total=3330**

Fuente: Elaboración propia

Media Aritmética	Desviación estándar	Error estándar de la media
$\bar{d} = \frac{\sum d_i}{n}$ $\bar{d} = \frac{975}{13}$ $\boldsymbol{\bar{d} = 75}$	$S_d = \sqrt{\frac{\sum (d_i - \bar{d})^2}{n-1}}$ $S_d = \sqrt{\frac{3330}{12}}$ $\boldsymbol{S_d = 16.583}$	$S_{\bar{d}} = \frac{S_d}{\sqrt{n}}$ $S_{\bar{d}} = \frac{16.58}{\sqrt{13}}$ $\boldsymbol{S_{\bar{d}} = 4.599}$

Repositorio Institucional – UNAMBA - PERÚ

Con todos los datos obtenidos calculamos T de student de muestras relacionadas.

$$t_c = \frac{\bar{d}}{S_{\bar{d}}}$$

$$t_c = \frac{75}{4.599}$$

$$\boldsymbol{t_c = 16.307}$$

Se realizó el análisis en el programa IBM SPSS y se observa que los valores obtenidos son los mismos.

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	riesgos_antes - riesgo_despues	75,000	16,583	4,599	64,979	85,021	16,307	12	,000

*Figura 12.*Resultados de muestras relacionadas en IBM SPSS objetibvo 1

c) Nivel de significancia

El nivel de significancia a considerar es**:**

α= 5% = 0.05

Para todo valor de probabilidad igual o menor que 0.05, se acepta H_1 y se rechaza H_0.

Zona de rechazo:

a. Si $\boldsymbol{t_c} > \boldsymbol{t_t}$ se rechaza H_0 (Hipótesis nula)

b. Si **P** <= **α** se rechaza H_0 (Hipótesis nula)

En SPSS, Sig (bilateral) = valor que permite decidir la aceptación o no de la hipótesis nula. Es la significación muestral de la hipótesis nula, es decir, el p-valor=P.

Repositorio Institucional – UNAMBA - PERÚ

d) Región crítica

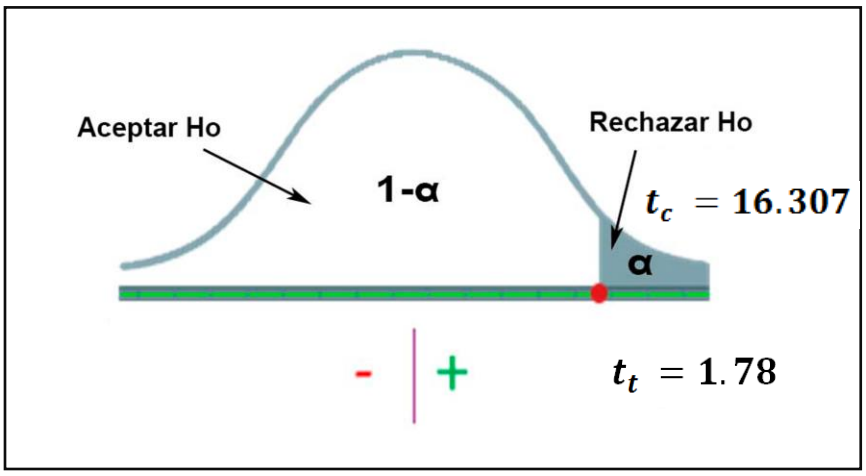


Figura 13. Región crítica de objetivo 1

Decisión

Dado que t_c = 16.3 se compara con los valores críticos de la distribución y se observa que a una probabilidad de α =0.05 le corresponde el valor crítico de t_t=1.78; entonces si $t_c > t_t$ se rechaza la hipótesis nula H_0 y se acepta la hipótesis alterna H_1.

En la figura número 12 se observa que el valor de la probabilidad de datos **P**=0.000 y el nivel de significancia es α=0.05; entonces si **P**<=α se rechaza la hipótesis nula H_0 .

Interpretación

La implementación del Sistema de Gestión de Seguridad de Información disminuye los niveles de riesgos de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.

Prueba de Hipótesis antes y después: La implementación del SGSI incrementará los controles de seguridad en la DTI de la UNAMBA

μ_1: Test/encuesta antes de la implementación del SGSI basado en ISO 27001/2013.

μ_2: Test/encuesta después de la implementación del SGSI basado en ISO 27001/2013.

a) Hipótesis estadística

$$H_0: \mu_1 = \mu_2$$
$$H_1: \mu_2 > \mu_1$$

Dónde:

H_0: La implementación del SGSI no incrementa los controles de seguridad en la DTI de la UNAMBA

H_1: La implementación del SGSI incrementa los controles de seguridad en la DTI de la UNAMBA

b) Estadístico

Se utiliza la distribución muestral de proporciones puesto que se cuenta con los las proporciones del antes y el después.

$$Z_c = \frac{p - P}{S_p} \qquad S_p = \sqrt{\frac{P(1-P)}{n}}$$

Dónde:

Z_c= Z calculada

P = Proporción de controles post test

p = Proporción de controles pre test

S_p = Error estándar de la proporción

n = Tamaño de la muestra

A continuación se muestra los resultados de los cálculos de los controles aplicados antes y después de la realización del plan de tratamientos de riesgos.

Datos:

P=15.78% que equivale a 18 controles

p=57.01% que equivale a 65 controles

n=114 controles

Error Estándar	Estadística de prueba
$S_p = \sqrt{\frac{P(1-P)}{n}}$ $S_p = \sqrt{\frac{0.1578(1-0.1578)}{114}}$	$Z_c = \frac{p - P}{S_p}$ $Z_c = \frac{0.5701 - 0.1578}{0.0341}$ $Z_c = \frac{0.4123}{0.0341}$ $Z_c = 12.09$

$S_p = \sqrt{\frac{0.1578(0.8422)}{114}}$ $S_p = \sqrt{\frac{0.1329}{114}}$ $S_p = \sqrt{0.0001165}$ $S_p = 0.0341$	$Z_t = 1.64$

c) Nivel de significancia

El nivel de significancia a considerar es**:**

α= 5% = 0.05

Para todo valor de probabilidad igual o menor que 0.05, se acepta H_1 y se rechaza H_0.

Zona de rechazo: Si $Z_c > t_t$ se rechaza $\mathbf{H_0}$ (Hipótesis nula)

d) Región crítica

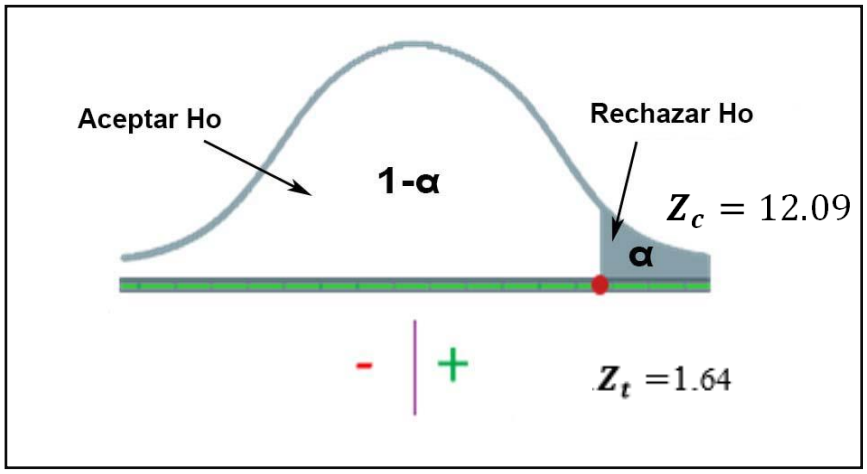


Figura 14. Región crítica de objetivo 2

Decisión

Dado que $\boldsymbol{Z_c}$=12.09 se compara con los valores críticos de la distribución y se observa que a una probabilidad de $\boldsymbol{\alpha}$ =0.05 le corresponde el valor crítico $\boldsymbol{Z_t}$= 1.64; entonces si $\boldsymbol{Z_c} > \boldsymbol{Z_t}$ se rechaza la hipótesis nula H_0 y se acepta la hipótesis alterna H_1.

Interpretación

La implementación del Sistema de Gestión de Seguridad de Información incrementa los controles de seguridad en la Dirección de Tecnologías de Información de la UNAMBA.

Prueba de Hipótesis antes y después: La implementación del SGSI mejorará el nivel de capacitación y formación de los usuarios de la DTI de la UNAMBA en temas de seguridad de la información

$\boldsymbol{\mu 1}$**:** Test/encuesta después de la implementación del SGSI basado en ISO 27001/2013.

$\boldsymbol{\mu 2}$**:** Test/encuesta antes de la implementación del SGSI basado en ISO 27001/2013

a) Hipótesis estadística

$$\mathbf{H_0: \mu_1 = \mu_2}$$
$$\mathbf{H_1: \mu_1 > \mu_2}$$

Dónde:

$\mathbf{H_0}$**:** La implementación del SGSI no mejora el nivel de capacitación y formación de los usuarios de la DTI de la UNAMBA en temas de seguridad de la información

$\mathbf{H_1}$**:** La implementación del SGSI mejora el nivel de capacitación y formación de los usuarios de la DTI de la UNAMBA en temas de seguridad de la información

b) Estadístico

Se utiliza la distribución T student puesto que se cuenta con n=20 encuestados.

$$t_c = \frac{\bar{d}}{S_{\bar{d}}} \qquad \bar{d} = \frac{\sum d_i}{n} \qquad S_d = \sqrt{\frac{\sum (d_i - \bar{d})^2}{n-1}} \qquad S_{\bar{d}} = \frac{S_d}{\sqrt{n}}$$

Repositorio Institucional – UNAMBA - PERÚ

Dónde:

$\boldsymbol{x}$ **=** encuesta antes de capacitación y formación de los usuarios de la DTI

$\boldsymbol{y}$ **=** encuesta después de capacitación y formación de los usuarios de la DTI

$\boldsymbol{d_i}$ = Diferencia por cada par de reporte

$\bar{\boldsymbol{d}}$ = Media aritmética de las diferencias

$\boldsymbol{S_d}$ = Desviación estándar o típica de las diferencias

$\boldsymbol{S_{\bar{d}}}$ = Error estándar o típica de la media

$\boldsymbol{t_c}$ = t de student calculado

$\boldsymbol{n}$ = Tamaño de la muestra

A continuación se muestra la tabla de resultados del cálculo de nivel de capacitación en temas de seguridad de información.

Tabla 8: *Cálculos sobre nivel de capacitación en temas de seguridad de información antes y después de la implementación del SGSI*

N°	x	y	d_i = y-x	$d_i - \bar{d}$	$(d_i - \bar{d})^2$
1	2	7	5	1.5	2.25
2	5	7	2	-1.5	2.25
3	1	7	6	2.5	6.25
4	7	7	0	-3.5	12.25
5	6	7	1	-2.5	6.25
6	2	7	5	1.5	2.25
7	3	6	3	-0.5	0.25
8	1	6	5	1.5	2.25
9	6	7	1	-2.5	6.25
10	4	5	1	-2.5	6.25
11	1	7	6	2.5	6.25
12	2	7	5	2.5	6.25
13	2	6	4	0.5	0.25
14	5	7	2	-1.5	2.25
15	3	7	4	0.5	0.25
16	1	6	5	1.5	2.25
17	5	7	2	-1.5	2.25
18	3	6	3	-0.5	0.25
19	2	7	5	1.5	2.25
20	6	7	1	-2.5	6.25
	Total=67	**Total=133**	**Total=67**	**Total=-3**	**Total=75**

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ

Media Aritmética	Desviación estándar	Error estándar de la media
$\bar{d} = \frac{\sum d_i}{n}$ $\bar{d} = \frac{67}{20}$ $\boldsymbol{\bar{d} = 3.35}$	$S_d = \sqrt{\frac{\sum(d_i - \bar{d})^2}{n-1}}$ $S_d = \sqrt{\frac{75}{19}}$ $\boldsymbol{S_d = 1.98}$	$S_{\bar{d}} = \frac{S_d}{\sqrt{n}}$ $S_{\bar{d}} = \frac{1.98}{\sqrt{20}}$ $\boldsymbol{S_{\bar{d}} = 0.4427}$

Con todos los datos obtenidos calculamos T de student de muestras relacionadas

$$t_c = \frac{\bar{d}}{S_{\bar{d}}}$$
$$t_c = \frac{3.35}{0.44}$$
$$\boldsymbol{t_c = 7.61}$$

Se realizó el análisis en el programa IBM SPSS y se observa que los valores obtenidos son los mismos.

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	capacitacion_despues - capacitación_antes	6,500	3,777	,844	4,732	8,268	7,697	19	,000

Figura 15. Resultados de muestras relacionadas en IBM SPSS de objetivo 3

c) Nivel de significancia

El nivel de significancia a considerar es**:**

α= 5% = 0.05

Para todo valor de probabilidad igual o menor que 0.05, se acepta H_1 y se rechaza H_o.

Zona de rechazo:

a. Si $\boldsymbol{t_c} > \boldsymbol{t_t}$ se rechaza H_0 (Hipótesis nula)

b. Si **P** <= **α** se rechaza H_0 (Hipótesis nula)

Repositorio Institucional – UNAMBA - PERÚ

En SPSS, Sig (bilateral) = valor que permite decidir la aceptación o no de la hipótesis nula. Es la significación muestral de la hipótesis nula, es decir, el p-valor=P.

d) Región crítica

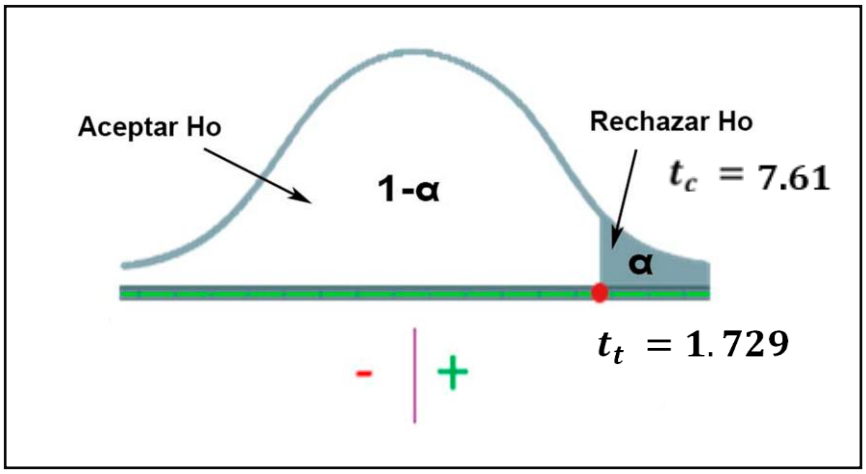


Figura 16. Región crítica de objetivo 3

Decisión

Dado que t_c = 7.61 se compara con los valores críticos de la distribución y se observa que a una probabilidad de 0.05 le corresponde t_t= 1.729; entonces si $t_c > t_t$ se rechaza la hipótesis nula H_0 y se acepta la hipótesis alterna H_1.

En la ilustración número 15 se observa que el valor de la probabilidad de datos **P**=0.000 y el nivel de significancia es α=0.05; entonces si **P**<=α se rechaza la hipótesis nula H_0.

Interpretación

La implementación del Sistema de Gestión de Seguridad de Información mejora el nivel de capacitación y formación de los usuarios de la Dirección de Tecnologías de Información de la UNAMBA en temas de seguridad de información.

Repositorio Institucional – UNAMBA - PERÚ

5.3 Discusión

En el año 2014, Martinez Ramos, Jainer; en la tesis titulada “Sistema de Gestión para mejorar la seguridad de la información en la institución servicios industriales de la marina”, formula la hipótesis “El Sistema de Gestión mejora la Seguridad de la Información en la Institución de Servicios Industriales de la Marina”, el cual se logra probar así mismo indica que el Sistema de Gestión mejoró en 58% la Seguridad de la Información en la Institución de Servicios Industriales de la Marina.

En el caso de esta investigación igualmente la hipótesis es similar “La implementación del SGSI basado en la norma ISO/IEC 27001:2013 mejora la seguridad de información en la Dirección de Tecnologías de la Información de la UNAMBA.”, el cual se logra probar según la metodología PHVA y el cumplimiento de todos los documentos solicitados por la norma ESO/IEC 27001, así poder indicar que se ha contribuido con 71.429% en mejorar el nivel de la seguridad de la información en la DTI de la UNAMBA implementando el SGSI basado en la norma ISO/IEC 27001:2013.

En lo que respecta a la hipótesis específica 1 y 2, se encuentra relación con la investigación realizada en el 2015 de Zeña Ortiz, Victor Eduardo; en la tesis titulada “Estándar internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG”, en la que concluye que la implementación del Sistema de Gestión de Seguridad de la Información en el proceso de Soporte de TI redujo el nivel de riesgo y los controles aplicados se incrementaron.

Repositorio Institucional – UNAMBA - PERÚ

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Con la implementación del Sistema de gestión de seguridad de la Información para la Dirección de Tecnologías de Información de la UNAMBA se logró el objetivo principal que fue de contribuir en mejorar el nivel de la seguridad de la información así logrando asegurar la confidencialidad, integridad y disponibilidad de los activos de información.
- Se logró contribuir en la disminución de los riegos de seguridad a los que se encontraban expuestos los activos de información de la Dirección de Tecnologías de Información a través del análisis y gestión de riesgos que se realizó con la metodología MAGERIT la cual incluye la identificación, diseño e implementación de controles para los riesgos más críticos.
- El desarrollo del análisis y gestión de riesgos permitió el incremento de controles de seguridad lo que indica que los riesgos Altos y Muy Altos se encuentran controlados y en un nivel aceptable.
- La capacitación y formación en temas de seguridad de la información para el personal de la DTI y usuarios de la DTI es de vital importancia ya que el SGSI se podría implementar en toda la institución. Después de la capacitación personal, entrega de material informativo físico y por correo institucional, los trabajadores son conscientes de que la información que ellos manejan es confidencial y que deben velar por su integridad total. La capacitación en temas de seguridad de información robustece al sistema implementado y genera una mejora continua. Esto también permitió que fuese más sencilla la implementación del SGSI.

6.2 Recomendaciones

- Implementar los controles faltantes que se ha determinado en el documento de Plan de Tratamiento de Riesgos y Declaración de Aplicabilidad, ya que no se ha podido implementar todos los controles por motivos de que no se cuenta con personal suficiente.
- Se recomienda realizar continuos talleres y capacitaciones en temas de seguridad de la información y sobre las políticas con las que se cuenta actualmente.

Repositorio Institucional – UNAMBA - PERÚ

- Se recomienda que todas las normas, políticas y reglamentos se aprueben en consejo para que tenga mayor relevancia, también es necesario implantar el SGSI de manera oficial, así mismo continuar con el ciclo PHVA ya que este trabajo de investigación abarco sólo las 2 primeras fases del ciclo PHVA que son “Planear” y “Hacer” y para continuar con las fases “Verificar” y “Actuar” necesariamente se tiene que implantar el SGSI.

Repositorio Institucional – UNAMBA - PERÚ

REFERENCIAS BIBLIOGRÁFICAS

1. RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM. *Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información.* Diario Oficial El Peruano, Lima Perú, 08 de Enero de 2016.

2. OFICINA NACIONAL DE GOBIERNO EECTRONICO E INFORMATICA-ONGEI**.** *Seguridad de la Información, nuevos escenarios* [Diapositiva]. Lima:2016.

3. VILCA MOSQUERA, Ehyetel Celestino. *Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa GEOSURVEY de la ciudad de lima.* Tesis de Pregrado.Universidad de Huanuco. Huanuco, 2017.

4. DORIA CORCHO, Andres Felipe. *Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la Universidad de Cordova*.Tesis de Pregrado.Universidad Nacional Abierta y a Distancia. Montería, 2015.

5. GUERRERO ANGULO, Yezid Camilo. *Sistema de Gestión de la Seguridad de Información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de informática y Telecomunicaciones de la Universidad de Nariño*.Tesis de Pregrado. Pasto, 2014.

6. MARTINEZ RAMOS, Jainer. *Sistema de Gestión para Mejorar la Seguridad de laInformación en la Institución Servicios Industriales de la Marina* .Tesis de Pregrado. Universidad Nacional del Santa.Nvo. Chimbote, 2014.

7. ALCANTARA FLORES, Julio Cesar. *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo*.Tesis de Pregrado. Universidad Catolica Santo Toribio de Mogrovejo. Chiclayo, 2015.

8. ALIAGA FLORES, Luis Carlos. *Diseño de un sistema de gestión de seguridad de la información para un instituto educativo*.Tesis de Pregrado.Pontificia Universidad Catolica del perú. Lima, 2013.

