UNIVERSIDAD NACIONAL "SANTIAGO ANTÚNEZ DE MAYOLO"

FACULTAD DE CIENCIAS

ESCUELA ACADÉMICO - PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

"DIAGNÓSTICO Y PROPUESTA DE MEJORA PARA LA GESTIÓN DE RIESGOS BASADO EN LA ISO/IEC 27002:2008 PARA LA OFICINA GENERAL DE ESTUDIOS UNASAM - HUARAZ, 2014"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE :

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bach. STEPHANIE GIULIANA CARRIÓN APÉSTEGUI

ASESOR:

Ing. ERICK GIOVANNY FLORES CHACÓN

HUARAZ - PERÚ

2015

N° Registro: T007

DEDICATORIA

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

A mi hermano y hermana, por sus muestras de cariño y compresión, son ellos quienes incentivan mi espíritu y me impulsan a seguir adelante, a pesar de las dificultades. Finalmente a los maestros, aquellos que marcaron cada etapa de nuestro camino universitario.

Stephanie Giuliana Carrión Apéstegui.

AGRADECIMIENTO

En primer lugar a Dios, que nos ofrece día a día el privilegio de vivir para aprovechar nuevas oportunidades que se nos presenta en el camino.

A mis padres, que siempre me han dado su apoyo incondicional y a quienes debo la vida, por todo su trabajo y dedicación para darme una formación académica y sobre todo humanista y espiritual. Para ellos es todo mi agradecimiento.

A mi Alma Mater, Universidad Nacional Santiago Antúnez de Mayolo, por ser quien me acogió durante estos 5 años en mi formación académica y profesional.

Al asesor de tesis, Ing. Flores Chacón Erick Giovanny, por su esfuerzo, dedicación e impulso brindado para la realización de la presente tesis.

Stephanie Giuliana Carrión Apéstegui

PRESENTACIÓN

Señores Miembros del Jurado Calificador:

En cumplimiento con el Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e Informática, de la Facultad de Ciencias, de la Universidad Nacional Santiago Antúnez de Mayolo, presento ante ustedes la tesis, que lleva por título **"Diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM – Huaraz, 2014".**

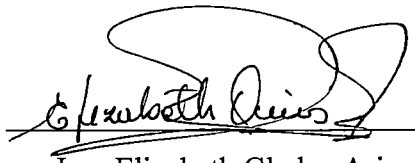
La presente tesis, fue realizada tomando como objeto de estudio a la Oficina General de Estudios y la gestión de riesgos de la misma. Contiene páginas preliminares y IX capítulos. En el capítulo I se determinan el problema que consiste en determinar de qué manera el diagnóstico de la gestión de riesgos contribuirá a la mejora de los procesos académicos de la OGE. En el capítulo II se consideró los antecedentes internacionales y nacionales, así como las teorías que sustentan el trabajo. En el capítulo III se define los materiales y métodos utilizados. En el capítulo IV, se realiza un diagnóstico de la situación actual en cuanto a la gestión de riesgos de la OGE. En el capítulo V se establecen los controles de seguridad y salvaguardas a tomar en cuenta por la OGE. En el capítulo VI y VII se plantea un plan de seguridad para la OGE. En el capítulo VIII se exponen los resultados obtenidos. En el capítulo IX se discute los resultados. Finalmente se presenta las conclusiones y recomendaciones.

Se espera que la presente tesis sea revisada y sustentada para su aprobación.

Atentamente,

Stephanie Giuliana Carrión Apéstegui.

HOJA DE VISTO BUENO



Ing. Elizabeth Gladys Arias Lazarte

Presidente

Ing. Luis Ruperto Alvarado Cáceres

Secretario

Ing. Erick Giovanny Flores Chacón

Vocal

RESUMEN

Actualmente la información es un valioso recurso, que posee cualquier organización. Pero la información está expuesta a riesgos y amenazas que atentan contra su integridad. La Oficina General de Estudios, maneja información de importancia para la comunidad universitaria, es por ello que el objetivo de este proyecto es hacer un diagnóstico de la gestión de riesgos para ayudar a la mejora de los procesos académicos que desarrollan dentro de ésta oficina (manejo de información).

Para este diagnóstico de la gestión de riesgo, me base en la ISO/IEC 27002:2008 y a su vez en la metodología MAGERIT, todo ello con el fin de poder identificar y minimizar los riesgos y amenazas a los que está expuesta la información, y también para poder establecer controles a tomar en cuenta de aquí en adelante, no sólo dentro de la oficina, sino también con miras a educar al usuario.

El nivel de riesgo a los que están expuestos los activos de la Oficina General de Estudios es alto, pero aprovechando el potencial humano con el que cuenta se puede contrarrestar todo ello y tomando las políticas y los controles adecuados estará preparado ante cualquier incidencia futura.

Palabras clave: Gestión de riesgos, seguridad de la información, riesgos, amenazas

ABSTRACT

Currently the information is a valuable resource, which owns any organization. But the information is exposed to risks and threats that undermine their integrity. The General Bureau of Studies, manages information of importance to the university community, which is why the aim of this project is to make a diagnosis of risk management to help improve academic processes that develop within this office (management information).

For the diagnosis of risk management, I based on ISO / IEC 27002: 2008 and turn on the MAGERIT methodology, all in order to identify and minimize risks and threats to which information is displayed, and also to establish controls to consider from now on, not only within the office, but also in order to educate the user.

The level of risk to which they are exposed assets of the General Bureau of Studies is high, but taking advantage of the human potential that account can counteract all this and taking appropriate policies and controls will be prepared for any future incidence.