9. ZEÑA ORTIZ, Victor Eduardo. *Estándar internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG*.Tesis de Pregrado.Universidad Nacional Pedro Ruiz Gallo. Lambayeque, 2015.

10. OFICINA NACIONAL DE GOBIERNO ELECTRONICO E INFORMATICA-ONGEI. *Taller de Implementación de la Norma ISO 27001*[Diapositiva]. Lima: 2016.

11. FERNANDEZ SANCHEZ,Carlos Manuel. La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información.*Seguridad y Salud*. España: Asociacion Española para la Calidad, 2012, pp. 40-44.

12. ISO/IEC. Estandar Internacional ISO/IEC 17799. Tecnología de información- Técnicas de seguridad-Código para la práctica de la gestión de la seguridad de la información.España, 2005.

13. ISO/IEC. Estandar Internacional ISO/IEC 27001. Tecnología de información- Técnicas de seguridad-Sistemas de gestión de seguridad de información- Requerimientos.España, 2013. 34 pp.

Repositorio Institucional – UNAMBA - PERÚ

14. LADINO, Martha Isabel, VILLA, Paula Andrea y LÓPEZ, Ana María. Fundamentos de iso 27001 y su aplicación en las empresas. *Scientia Et Technica.* Colombia: Universidad Tecnológica de Pereira, 2011, **17**(47), pp. 334-339. ISSN: 0122-1701

15. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónic. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.

16. Universidad Nacional Micaela Bastidas de Apurímac. Reglamento de organización y funciones (ROF). Abancay, 2017. 78 pp.

17. ISO/IEC. Estandar Internacional ISO/IEC 27000. Tecnología de información- Técnicas de seguridad-Sistemas de gestión de seguridad de información- Revisión y vocabulario.Vernier, 2018. pp. 1-11.

18. HURTADO, Ivan y TORO, Josefina. *Paradigmas y Métodos de investigación en tiempos de cambio*.5ta Edición. Valencia : Episteme Consultores Asociados C.A., 2005. ISBN 980-328-413-4.

19. BALESTRINI, Miriam. *Como se elabora el Proyecto de Investigación.* 7ma Edición.Caracas : Editorial BL Consultores Asociados, 2006. ISBN: 980-6293-03-7

20. KINNEAR, Thomas y TAYLOR, James. *Investigación de mercados: un enfoque aplicado*. 5ta Edición. Mexico : McGraw-Hill, 1998. ISBN: 958-6007-82-0

Repositorio Institucional – UNAMBA - PERÚ

ANEXOS

Anexo 1 – Carta de presentación

Anexo 2 – Carta de autorización para realizar proyecto de tesis.

Anexo 3 – Constancia de ejecución de proyecto de tesis

Anexo 4 – Guía de entrevista sobre existencia de controles generales

Anexo 5 – Checklist de control de cumplimiento de fases del SGSI

Anexo 6 – Checklist de controles existentes en la DTI

Anexo 7 – Cuestionario de aplicación antes y después de la implementación de SGSI

Anexo 8 – Tabulación de resultados de cuestionario de aplicación antes y después de la implementación de SGSI, cuestionario para variables dependientes

Anexo 9 – Resultados detallados de cuestionario de aplicación antes y después de la implementación de SGSI, cuestionario para variables dependientes

Anexo 10 – Alcance

Anexo 11 – Políticas General de seguridad de información

Anexo 12 – Políticas de seguridad de información

Anexo 13 – Metodología de evaluación y tratamiento de riesgo

Anexo 14 – Declaración de aplicabilidad

Anexo 15 – Plan de tratamiento de riesgo

Anexo 16 – Controles implementados

Anexo 17 – Material de capacitación

Anexo 18 – Declaración de confidencialidad

Anexo 19 – Matriz de consistencia

Repositorio Institucional – UNAMBA - PERÚ

Anexo 1 – Carta de presentación

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC
FACULTAD DE INGENIERÍAS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA Y

"Año de la lucha Contra la Corrupción e Impunidad"

CARTA DE PRESENTACIÓN N° 001

Abancay, 04 de febrero del 2019

CARTA N°0418-2019- EAPIIS-UNAMBA.

Señor:
Ing. Evelyn Yeni Medrano Kari
Director de Tecnología de información de la Universidad Nacional Micaela Bastidas de Apurímac

Presente.-

Universidad Nacional Micaela Bastidas de Apurimac
OFICINA DE TECNOLOGIA DE INFORMACION
Nº Registro 037 Folios : 02
Fecha : 06/03/19 Hora : 12:57
Firma

Asunto: Carta de Presentación para la realización de proyecto de tesis
Ref : Solicitud de estudiante.

De mi mayor consideración:

Previo cordial saludo, y en atención al documento de la referencia antes citada, remito la Carta de Presentación a favor del bachiller **JESSICA NORALINA HUALLPA LAGUNA** con código Nro. **101118** de la **E.A.P. de Ingeniería Informática y Sistemas**, para que realice su proyecto de tesis en la Director de Tecnología de información de la Universidad Nacional Micaela Bastidas de Apurímac.

Agradeciendo anticipadamente la atención que le brinde al presente y acogiéndome a su espíritu colaborador e identificación con los jóvenes estudiantes de la UNAMBA, aprovecho la oportunidad para expresarle las muestras de mi aprecio y estima personal

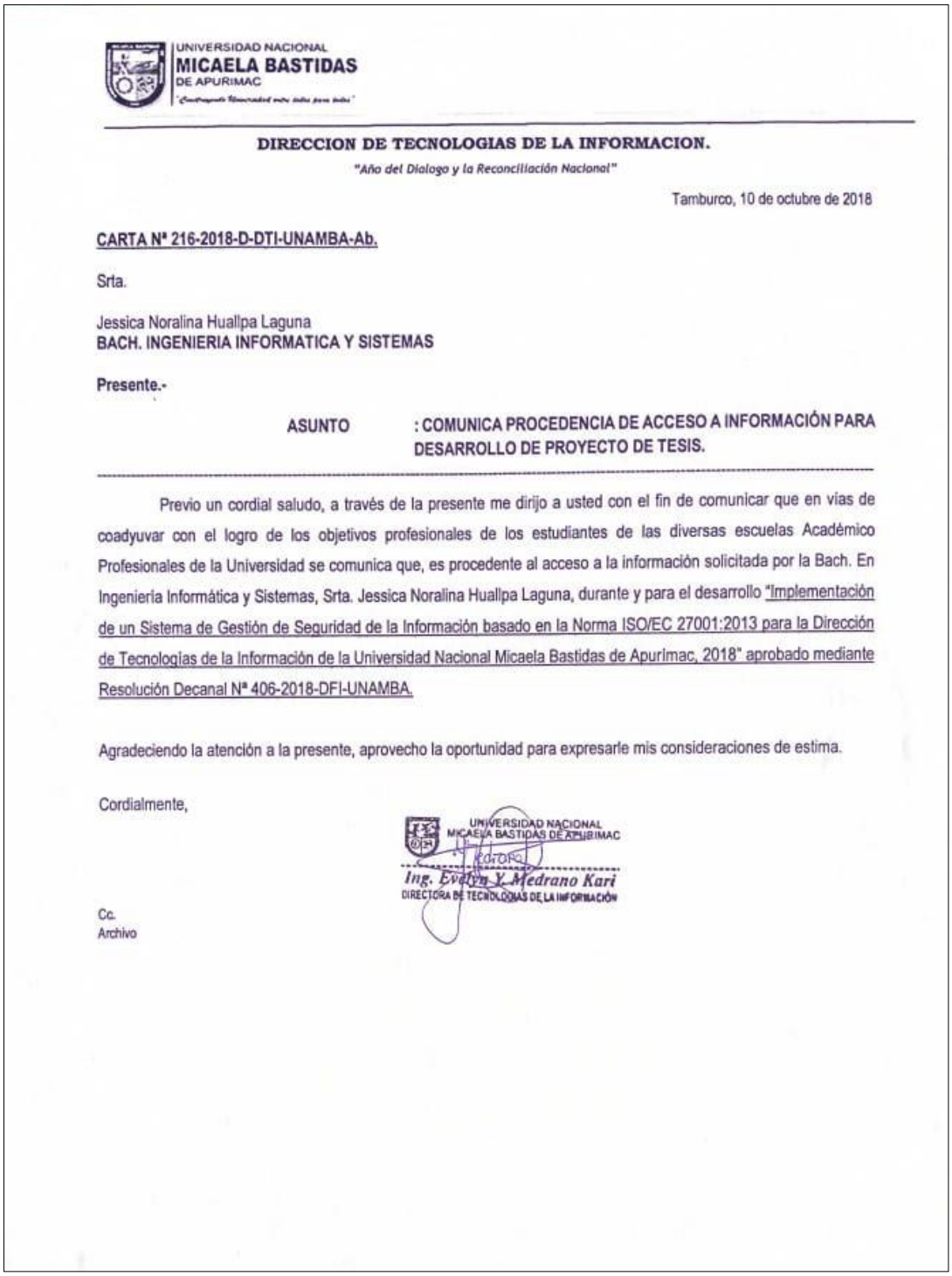
Atentamente,

Cc
Archivo
EAPIIS

Campus Universitario S/N Tamburco Abancay-Apurímac
Carretera Panamericana Abancay Cusco Km 5

Figura 17. *Carta de presentación*

Anexo 2 – Carta de autorización para realizar proyecto de tesis.



UNIVERSIDAD NACIONAL
MICAELA BASTIDAS
DE APURIMAC

DIRECCION DE TECNOLOGIAS DE LA INFORMACION.

"Año del Dialogo y la Reconciliación Nacional"

Tamburco, 10 de octubre de 2018

CARTA N° 216-2018-D-DTI-UNAMBA-Ab.

Srta.

Jessica Noralina Huallpa Laguna
BACH. INGENIERIA INFORMATICA Y SISTEMAS

Presente.-

ASUNTO : COMUNICA PROCEDENCIA DE ACCESO A INFORMACIÓN PARA DESARROLLO DE PROYECTO DE TESIS.

Previo un cordial saludo, a través de la presente me dirijo a usted con el fin de comunicar que en vías de coadyuvar con el logro de los objetivos profesionales de los estudiantes de las diversas escuelas Académico Profesionales de la Universidad se comunica que, es procedente al acceso a la información solicitada por la Bach. En Ingeniería Informática y Sistemas, Srta. Jessica Noralina Huallpa Laguna, durante y para el desarrollo "Implementación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/EC 27001:2013 para la Dirección de Tecnologías de la Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018" aprobado mediante Resolución Decanal N° 406-2018-DFI-UNAMBA.

Agradeciendo la atención a la presente, aprovecho la oportunidad para expresarle mis consideraciones de estima.

Cordialmente,

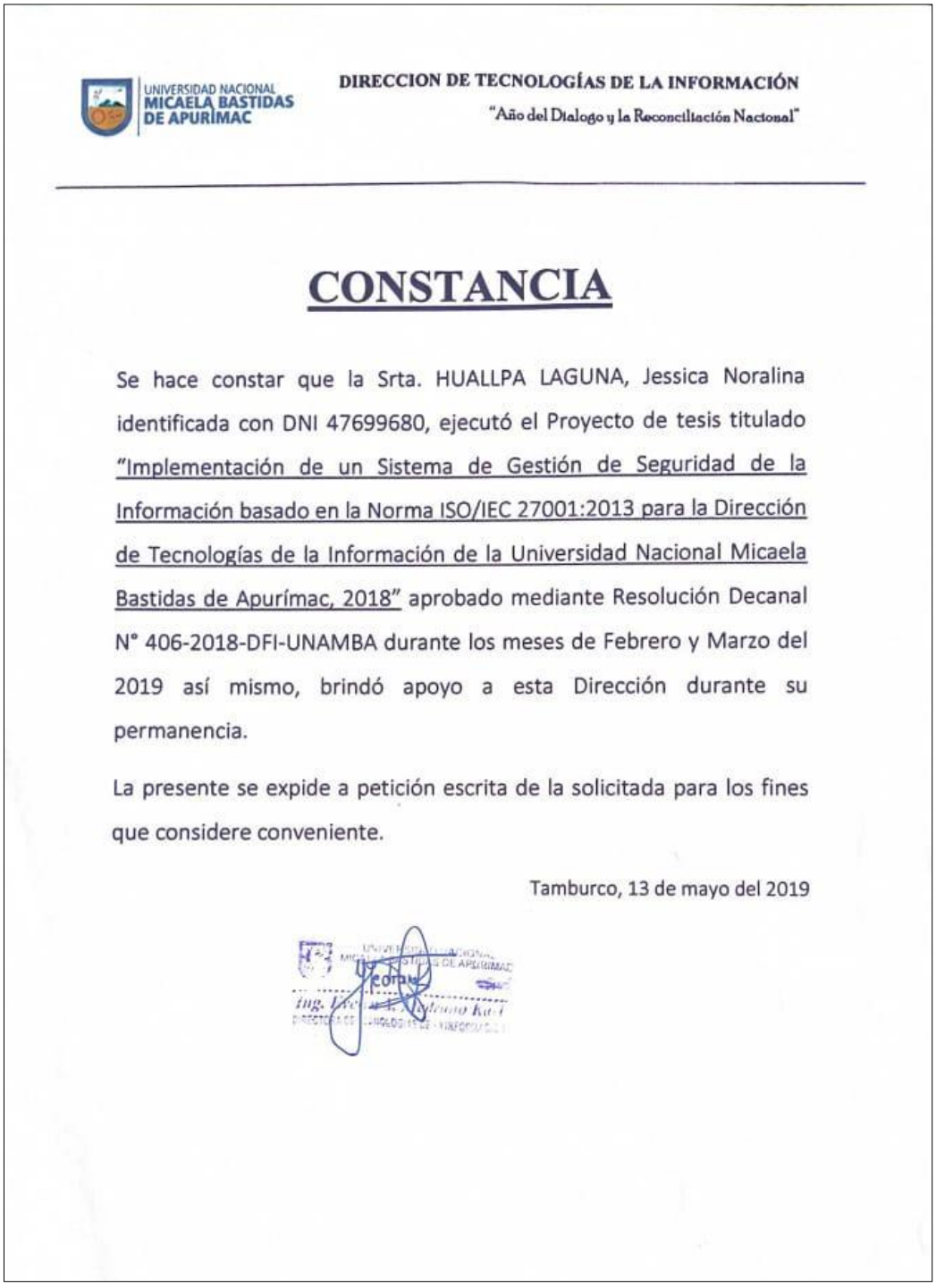
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURIMAC
Ing. Evelyn Y. Medrano Kari
DIRECTORA DE TECNOLOGIAS DE LA INFORMACIÓN

Cc.
Archivo

Figura 18. *Carta de Autorización*

Repositorio Institucional – UNAMBA - PERÚ

Anexo 3 – Constancia de ejecución de proyecto de tesis



UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

DIRECCION DE TECNOLOGÍAS DE LA INFORMACIÓN

"Año del Dialogo y la Reconciliación Nacional"

CONSTANCIA

Se hace constar que la Srta. HUALLPA LAGUNA, Jessica Noralina identificada con DNI 47699680, ejecutó el Proyecto de tesis titulado "Implementación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 para la Dirección de Tecnologías de la Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018" aprobado mediante Resolución Decanal N° 406-2018-DFI-UNAMBA durante los meses de Febrero y Marzo del 2019 así mismo, brindó apoyo a esta Dirección durante su permanencia.

La presente se expide a petición escrita de la solicitada para los fines que considere conveniente.

Tamburco, 13 de mayo del 2019

Figura 19. *Constancia de ejecución de proyecto de tesis*

Repositorio Institucional – UNAMBA - PERÚ

Anexo 4 – Guía de entrevista sobre existencia de controles generales.

Esta guía de entrevista se aplicó antes y después de la implementación de SGSI, para diagnosticar si se cuentan con controles generales.

GUÍA DE ENTREVISTA

Estimado(a), de manera muy cordial se le invita a responder el siguiente cuestionario, estas preguntas tienen el objetivo de recolectar su importante opinión referente a la importancia del Sistema de Gestión de Seguridad de la Información. Gracias por su participación.
Instrucciones: Debe responder las preguntas de manera honesta y responsable. Sus respuestas deben ser claras y concisas.

1. ¿Su computadora recibe mantenimiento de manera periódica?
   - ☐ SI ☐ NO
2. ¿Realiza copias de información de su labor diaria?
   - ☐ SI ☐ NO
3. ¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?
   - ☐ Ingreso de usuario y contraseña ☐ Tarjeta inteligente
   - ☐ Lector de huellas dactilares ☐ Ninguno
4. ¿Tiene conocimiento sobre el plan de inventario de equipos?
   - ☐ SI ☐ NO
5. ¿Tiene conocimiento sobre el control registros de incidentes?
   - ☐ SI ☐ NO
6. ¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?
   - ☐ 1 horas ☐ 2 horas
   - ☐ 12horas ☐ 24horas ☐ Otros
7. ¿Ud. apaga o bloque su computadora cuando se va almorzar?
   - ☐ SI ☐ NO
8. ¿Con que frecuencia cambia su contraseña del equipo?
   - ☐ Nunca ☐ cada mes
   - ☐ cada 3 meses ☐ cada 6 meses ☐ cada 12 meses
9. ¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?
   - ☐ SI ☐ NO
10. ¿Tiene alguna restricción para ingresar a los servicios de Internet?
    - ☐ SI ☐ NO
11. ¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?
    - ☐ Ninguno ☐ Usuario y contraseña
12. ¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información de la institución?
    - ☐ SI ☐ NO

Figura 20. *Guía de entrevista*

Repositorio Institucional – UNAMBA - PERÚ

Anexo 5 – Checklist de control de cumplimiento de fases del SGSI

CHECKLIST

CUESTIONARIO DE CONTROL DE CUMPLIMIENTO DE FASES DEL CICLO PHVA DEL SGSI

Tabla 9: *Checklist control de cumplimiento de fases PHVA del SGSI*

NOMBRE DE EVALUADORES		
DOMINIO	Fases del SGSG	
OBJETIVO DEL CONTROL	Evaluación de cumplimiento de Fases del SGSI según la norma ISO/IEC 27001	

CUESTIONARIO			
FASE	**PREGUNTA**	**SI**	**NO**
Planear-plan (57,143%)	¿Se realizó el alcance del SGSI? (4.-Contexto de organización)		
	¿Se realizó las políticas y objetivos de seguridad de la información? (5.- Liderazgo)		
	¿Se realizó el análisis y evaluación de riesgos? (6.-Planificación)		
	¿Se realizó capacitación y formación en temas de seguridad al personal? (7.- Soporte)		
Hacer-do (14,286%)	¿Se definió el plan de tratamiento de riesgos? (8.-Operación)		
Verificar-check (14,286%)	¿Se realizó auditoría interna? (9.-Evaluación de desempeño)		
Actuar-act (14,286%)	¿Se realizó mejora continua? (10.-Mejora)		

Fuente: Elaboración propia

Anexo 6 – Checklist de controles existentes en la DTI

CHECKLIST

CHECKLIST DE CONTROLES PREVIOS AL PROYECTO/ CHECKLIST DE CONTROLES POSTERIORES AL PROYECTO

Tabla 10: *Checklist de controles*

A.5 Políticas de seguridad de la información			
A.5.1 Dirección de la gerencia para la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	SI ( )	NO ( )
A.5.1.2	Revisiones para las políticas de la seguridad de la información	SI ( )	NO ( )
A.6 Organización de la seguridad de la información			
A.6.1 Organización interna			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI ( )	NO ( )
A.6.1.2	Segregación de funciones	SI ( )	NO ( )
A.6.1.3	Contacto con autoridades	SI ( )	NO ( )
A.6.1.4	Contacto con grupos especiales de interés	SI ( )	NO ( )
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI ( )	NO ( )

Repositorio Institucional – UNAMBA - PERÚ

A.6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política de dispositivos móviles	SI ( )	NO ( )
A.6.2.2	Teletrabajo	SI ( )	NO ( )
A.7 Seguridad de los recursos humanos			
A.7.1 Antes del empleo			
A.7.1.1	Selección	SI ( )	NO ( )
A.7.1.2	Términos y condiciones del empleo	SI ( )	NO ( )
A.7.2 Durante el empleo			
A.7.2.1	Responsabilidades de la gerencia	SI ( )	NO ( )
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	SI ( )	NO ( )
A.7.2.3	Proceso disciplinario	SI ( )	NO ( )
A.7.3 Terminación y cambio de empleo			
A.7.3.1	Terminación o cambio de responsabilidades del empleo	SI ( )	NO ( )
A.8 Gestión de activos			
A.8.1 Responsabilidad por los activos			
A.8.1.1	Inventario de activos	SI ( )	NO ( )
A.8.1.2	Propiedad de los activos	SI ( )	NO ( )
A.8.1.3	Uso aceptable de los activos	SI ( )	NO ( )
A.8.1.4	Retorno de los activos	SI ( )	NO ( )
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	SI ( )	NO ( )
A.8.2.2	Etiquetado de la información	SI ( )	NO ( )
A.8.2.3	Manejo de activos	SI ( )	NO ( )
A.8.3 Manejo de los medios			
A.8.3.1	Gestión de medios removibles	SI ( )	NO ( )
A.8.3.2	Disposición de medios	SI ( )	NO ( )
A.8.3.3	Transferencia de medios físicos	SI ( )	NO ( )
A.9 Control de acceso			
A.9.1 Requisitos de la empresa para el control de acceso			
A.9.1.1	Política de control de acceso	SI ( )	NO ( )
A.9.1.2	Acceso a redes y servicios de red	SI ( )	NO ( )
A.9.2 Gestión de acceso de usuario			
A.9.2.1	Registro y baja de usuarios	SI ( )	NO ( )
A.9.2.2	Aprovisionamiento de acceso a usuario	SI ( )	NO ( )
A.9.2.3	Gestión de derechos de acceso privilegiados	SI ( )	NO ( )
A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI ( )	NO ( )
A.9.2.5	Revisión de derechos de acceso de usuarios	SI ( )	NO ( )
A.9.2.6	Remoción o ajuste de derechos de acceso	SI ( )	NO ( )
A.9.3 Responsabilidades de los usuarios			
A.9.3.1	Uso de información de autenticación secreta	SI ( )	NO ( )
A.9.4 Control de acceso a sistema y aplicación			
A.9.4.1	Restricción de acceso a la información	SI ( )	NO ( )

Repositorio Institucional – UNAMBA - PERÚ

A.9.4.2	Procedimientos de ingreso seguro	SI ( )	NO ( )
A.9.4.3	Sistema de gestión de contraseñas	SI ( )	NO ( )
A.9.4.4	Uso de programas utilitarios privilegiados	SI ( )	NO ( )
A.9.4.5	Control de acceso al código fuente de los programas	SI ( )	NO ( )
A.10 Criptografía			
A.10.1 Controles criptográficos			
A.10.1.1	Política sobre el uso de controles criptográficos	SI ( )	NO ( )
A.10.1.2	Gestión de claves	SI ( )	NO ( )
A.11 Seguridad física y ambiental			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	SI ( )	NO ( )
A.11.1.2	Controles de ingreso físico	SI ( )	NO ( )
A.11.1.3	Asegurar oficinas, áreas e instalaciones	SI ( )	NO ( )
A.11.1.4	Protección contra amenazas externas y ambientales	SI ( )	NO ( )
A.11.1.5	Trabajo en áreas seguras	SI ( )	NO ( )
A.11.1.6	Áreas de despacho y carga	SI ( )	NO ( )
A.11.2 Equipos			
A.11.2.1	Emplazamiento y protección de los equipos	SI ( )	NO ( )
A.11.2.2	Servicios de suministro	SI ( )	NO ( )
A.11.2.3	Seguridad del cableado	SI ( )	NO ( )
A.11.2.4	Mantenimiento de equipos	SI ( )	NO ( )
A.11.2.5	Remoción de activos	SI ( )	NO ( )
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI ( )	NO ( )
A.11.2.7	Disposición o reutilización segura de los equipos	SI ( )	NO ( )
A.11.2.8	Equipos de usuario desatendidos	SI ( )	NO ( )
A.11.2.9	Política de escritorio limpio y pantalla limpia	SI ( )	NO ( )
A.12 Seguridad de las operaciones			
A.12.1 Procedimientos y responsabilidades operativas			
A.12.1.1	Procedimientos operativos documentados	SI ( )	NO ( )
A.12.1.2	Gestión del cambio	SI ( )	NO ( )
A.12.1.3	Gestión de la capacidad	SI ( )	NO ( )
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	SI ( )	NO ( )
A.12.2 Protección contra códigos maliciosos			
A.12.2.1	Controles contra códigos maliciosos	SI ( )	NO ( )
A.12.3 Respaldo			
A.12.3.1	Respaldo de la información	SI ( )	NO ( )
A.12.4 Registros y monitoreo			
A.12.4.1	Registro de eventos	SI ( )	NO ( )
A.12.4.2	Protección de información de registros	SI ( )	NO ( )
A.12.4.3	Registros del administrador y del operador	SI ( )	NO ( )
A.12.4.4	Sincronización de reloj	SI ( )	NO ( )
A.12.5 Control del Software operacional			

Repositorio Institucional – UNAMBA - PERÚ

A.12.5.1	Instalación de software en sistemas operacionales	SI ( )	NO ( )
A.12.6 Gestión de vulnerabilidad técnica			
A.12.6.1	Gestión de vulnerabilidades técnicas	SI ( )	NO ( )
A.12.6.2	Restricciones sobre la instalación de software	SI ( )	NO ( )
A.12.7 Consideraciones para la auditoría de los sistemas de información			
A.12.7.1	Controles de auditoría de sistemas de información	SI ( )	NO ( )
A.13 Seguridad e las comunicaciones			
A.13.1 Gestión de seguridad de la red			
A.13.1.1	Controles de la red	SI ( )	NO ( )
A.13.1.2	Seguridad de servicios de red	SI ( )	NO ( )
A.13.1.3	Segregación en redes	SI ( )	NO ( )
A.13.2 Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de la información	SI ( )	NO ( )
A.13.2.2	Acuerdo sobre la transferencia de información	SI ( )	NO ( )
A.13.2.3	Mensajes electrónicos	SI ( )	NO ( )
A.13.2.4	Acuerdos de confidencialidad o no divulgación	SI ( )	NO ( )
A.14 Adquisición, desarrollo y mantenimiento de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI ( )	NO ( )
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	SI ( )	NO ( )
A.14.1.3	Protección de transacciones en servicios de aplicación	SI ( )	NO ( )
A.14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	SI ( )	NO ( )
A.14.2.2	Procedimientos de control de cambio de sistema	SI ( )	NO ( )
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operati	SI ( )	NO ( )
A.14.2.4	Restricciones sobre cambios a los paquetes de software	SI ( )	NO ( )
A.14.2.5	Principios de ingeniería de sistemas seguros	SI ( )	NO ( )
A.14.2.6	Ambiente de desarrollo seguro	SI ( )	NO ( )
A.14.2.7	Desarrollo contratado externamente	SI ( )	NO ( )
A.14.2.8	Pruebas de seguridad del sistema	SI ( )	NO ( )
A.14.2.9	Pruebas de aceptación del sistema	SI ( )	NO ( )
A.14.3 Datos de prueba			
A.14.3.1	Protección de datos de prueba	SI ( )	NO ( )
A.15 Relaciones con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedor	SI ( )	NO ( )
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	SI ( )	NO ( )
A.15.1.3	Cadena de suministro tecnología de información y comunicación	SI ( )	NO ( )
A.15.2 Gestión de entrega de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	SI ( )	NO ( )
A.15.2.2	Gestión de cambios a los servicios de proveedores	SI ( )	NO ( )
A.16 Gestión de incidentes de seguridad de la información			

Repositorio Institucional – UNAMBA - PERÚ

A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos	SI ( )	NO ( )
A.16.1.2	Reporte de eventos de seguridad de información	SI ( )	NO ( )
A.16.1.3	Reportes de debilidades de seguridad de información	SI ( )	NO ( )
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de información	SI ( )	NO ( )
A.16.1.5	Respuesta a incidentes de seguridad de información	SI ( )	NO ( )
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI ( )	NO ( )
A.16.1.7	Recolección de información	SI ( )	NO ( )
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio			
A.17.1 Continuidad de seguridad de la información			
A.17.1.1	Planificación de continuidad de seguridad de la información	SI ( )	NO ( )
A.17.1.2	Implementación de continuidad de seguridad de la información	SI ( )	NO ( )
A.17.1.3	Verificación , revisión y evaluación de continuidad de seguridad de informaci	SI ( )	NO ( )
A.17.2 Redundancias			
A.17.2.1	Instalaciones de procesamiento de la información	SI ( )	NO ( )
A.18 Cumplimiento			
A.18.1 Cumplimiento con requisitos legales y contractuales			
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	SI ( )	NO ( )
A.18.1.2	Derechos de propiedad intelectual	SI ( )	NO ( )
A.18.1.3	Protección de registros	SI ( )	NO ( )
A.18.1.4	Privacidad y protección de datos personales	SI ( )	NO ( )
A.18.1.5	Regulación de controles criptográficos	SI ( )	NO ( )
A.18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	SI ( )	NO ( )
A.18.2.2	Cumplimiento de políticas y normas de seguridad	SI ( )	NO ( )
A.18.2.3	Revisión del cumplimiento técnico	SI ( )	NO ( )

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ

Anexo 7 – Cuestionario de aplicación antes y después de la implementación de SGSI sobre conocimiento en seguridad de información.

CUESTIONARIO SOBRE CONOCIMIENTO EN SEGURIDAD DE INFORMACIÓN

Estimado(a), de manera muy cordial se le invita a responder el siguiente cuestionario, estas preguntas tienen el objetivo de recolectar su importante opinión referente a la importancia del Sistema de Gestión de Seguridad de la Información. Gracias por su participación.

Instrucciones: Debe responder las preguntas de manera honesta y responsable. Sus respuestas deben ser claras y concisas.

Tabla 11: *Cuestionario sobre conocimientos de seguridad de información*

1. ¿Considera que la seguridad de la información es importante en toda la institución?

   ☐ SI ☐ NO

2. ¿Tiene conocimiento sobre las políticas de seguridad de la información?

   ☐ SI ☐ NO

3. ¿Usted sabe que son las copias de respaldo de información?

   ☐ SI ☐ NO

4. ¿Usted conoce sobre las amenazas informáticas?

   ☐ SI ☐ NO

5. ¿Usted conoce cuales son los activos informáticos en su área de trabajo?

   ☐ SI ☐ NO

6. ¿Conoce los riesgos a los que está expuesto los activos con los que trabaja?

   ☐ SI ☐ NO

7. ¿Considera que los activos de la información de la organización están bien protegidos?

   ☐ SI ☐ NO

Fuente: Ehytel Celestino Vilca Mosquera (3)

Anexo 8 – Tabulación de resultados de cuestionario de aplicación antes y después de la implementación de SGSI sobre conocimiento en seguridad de información.

A continuación se muestra los resultados del Pre test y Post test, se consideró n=20 encuestados y cada cuestionario de 07 preguntas.

Para la obtención del puntaje se utilizó:

SI	**NO**
1 punto	0 puntos

Se consideró 0 debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que se consideró 1 por representar el puntaje óptimo.

Repositorio Institucional – UNAMBA - PERÚ

Tabla 12: *Resultado por pregunta-Pre test*

	PRE TEST																		
N°	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
P1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
P2	0	0	0	1	1	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1
P3	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	0	0	0
P4	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	0	1	1	0	1
P5	0	1	0	1	1	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1
P6	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1
P7	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
T.	**2**	**5**	**1**	**7**	**6**	**2**	**3**	**1**	**6**	**4**	**1**	**2**	**2**	**5**	**3**	**1**	**5**	**3**	**2**	**6**

Fuente: Elaboración propia

Tabla 13: *Resultado por pregunta - Post test*

	POST TEST																			
N°	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
P1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P2	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1
P3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P6	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
P7	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	0	1	0	1	1
T.	**7**	**7**	**7**	**7**	**7**	**7**	**6**	**6**	**7**	**5**	**7**	**7**	**6**	**7**	**7**	**6**	**7**	**6**	**7**	**7**

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ

Anexo 9 – Resultados detallados de cuestionario de aplicación antes y después de la implementación de SGSI sobre conocimiento en seguridad de información.

Pregunta 1: ¿Considera que la seguridad de la información es importante en toda la institución?

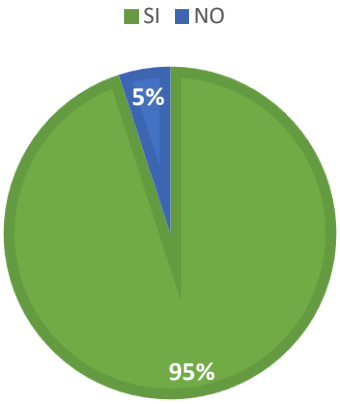
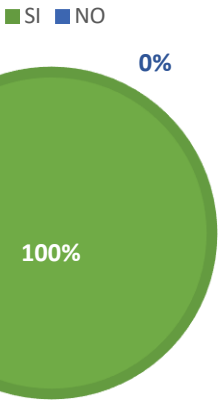
1. ¿Considera que la seguridad de la información es importante en toda la institución?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	19	95%	20	100%
No	1	5%	0	0%

Figura 21. *Resultado de encuesta - pregunta 1*

Interpretación:

En la figura anterior se puede observar que antes de la implementación del SGSI, el personal encuestado consideraba la seguridad de la información muy importante (95%) por lo que después de la implementación todos los encuestados en general son conscientes de ello (100%).

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 2: ¿Tiene conocimiento sobre las políticas de seguridad de la información?

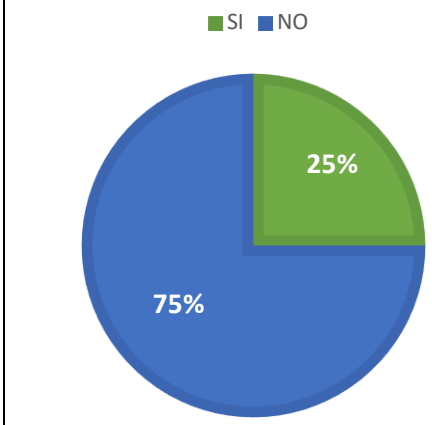
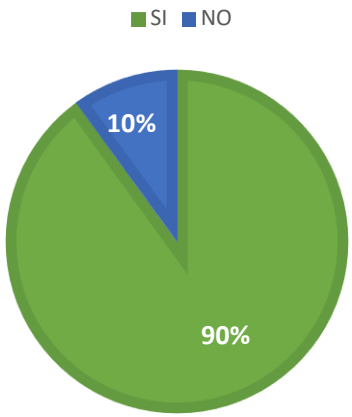
2. ¿Tiene conocimiento sobre las políticas de seguridad de la información?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	5	25%	18	90%
No	15	75%	2	10%

Figura 22. *Resultado de encuesta - pregunta 2*

Interpretación:

En la figura anterior se puede observar que solo el 25% de los encuestados tenía conocimiento sobre las políticas de seguridad de la información. Sin embargo esto se revierte después de la implementación del SGSI incrementándose a 90%.

Es muy importante tener conocimiento sobre las políticas de seguridad de información, ya que este conjunto de medidas y procedimientos permiten salvaguardar la información así mismo proteger la confidencialidad, disponibilidad de los datos.

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 3: ¿Usted sabe que son las copias de respaldo de información?

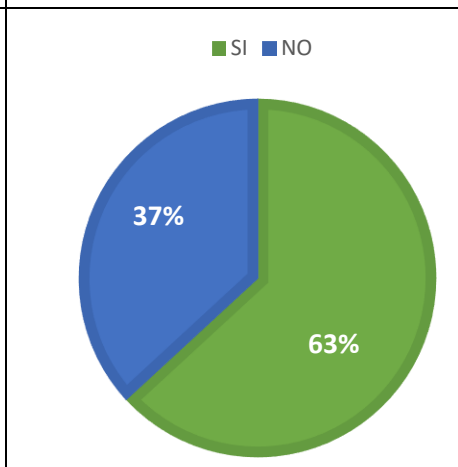
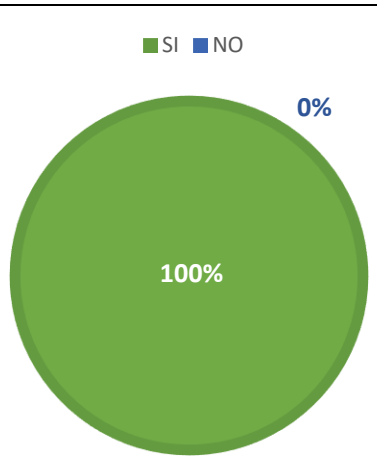
3. ¿Usted sabe que son las copias de respaldo de información?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	12	60%	20	100%
No	8	40%	0	0%

Figura 23. *Resultado de encuesta - pregunta 3*

Interpretación:

En la figura anterior se puede observar que el 60% de los encuestados tenía conocimiento sobre que son las de copias de respaldo de información pero muchos de ellos no sabían que procedimiento se debe realizar para tener copia de seguridad de su información por lo que mediante volantes informativos y capacitación personal después de la implementación del SGSI el 100% tiene conocimiento sobre ello y como realizarlos.

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 4: ¿Usted conoce sobre las amenazas informáticas?

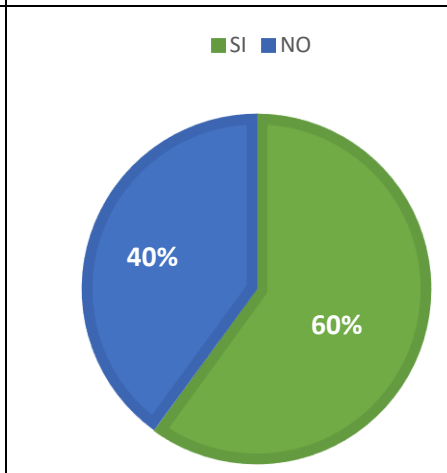
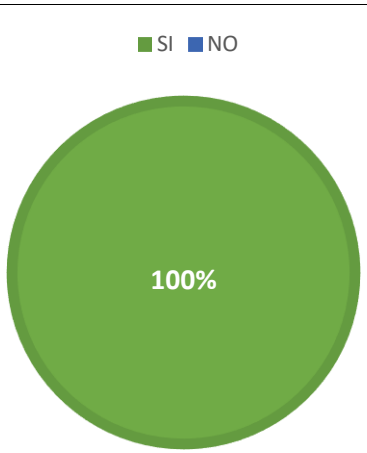
4. ¿Usted conoce sobre las amenazas informáticas?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	12	60%	20	100%
No	8	40%	0	0%

Figura 24. *Resultado de encuesta - pregunta 4*

Interpretación:

En la figura anterior se puede observar que en su mayoría (60%) los trabajadores encuestados tienen noción sobre las amenazas informáticas, pero al dialogar sobre ello tienen conocimientos generales mas no saben cómo prevenirlos o contrarrestarlos, después de la implementación del SGSI el total (100%) de los encuestados son conscientes a qué tipo de amenazas se encuentran expuestas los activos con los que trabajan.

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 5: ¿Usted conoce cuales son los activos informáticos en su área de trabajo?

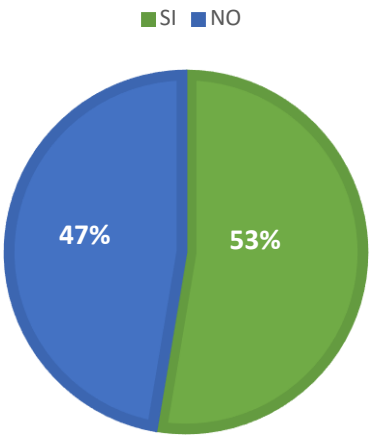
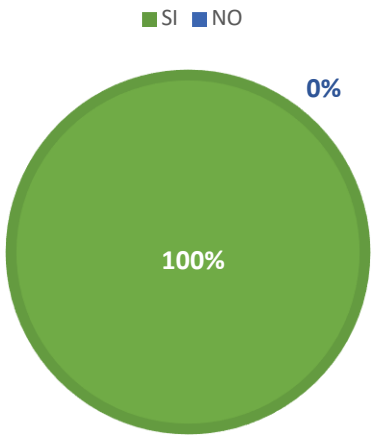
5. ¿Usted conoce cuales son los activos informáticos en su área de trabajo?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	10	50%	20	100%
No	10	50%	0	0%

Figura 25. Resultado de encuesta - pregunta 5

Interpretación:

En la figura anterior se puede observar que la mitad (50%) de los encuestados conocen los activos informáticos en su área de trabajo así mismo son conscientes de la importancia de ello. Después de haber realizado la implementación del SGSI se observa 100% del personal encuestado conocen los activos con los que trabajan.

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 6: ¿Conoce los riesgos a los que está expuesto los activos con los que trabaja?