Keywords: Risk management, information security, risks, threats

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

ÍNDICE DE CUADROS

CAPÍTULO I: GENERALIDADES

1.1. Realidad problemática

La Universidad Nacional de Ancash Santiago Antúnez de Mayolo, desde sus inicios tuvo una álgida preocupación por permanecer en constante desarrollo tecnológico y científico, con miras a convertirse en una de las mejores universidades nacionales, brindando una educación de calidad y formando profesionales competitivos y acordes a nuestra realidad. Para ello, de manera institucional, ha sido conformada por distintos órganos de apoyo que en conjunto con los altos mandos, se espera que lleven a esta universidad al cumplimiento de sus objetivos. Tal es el caso de la Oficina General de Estudios (OGE), el cual es un Órgano de Apoyo del Vice Rectorado Académico encargada de programar, organizar y evaluar la gestión académica, el archivo y registro central académico, así como de apoyo a las Facultades.

La OGE es uno de los órganos de apoyo que destacan por su papel dentro la gestión académica de la UNASAM, ya que dentro de sus instalaciones manejan una gran cantidad de información considerada de vital importancia para las autoridades universitarias, así como también para alumnos y ex alumnos de esta casa superior de estudios. Para ello y conforme a los objetivos de la UNASAM, ha ido implementando tecnologías de información para el soporte y ayuda de sus procesos y manejo de información, tal es el caso del sistema de información que maneja conocido como: Sistema de Gestión Académica – SIGA UNASAM, a su vez han ido mejorando y adquiriendo equipo informático para complementar y hacer aún más óptimo el manejo de la información.

Pero en la actualidad, en las tecnologías de información que posee la OGE, se pueden apreciar ciertas debilidades, vulnerabilidades y deficiencias. Por ejemplo

se puede ver que el SIGA funciona de manera ineficiente presentando problemas de lentitud al acceder desde la web, esto debido a que la línea de internet de 2 Mb que llega al servidor de la OGE no es suficiente ante las solicitudes de los distintos procesos que realizan los usuarios. Además la base de datos con la que trabaja el SIGA presenta redundancia de información y mala estructura de la misma, debido a que fue desarrollado sin tener en cuenta el crecimiento del sistema y de la información, perjudicando la velocidad de respuesta a las consultas, todo ello por carecer de un orden y por tener datos de más. Otro problema a destacar es la incompatibilidad del servidor web, este problema se presenta debido a que cuando el equipo desarrollador del diseño del SIGA no tuvo una visión del crecimiento del sistema, lo cual origina que en la actualidad el software se encuentre un tanto desactualizado y por ende presentará posibles problemas a los intentos de actualizarlo.

Punto aparte es el tema de la seguridad, ya que actualmente un usuario con conocimientos intermedios puede acceder libremente con todos los permisos de la base de datos y por ende a la data que se maneja en el SIGA UNASAM, creando un problema de alto índole que se debe de tomar en consideración lo antes posible. Este problema también se debe a una falta de configuración del servidor proxy, que si se realizara óptimamente solucionaría problemas de seguridad, rendimiento y hasta conectividad. A su vez cabe mencionar que la base de datos del SIGA no posee un servidor propio, haciendo que este sea vulnerable puesto que está alojado dentro del servidor web.

Esta es una breve descripción de la realidad problemática que atraviesa actualmente la OGE, realidad que se espera cambiar con la ayuda del proyecto. Como vemos la UNASAM presenta dificultades en el manejo de información y la seguridad de la misma, estos problemas deben de tener un tratamiento de manera rápida. Para hacer esto posible, la UNASAM debe de tomar en consideración la importancia de la seguridad de la información y los riesgos a los cuales están expuestos y no sólo en la OGE sino también en todas sus dependencias con el

objetivo de impulsar de una manera conjunta y coherente los diferentes elementos que ayudarán a su crecimiento y desarrollo institucional y tecnológico.

1.2. Enunciado del problema

¿De qué manera el diagnóstico de la gestión de riesgos basado en la ISO/IEC 27002:2008 contribuirá a la mejora de los procesos académicos de la Oficina General de Estudios UNASAM – Huaraz, 2014?

1.3. Hipótesis

El diagnóstico de la gestión de riesgos basado en la ISO/IEC 27002:2008 contribuye a la mejora de los procesos académicos de la Oficina General de Estudios UNASAM – Huaraz, 2014.

1.4. Objetivo

1.4.1. Objetivo general

Realizar el diagnóstico de la gestión de riesgos para la mejora de los procesos académicos de la Oficina General de Estudios de la UNASAM.

1.4.2. Objetivo específico

- Diagnosticar el nivel de la Gestión de Riesgos la Oficina General de Estudios.
- Obtener información real sobre la situación actual de la seguridad de la información de la Oficina General de Estudios.

- Proponer estrategias de mejora para la seguridad de la información de la Oficina General de Estudios.

1.5. Justificación

El presente proyecto pretende realizar un Diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la Oficina General de Estudios UNASAM y a su vez proponer mejoras en base a los lineamientos de las buenas prácticas, cuyos beneficios se verán reflejados en la calidad de la información y en la seguridad para su manipulación. Esto beneficiará a la comunidad universitaria en general, ya que tendrán la certeza de que su información académica se encuentra segura y libre de riesgos informáticos. Cabe señalar que es un proyecto viable y de gran utilidad no sólo para la OGE, sino también para la UNASAM.