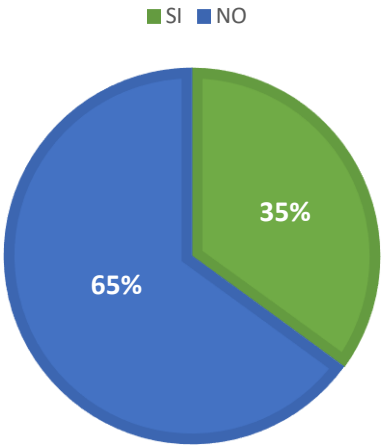
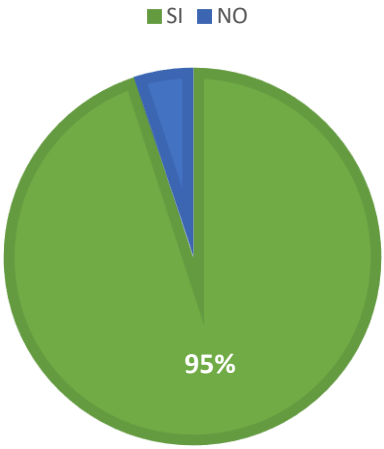
6. ¿Conoce los riesgos a los que está expuesto los activos con los que trabaja?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	7	35%	19	95%
No	13	65%	1	5%

Figura 26. Resultado de encuesta - pregunta 6

Interpretación:

En la figura anterior se puede observar que antes de la implementación del SGSI algunos de los encuestados (35%) tenían conocimiento sobre los activos informáticos con los que trabajan pero muchos de ellos no sabían de qué riesgos protegerlos ya que no se contaba con un mapa de riesgos. Luego de la implementación del SGSI esto cambia ya que la mayoría (95%) es consciente de las vulnerabilidades y amenazas que podrían aprovecharse de estas.

.

Repositorio Institucional – UNAMBA - PERÚ

Pregunta 7: ¿Considera que los activos de la información de la organización están bien protegidos?

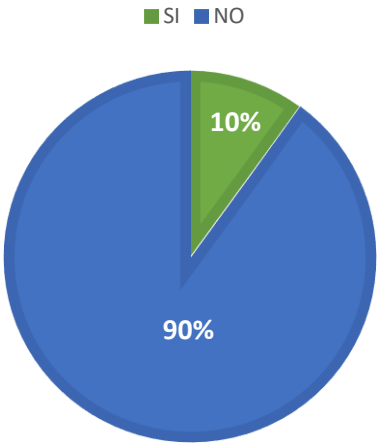
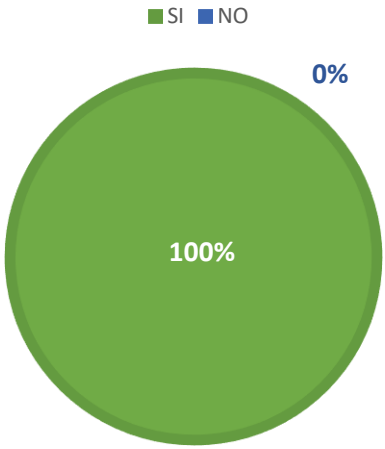
7. ¿Considera que los activos de la información de la organización están bien protegidos?				
	Pre test		Post test	
				
Respuesta	Frecuencia	Porcentaje	Frecuencia	Porcentaje
Si	2	10%	16	80%
No	18	90%	4	20%

Figura 27. Resultado de encuesta - pregunta 7

Interpretación:

En la figura anterior se puede observar que la mayoría (90%) de los encuestados considera que los activos de la información no se encuentran bien protegidos, pero después de la implementación del SGSI, con políticas de seguridad de la información y los controles diseñados se redujeron a 20%, logrando de que el 80% de los encuestados indiquen que sus activos se encuentran protegidos.

Repositorio Institucional – UNAMBA - PERÚ

Anexo 10 – Alcance

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

DOCUMENTO SOBRE EL ALCANCE DEL SGSI

Código	DTI-001
Versión	01
Fecha de la versión	23/01/2019
Creado por	Huallpa Laguna Jessica Noralina
Aprobado por	Ing. Evelyn Yeni Medrano Kari
Nivel de confidencialidad	Baja

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este documento es definir claramente el alcance y los límites del Sistema de gestión de seguridad de la información (SGSI) en la Dirección de tecnologías de la información – UNAMBA. Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los miembros de la Dirección de tecnologías de la información – UNAMBA, los miembros del equipo del proyecto que implementa el SGSI y los colaboradores que formaran parte de la institución en mención.

II. DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los siguientes:

- Norma ISO/IEC 27001, capítulos 4.3

III. DEFINICION DEL ALCANCE DEL SGSI

La Dirección de Tecnologías de Información necesita definir los límites del SGSI para decidir qué información quiere proteger. Esa información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre esa información.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

3.1 PROCESOS Y SERVICIOS

Dentro de los procesos y servicios que se dan en la Dirección de Tecnologías de Información de la UNAMBA contamos con lo siguiente:

Repositorio Institucional – UNAMBA - PERÚ

- Analizar, desarrollar y evaluar sistemas de información, y proyectos informáticos requeridos por la universidad y administrar la operatividad de los mismos.
- Establecer conectividad del servicio de red local – LAN/internet, Wireless requerida por la universidad.
- Proporcionar soporte técnico para asegurar la operatividad continua de los equipos de cómputo y comunicaciones.
- Evaluar, proponer e implementar nuevas tecnologías como soluciones para la optimización de los procesos administrativos y gestión universitaria.
- Promover y apoyar la capacitación a docentes y personal administrativo en el manejo de los sistemas de información y manejo de recursos informáticos.
- Elaborar planes, políticas, normas, reglamentos, directivas y estándares para el desarrollo y uso de los recursos informáticos, redes y conectividad en la universidad.

3.2 UNIDADES ORGANIZATIVAS

La dirección de Tecnologías de información de la UNAMBA se estructura de la manera siguiente:

- Área de gestión de proyectos e infraestructura de red corporativa.
- Área de soporte técnico y mantenimiento.

3.3 UBICACIÓN

El SGSI cubrirá los procesos y activos de información que pertenecen a la Dirección de Tecnologías de Información:

- Universidad Nacional Micaela Bastidas de Apurímac - Av. Inca Garcilaso de la vega S/N, Tamburco-Abancay-Apurímac.

Repositorio Institucional – UNAMBA - PERÚ

Anexo 11 – Política General de seguridad de información

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código	DTI-002
Versión	01
Fecha de la versión	23/01/2019
Creado por	Huallpa Laguna Jessica Noralina
Aprobado por	Ing. Evelyn Yeni Medrano Kari
Nivel de confidencialidad	Baja

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información. Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en el Documento del Alcance del SGSI. Los usuarios de este documento son todos los trabajadores de la Dirección de tecnologías de Información, como también los usuarios de las tecnologías de información que incluye a docentes, alumnos y personal administrativo.

II. DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los siguientes:

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales

III. DEFINICIONES

- **Confidencialidad:** característica de la información que está disponible solo para personas o sistemas autorizados.
- **Integridad:** característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad:** característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.
- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de gestión de seguridad de la información:** parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Repositorio Institucional – UNAMBA - PERÚ

- **Activo:** es cualquier recurso que genere valor para la institución. Dentro de los activos informáticos se encuentran las bases de datos, sistemas operativos, software, aplicaciones, códigos fuentes, dispositivos de redes y comunicaciones, etc.

IV. OBJETIVOS GENERALES

En su propósito de lograr niveles adecuados de integridad, confidencialidad y disponibilidad de la información, la Dirección de Tecnologías de Información tendrá como objetivos generales lo siguiente:

- Mantener los niveles óptimos de confidencialidad, integridad y disponibilidad de la información del personal administrativo, docentes, estudiantes y entre otros usuarios.
- Concientizar al personal en seguridad de la información y buenas prácticas de seguridad con el fin de minimizar riesgos.
- Establecer controles físicos y lógicos en los activos informáticos para prevenir el ingreso, modificación, sustracción y/o divulgación de la información de personas no autorizadas.

V. ALCANCE E IMPORTANCIA

Este documento establece la Política de seguridad de la información únicamente de la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac en pro de ayudar a conseguir los objetivos institucionales.

Esta oficina que administrativamente depende del Rectorado, juega un papel importante en el desarrollo de los procesos académicos y administrativos, brindando servicios de análisis y desarrollo de software y sistemas, implementación de redes y conectividad y soporte tecnológico a toda la institución; por ello es imprescindible cumplir a cabalidad las políticas de seguridad de la información establecidas en el presente documento.

VI. GENERALIDADES

La Dirección de Tecnologías de Información de la Universidad Nacional Micaela bastidas de Apurímac reconoce la importancia de la información, así como el aseguramiento de la

Repositorio Institucional – UNAMBA - PERÚ

confidencialidad, disponibilidad e integridad de las mismas. Por lo que se establece mecanismos para su protección y disminuir las vulnerabilidades y protegerlas de las amenazas a las que se encuentran expuestos.

VII. POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN

La Dirección de Tecnologías de Información (DTI) de la Universidad Nacional Micaela Bastidas de Apurímac considera a la información como un activo de vital importancia así como el aseguramiento de la confidencialidad, disponibilidad e integridad de la información para realizar con normalidad sus actividades institucionales. Por tanto todos los directivos y funcionarios se comprometerán a mantener la información lo más segura posible. Se prohíbe la reproducción total o parcial de los documentos clasificados como confidenciales, sin la debida autorización o consentimiento del ente competente, así como el deterioro adrede de los dispositivos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo institucional.

Se establecerán políticas y lineamientos de seguridad que fuercen a mantener la información de estudiantes, docentes y administrativos en un ambiente seguro.

VIII. RESPONSABILIDAD

Cada persona administrativa de la Dirección de Tecnologías de Información velará por la seguridad de los activos informáticos que están a su disposición, así como se comprometerá a seguir los lineamientos estipulados en este documento de una manera satisfactoria y de acuerdo a las reglamentaciones contractuales.

El no actuar con responsabilidad frente a la Política de la Seguridad de la Información, será sancionado de acuerdo al código ético de la Universidad.

IX. SANCIONES

La violación de un control de seguridad o de la presente política justifica la aplicación de sanciones disciplinarias de acuerdo al reglamento interno de trabajo, las cuales serán

Repositorio Institucional – UNAMBA - PERÚ

aplicadas teniendo en consideración lo siguiente: naturaleza y gravedad de la falta, reincidencia y circunstancias en que se cometió la falta.

De acuerdo a la gravedad de falta cometida podrá aplicar cualquiera de las siguientes sanciones:

- Amonestación verbal
- Amonestación por escrito
- Suspensión de labores
- Despido

La amonestación verbal se les impondrá a los trabajadores que comentan faltas por primera vez y que sean faltas leves.

La amonestación por escrito se les impondrá a los trabajadores que sean reincidentes en faltas leves o si realizan faltas que se consideren más que una amonestación verbal.

La suspensión de labores se impondrá a los trabajadores que hayan sido amonestados de manera reiterativa tanto verbal como escrita o faltas que no constituyan despido.

Las sanciones no necesariamente se impondrán de forma progresiva. La gravedad de la falta determinara la sanción a imponerse.

Repositorio Institucional – UNAMBA - PERÚ

Anexo 12 – Políticas de seguridad de información

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

Apurímac – 2019

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVOS

Establecer normas y procedimientos para el uso adecuado de los equipos de cómputo y servicios informáticos para mantener y preservar la integridad, disponibilidad, seguridad y confiabilidad de la información en la Universidad nacional Micaela Bastidas de Apurímac.

II. FINALIDAD

El presente documento, tiene como finalidad proporcionar conceptos básicos y normas para el uso y cuidado de los equipos de cómputo y de los servicios informáticos, a fin de garantizar una adecuada calidad de servicio, y a su vez lograr y mantener los estándares de seguridad en la Red Universitaria.

III. BASE LEGAL

- Ley N° 30220- Ley universitaria
- Reglamento de organización y funciones (ROF) 2018
- Resolución Ministerial N° 004-2016-PCM "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición"
- Resolución Ministerial Nº 224-2004-PCM "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 1ª Edición."

IV. ALCANCE

El alcance de la directiva incluye a todo el personal docente y administrativo nombrados o por contratación de administración de servicios (CAS), que brindan servicios en las diferentes dependencias administrativas y académicas de la Universidad Nacional Micaela Bastidas de Apurímac (UNAMBA) tanto en la sede central como en las subsedes, quienes hacen uso de los diversos equipos y servicios informáticos.

a) Rectorado.
b) Vicerrectorado Académico.
c) Vicerrectorado de Investigación.

Repositorio Institucional – UNAMBA - PERÚ

d) Dirección General de Administración.
e) Facultades, Decanaturas, Escuelas Profesionales, Departamentos Académicos, Subsedes.
f) Direcciones, Oficinas, Unidades.
g) Escuela de Postgrado
h) Centro Pre Universitario.
i) Centro de Idiomas
j) Centro de Informática e Internet.
k) Docentes, estudiantes y personal administrativo.

V. DISPOSICIONES GENERALES

1. Todos los equipos y servicios informáticos que son asignados por la entidad deben de ser cuidados y utilizados de manera correcta.

VI. DISPOSICIONES ESPECIFICAS

La Universidad Nacional Micaela Bastidas de Apurímac y la Dirección de Tecnologías de Información, consideran necesario que todo el personal que utilice los equipos y las herramientas de comunicación (Internet, Correo Electrónico, Transferencia de Archivos, comunicaciones, etc.), esté consciente de los compromisos y normas que rigen la utilización de estos servicios.

Estos lineamientos tienen como objeto normar el uso de equipos y la prestación de servicios informáticos a los usuarios de la UNAMBA.

El uso de la red y recursos informáticos de la UNAMBA, está disponible para fortalecer el flujo de información interna y externa, apoyando las diferentes tareas encomendadas para el mejoramiento de dichas labores.

El uso de la red Internet no es un derecho, es un privilegio que puede ser revocado temporal o permanentemente como respuesta a una conducta abusiva o bien porque las responsabilidades de un funcionario no lo justifican.

Los servicios de acceso a Internet se proveen para facilitar el trabajo dentro de la Institución. Los usos para otros propósitos no son aceptables, el uso de los recursos deberá tomar en cuenta que se guarden las medidas de seguridad que garanticen la

Repositorio Institucional – UNAMBA - PERÚ

integridad y seguridad necesaria, con el fin de llevar a cabo un trabajo eficiente y productivo.

6.1 DE LA OFICINA DE TECNOLOGIA INFORMÁTICA

6.1.1 DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

La Dirección de Tecnologías de Información es la encargada de administrar las tecnologías y la información de la universidad, a través de la web e intranet, analiza y desarrolla software y sistemas de información e implementa redes y conectividad, orientados a dar soporte a la tecno estructura de la UNAMBA, presta además servicio de soporte técnico a los usuarios.

6.2 DE LOS USUARIOS

6.2.1 USUARIO DE LOS SERVICIOS

Se consideran usuarios a todos aquellas personas que conforman la Comunidad Universitaria así: personal administrativo y/o docente, dependencias académicas, dependencias administrativas.

6.3 USO DE EQUIPOS INFORMÁTICOS

Los usuarios que hagan uso de las computadoras institucionales, impresoras y otros equipos y/o accesorios ubicados en las distintas oficinas deben cumplir estrictamente con las siguientes disposiciones.

6.3.1 Antes de insertar un dispositivo de almacenamiento externo (USB, disco duro u otros) a una PC, deberá revisarse a través del antivirus a fin de evitar contagio de virus y su propagación en la red.

6.3.2 Los equipos informáticos (computadoras, impresoras, proyectores multimedia y demás accesorios) serán utilizados exclusivamente para trabajos de fines institucionales, quedando por tanto prohibido su uso para fines particulares o de terceros.

6.3.3 El usuario está obligado y bajo responsabilidad, del jefe/director de oficina, dar custodia a todos los equipos informáticos asignados.

6.3.4 El usuario de cada equipo informático es responsable del correcto encendido y apagado de los mismos para evitar deterioros.

Repositorio Institucional – UNAMBA - PERÚ

6.3.5 Ningún usuario podrá desarmar, cambiar accesorios, cambiar la configuración de los equipos informáticos ya que es responsabilidad de la Dirección de Tecnologías de Información, salvo autorización expresa de dicha dependencia.

6.3.6 Las computadoras portátiles institucionales y proyectores multimedia por ningún motivo deben sacarse fuera de la institución, salvo cumplir con funciones de interés institucional para lo cual debe contar con el permiso respectivo firmado por la jefatura de la Unidad de control patrimonial y el jefe responsable de la oficina, dirección o unidad.

6.3.7 Queda prohibido para los usuarios de los centros o laboratorios de cómputo y equipos de cómputo de las oficinas introducir cualquier tipo de alimentos, bebidas o fumar en el interior del mismo.

6.3.8 Antes de salir de refrigerio o retirarse temporalmente de su área de trabajo el usuario debe realizar lo siguiente:

a) Bloquear el equipo para impedir el acceso a otros usuarios.

b) Poner el equipo en estado “hibernar” o “suspender” a fin de cumplir con los lineamientos de austeridad y racionalidad y protección del medio ambiente.

6.4 USO Y ADMINISTRACIÓN DE SOFTWARE

6.4.1 Está prohibida la copia de software con licencia adquirida por la UNAMBA, con excepción de las copias realizadas con fines de seguridad.

6.4.2 El software básico instalado en los equipos de cómputo de la UNAMBA es el siguiente:

- Sistema operativo Microsoft Windows
- Suite ofimática basada en Microsoft
- Navegador web Microsoft Internet explorer y/o Mozilla Firefox y/o Google Chrome.
- Antivirus
- Visualizador de PDF
- Software para compresión de archivos.

6.4.3 La instalación y desinstalación es facultad exclusiva de la Dirección de Tecnologías de Información, si el usuario del equipo instala un programa sin

Repositorio Institucional – UNAMBA - PERÚ

previa autorización, cualquier consecuencia por dicha instalación será responsabilidad del mismo.

6.5 USO DE REDES Y TELEFONÍA

6.5.1 Todo trabajo de cableado estructurado será realizado por la Dirección de Tecnologías de Información a través de su unidad de Redes y comunicaciones y la unidad de Soporte Técnico y mantenimiento.

6.5.2 Ningún usuario debe hacer cambios en las direcciones IP, nombre de grupos o nombres de las computadoras y/o equipos asignados a su cargo sin la autorización del personal de la Dirección de Tecnologías de Información.

6.5.3 Los usuarios tienen acceso a los recursos que les ofrece la red LAN, tales como compartir impresoras, archivos, almacenar archivos en los servidores principales, hacer uso del correo electrónico, así como acceder a intranet e internet.

6.5.4 Ningún usuario personal docente y administrativo nombrados o por contratación de administración de servicios (CAS) podrá trasladar, adicionar o modificar los puntos de red en la red de datos de la UNAMBA que es responsabilidad de la Dirección de Tecnologías de Información para realizar el cambio respectivo.

6.6 USO DEL INTERNET

Todo usuario del servicio de internet WIFI y cableado dentro del campus universitario debe respetar las siguientes disposiciones.

6.6.1 El acceso a internet será exclusivamente para fines académicos, de investigación y asuntos laborales.

6.6.2 No está permitido los accesos a las redes sociales de interés particular, por lo cual se realizará inspecciones periódicas, para comprobar el no acceso a las mismas.

6.6.3 Queda prohibido usar software para ver videos en línea, juegos en tiempo real, radio, mensajería instantánea o de cualquier otro tipo que sature la red.

6.6.4 No está permitido la descarga de programas, videos y músicas o de cualquier otro tipo que sature la red.

6.6.5 Está prohibido el uso de internet para fines particulares o a favor de terceros.

Repositorio Institucional – UNAMBA - PERÚ

6.6.6 Se prohíbe acceder a servicios locales o remotos a los que no se tenga autorización.

6.6.7 El personal docente y administrativo nombrado o por contratación de administración de servicios (CAS), será asignado con un correo institucional y su respectiva contraseña, el que dispondrá para usos institucionales de manera obligatoria y personal.

6.7 COPIAS DE SEGURIDAD

6.7.1 El usuario será responsable de la información que se encuentre en los equipos informáticos como: CPU, laptop, asignados a su persona para el desarrollo de sus actividades, por lo que deberá realizar periódicamente copia de seguridad de la información más importante o crítica en medios externos para salvaguardar la información en caso de robo o pérdida de información por infección de virus u otros.

6.8 USO DE LABORATORIOS O CENTROS DE CÓMPUTO

Los equipos informáticos y los distintos accesorios de los laboratorios o centros de cómputo de la UNAMBA, están destinados como soporte tecnológico para la enseñanza y la investigación. Los jefes o encargados de los laboratorios o centros de cómputo tienen por custodia y bajo la responsabilidad todos los equipos informáticos instalados en los laboratorios o centros de cómputo a su cargo.

Es responsabilidad del jefe o responsable de laboratorios o centros de cómputo, administrar adecuadamente los equipos informáticos, así como hacer cumplir las normas establecidas en la presente directiva bajo responsabilidad.