1.5.1. Justificación operativa

La OGE está compuesta por la Unidad de Programación Académica (UPCA), la Unidad de Registro y Control Académico (URCA) y la Administración de la Base de Datos. Todos ellos en conjunto se encargan del manejo de la información académica de los estudiantes, así como la programación de cada ciclo académico y llevar el cumplimiento del mismo, conjuntamente en trabajo coordinado con la Vice – Rectoría Académica. De los tres entes que componen la OGE, quizás es la Administración de la Base de Datos la que cumple y juega un papel importante en el cumplimiento de las actividades señaladas, ya que es aquí donde se administra la información y se vela por el correcto funcionamiento del sistema. Éste ente cuenta con el personal calificado, el cual fácilmente puede ser capacitado para garantizar el cumplimiento de los lineamientos que se establezcan en cuanto a la seguridad informática se refiere, no presentando mayores inconvenientes si se hace de manera oportuna.

1.5.2. Justificación tecnológica

Tecnológicamente hablando, el proyecto es factible puesto que con el pasar de los años han ido mejorando los equipos necesarios para este tipo de proyecto. Pero aun así hay deficiencias pendientes a corregir y mejorar, lo cual a futuro traerá beneficios para la institución.

1.5.3. Justificación económica

El proyecto es económicamente viable ya que se llegará hasta la fase de diseño, obteniendo al final una propuesta que dependerá de las autoridades la aplicación y puesta en marcha de la misma.

En lo que respecta a la etapa de elaboración del informe, será autofinanciado por la tesista, lo cual implica que no generará ningún costo para la OGE.

1.5.4. Justificación normativa

Este proyecto tiene su justificación legal en la ISO/IEC 27002 nueva denominación para ISO 17799:2005, para que sean seleccionadas por las organizaciones en el desarrollo de sus SGSI. Está norma esta traducida para el Perú desde el año 2007, aún como ISO 17799, la cual fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información, 2da Edición, el 22 de enero del 2007. Esta Norma Técnica Peruana ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

1.6. Limitaciones

Las limitaciones que presenta el siguiente proyecto se detallan a continuación:

- Este proyecto de tesis consistirá solo en el diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008, pero no abarca la parte de la implementación.

- El proyecto plantea algunos controles, que serán indispensables para proteger los activos de información más importantes de la Oficina General de Estudios de la UNASAM, pero si cambia alguna regulación a nivel nacional e incluso internacional, la cual le exija a la oficina muchos controles extras, la propuesta de mejora que se planteará no podrá abarcar esa necesidad contractual que tendría la Oficina General de Estudios.

1.7. Descripción y sustentación de la solución

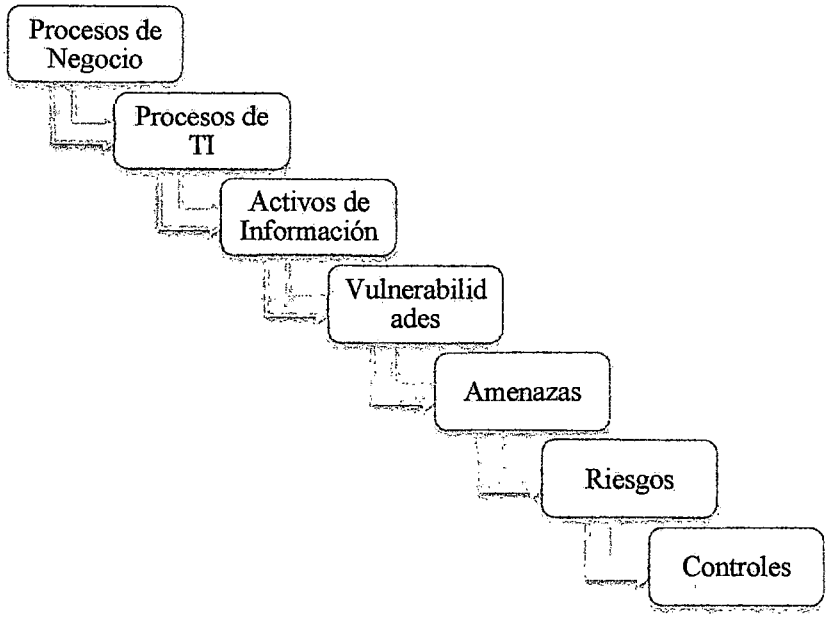
La propuesta de mejora será para que los distintos usuarios del SIGA WEB puedan tener la confianza de que la información que maneja este segura, ya que esta información es de suma importancia no sólo para los usuarios sino también para la comunidad universitaria en general. Cabe recalcar que nada es 100% seguro, pero tomando las medidas preventivas adecuadas, se puede contrarrestar las amenazas y riesgos que ocasionan las distintas situaciones.

- **Viabilidad técnica**

  Para la realización de este proyecto de tesis, es decir, para el diagnóstico y la propuesta de mejora en cuanto a la gestión de riesgo se refiere, se necesitarán una serie de informaciones, que juntas forman una cadena de acción que nos permitirá obtener información clara y precisa para obtener una propuesta muy

de acorde a la realidad por la que atraviesa la Oficina General de Estudios, tal como se muestra a continuación:

Gráfico 1.1. Escalera de la seguridad de la información



Fuente: Elaboración propia

- **Viabilidad operativa**

La propuesta está orientada a gestionar los riesgos en cuanto a seguridad de la información se refiere para la Oficina General de Estudios, mediante un diagnóstico previo de su situación actual. Todo ello será posible ya que se proporcionará la información necesaria por parte de los encargados del manejo de la información, además de que siendo usuario del SIGA WEB, se puede hacer un análisis más detallado sobre las deficiencias que presenta en cuanto a seguridad.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Internacionales

- (Alvarez Basaldúa 2005), en su tesis magistral de *Seguridad en informática (Auditoría de Sistemas)*, Universidad Iberoamericana – México D.F – México, el tesista logró el siguiente objetivo: Proponer lineamientos que se deben tomar en cuenta en cuanto a la seguridad informática, así como también ver la importancia de realizar auditoría de sistemas en las organizaciones. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades.