Podrán hacer uso de los centros o laboratorios de cómputo todos los alumnos matriculados en su respectiva escuela académica profesional o programa académico y dentro del horario correspondiente.

Los usuarios de los laboratorios o centros de cómputo de la UNAMBA, deben cumplir estrictamente las siguientes normas de uso y conducta:

6.8.1 No instalar o desinstalar aplicaciones (software) sin autorización del jefe de laboratorio.

6.8.2 No deteriorar los equipos y accesorios informáticos.

6.8.3 No modificar la configuración de los equipos.

Repositorio Institucional – UNAMBA - PERÚ

6.8.4 No provocar la infección de los equipos con virus informáticos.

6.8.5 No comer, beber o fumar dentro del laboratorio.

6.8.6 No realizar desconexiones o reubicaciones de los equipos instalados.

6.8.7 No cambiar los accesorios de los equipos.

6.8.8 No provocar desorden y/o molestia a los demás usuarios.

6.8.9 Durante el desarrollo de clases, no se podrá hablar en voz alta.

6.8.10 No utilizar los equipos para fines comerciales ni de entretenimiento.

6.8.11 No apagar o encender indebidamente los equipos.

6.8.12 El acceso al será según orden de llegada, ningún usuario tendrá el privilegio de reservar los equipos.

6.8.13 No se puede congestionar los sistemas ni las comunicaciones de manera intencional.

6.8.14 El usuario que deteriore intencionalmente los equipos o accesorios deberá reponer obligatoriamente por otro de características técnicas iguales o superiores.

6.9 SANCIONES

6.9.1 Es causal para perder el derecho de servicio, el incurrir en cualquier acto que infrinja esta Directiva, los cuales consisten en: amonestación verbal, suspensión y cancelación del servicio, dependiendo de la gravedad de la falta. Sin perjuicio del proceso administrativo si la falta genera daños en el adecuado funcionamiento de la Red Universitaria o en el deterioro o uso indebido de los equipos informáticos.

VII. RESPONSABILIDAD

7.1 La dirección de Tecnologías de Información es el responsable funcional de velar por el buen uso de los equipos y servicios informáticos.

7.2 Todo usuario deberá acatar las disposiciones vigentes del presente reglamento, los aspectos no contemplados en el presente reglamento, serán resueltos por la Dirección de Tecnologías de Información y en última instancia Consejo Universitario.

7.3 Usuario que fuera sorprendido malogrando los equipos de cómputo deberá reponer o pagar de acuerdo a la magnitud del daño ocasionado.

Repositorio Institucional – UNAMBA - PERÚ

Anexo 13 – Metodología de evaluación y tratamiento de riesgo

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Código	DTI-003
Versión	01
Fecha de la versión	23/01/2019
Creado por	Huallpa Laguna Jessica Noralina
Aprobado por	Ing. Evelyn Yeni Medrano Kari
Nivel de confidencialidad	Baja

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Dirección de Tecnologías de Información y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos que se utilizan dentro de la institución o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnologías de Información que participan en la evaluación y tratamiento de riesgos

II. DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los siguientes:

- Norma ISO/IEC 27001, capítulos 6.1.2, 6.1.3, 8.2, y 8.3
- Políticas de seguridad de la información
- Lista de documentos regulatorios, legales y contractuales
- Declaración de aplicabilidad

III. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

3.1. METODOLOGÍA MAGERIT

El análisis de riesgos realizado en la DTI obedece a la metodología basada en MAGERIT, una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE (Consejo Superior de Administración Electrónica) que supone los beneficios evidentes de emplear las tecnologías de información, pero gestionando los riesgos inherentes a ella, donde actualmente está en su versión 3.

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad propuestas:

Repositorio Institucional – UNAMBA - PERÚ

DIMENSION DE SEGURIDAD	NOMENCLATURA	DEFINICION
Disponibilidad	D	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].

Para el proceso de Gestión de Riesgos, MAGERIT contempla 2 tareas: Análisis de Riesgos y Control de Riesgos. El Análisis de riesgos consiste en calificar los riesgos encontrados cuantificando sus consecuencias (análisis cuantitativo) o determinando su importancia relativa (análisis cualitativo), este proceso de análisis conlleva la identificación de los activos, sus amenazas y los controles de seguridad propuestos, así estimando el impacto y el riesgo al que están expuestos cada uno de los activos y su repercusión en el nivel de seguridad de la información en una organización. Por su parte, el Tratamiento de Riesgos consta de las actividades que se ejecutan para modificar la situación o nivel de riesgo.

Los pasos para realizar la gestión de riesgos según MAGERIT son los siguientes:

1. **Inventario de activos:** Los activos son aquellos componentes o funcionalidades de un sistema de información que son susceptibles a ser atacados deliberada o intencionalmente con consecuencias para una organización. Son también los elementos que una organización posee para el tratamiento de la información. MAGERIT clasifica los activos en los siguientes tipos:

Repositorio Institucional – UNAMBA - PERÚ

TIPO DE ACTIVO	NOMENCLATURA	DEFINICION
Activos esenciales	[Essential]	Son aquellos que son esenciales para la supervivencia de la organización y que su carencia o daño afectaría directamente su existencia. Generalmente desarrollan misiones críticas.
Arquitectura del sistema	[Arch]	Son aquellos que permiten estructurar el sistema, su arquitectura interna y sus relaciones con el exterior.
Datos/información	[D]	Es aquella información que le permite a una organización prestar sus servicios.
Claves criptográficas	[K]	Son aquellos que permiten cifrar la información. Incluye los algoritmos de encriptación.
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios.
Software/Aplicaciones informáticas	[SW]	Son aquellos que procesan los datos y permiten brindar información para la prestación de servicios.
Hardware/equipamiento	[HW]	Son los medios físicos donde se depositan los datos y prestan directa o indirectamente un servicio.
Redes de comunicaciones	[COM]	Son los medios de transporte por donde viajan los datos.
Soportes de información	[media]	Son los dispositivos físicos que permiten el almacenamiento temporal o permanente de la información.
Equipamiento Auxiliar	[AUX]	Son aquellos equipos que brindan soporte a los sistemas de información sin estar relacionado con los datos.
Instalaciones	[L]	Son los lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	[P]	Son las personas relacionadas con los sistemas de información

2. **Valoración de los Activos:** Los activos que generan valor son aquellos que se necesitan proteger, y cada activo tiene una importancia mayor o menor en la organización. MAGERIT establece dos tipos de valoraciones: Cualitativa que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización y la Cuantitativa que estima el costo del activo (incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.). Mientras que la Cualitativa permite establecer órdenes de magnitud (MA [Muy Alto], A [Alto], M [Medio], B [Bajo] y MB [Muy Bajo]) y no genera valores numéricos, la cuantitativa sí permite calcular el costo y/o valor monetario.

Repositorio Institucional – UNAMBA - PERÚ

valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Escalas estándar:

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Repositorio Institucional – UNAMBA - PERÚ

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Repositorio Institucional – UNAMBA - PERÚ

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Repositorio Institucional – UNAMBA - PERÚ

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

3. **Identificación y valoración de amenazas:** MAGERIT establece cinco Dimensiones de Seguridad (D [Disponibilidad], I [Integridad], C [Confidencialidad], A [Autenticidad] y T [Trazabilidad]) donde es necesario determinar los criterios de valoración en cada dimensión. Estos valores y/o criterios son similares a los establecidos en la tabla de Valoración cualitativa de los activos informáticos en MAGERIT.

   - **Identificación de Amenazas:** Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a una organización. MAGERIT emplea un catálogo de amenazas posibles sobre los activos de un sistema de información, los cuales están clasificados de la siguiente manera:

Repositorio Institucional – UNAMBA - PERÚ

TIPO DE AMENAZA	NOMENCLATURA	DEFINICION
Desastres Naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	[E]	Fallos no intencionales causados por las personas.
Ataques Intencionados	[A]	Fallos deliberados causados por las personas.

- **Valoración de Amenazas:** Para establecer la valoración de las amenazas es necesario determinarla frecuencia o probabilidad de ocurrencia. En MAGERIT, las frecuencias o probabilidades se muestran a continuación:

FRECUENCIA DE OCURRENCIA	NOMENCLATURA	VALOR	RANGO
MUY ALTO	MA	100	1 vez al día
ALTO	A	70	1 vez cada semana
MEDIO	M	50	1 vez cada 2 meses
BAJO	B	10	1 vez cada 6 meses
MUY BAJO	MB	5	1 vez al año

- **Impacto Potencial:** Se determina el nivel de daño o impacto que tendría un activo si se llegara a materializar una amenaza determinada en cada una de sus dimensiones de seguridad.

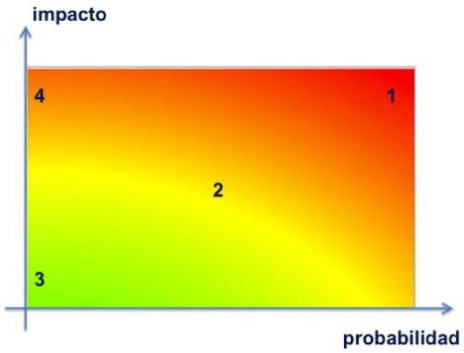
IMPACTO	NOMENCLATURA	DESCRIPCION
MUY ALTO	MA	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles.
ALTO	A	El daño tiene consecuencias muy graves para la organización.
MEDIO	M	El daño contiene consecuencias relevantes para la organización y su operación
BAJO	B	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la organización.
MUY BAJO	MB	El daño no contiene consecuencias relevantes para la organización

Repositorio Institucional – UNAMBA - PERÚ

- **Riesgo Potencial:** El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Frecuencia x Impacto.

El riesgo crece con el impacto y con la probabilidad como se muestra en la siguiente ilustración:



Donde las zonas identifican lo siguiente:

- **Zona 1:** Riesgos muy probables y de muy alto impacto (MA: Críticos).
- **Zona 2:** Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables pero de impacto bajo o muy bajo (M: Apreciables).
- **Zona 3:** Riesgos improbables y de bajo impacto (MB, B: Despreciables o Bajos).
- **Zona 4:** Riesgos improbables pero de muy alto impacto (A: Importantes).

A su vez, la relación de la probabilidad e impacto para determinar el riesgo de forma cualitativa se muestra en la siguiente tabla:

RIESGO		**FRECUENCIA**				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Repositorio Institucional – UNAMBA - PERÚ

4. **Controles de Seguridad (Salvaguardas):** Los Controles de Seguridad o Salvaguardas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, donde se deben establecer los controles para cada amenaza de cada activo. Las salvaguardas propuestas en MAGERIT se clasifican en los siguientes:

SALVAGUARDAS	NOMENCLATURA
Protecciones generales u horizontales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (software)	SW
Protección de los equipos (hardware)	HW
Protección de las comunicaciones	COM
Protección en puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Salvaguardas relativas al personal	PS
Salvaguardas de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E

3.2. Inventario y clasificación de activos informáticos

Un activo informático está representado por los objetos físicos, objetos abstractos e incluso el personal de trabajo y las instalaciones físicas. Dentro de los activos informáticos encontrados en la Dirección de Tecnologías de Información de la UNAMBA se encuentran los siguientes:

ACTIVO	DESCRIPCION
Copias de respaldo	Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.
Código fuente	Archivos de códigos fuentes de los diferentes Sistemas de Información propios desarrollados.
Página web	Páginas, portales, ambientes virtuales de aprendizaje, sitios y aplicativos que son disponibles para el acceso público.

Repositorio Institucional – UNAMBA - PERÚ

Software estándar	Software desarrollado por terceros y adaptado a la institución. Software que soporta los procesos administrativos.
Gestor de base de datos	Administran y gestionan las bases de datos que se utilizan para soportar todo el software académico, administrativo, educativo y demás que apoyan a los demás procesos institucionales.
ofimática	Software necesario para la realización de las actividades diarias, así como la producción de recursos.
Software de antivirus	Software para prevenir y eliminar el malware.
Sistema operativo	Software que administra los recursos de las computadoras de uso institucional
Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.
Computadora de escritorio de uso institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).
Switch	Administra las VLANS el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.
Punto de Acceso	Amplían la cobertura de la red por medio de conexiones inalámbricas.
Sistema de alimentación ininterrumpida	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.
Administrador de sistemas	Personal encargado de la administración de los sistemas informáticos así mismo dar soporte en cuanto a ello.
Administrador de comunicación	Personal encargado de administrar las redes y brindar soporte técnico en redes e internet

Estos activos se clasifican según el Tipo de Activo en la metodología MAGERIT de la siguiente manera:

[D]DATOS/INFORMACIÓN

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
D_CR	[backup]	Copias de respaldo	Archivos de copias de respaldo de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.	Jefe de DTI

[S]SERVICIO

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
S-CE	[email]	Correo electrónico	Correo electrónico institucional usado por el personal administrativo, docentes, etc.	Jefe de DTI
S_WWW	[www]	Página web	Páginas, portales, aula virtual de aprendizaje.	Jefe de DTI

Repositorio Institucional – UNAMBA - PERÚ

[SW]SOFTWARE

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
SW_EST	[std]	Software Estándar	Software desarrollado por terceros y adaptado a la institución. Software que soporta los procesos administrativos.	Jefe de DTI
SW_BDS	[dbms]	Gestores de base de datos	Es el que administra y gestiona la base de datos que se utilizan para soportar todo el software académico, administrativo, educativo y demás que apoyan a los demás procesos institucionales.	Jefe de DTI
SW_OFM	[office]	Ofimática	Software necesario para la realización de las actividades diarias, así como la producción de recursos.	Jefe de DTI
SW_AVR	[av]	Software de antivirus	Software para prevenir y eliminar virus, malware.	Jefe de DTI
SW_SO	[so]	Sistema operativo	Software que administra los recursos de las computadoras de uso institucional.	Jefe de DTI

[HW] HARDWARE

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
HW_HOS	[host]	Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.	Jefe de DTI
HW_PC	[pc]	Computadora de escritorio de uso institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	Jefe de DTI
HW_ROU	[router]	Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet)	Jefe de DTI
HW_SWH	[switch]	Switch	Dispositivo que resuelve problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.	Jefe de DTI
HW_AP	[wap]	Punto de Acceso	Amplían la cobertura de la red por medio de conexiones inalámbricas	Jefe de DTI
HW_PRT	[print]	Impresoras	Dispositivos para la impresión en papel.	Jefe de DTI

Repositorio Institucional – UNAMBA - PERÚ

[COM]COMUNICACIONES

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
COM_INT	[Internet]	Internet	Permite acceso a recursos de la web.	Jefe de DTI
COM_LAN	[lan]	Red de Área Local	Permite la interconexión de las computadoras institucionales así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.	Jefe de DTI
COM_WIFI	[wifi]	Conectividad inalámbrica	Permite la conectividad inalámbrica de las computadoras institucionales, así como ampliar la cobertura.	Jefe de DTI

[L]INSTALACIONES

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
L_SIT	[site]	Dirección de Tecnologías de Información	Estructura física que alberga a la Dirección de Tecnologías de Información	Jefe de DTI

[P]PERSONAL

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO	RESPONSABLE
P_ADM	[adm]	Administrador de sistemas	Persona encargada de administrar, gestionar, solucionar y ayudar en el correcto funcionamiento de los diferentes Sistemas de Información.	Jefe de Recursos humanos
P-SOP	[com]	Administrador de comunicación	Persona encargada de administrar y gestionar el tráfico de datos en la red interna, así como configurar los diferentes dispositivos de comunicaciones que garanticen un óptimo rendimiento para el acceso a servicios y Sistemas de Información.	Jefe de Recursos humanos
P_DBA	[dba]	Administrador de Base de datos	Persona que administra, configura y optimiza el rendimiento de las diferentes bases de datos que utilizan los Sistemas de Información para el soporte de los procesos institucionales.	Jefe de Recursos humanos

Repositorio Institucional – UNAMBA - PERÚ

3.3. VALORACIÓN DE LOS ACTIVOS DE ACUERDO A LAS DIMENSIONES DE SEGURIDAD

[D]DATOS/INFORMACIÓN

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
D_BCK	Copias de respaldo de los sistemas de información	3		2

CODIGO	DIMENSION DE SEGURIDAD	RAZON
D_BCK	[D]	3. adm: Probablemente impediría la operación efectiva de una parte de la Organización.
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización.

[S]SERVICIO

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
S-CE	Correo electrónico	3		
S_WWW	Página web	3		

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
S-CE	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
S_WWW	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización

[SW]SOFTWARE

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
SW_EST	Software Estándar	3		4
SW_BDS	Gestores de base de datos	7	7	7
SW_OFM	Ofimática	1		
SW_AVR	Software de antivirus			7
SW_SO	Sistema operativo	5	7	

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
SW_EST	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	4.pi1: Probablemente afecte a un grupo de individuos

Repositorio Institucional – UNAMBA - PERÚ

	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
SW_BDS	[D][I][A]	7.adm: Probablemente impediría la operación efectiva de la Organización
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
SW_OFM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
SW_A VR	[C]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
SW_SO	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[HW] HARDWARE

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
HW_HOS	Servidores	5		7
HW_PC	Computadora de escritorio de uso institucional	1		
HW_ROU	Router	5		
HW_SWH	Switch	5		
HW_AP	Punto de Acceso	1		
HW_PRT	Impresoras	1		

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
HW_HOS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C][A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_PC	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
HW_ROU	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_SWH	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_AP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
HW_PRT	[D]	1.pi1: Pudiera causar molestias a un individuo

[COM]COMUNICACIONES

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
COM_INT	Internet	3		
COM_LAN	Red de Área Local	5		
COM_WIFI	Conectividad inalámbrica	1		

Repositorio Institucional – UNAMBA - PERÚ

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
COM_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
COM_LAN	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
COM_WIFI	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización

[L]INSTALACIONES

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
L_SIT	Dirección de Tecnologías de información	7		

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
L_SIT	[D]	7.adm: Probablemente impediría la operación efectiva de la Organización

[P]PERSONAL

CODIGO	DESCRIPCION	DIMENSION DE SEGURIDAD		
		[D]	[I]	[C]
P_ADM	Administrador de sistemas	5		
P-COM	Administrador de comunicación	5		
P_DBA	Administrador de base de datos	5		

CODIGO	DIMENSION DE SEGURIDAD	DESCRIPCION
P_ADM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P-COM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DBA	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización

Repositorio Institucional – UNAMBA - PERÚ

3.4. VALORACIÓN DE LOS ACTIVOS DE ACUERDO AL IMPACTO

[D]DATOS/INFORMACIÓN

CODIGO	DESCRIPCION	IMPACTO	RAZON
D_BCK	Copias de respaldo de los sistemas de información	MA	Los archivos de copias de seguridad son determinantes para la recuperación de desastres.

[S]SERVICIO

CODIGO	DESCRIPCION	IMPACTO	RAZON
S-CE	Correo electrónico	M	El correo electrónico se utiliza para la comunicación interna de los funcionarios, docentes y estudiantes.
S_WWW	Página web	A	Acceso a la página web institucional y otros sitos que ofrecen servicios al personal administrativo, docentes, estudiantes y público en general

[SW]SOFTWARE

CODIGO	DESCRIPCION	IMPACTO	RAZON
SW_EST	Software Estándar	MA	Utilizados para el normal desarrollo de los procesos institucionales. Dentro de ellos se encuentran el SIGA, SIAF.
SW_BDS	Gestores de base de datos	MA	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones. Dentro de ellos se encuentran SQL Server 2008 R2, MySQL 5.5.
SW_OFM	Ofimática	B	Utilizado para la ejecución de tareas
SW_A VR	Software de antivirus	M	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
SW_SO	Sistema operativo	M	Administra los recursos de software y hardware de las diferentes computadoras de uso institucional.

[HW] HARDWARE

CODIGO	DESCRIPCION	IMPACTO	RAZON
HW_HOS	Servidores	MA	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos institucionales. Dentro de ellos se encuentran los Servidores de

Repositorio Institucional – UNAMBA - PERÚ

			Aplicaciones, DNS, Bases de Datos y Web.
HW_PC	Computadora de escritorio de uso institucional	B	Dispositivos para la ejecución de tareas.
HW_ROU	Router	A	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
HW_SWH	Switch	A	Esencial para direccionar el tráfico de datos interno, administración de VLAN y segmentar el ancho de banda con el fin de optimizarla. Dentro de ellas se encuentran las VLAN administrativa, docentes y estudiantes.
HW_AP	Punto de Acceso	B	Dispositivos que amplían la cobertura de la red para dar acceso inalámbrico.
HW_PRT	Impresoras	MB	Dispositivo para realizar impresiones en papel.

[COM]COMUNICACIONES

CODIGO	DESCRIPCION	IMPACTO	RAZON
COM_INT	Internet	MA	Esencial para tener acceso a redes externas.
COM_LAN	Red de Área Local	MA	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos institucionales. Incluye todo el cableado estructurado.
COM_WIFI	Conectividad inalámbrica	B	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos.