- (Ferrero Recaséns 2006), en su proyecto de fin de carrera *Análisis y Gestión de Riesgos del Servicio Imat del Sistema de Información de I.C.A.I.*, Universidad Pontificia Comillas – Madrid – España, el tesista logró el siguiente objetivo: Realizar la definición concreta del sistema y el alcance que este posee, la importancia que tiene para la organización para plantear los objetivos y estrategias que se van a adoptar para la seguridad del sistema de TI. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: la importancia de este proyecto radica en la posibilidad de ver que un sistema de información no se queda en la superficie del código o el diseño de hardware o las comunicaciones; hay toda una estructura detrás que ha de funcionar

para que el sistema no sufra una amenaza frente a la cual no está preparado.

- (Cedillo Viera, Desiderio Calderón y Quintero Vinces 2009), en su tesis *Análisis, Diseño e Implementación del módulo control de procesos de Gestión y apoyo del Sistema Estratégico de Calidad de Compulead S.A.*, Escuela Superior Politécnica del Litoral – Guayaquil – Ecuador, los tesistas lograron el siguiente objetivo: analizar, diseñar e implementar un sistema de información que soporte el modelo de competitividad implantado en la empresa de computación COMPULEAD S.A. Tipo: Aplicado. Nivel: Explicativo (carácter experimental). Diseño: Aplicativo. Conclusión: Se realizó el análisis y se comprendió el Módulo Control de Procesos de Gestión y Apoyo (CPGA) del Sistema Estratégico de Calidad de COMPULEAD S.A, lo cual mejoró el rendimiento en cuanto al mantenimiento del Sistema Estratégico de Calidad como se evidenció en la validación del Sistema de Información.

- (Pallas Mega 2009), en su tesis magistral *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*, Universidad de la República – Montevideo – Uruguay, el tesista logró el siguiente objetivo: dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, para una empresa perteneciente a un grupo empresarial. Tipo: aplicado. Nivel: experimental. Diseño: aplicativo. Conclusión: En referencia a la estrategia de análisis y gestión de riesgos así como de planificación, implementación y seguimiento del SGSI, proponemos un enfoque mixto, de dirección centralizada pero con la autonomía necesaria a nivel de cada dominio y cada empresa, fundamentalmente en la gestión de controles y en la percepción del impacto de los riesgos locales.

- (Duque Ochoa 2010), en su estudio *Metodologías de Gestión de Riesgos (Octave, Magerit, DAFP)*, Universidad de Caldas – Caldas – Colombia, la tesista logró el siguiente objetivo: dar a conocer algunas metodologías existentes en cuanto a la Gestión de Riesgos. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: En toda organización se requiere la creación de una "cultura de seguridad" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia. Son dos los pilares fundamentales para la creación de esta cultura: una política de seguridad corporativa y una formación continua a todos los niveles.

- (Larrondo Quirós 2010), en su proyecto fin de carrera de *Uso de la norma ISO/IEC 27004 para Auditoría Informática,* Universidad Carlos III de Madrid – Madrid – España, el tesista logró el siguiente objetivo: evaluar la eficacia de un sistema de gestión de la información aplicadas de seguridad (SGSI) y controles o grupos de controles, tal como se especifica en la norma ISO/IEC 27004. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: Si nos encontramos ante un control el cual no sabemos cómo medir, aquí seria donde entraría el estándar ISO/IEC 27004, el cual nos proporciona la ayuda necesaria para realizar dicha medición.

- (Martínez Saravia 2010), en su tesis magistral *Concienciación en Seguridad de la Información, la estrategia para fortalecer el eslabón más débil de la cadena,* Fundación Universitaria Iberoamericana – Cartagena de Indias – Colombia, el tesista logró el siguiente objetivo: proponer una solución a los problemas de seguridad de la información de una compañía, con la implantación de un programa de concienciación y sensibilización en Seguridad que incorpore buenas prácticas para que los usuarios en sus actividades diarias. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: La

seguridad de la Información es para muchas organizaciones la asignatura pendiente, porque consideran prioritario invertir en estrategias de mercadeo y ventas, o quien sabe en qué. El hecho, es que la Seguridad de la Información es una estrategia tan necesaria como otras.

- (Ripoll Ripoll 2014), en su estudio *Seguridad en los Sistemas de Información (SSI),* Universidad Politécnica de Valencia – Valencia – España, el tesista logró el siguiente objetivo: proporcionar apuntes y el material de apoyo de la asignatura de "Seguridad en los Sistemas Informáticos" que se imparte en la Escuela Técnica Superior de Ingeniería Informática de la Universidad Politécnica de Valencia. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: estos apuntes se ha elaborado con la intención de servir de apoyo a la impartición de las clases. Puede que algunos temas o conceptos no se expliquen con la extensión y detalle necesarios; siendo necesario consultar otras fuentes para completar la formación.