[L]INSTALACIONES

CODIGO	DESCRIPCION	IMPACTO	RAZON
L_SIT	Dirección de Tecnologías de Información	MA	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos institucionales.

Repositorio Institucional – UNAMBA - PERÚ

[P]PERSONAL

CODIGO	DESCRIPCION	IMPACTO	RAZON
P_ADM	Administrador de sistemas	A	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos institucionales y sus servicios.
P-COM	Administrador de comunicación	MA	Personas encargadas de administrar, configurar y operar las redes de comunicación de datos que dan soporte al normal funcionamiento de los servicios internos.
P_DBA	Administrador de base de datos	MA	Persona encargada de administrar, configurar y optimizar el rendimiento de las bases de datos que contienen los datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros.

3.5. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

[D]DATOS/INFORMACIÓN

CODIGO	FRECUENCIA
Copias de respaldo de los sistemas de información	
5.3.1. [E.1] Errores de los usuarios	70
5.3.10. [E.15] Alteración accidental de la información	5
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.3.2. [E.2] Errores del administrador	5
5.3.9. [E.14] Escapes de información	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.9. [A.11] Acceso no autorizado	5

Repositorio Institucional – UNAMBA - PERÚ

[S]SERVICIO

CODIGO	FRECUENCIA
Correo electrónico	
5.3.1. [E.1] Errores de los usuarios	50
5.3.10. [E.15] Alteración accidental de la información	10
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50
5.3.9. [E.14] Escapes de información	50
5.4.11. [A.13] Repudio	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	10
.4.18. [A.24] Denegación de servicio	5
5.4.3. [A.5] Suplantación de la identidad del usuario	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	10
Página web	
5.3.10. [E.15] Alteración accidental de la información	10
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50
5.4.14. [A.18] Destrucción de información	5
5.4.18. [A.24] Denegación de servicio	5

[SW]SOFTWARE

CODIGO	FRECUENCIA
Software Estándar	
5.2.6. [I.5] Avería de origen físico o lógico	5
5.3.1. [E.1] Errores de los usuarios	50
5.3.10. [E.15] Alteración accidental de la información	5
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50
5.3.2. [E.2] Errores del administrador	10
5.3.6. [E.8] Difusión de software dañino	10

Repositorio Institucional – UNAMBA - PERÚ

5.3.9. [E.14] Escapes de información	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.16. [A.22] Manipulación de programas	5
5.4.3. [A.5] Suplantación de la identidad del usuario	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.6. [A.8] Difusión de software dañino	10
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	5
Gestores de base de datos	
5.2.6. [I.5] Avería de origen físico o lógico	5
5.3.1. [E.1] Errores de los usuarios	10
5.3.10. [E.15] Alteración accidental de la información	5
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10
5.3.2. [E.2] Errores del administrador	10
5.3.6. [E.8] Difusión de software dañino	5
5.3.9. [E.14] Escapes de información	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.16. [A.22] Manipulación de programas	5
5.4.3. [A.5] Suplantación de la identidad del usuario	10
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.6. [A.8] Difusión de software dañino	5
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	5
Ofimática	
5.2.6. [I.5] Avería de origen físico o lógico	10
5.3.1. [E.1] Errores de los usuarios	50

Repositorio Institucional – UNAMBA - PERÚ

5.3.13. [E.20] Vulnerabilidades de los programas (software)	50
5.3.6. [E.8] Difusión de software dañino	10
5.4.5. [A.7] Uso no previsto	50
5.4.6. [A.8] Difusión de software dañino	5
5.4.9. [A.11] Acceso no autorizado	5
Software de antivirus	
5.2.6. [I.5] Avería de origen físico o lógico	5
5.3.1. [E.1] Errores de los usuarios	50
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10
5.3.6. [E.8] Difusión de software dañino	10
5.4.5. [A.7] Uso no previsto	5
5.4.6. [A.8] Difusión de software dañino	5
5.4.9. [A.11] Acceso no autorizado	5
Sistema operativo	
5.2.6. [I.5] Avería de origen físico o lógico	5
5.3.1. [E.1] Errores de los usuarios	10
5.3.10. [E.15] Alteración accidental de la información	10
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5
5.3.2. [E.2] Errores del administrador	10
5.3.6. [E.8] Difusión de software dañino	10
5.3.9. [E.14] Escapes de información	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.16. [A.22] Manipulación de programas	5
5.4.3. [A.5] Suplantación de la identidad del usuario	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.6. [A.8] Difusión de software dañino	5
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	5

Repositorio Institucional – UNAMBA - PERÚ

[HW] HARDWARE

CODIGO	FRECUENCIA
Servidores	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.3.2. [E.2] Errores del administrador	50
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
Computadora de escritorio de uso institucional	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.3.2. [E.2] Errores del administrador	50
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
5.4.4. [A.6] Abuso de privilegios de acceso	5

Repositorio Institucional – UNAMBA - PERÚ

5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
Router	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.3.2. [E.2] Errores del administrador	50
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
Switch	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.3.2. [E.2] Errores del administrador	50
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
5.4.4. [A.6] Abuso de privilegios de acceso	5

Repositorio Institucional – UNAMBA - PERÚ

5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
Punto de Acceso	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5
5.3.17. [E.25] Pérdida de equipos	5
5.3.2. [E.2] Errores del administrador	50
5.4.17. [A.23] Manipulación de los equipos	5
5.4.18. [A.24] Denegación de servicio	5
5.4.19. [A.25] Robo	5
5.4.4. [A.6] Abuso de privilegios de acceso	5
5.4.5. [A.7] Uso no previsto	5
5.4.9. [A.11] Acceso no autorizado	5
Impresoras	
5.2.1. [I.1] Fuego	5
5.2.2. [I.2] Daños por agua	5
5.2.6. [I.5] Avería de origen físico o lógico	5
5.2.7. [I.6] Corte del suministro eléctrico	50
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10
5.3.17. [E.25] Pérdida de equipos	5
5.4.19. [A.25] Robo	5

[COM]COMUNICACIONES

CODIGO	**FRECUENCIA**
Internet	
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70

Repositorio Institucional – UNAMBA - PERÚ

5.3.2. [E.2] Errores del administrador	5
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	10
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	10
Red de Área local	
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70
5.3.2. [E.2] Errores del administrador	10
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	70
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	50
Conectividad inalámbrica	
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70
5.3.2. [E.2] Errores del administrador	10
5.3.7. [E.9] Errores de [re-]encaminamiento	5
5.4.10. [A.12] Análisis de tráfico	5
5.4.12. [A.14] Interceptación de información (escucha)	5
5.4.18. [A.24] Denegación de servicio	70
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5
5.4.8. [A.10] Alteración de secuencia	5
5.4.9. [A.11] Acceso no autorizado	50

Repositorio Institucional – UNAMBA - PERÚ

[L]INSTALACIONES

CODIGO	FRECUENCIA
Dirección de Tecnologías de Información	
5.1.3. [N.*] Desastres Naturales	5
5.2.12. [I.11] Emanaciones electromagnéticas	5
5.3.10. [E.15] Alteración accidental de la información	5
5.3.11. [E.18] Destrucción de información	5
5.3.12. [E.19] Fugas de información	5
5.4.13. [A.15] Modificación deliberada de la información	5
5.4.14. [A.18] Destrucción de información	5
5.4.15. [A.19] Divulgación de información	5
5.4.20. [A.26] Ataque destructivo	5
5.4.9. [A.11] Acceso no autorizado	5

[P]PERSONAL

CODIGO	FRECUENCIA
Administrador de Bases de Datos	
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.3.5. [E.7] Deficiencias en la organización	5
5.4.22. [A.28] Indisponibilidad del personal	5
Administrador de comunicaciones	
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.3.5. [E.7] Deficiencias en la organización	5
5.4.22. [A.28] Indisponibilidad del personal	5
Administrador de Sistemas	
5.3.12. [E.19] Fugas de información	5
5.3.18. [E.28] Indisponibilidad del personal	10
5.3.5. [E.7] Deficiencias en la organización	5
5.4.22. [A.28] Indisponibilidad del personal	5

Repositorio Institucional – UNAMBA - PERÚ

3.1. RIESGO POTENCIAL

Se determina el nivel de riesgo potencial de cada uno de los activos en una valoración cualitativa de acuerdo a las zonas de riesgo que propone MAGERIT. El riesgo es calculado en base al impacto que tiene cada activo y según el tipo de amenaza general (Naturales, Industriales, Errores No Intencionados, Ataques Intencionados); es decir, no se calcula en cada dimensión de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad). Sólo se toma en cuenta que ocurra cualquier amenaza dentro de su respectiva categoría y se escoge el peor de los casos.

[D]DATOS/INFORMACIÓN

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
D_CR	Copias de respaldo	MA	MB	E*, A*	R_D_CR	A

[S]SERVICIO

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
S-CE	Correo electrónico	M	M	E*, A*	R_ S-CE	M
S_WWW	Página web	A	M	E*, A*	R_ S_WWW	A

[SW]SOFTWARE

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
SW_EST	Software Estándar	MA	M	I*, E*, A*	R_ SW_EST	MA
SW_BDS	Gestores de base de datos	MA	B	I*, E*, A*	R_ SW_BDS	MA
SW_OFM	Ofimática	B	M	I*, E*, A*	R_ SW_OFM	B
SW_AVR	Software de antivirus	M	M	I*, E*, A*	R_ SW_AVR	M
SW_SO	Sistema operativo	M	B	I*, E*, A*	R_ SW_SO	M

Repositorio Institucional – UNAMBA - PERÚ

[HW] HARDWARE

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
HW_HOS	Servidores	MA	M	I*, E*, A*	R_ HW_HOS	MA
HW_PC	Computador de escritorio de uso institucional	B	M	I*, E*, A*	R_ HW_PC	B
HW_ROU	Router	A	M	I*, E*, A*	R_ HW_ROU	A
HW_SWH	Switch	A	M	I*, E*, A*	R_ HW_SWH	A
HW_AP	Punto de Acceso	B	M	I*, E*, A*	R_ HW_AP	B
HW_PRT	Impresoras	MB	M	I*, E*, A*	R_ HW_PRT	MB

[COM]COMUNICACIONES

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
COM_INT	Internet	MA	A	E*, A*	R_ COM_INT	MA
COM_LAN	Red de Área Local	MA	A	E*, A*	R_ COM_LAN	MA
COM_WIFI	Conectividad inalámbrica	B	A	E*, A*	R_ COM_WIFI	M

[L]INSTALACIONES

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
L_SIT	Dirección de Tecnologías de Información	MA	MB	N*, I*, E*, A*	R_ L_SIT	A

[P]PERSONAL

CODIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO ID	RIESGO
P_ADM	Administrador de sistemas	A	B	E*, A*	R_ P_ADM	A
P-COM	Administrador de comunicaci	MA	B	E*, A*	R_ P_COM	MA
P_DBA	Administrador de Base de datos	MA	B	E*, A*	R_ P_DBA	MA

Repositorio Institucional – UNAMBA - PERÚ

Se clasifican los riesgos de acuerdo a las zonas establecidas en MAGERIT de la siguiente manera:

RIESGO		**PROBABILIDAD**				
		MB	B	M	A	MA
IMPACTO	MA	R_D_CR, R_L_SIT	R_SW_DBS, R_P_COM, R_P_DBA	R_SW_EST, R_HW_HOS,	R_COM_LAN, R_COM_INT	
	A		R_P_ADM	R_S_WWW, R_HW_ROU, R_HW_SWH,		
	M		R_SW_SO,	R_SW_AVR , R_S_CE		
	B			R_HW_PC, R_SW_OFM, R_HW_AP	R_COM_WIFI	
	MB			R_HW_PRT		

Repositorio Institucional – UNAMBA - PERÚ

Anexo 14 – Declaración de aplicabilidad

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

DECLARACIÓN DE APLICABILIDAD

Código	DTI-004
Versión	01
Fecha de la versión	23/01/2019
Creado por	Huallpa Laguna Jessica Noralina
Aprobado por	Ing. Evelyn Yeni Medrano Kari
Nivel de confidencialidad	Baja

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir qué controles son adecuados para implementar en la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos empleados de Dirección de Tecnologías de Información – UNAMBA así mismo colaboradores que cumplen una función dentro del SGSI.

II. DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los siguientes:

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de Seguridad de la Información
- Metodología de evaluación y tratamiento de riesgos

III. APLICABILIDAD DE LOS CONTROLES

Son aplicables los siguientes controles del Anexo A de la norma ISO 27001:

Repositorio Institucional – UNAMBA - PERÚ

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.5	Políticas de seguridad de la información		
A.5.1	Dirección de la gerencia para la seguridad de la información		
A.5.1.1	Políticas para seguridad de la información	SI	Se redactan y documentan las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los empleados de DTI y administrativos en general.
A.5.1.2	Revisión de políticas para seguridad de la información	SI	Las políticas de seguridad de la información se revisan y evalúan periódicamente y/o cuando sea necesario por la persona designada a la política.
ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	SI	Los roles y responsabilidades de la seguridad de la información están definidas.
A.6.1.2	Segregación de deberes	SI	El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con autoridades	SI	El Jefe de Seguridad mantiene los contactos actualizados para incidentes de seguridad.
A.6.1.4	Contacto con grupos de interés especial	SI	El Jefe de Seguridad mantiene contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.
A.6.1.5	Seguridad de la información en gestión de proyectos	SI	El Jefe de Seguridad es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.
A.6.2	Dispositivos móviles y tele-trabajo		
A.6.2.1	Política sobre dispositivos móviles	NO	

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		
A.8.1.1	Inventario de activos	SI	El Jefe de Seguridad realiza el inventario de activos y se documentan con su clasificación y responsable.
A.8.1.2	Propiedad de los activos	SI	Los activos inventariados tienen asignados los funcionarios responsables.

Repositorio Institucional – UNAMBA - PERÚ

A.8.1.3	Uso aceptable de los activos	SI	Los funcionarios se comprometen a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Retorno de activos	SI	Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	SI	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos
A.8.2.2	Etiquetado de la información	SI	Cada uno de los activos inventariados está etiquetados con la clasificación de la información asociada.
A.8.2.3	Manejo de activos	SI	El Jefe de Seguridad junto a los funcionarios realizan y documentan los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		
A.9.1.1	Política de control de acceso	SI	La política de control de acceso está documentada en las Políticas de la Seguridad de Información.
A.9.1.2	Acceso a redes y a servicios en red	SI	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación de registro de usuarios	NO	
A.9.2.2	Suministro de acceso de usuario	NO	
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	A los funcionarios se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los funcionarios son agrupados bajo Perfiles de Usuario.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
A.9.2.5	Revisión de los derechos de acceso de usuarios	SI	El Jefe de Seguridad junto a los funcionarios encargados verifican que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación

Repositorio Institucional – UNAMBA - PERÚ

			se realiza de forma periódica y cualquier anormalidad es debidamente documentada.
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	El Jefe de Seguridad verifica y elimina los permisos asignados al personal que sea retirado.
A.9.3	**Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta	SI	La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	SI	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del empleado en la organización.
A.9.4.2	Procedimiento de ingreso seguro	SI	Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro. Se emplean mecanismos seguros de cifrado de información.
A.9.4.3	Sistema de gestión de contraseñas	NO	
A.9.4.4	Uso de programas utilitarios privilegiados	SI	El Jefe de Seguridad verifica que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados. Se realiza una verificación de forma aleatoria.
A.9.4.5	Control de acceso a códigos fuente de programas	SI	El Jefe de Seguridad verifica que los códigos fuentes de los programas permanecen de forma confidencial.

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.11	Seguridad física y ambiental		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad	SI	El perímetro físico controlado por personal de seguridad y cámaras de vigilancia en la infraestructura que contiene el hardware de las operaciones críticas.
A.11.1.2	Controles de ingreso físico	SI	El acceso físico a la infraestructura que contiene el hardware de las operaciones críticas permite el acceso a sólo el personal autorizado y se encuentran vigilados por cámaras de vigilancia en la parte externa.
A.11.1.3	Asegurar oficinas, áreas e instalaciones	NO	
A.11.1.4	Protección contra amenazas externas y ambientales	NO	
A.11.1.5	Trabajo en áreas seguras	NO	

Repositorio Institucional – UNAMBA - PERÚ

A.11.1.6	Áreas de despacho y carga	NO	
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los equipos	SI	Los equipos están ubicados en un lugar donde se encuentran protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. y existen políticas de seguridad de la información documentadas para su uso.
A.11.2.2	Servicios de suministro	NO	
A.11.2.3	Seguridad del cableado	SI	El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
A.11.2.4	**Mantenimiento de equipos**	**SI**	**Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.**
A.11.2.5	Retiro de activos	SI	El Jefe de Mantenimiento en concordancia con el Líder del Proceso de Desarrollo Tecnológico documenta el retiro de los activos.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	NO	
A.11.2.7	Disposición segura o reutilización de equipos	SI	El Jefe de Mantenimiento realiza un procedimiento seguro y documentado para la disposición o reutilización de equipos.
A.11.2.8	Equipos de usuario desatendido	SI	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	SI	El Jefe de Seguridad garantiza que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.12	Seguridad de las Operaciones		
A.12.1	Procedimientos y responsabilidades operativas		
A.12.1.1	Procedimientos operativos documentados	NO	
A.12.1.2	Gestión del cambio	SI	El Jefe de Seguridad verifica que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
A.12.1.3	Gestión de la capacidad	SI	El Jefe de DTI y los funcionarios realizan un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo a las necesidades críticas de la organización.

Repositorio Institucional – UNAMBA - PERÚ

A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	SI	El Jefe de Seguridad asegura que los ambientes de desarrollo, pruebas y operación están debidamente separados y no ponen en riesgo la información.

A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	SI	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el software de código malicioso. El Jefe de Seguridad y los funcionarios verifican que el software está protegido con antivirus y existe una política documentada de actualización de todo el software utilizado, antivirus y sistema operativo.
A.12.3	Respaldo		
A.12.3.1	Respaldo de la información	SI	El Jefe de Seguridad y funcionarios pertinentes realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	Registros y monitoreo		
A.12.4.1	Registros de eventos	SI	El Jefe de Seguridad y funcionarios pertinentes revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información.
A.12.4.2	Protección de información de registros	SI	Se implementan controles de seguridad que garanticen la protección de la información de los registros.
A.12.4.3	Registros del administrador y del operador	SI	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de reloj	SI	El Jefe de la DTI asegura que todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.
A.12.5	Controles del software operacional		
A.12.5.1	Instalación de software en sistemas operacionales	SI	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumpla con las políticas de seguridad de la información.
A.12.6	Gestión de vulnerabilidad técnica		
A.12.6.1	Gestión de vulnerabilidades técnicas	SI	Existe una metodología de análisis y evaluación de riesgos sistemática y documentada.
A.12.6.2	Restricciones sobre la instalación de software	SI	La instalación de software es realizada sólo por el personal autorizado y con software probado y licenciado, además de otorgar el principio del

Repositorio Institucional – UNAMBA - PERÚ

			menor privilegio. El procedimiento de instalación es documentado.
A.12.7	Consideraciones para la auditoria de los sistemas de información		
A.12.7.1	Controles de auditoria de sistemas de información	NO	

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	SI	Se tiene los controles de redes documentado.
A.13.1.2	Seguridad de los servicios de red	SI	El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
A.13.1.3	Separación en las redes	SI	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.13.2	Transferencia de información		
A.13.2.1	Política y procedimiento de transferencia de información	NO	
A.13.2.2	Acuerdos sobre transferencia de información	NO	
A.13.2.3	Mensajería electrónica	SI	El Jefe de Seguridad y el Administrador de Redes implementan un firewall que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.2.4	Acuerdos de confidencialidad y de no divulgación	NO	

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.14	Adquisición desarrollo y mantenimiento de sistemas		
A.14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	NO	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	NO	
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	NO	
A.14.2	Seguridad en los procesos de desarrollo y soporte		

Repositorio Institucional – UNAMBA - PERÚ

A.14.2.1	Política de desarrollo seguro	NO	
A.14.2.2	Procedimientos de control de cambios en sistemas	NO	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	NO	
A.14.2.4	Restricciones en los cambios a los paquetes de software	NO	
A.14.2.5	Principios de construcción de los sistemas seguros	NO	
A.14.2.6	Ambiente de desarrollo seguro	NO	
A.14.2.7	Desarrollo contratado externamente	SI	El Jefe de Seguridad y los funcionarios pertinentes evalúan el software desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información.
A.14.2.8	Pruebas de seguridad de sistemas	SI	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	**Pruebas de aceptación de sistemas**	**SI**	**El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.**
A.14.2.10	Datos de prueba	NO	

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Método de implementación
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras de la seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos	SI	El Jefe de la DTI, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	SI	Los funcionarios están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados.

Repositorio Institucional – UNAMBA - PERÚ

			Se establecen los procedimientos a seguir.
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	El Jefe de la DTI, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recolección de evidencia	NO	

Repositorio Institucional – UNAMBA - PERÚ

Anexo 15 – Plan de tratamiento de riesgo

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN
UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC

PLAN DETRATAMIENTO DE RIESGO

Código	DTI-005
Versión	01
Fecha de la versión	23/01/2019
Creado por	Huallpa Laguna Jessica Noralina
Aprobado por	Ing. Evelyn Yeni Medrano Kari
Nivel de confidencialidad	Baja

Repositorio Institucional – UNAMBA - PERÚ

I. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este documento es definir cuáles controles de seguridad o salvaguardas de MAGERIT son los apropiados para enfrentar las amenazas de cada uno de los activos y mitigar los riesgos en la Dirección de tecnologías de la información – UNAMBA, así como definir el tratamiento de cada uno de ellos.

Este documento también determina cuáles controles de seguridad del Anexo A del estándar ISO/IEC 27001:2013 son aplicables a todo el alcance del Sistema de Gestión de la Seguridad de la Información.

II. DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los siguientes:

- Norma ISO/IEC 27001, capítulo 8.2 y 8.3
- Anexo A de la norma ISO/IEC 27001
- Metodología de evaluación y tratamiento de riesgos
- Documento de la Política de seguridad de información

III. TRATAMIENTO DE RIESGOS

El tipo de tratamiento que se le dará a cada riesgo: Asumirlos (AS), Definir Controles (DC) o Transferirlos a Terceros (TT).

IV. APLICABILIDAD DE CONTROLES DE SEGURIDAD

Con el objetivo de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad basados en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013.

Repositorio Institucional – UNAMBA - PERÚ

[D]DATOS/INFORMACIÓN

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
D_CR	Copias de respaldo	E*, A*	R_D_CR	A	DC	➢ D Protección de la Información ➢ D.A Copias de seguridad de los datos (backup)	➢ A.8.2.* ➢ A.12.3.1	B

[S]SERVICIO

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
S-CE	Correo electrónico	E*, A*	R_ S-CE	M	DC	➢ S.email Protección del correo electrónico ➢ S.www Protección de servicios y aplicaciones web	➢ A.13.2.3 ➢ A.12.5.1	B
S_WWW	Página web	E*, A*	R_ S_WWW	A	DC	➢ S.A Aseguramiento de la disponibilidad ➢ S.www Protección de servicios y aplicaciones web	➢ A.12.5.1	B

[SW]SOFTWARE

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
SW_EST	Software Estándar	I*, E*, A*	R_ SW_EST	MA	DC	➢ SW Protección de las Aplicaciones Informáticas ➢ SW.A Copias de seguridad (backup) ➢ SW.SC Se aplican perfiles de seguridad	➢ A.14.2.* ➢ A.12.3.1	B
SW_BDS	Gestores de base de datos	I*, E*, A*	R_ SW_BDS	MA	DC	➢ SW Protección de las Aplicaciones Informáticas ➢ SW.A Copias de seguridad (backup) ➢ SW.CM Cambios (actualizaciones y mantenimiento) ➢ SW.SC Se aplican perfiles de seguridad	➢ A.14.2.* ➢ A.12.3.1	B
SW_OFM	Ofimática	I*, E*, A*	R_ SW_OFM	B	DC	➢ SW Protección de las Aplicaciones Informáticas ➢ SW.A Copias de seguridad (backup) ➢ SW.SC Se aplican perfiles de seguridad	➢ A.14.2.* ➢ A.12.3.1	MB
SW_AVR	Software de antivirus	I*, E*, A*	R_ SW_AVR	M	DC	➢ SW Protección de las Aplicaciones Informáticas ➢ SW.SC Se aplican perfiles de seguridad	➢ A.12.2.1	MB

Repositorio Institucional – UNAMBA - PERÚ

SW_SO	Sistema operativo	I*, E*, A*	R_ SW_SO	M	DC	➢ SW Protección de las Aplicaciones Informáticas ➢ SW.A Copias de seguridad (backup) ➢ SW.SC Se aplican perfiles de seguridad	➢ A.14.2.* ➢ A.12.3.1 ➢ A.12.2.1 ➢ A.12.5.1 ➢ A.12.6.*	MB

[HW] HARDWARE

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
HW_HOS	Servidores	I*, E*, A*	R_ HW_HOS	MA	DC	➢ HW Protección de los Equipos Informáticos ➢ HW.A Aseguramiento de la disponibilidad ➢ HW.SC Se aplican perfiles de seguridad	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	B
HW_PC	Computador de escritorio de uso institucional	I*, E*, A*	R_ HW_PC	B	DC	➢ HW Protección de los Equipos Informáticos	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	MB
HW_ROU	Router	I*, E*, A*	R_ HW_ROU	A	DC	➢ HW Protección de los Equipos Informáticos ➢ HW.A Aseguramiento de la disponibilidad ➢ HW.SC Se aplican perfiles de seguridad	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	MB
HW_SWH	Switch	I*, E*, A*	R_ HW_SWH	A	DC	➢ HW Protección de los Equipos Informáticos ➢ HW.A Aseguramiento de la disponibilidad ➢ HW.SC Se aplican perfiles de seguridad	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	MB
HW_AP	Punto de Acceso	I*, E*, A*	R_ HW_AP	B	DC	➢ HW Protección de los Equipos Informáticos ➢ HW.A Aseguramiento de la disponibilidad	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	MB
HW_PRT	Impresoras	I*, E*, A*	R_ HW_PRT	MB	AS	➢ HW Protección de los Equipos Informáticos ➢ HW.print Reproducción de documentos	➢ A.11.1.1 ➢ A.11.1.2 ➢ A.11.2.1	MB

Repositorio Institucional – UNAMBA - PERÚ

[COM]COMUNICACIONES

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
COM_INT	Internet	E*, A*	R_ COM_INT	MA	DC	➢ COM Protección de las Comunicaciones ➢ COM.A Aseguramiento de la disponibilidad	➢ A.9.1.2 ➢ A.11.2.3 ➢ A.13.1.*	M
COM_LAN	Red de Área Local	E*, A*	R_ COM_LAN	MA	DC	➢ COM Protección de las Comunicaciones ➢ COM.A Aseguramiento de la disponibilidad	➢ A.9.1.2 ➢ A.10.1.1 ➢ A.11.2.3 ➢ A.13.1.*	B
COM_WIFI	Conectividad inalámbrica	E*, A*	R_ COM_WIFI	M	DC	➢ COM Protección de las Comunicaciones ➢ COM.A Aseguramiento de la disponibilidad ➢ COM.wifi Seguridad Wireless(WiFi)	➢ A.9.1.2 ➢ A.10.1.1 ➢ A.13.1.*	MB

[L]INSTALACIONES

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
L_SIT	Dirección de Tecnologías de Información	N*, I*, E*, A*	R_ L_SIT	A	AS	➢ L. Protección de las Instalaciones ➢ L.A Aseguramiento de la disponibilidad ➢ L.AC Control de los accesos físicos	➢ A.11.1.*	B

Repositorio Institucional – UNAMBA - PERÚ

[P]PERSONAL

CODIGO	ACTIVO	AMENAZA	RIESGO ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013	RIESGO
P_ADM	Administrador de sistemas	E*, A*	R_ P_ADM	A	TT	➢ PS Gestión del Personal ➢ PS.A Aseguramiento de la disponibilidad ➢ PS.AT Formación y concienciación	➢ A.7.*	MB
P-COM	Administrador de comunicaci	E*, A*	R_ P_COM	MA	TT	➢ PS Gestión del Personal ➢ PS.A Aseguramiento de la disponibilidad ➢ PS.AT Formación y concienciación	➢ A.7.*	MB
P_DBA	Administrador de Base de datos	E*, A*	R_ P_DBA	MA	TT	➢ PS Gestión del Personal ➢ PS.A Aseguramiento de la disponibilidad ➢ PS.AT Formación y concienciación	➢ A.7.*	MB

Repositorio Institucional – UNAMBA - PERÚ

Anexo 16 – Controles implementados

Los controles que se ha podido implementar son los siguientes:

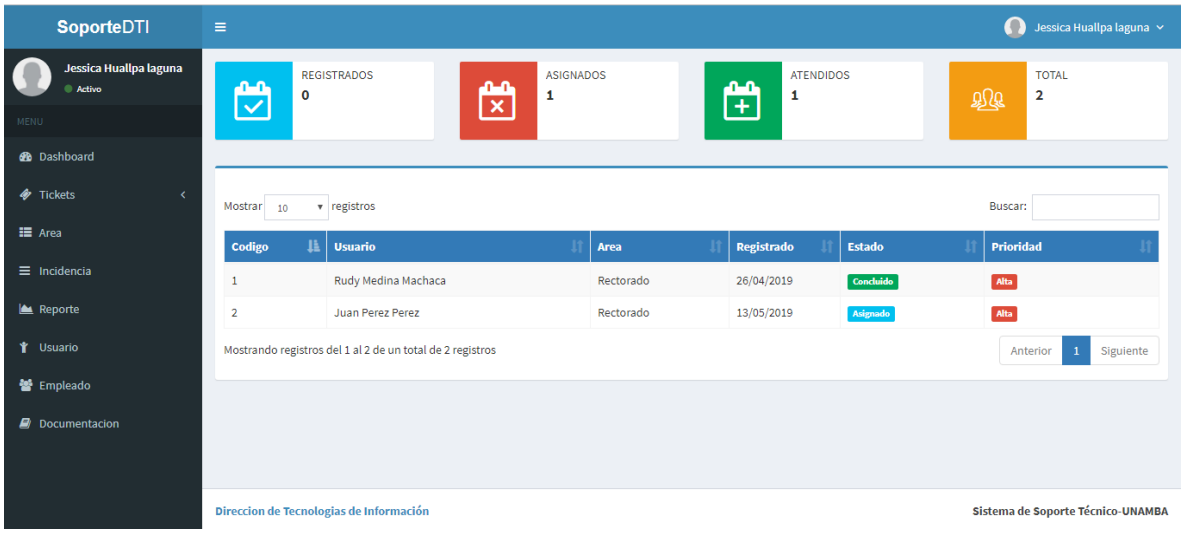
- **A.5** Políticas de seguridad de información (ver anexo 11,12).
- **A.7** Conciencia, educación y capacitación sobre la seguridad de la información (material de capacitación ver anexo 17), declaración de confidencialidad (ver anexo 18).
- **A.8** Gestión de activos-Inventario de activos (ver anexo 10), Política de uso aceptable de los activos (ver anexo 9)
- **A.11** Seguridad física y ambiental- Política de escritorio limpio (ver anexo 12)
- **A.12** Seguridad de Operaciones – Política de copias de seguridad (ver anexo 12)
- **A.16** Gestión de los incidentes de seguridad de la información**:** para la gestión de incidentes se ha realizado un pequeño sistema el cual va a facilitar el fácil manejo de todos los incidentes presentados.

  A continuación se presenta el Sistema de Gestión de Control de Incidentes SOPORTETICK realizado para controlar las incidencias presentadas en la UNAMBA, con esto se resuelve la perdida de activos de información, traspapelación de documentos recepcionados en la DTI, desorden en la DTI debido a que frecuentemente personal administrativo, docentes y alumnos solicitan soporte de manera personal.

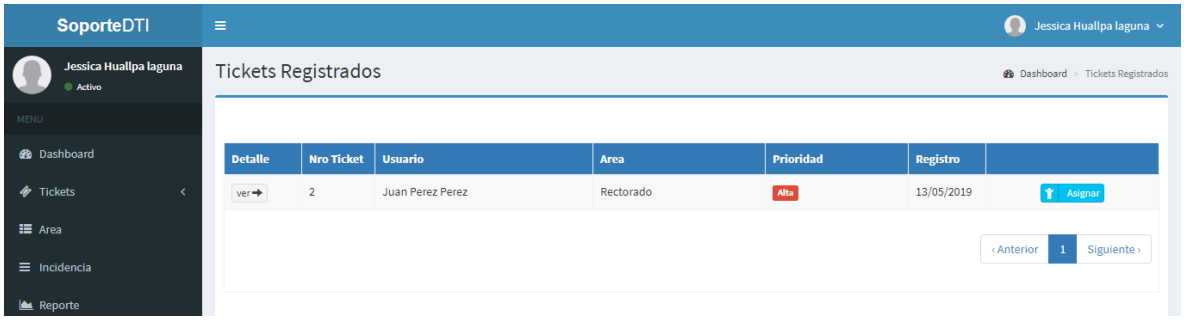
  Cada módulo cuenta con agregar, eliminar y editar excepto del módulo Tickets ya que solo lo ingresa el usuario.

Interfaz de Login

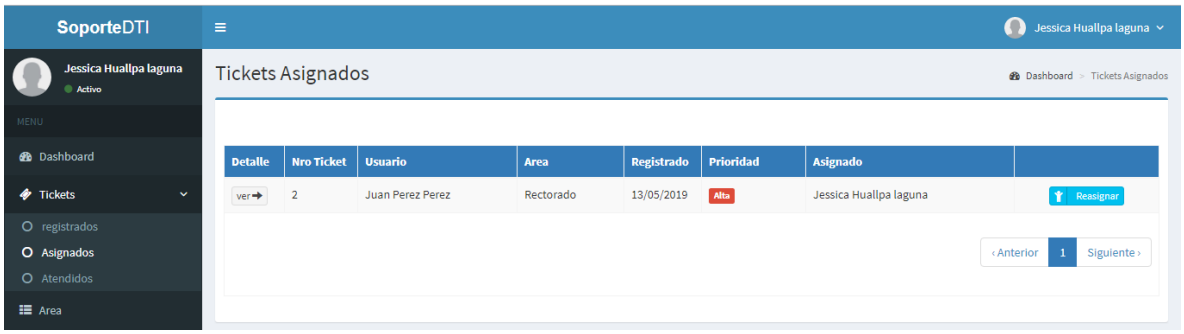
Interfaz de Administrador - inicio



Interfaz de Administrador – tickets registrados

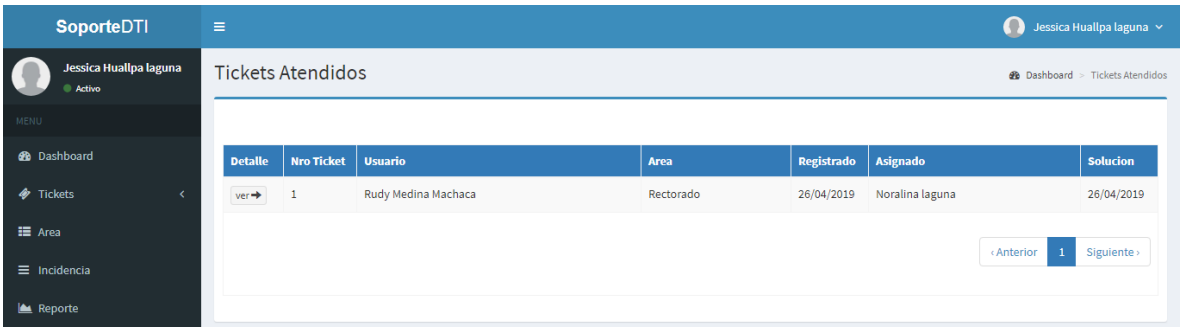


Interfaz de Administrador – tickets asignados



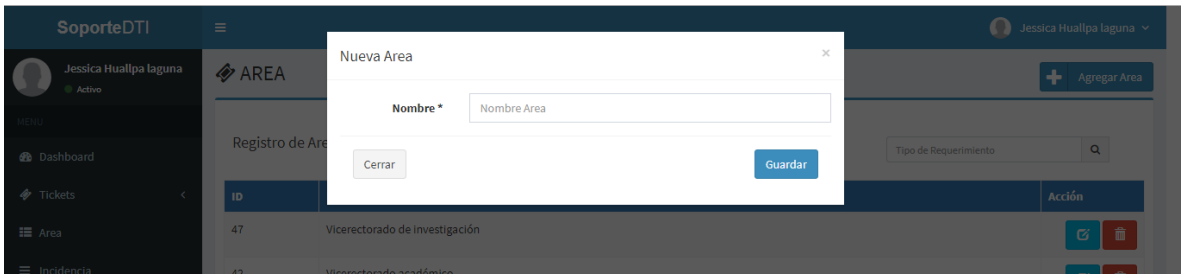
Repositorio Institucional – UNAMBA - PERÚ

Interfaz de Administrador – tickets atendidos



Interfaz de Administrador – Área

Interfaz de Administrador – Ingresar Área

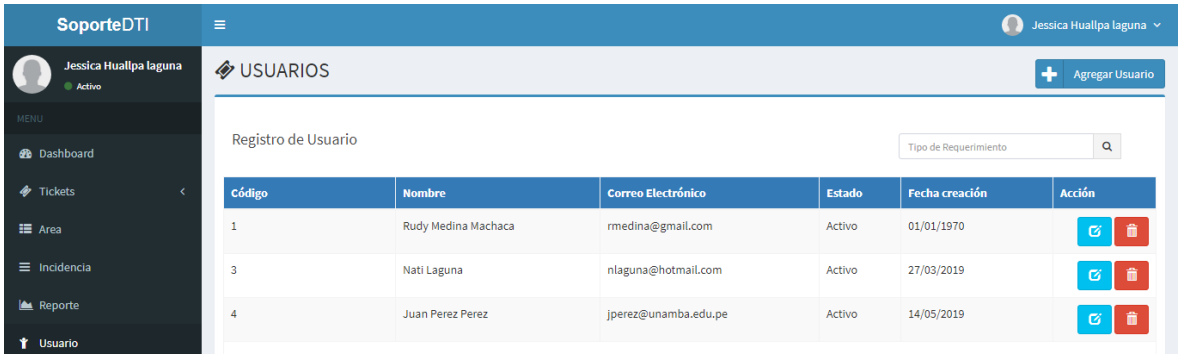


Interfaz de Administrador – Incidencia

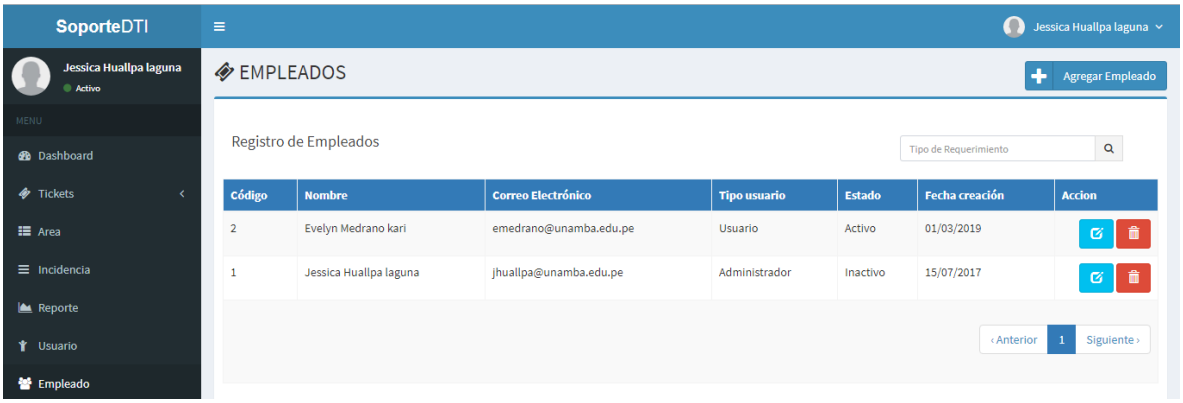
Repositorio Institucional – UNAMBA - PERÚ