2.1.2. Nacionales

- (Camacho Gomez y Ramos Arrieta 2010), en su tesis *Metodología táctica para la implantación de sistemas de información basado en métrica y COBIT,* Universidad Nacional Mayor de San Marcos – Lima - Perú, los tesistas lograron el siguiente objetivo: Elaborar una metodología a nivel táctico, orientada a satisfacer las necesidades gerenciales y/o de jefe de proyectos a fin de implementar sistemas de información. Tipo: Descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: El proceso de puesta en marcha de un sistema de información será realizado con mayor fluidez y ordenamiento. Con el previo análisis de las metodologías existentes, se ha logrado obtener un producto capaz de mantener estándares de auditoria. La simplicidad que

refleja permitirá realizar el proceso de toma de decisiones gerenciales de una manera eficaz y eficiente.

- (Córdova Rodríguez 2003), en su monografía *Plan de Seguridad Informática para una entidad financiera*, Universidad Nacional Mayor de San Marcos – Lima – Perú, la tesista logró el siguiente objetivo: definir un Plan de Seguridad para una entidad financiera, para ello empieza por definir la estructura organizacional (roles y funciones), después pasa a definir las políticas para finalmente concluir con un plan de implementación o adecuación a las políticas anteriormente definidas. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: La clave para desarrollar con éxito un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica.

- (Villena Aguilar 2006), en su tesis *Sistema de Gestión de Seguridad de Información para una institución financiera*, Pontificia Universidad Católica del Perú – Lima – Perú, el tesista logra el siguiente objetivo: establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú. Tipo: aplicado. Nivel: experimental. Diseño: aplicativo. Conclusión: Para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera.

- (Ampuero Chang 2011), en su tesis *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros*, Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: utilizar estándares y buenas prácticas reconocidos mundialmente para poder desarrollar cada una de las etapas del diseño del Sistema de Gestión de Seguridad de Información (SGSI) y así poder tener una base que se pueda implementar en cualquier compañía de seguros. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. Conclusión: En la actualidad, con el desarrollo de la tecnología, la información ha tomado mayor fuerza en las empresas, convirtiéndose en la mayoría de los casos en el activo más importante que tienen. Es por esta razón que tienen la obligación de proteger aquella información que es importante para ellas y que tiene relación ya sea con el negocio o con los clientes.

- (Espinoza Aguinaga 2013), en su tesis *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*, Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: tomar en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. Conclusión: En los últimos 20 años la información se ha convertido en un activo muy importante y crucial dentro de las organizaciones, es por ello que tiene la necesidad de protegerla si es que la información tiene relación ya sea con el negocio o con sus clientes.

2.1.3. Locales

No se han hallado antecedentes locales sobre este tipo de estudios.

2.2. Teorías que sustentan el trabajo

2.2.1. Sistema de gestión de seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en una empresa u organización.

Antes de profundizar sobre este tipo de sistemas, es importante diferenciar entre seguridad informática y seguridad de la información. A primera vista "Seguridad Informática" y "Seguridad de la Información" pueden parecer exactamente lo mismo, sobre todo si se tiene en cuenta que el desarrollo y la evolución de la tecnología tienden hacia el modelo de "digitalizar" y "manejar" cualquier tipo de información mediante un sistema informático. No obstante, aunque están destinados a vivir en armonía y trabajar conjuntamente, cada uno de las áreas de Seguridad tiene objetivos y actividades diferentes.

La Seguridad Informática (IT Security) se describe como la distinción táctica y operacional de la Seguridad, mientras la Seguridad de la Información (Information Security) sería la línea estratégica de la Seguridad.

- **Seguridad informática**

  Seguridad Informática, es la disciplina que se encarga de las implementaciones técnicas de la protección de la información, el

despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que -articulados con prácticas de gobierno de tecnología de información- establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano 2011)

Por lo tanto la seguridad informática sería la disciplina que se encargaría de llevar a cabo las soluciones técnicas de protección de la información (los activos).

- **Seguridad de la información**

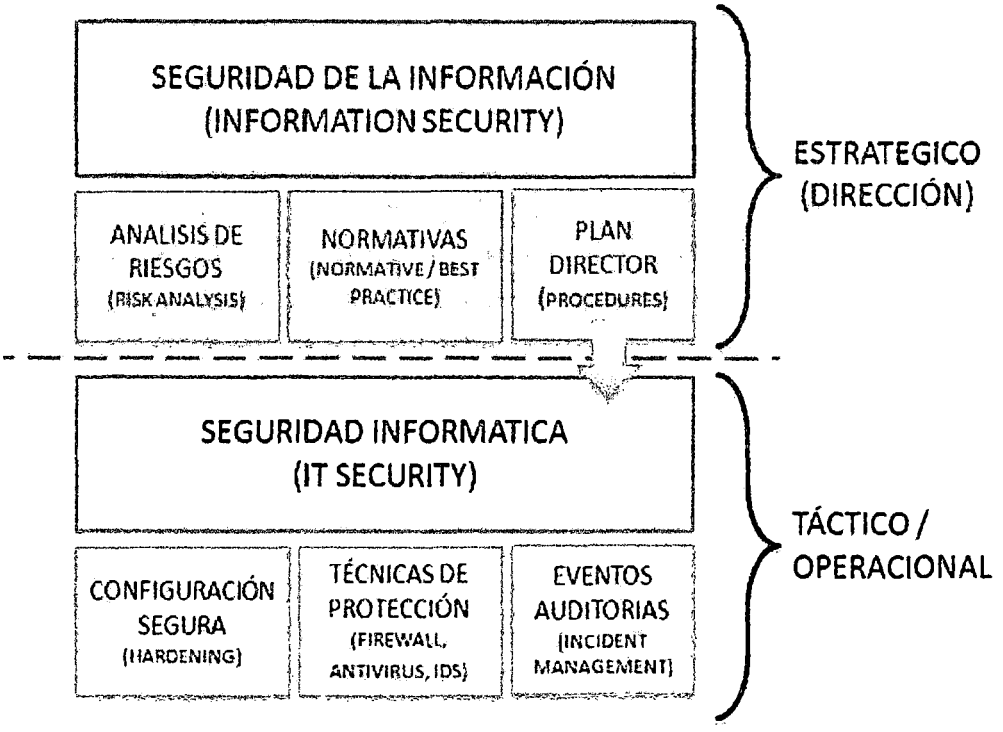
  Seguridad de la Información es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. (Cano 2011)

  Por lo tanto la seguridad de la información sería la disciplina que encargaría de proporcionar evaluar el riesgo y las amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo normativa o buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad en el manejo de la información (activos).

La Seguridad de la Información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para alcanzar el objetivo se apoya en la Seguridad Informática (que estaría gobernada por las directrices de la Seguridad de la Información), es decir, a pesar de ser disciplinas diferentes, la una no puede "ir" sin la otra. De modo que la Seguridad de la Información será la encargada de "regular" y

establecer las pautas a seguir para la protección de la información (Ver Gráfico 2.1.).

Gráfico 2.1. Seguridad de la información vs. Seguridad informática



Fuente: http://www.seguridadparatodos.es/

Pues bien, ahora que sabemos la diferencia entre seguridad informática y seguridad de la información podemos saber lo que es un Sistema de Gestión de la Seguridad de la Información. Conocemos por Sistema de Gestión de Seguridad de la Información o SGSI, a las directrices, procedimientos y controles de seguridad que se utilizan para gestionar la información.

De una manera más estricta, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende de lo siguiente para implantar la gestión de la seguridad de la información.

- La política.

- La estructura organizativa.
- Los procedimientos.
- Los procesos y
- Los recursos necesarios.

Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente.

Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello.

Por tanto definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

a. Análisis y valoración de los riesgos

En primer lugar conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

Amenaza: es la causa potencial de un daño a un activo.

Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.

Impacto: consecuencias de que la amenaza ocurra.

Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.

Salvaguarda: medida técnica u organizativa que ayuda a paliar el riesgo.

Riesgo residual: riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Gráfico 2.2. Análisis de riesgos

Fuente: Presentación PPT de Seguridad de la Información en el Sistema Nacional de Informática - ONGEI

A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuántos recursos se

cuenta (económicos, humanos, técnicos, etc.) pero no es tan fácil saber a ciencia cierta cuales son las necesidades de seguridad.

Hacer un análisis de riesgos permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información ya será posible tomar decisiones bien fundamentadas acerca de qué medidas de seguridad deben implantarse.

b. Gestión de riesgo

La gestión de esos riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados.

La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

i. Mitigar el riesgo

Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

ii. Asumir el riesgo

El ente encargado asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que el ente encargado conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

iii. Transferir el riesgo a un tercero

Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

iv. Eliminar el riesgo

Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No caben más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el riesgo residual. Este se define como el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad apropiadas

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

2.2.2. Metodología del desarrollo del proyecto

La ISO 27002 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de las tecnologías de información sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja.[1] La norma considera también los riesgos

[1] Ethical Shields. 2010. http://www.ethicalshields.com/iso.php

organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica.

Desde el 1 de julio de 2007, la ISO 27002 es el nuevo nombre de ISO 17799:2005. Esta guía nos da las mejores prácticas mediante la aplicación de objetivos y controles necesarios a implementar, recomendables en cuanto a seguridad de la información. No es certificable, sólo hace recomendaciones sobre el uso de 39 objetivos de control, 133 controles de seguridad diferentes aplicados en 11 áreas de control o dominios.

La ISO 27002, antes de desarrollar los objetivos de control nos hace mención de la **Evaluación y Tratamiento del Riesgo.** Esto es clave para el desarrollo de este proyecto, ya que nos proporciona indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información. La evaluación y tratamiento de riesgo se desarrollará teniendo en cuenta la realidad problemática expuesta con anterioridad. Como vemos considera dos puntos muy importantes para poder establecer objetivos de control en una organización:

Gráfico 2.3. Evaluación y tratamiento de riesgo – ISO/IEC 27002:2008

Fuente: Elaboración propia

a. Evaluando los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Lineamientos para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad de Tecnologías de Información).

b. Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:
a) aplicar los controles apropiados para reducir los riesgos;
b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;
c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;
d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos

identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:

b) objetivos organizacionales;

c) requerimientos y restricciones operacionales;

d) costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

e) la necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones.

Se debieran considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño. El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Se debiera tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que se debiera implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización.

2.2.3. Normatividad y modelos

a. Magerit:

Es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la cual fue elaborada por el Consejo Superior de Administración Electrónica, esto en respuesta a que el manejo y administración de información depende de forma creciente de las tecnologías de la información para el cumplimiento de su objetivo.