Interfaz de Administrador – reporte

Interfaz de Administrador – Usuarios

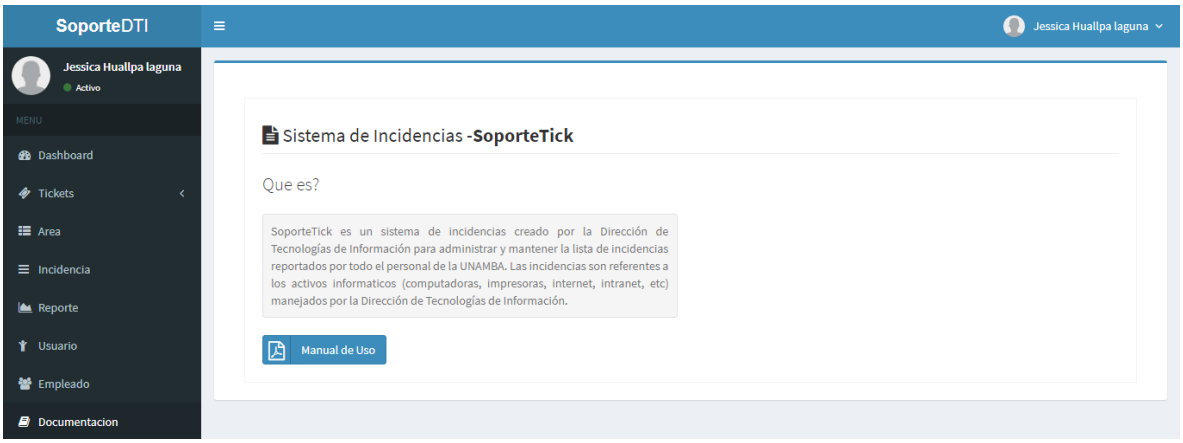


Interfaz de Administrador – Empleado



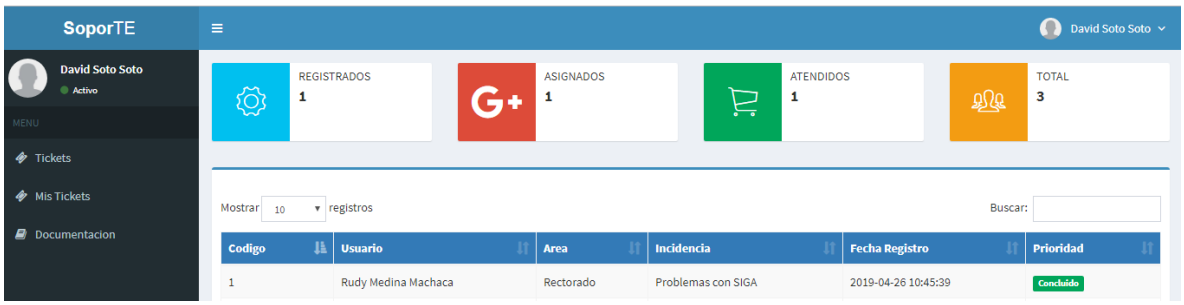
Repositorio Institucional – UNAMBA - PERÚ

Interfaz de Administrador – Documentación



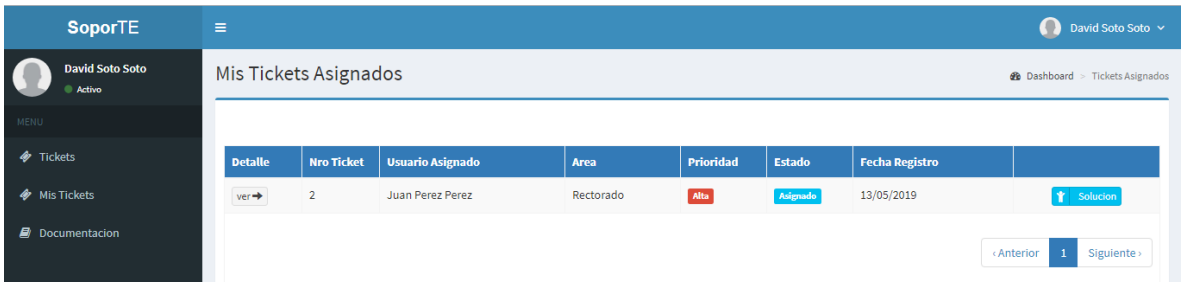
Manual de uso de **SoporteTick** para administrador

Interfaz de Empleado - inicio

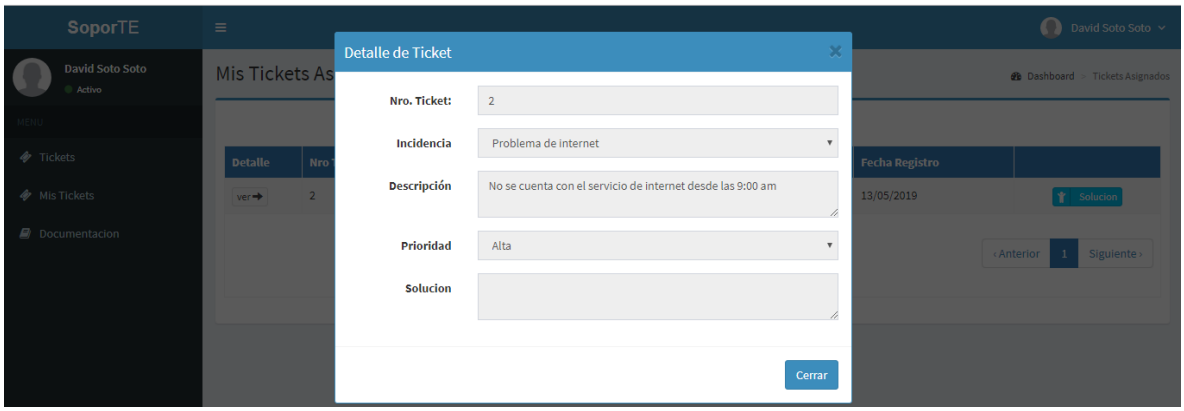


Repositorio Institucional – UNAMBA - PERÚ

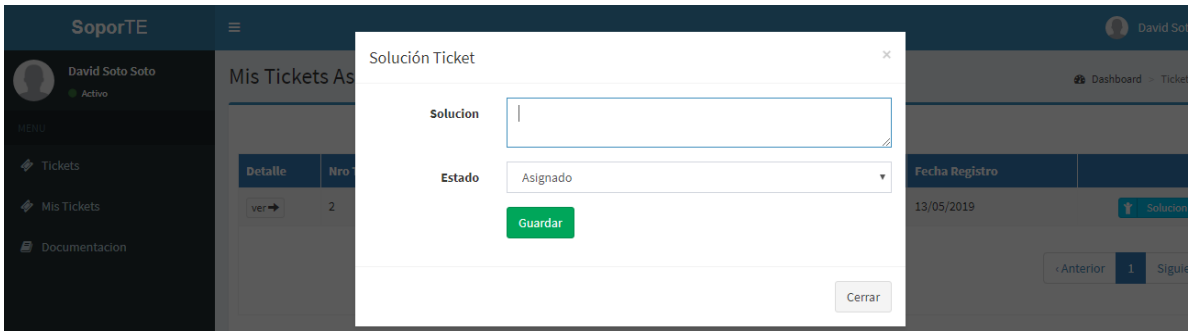
Interfaz de Empleado – tickets asignados



Interfaz de Empleado – Ver detalle de Ticket

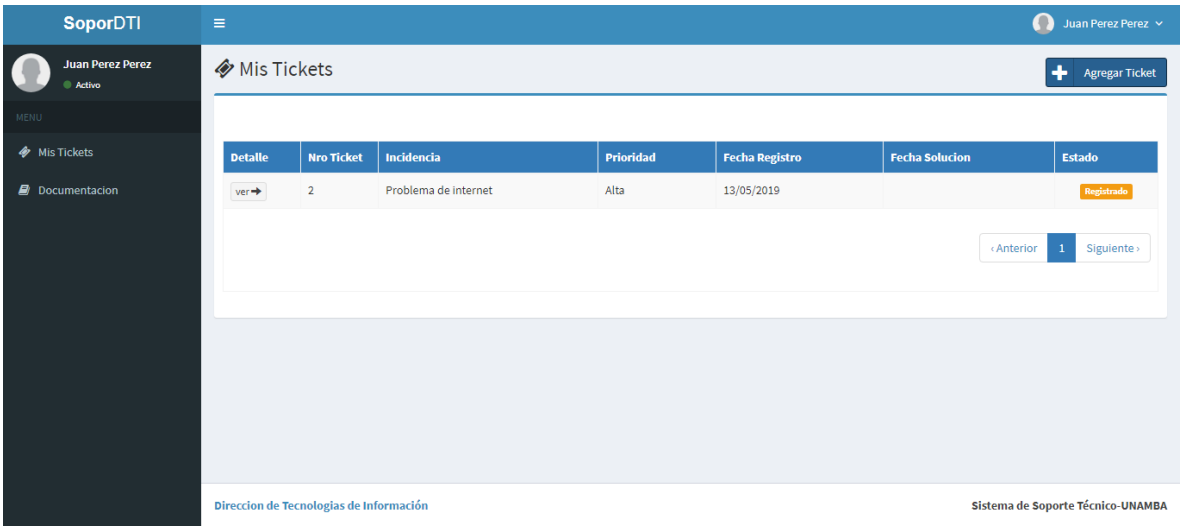


Interfaz de Empleado – Registro de solución de incidencia

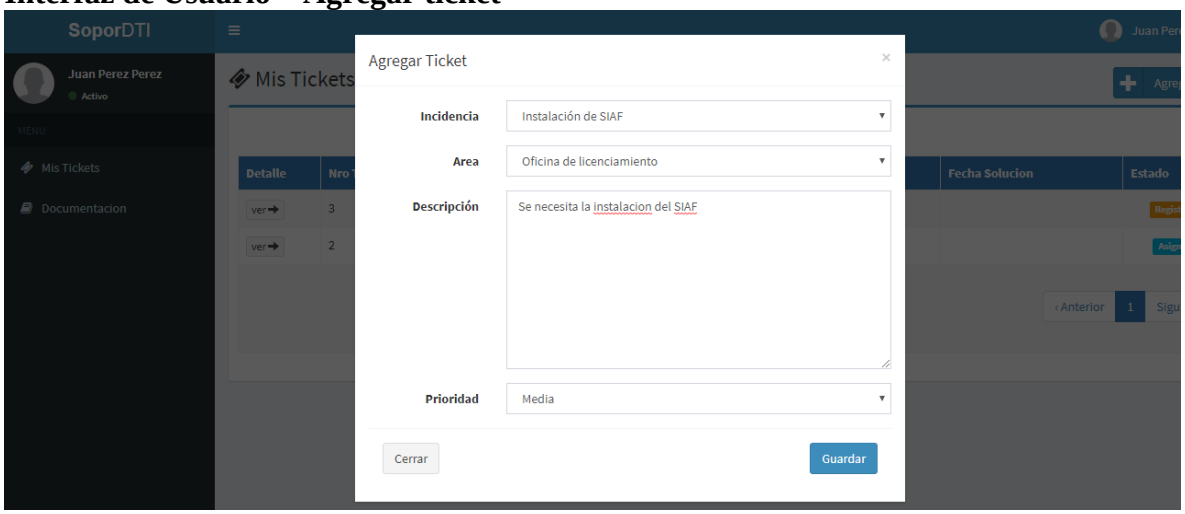


Repositorio Institucional – UNAMBA - PERÚ

Interfaz de Usuario – Inicio



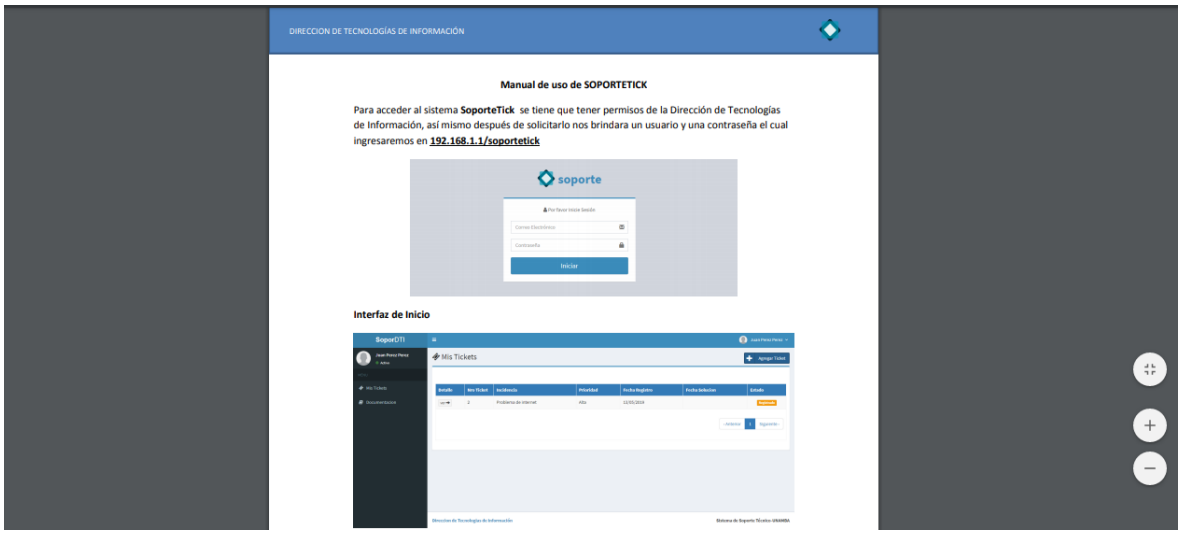
Interfaz de Usuario – Agregar ticket



Interfaz de Usuario – Editar perfil

Repositorio Institucional – UNAMBA - PERÚ

Interfaz de Usuario – Documentación



Repositorio Institucional – UNAMBA - PERÚ

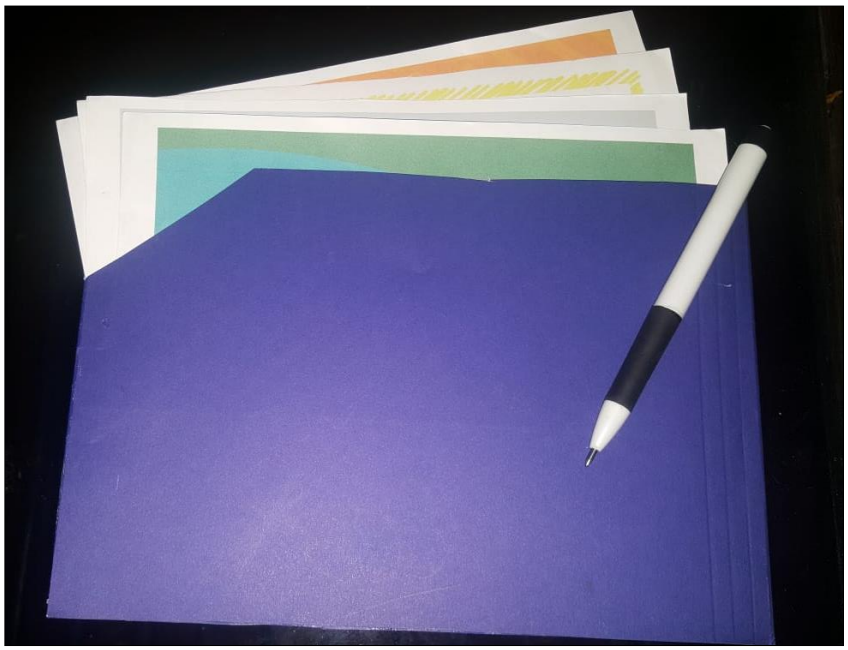
Anexo 17 – Material de capacitación

Al inicio del proyecto de investigación los usuarios de la Dirección de Tecnologías de Investigación de la UNAMBA no se encontraban capacitado o no tenía conocimiento de la importancia y definición de la seguridad de la información, por lo que después de la implementación se pudo capacitar y concientizar a todo la muestra poblacional. Los temas que se tomaron en la concienciación fueron: - Definición de la seguridad de la información - Política de la seguridad de la información (Uso de equipos informáticos, uso de redes y telefonía, uso de internet, copias de seguridad, uso de laboratorios) - Incidentes de seguridad de la información - Consecuencias / Beneficios de la seguridad de la información.

Para la capacitación y concientización se preparó material de capacitación, los cuales contaba con:

- Sobre Azul
- Volantes informativos, con los temas mencionados anteriormente
- 01 lapicero

Material de Capacitación



Repositorio Institucional – UNAMBA - PERÚ

Material de Capacitación

Material de Capacitación

Repositorio Institucional – UNAMBA - PERÚ

Anexo 18 – Declaración de confidencialidad

ACUERDO DE CONFIDENCIALIDAD PERSONAL INTERNO

Como parte de la política de seguridad de la información de la Dirección de Tecnologías de Información, tenemos al Sr(a). _____, Jefe de la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas:

CONSIDERACIONES

Debido a la naturaleza del trabajo, se hace necesario que se maneje información confidencial y/o información sujeta a derechos de propiedad intelectual, antes, durante y en la etapa posterior.

CLÁUSULAS

PRIMERA

OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes, inversionistas, empleados y contractuales y cualquier información revelada sobre terceras personas.

SEGUNDA

CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el tiempo que el personal labore en la Institución, será mantenida en estricta confidencialidad. La parte receptora correspondiente solo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata. Se considera también información confidencial: a) Aquella que como conjunto o por su naturaleza, no sea conocida entre el resto de personal. b) La que no sea de fácil acceso, y e) Aquella información que esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

TERCERA

EXCEPCIONES. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, e) Cuando la información deje de ser confidencial por ser revelada al resto de personal.

Repositorio Institucional – UNAMBA - PERÚ

CUARTA

DURACION. Este acuerdo regirá durante todo el tiempo que el personal labore en la Institución.

QUINTA.

DERECHOS DE PROPIEDAD. Toda información intercambiada es de propiedad exclusiva de la Institución. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso.

SEXTA

MODIFICACIÓN. Este acuerdo solo podrá ser modificado por el Jefe de la Dirección de Tecnologías de Información, y este se encargará de comunicar al personal responsable para su respectiva difusión y publicación en los medios utilizados actualmente.

Tamburco, ____ de _____ de _____.

_____	_____
Jefe de la DTI	Trabajador

Repositorio Institucional – UNAMBA - PERÚ

Anexo 19 – Matriz de consistencia

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL MICAELA BASTIDAS DE APURÍMAC, 2018"

Tabla 14. Matriz de consistencia

PROBLEMA	HIPOTESIS	OBJETIVOS	VARIABLES	DIMENSIÓN	INDICADOR	DISEÑO METODOLOGICO
PROBLEMA GENERAL **PG.-** ¿En qué medida la implementación del SGSI basado en la norma ISO/IEC 27001:2013, contribuirá en mejorar el nivel de seguridad de la información de la DTI de la UNAMBA?	**HIPOTESIS GENERAL** **HG.-** La implementación del SGSI basado en la norma ISO/IEC 27001:2013 mejorará la seguridad de información en la Dirección de tecnologías de la Información de la UNAMBA	**OBJETIVOS GENERAL** **OG.-** Contribuir a mejorar el nivel de la seguridad de la información en la Dirección de Tecnologías de la Información de la UNAMBA implementando el SGSI basado en la norma 27001:2013	**INDEPENDIENTE** Sistema de gestión de seguridad de la información ISO/IEC 27001:2013	Metodología PHVA	Según fase Planear Según fase hacer Según fase verificar Según fase actuar	**TIPO DE INVESTIGACIÓN:** Aplicada **NIVEL DE INVESTIGACIÓN:** Explicativo **DISEÑO DE INVESTIGACIÓN:** Pre experimental **ESQUEMA DE DISEÑO** G: O1 X O2 •Donde: G= Grupo de investigación X= Aplicación de la variable O1= Medición de Pre Observación O2 = Medición de Post Observación **METODOLOGÍA DE SGSI:** Metodología Deming PDCA **METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE SGSI:** Magerit III **POBLACIÓN Y MUESTRA** • Personal Administrativos • 20 personas
PROBLEMA ESPECIFICO **PE1.-** ¿En qué medida se disminuirá los niveles de riesgos de seguridad en la DTI de la UNAMBA? **PE2.-** ¿En qué medida incrementará los controles de Seguridad en la DTI de la UNAMBA? **PE3.-** ¿En qué medida se mejorará el nivel de capacitación y formación en temas de seguridad de la información en los usuarios de DTI de la UNAMBA?	**HIPOTESIS ESPECÍFICO** **H1.-** La implementación del SGSI disminuirá los niveles de riesgos de seguridad en la DTI de la UNAMBA. **H2.-** La implementación del SGSI incrementará los controles de seguridad en la DTI de la UNAMBA. **H3.-** La implementación del SGSI mejorará el nivel de capacitación y formación de los usuarios de la DTI de la UNAMBA en temas de seguridad de la información.	**OBJETIVOS ESPECÍFICOS** **OE1.-** Disminuir los niveles de riesgos de seguridad en la DTI de la UNAMBA. **OE2.-** Incrementar los controles de Seguridad en la DTI de la UNAMBA. **OE3.-** Mejorar el nivel de capacitación y formación en temas de seguridad de la información en los usuarios de la DTI de la UNAMBA.	**DEPENDIENTE** Seguridad de Información	Riesgos Controles Uso de la información y manejo de equipos	*Nivel de Riesgos *Controles aplicados *Nivel de capacitación y formación en temas de seguridad de la información	

Fuente: Elaboración propia

Repositorio Institucional – UNAMBA - PERÚ