La Universidad Francisco de Paula Santander sostiene que: Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información, esto supone beneficios para los usuarios; y da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. (Universidad Francisco de Paula Santander 2014)

Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si éstos, son valiosos, Magerit permitirá saber cuánto valor está en juego y ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es imprescindible para poder gestionarlos. Con Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (Ver Gráfico 2.4.)

i. Objetivos de Magerit:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

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

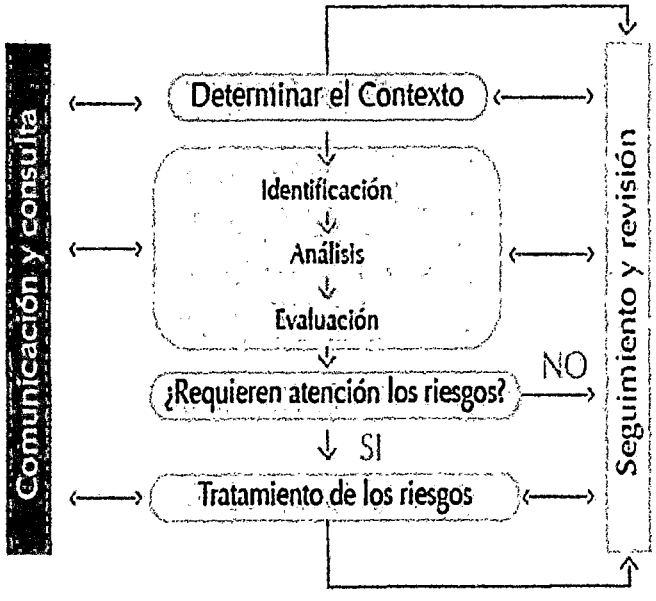
ii. Ventajas de Magerit:

Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles

iii. Desventajas de Magerit:

El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

Gráfico 2.4. Proceso de gestión de riesgos



Fuente: Magerit versión 3.0

b. La Norma ISO 27002:

Esta norma contiene 11 dominios, 39 objetivos de control de seguridad que contienen un total de 133 controles de seguridad. Puede servir de guía práctica para la gestión de la seguridad de la información. No es una norma certificable, esto debido a que el original en inglés de la ISO 27002 usa la expresión verbal "should", un término presente en otras normas ISO y también del IETF y del IEEE, que por convención expresa una forma condicional a modo de recomendación y no de imposición, lo que hace precisamente que no sea certificable.

Los dominios contemplados en la Norma son:

i. Política de Seguridad: Documento de política de seguridad y su gestión.
ii. Aspectos Organizativos de la Seguridad de la Información: Organización interna; organización externa.
iii. Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.
iv. Seguridad Ligada a los Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.
v. Seguridad Física del Entorno: Áreas seguras; seguridad de los equipos.
vi. Gestión de Comunicaciones y Operaciones: procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.
vii. Control Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control

de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

viii. Adquisición, desarrollo y mantenimiento de sistemas de información: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.

ix. Gestión de incidentes en la Seguridad de la Información: Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.

x. Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.

xi. Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

La Norma contiene explicaciones exhaustivas y de cómo se puede implantar cada uno de los controles, pero hay que tener en cuenta que no es una norma preceptiva sino informativa, por lo que la información que da puede y debe ser adaptada a las necesidades y situación específica de la organización. Debe evitarse caer en el error de tratar de seguir al pie de la letra las indicaciones que se dan, ya que pueden ser excesivamente complejas e innecesarias para muchas organizaciones.

2.3. Definición de términos

Investigación: Está determinada por la averiguación de datos o la búsqueda de soluciones para ciertos inconvenientes.

Norma: Regla o conjunto de reglas que hay que seguir apara llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo.

ISO: Organización de Estandarización Internacional.

Muestreo: Es la acción de escoger muestras representativas de la calidad o condiciones medidas de un todo.

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Riesgo: Es un problema potencial que puede ocurrir dentro de una organización.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Riesgo Residual: Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

OGE: Oficina General de Estudios.

SGSI: Sistema de Gestión de Seguridad de la Información. Es una herramienta de gestión.

Mitigar: Disminuir la intensidad, la gravedad o la importancia de algo.

Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Impacto: consecuencia que sobre un activo tiene la materialización de una amenaza.

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Vulnerabilidad: Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia.

Seguridad de la información: Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.

CAPITULO III: MATERIALES Y MÉTODOS

3.1. Materiales

3.1.1. Instrumental usado

- Laboratorios

  Las instalaciones de la Facultad de Ciencias, así como también la Oficina General de Estudio en su conjunto, siendo la más importante a tratar la Unidad de Administración de Base de Datos.

- Software

  Para el desarrollo del presente proyecto se hizo empleo de los siguientes:

Cuadro 3.1. Recursos en software

Software	Descripción
Sistema operativo Windows 7	Sistema operativo de la Mini note
Sistema operativo Windows 8	Sistema operativo de a Lap top
MS Word 2013	Procesador de texto
MS Excel 2013	Para cálculos estadísticos

Fuente: Elaboración propia

- Recursos computacionales

  Se hizo uso de los siguientes recursos computacionales

Cuadro 3.2. Recursos computacionales

Equipo	Detalles	Características
1 Laptop	Procesador	Intel Core i3 1.70 GHz
	Sistema Operativo	Windows 8.1 64 bits

	Memoria RAM	4 GB
	Disco Duro	689 GB
1 Mini Note	Microprocesador	Intel Atom N455 1.66 GHz
	Sistema Operativo	Windows 7 Starter 32 bits
	Memoria RAM	2 GB
	Disco Duro	320 GB
1 Impresora	Impresora multifuncional HP Deskjet F4400	Impresora Escáner Copiadora
1 Disco duro externo	Capacidad	700 GB
2 Pen Drive	Capacidad	Uno de 8 GB y otro de 4 GB
Internet móvil	Modem de internet	Internet móvil de Claro de 3 GB

Fuente: Elaboración propia

3.1.2. Población y Muestra

- Unidad de análisis

  Alumnos, docentes y administrativos de la UNASAM que hacen uso del servicio de la Oficina General de Estudios y que requieren información que ésta maneja.

- Población

  La población de las zonas de influencia de la UNASAM corresponde al siguiente cuadro:

Cuadro 3.3. Población total

N°	Descripción	Población total
1	Alumnos	6274

2	Personal docente	480
3	Personal administrativo	60
Total		**6814**

Fuente: OGE, OGPER - UNASAM

Se está considerando el criterio de población beneficiaria a todos los alumnos de la UNASAM que hacen uso del SIGA WEB UNASAM, el cual es administrado directamente por la OGE. Además también se está considerando a los docentes y administrativos de todas las facultades que hacen uso del mismo. Se está tomando esta población ya que son los mayores beneficiarios al ser los usuarios principales del SIGA WEB UNASAM.

Hay que tener en cuenta que personal administrativo se está considerando al personal que hace uso del SIGA WEB y de la data que está contenida dentro de este, tal es el caso de directores de escuela, jefes de departamento y secretarias.

- Muestra

  Teniendo en cuenta la población, tendremos un total de 3 muestras, ya que cada uno de ellos hace un uso distinto del SIGA WEB. Es por ello que tendremos la Muestra 1 conformada por los alumnos de la UNASAM, la Muestra 2 conformada por el personal docente y la Muestra 3 conformada por el personal administrativo. Además cada una de las muestras se diferenciará por facultades.

Muestra 1: Tamaño de muestra para una proporción; siendo el tamaño de muestra igual a 362 para la población 1, teniendo en cuenta un nivel de confianza del 95%, error de muestreo de 5% y uso de la fórmula general.

Cuadro 3.4. Muestra 1 - Alumnos

N°	Facultad	Cant. Alumnos	Muestra
1	Facultad de Ciencias Agrarias	777	45
2	Facultad de Ingeniería de Minas, Geología y Metalurgia	378	22
3	Facultad de Ingeniería Civil	557	32
4	Facultad de Ingeniería de Industrias Alimentarias	294	17
5	Facultad de Ciencias del Ambiente	673	39
6	Facultad de Economía y Contabilidad	844	49
7	Facultad de Administración y Turismo	614	35
8	Facultad de Ciencias Médicas	464	27
9	Facultad de Ciencias sociales, Educación y de la Comunicación	776	45
10	Facultad de Ciencias	490	28
11	Facultad de Derecho y Ciencias Políticas	407	23
TOTAL		**6274**	**362**

Fuente: Elaboración propia

Tamaño de muestra de la población:

$$n = \frac{(\sum W_h * \sqrt{P_h * Q_h})^2}{(\frac{E}{Z})^2 + \frac{\sum W_h * P_h * Q_h}{N}}$$

Donde: nh = n(wh) ⇨ Tamaño de muestra en estratos.

De este modo obtenemos las muestras para cada facultad.

Muestra 2: Muestreo estratificado para la proporción, siendo el tamaño de muestra obtenido de 212, para lo cual se tuvo en cuenta un nivel de confianza del 95% y error de muestreo del 5%.

Cuadro 3.5. Muestra 2 - Docentes

N°	Facultad	Cant. Docentes	Muestra
1	Facultad de Ciencias Agrarias	32	14
2	Facultad de Ingeniería de Minas, Geología y Metalurgia	19	8
3	Facultad de Ingeniería Civil	32	14
4	Facultad de Ingeniería de Industrias Alimentarias	17	8
5	Facultad de Ciencias del Ambiente	30	13
6	Facultad de Economía y Contabilidad	46	20
7	Facultad de Administración y Turismo	30	13
8	Facultad de Ciencias Médicas	62	28
9	Facultad de Ciencias sociales, Educación y de la Comunicación	75	33
10	Facultad de Ciencias	113	50
11	Facultad de Derecho y Ciencias Políticas	24	11
TOTAL		**480**	**212**

Fuente: Elaboración propia

Tamaño de muestra de la población:

$$n = \frac{(\sum W_h * \sqrt{P_h * Q_h})^2}{(\frac{E}{Z})^2 + \frac{\sum W_h * P_h * Q_h}{N}}$$

Donde: nh = n(wh) ⇨ Tamaño de muestra en estratos.

Muestra 3: Muestreo estratificado para la proporción, siendo el tamaño de muestra obtenido de 50, para lo cual se tuvo en cuenta un nivel de confianza del 95% y error de muestreo del 5%.

Cuadro 3.6. Muestra 3 – Administrativos

N°	Facultad	Cant. Admin.	Muestra
1	Facultad de Ciencias Agrarias	6	5
2	Facultad de Ingeniería de Minas, Geología y Metalurgia	4	3
3	Facultad de Ingeniería Civil	4	3
4	Facultad de Ingeniería de Industrias Alimentarias	5	4
5	Facultad de Ciencias del Ambiente	5	4
6	Facultad de Economía y Contabilidad	6	5
7	Facultad de Administración y Turismo	5	4
8	Facultad de Ciencias Médicas	5	4
9	Facultad de Ciencias sociales, Educación y de la Comunicación	10	9
10	Facultad de Ciencias	7	6
11	Facultad de Derecho y Ciencias Políticas	3	3
TOTAL		**60**	**50**

Fuente: Elaboración propia

Tamaño de muestra de la población:

$$n = \frac{(\sum W_h * \sqrt{P_h * Q_h})^2}{(\frac{E}{Z})^2 + \frac{\sum W_h * P_h * Q_h}{N}}$$

Donde: nh = n(wh) ⇨ Tamaño de muestra en estratos.

Entonces la muestra total será:

Cuadro 3.7. Muestra total

N°	Descripción	Muestra
1	Alumnos	362
2	Personal docente	212
3	Personal administrativo	50
	TOTAL	**624**

Fuente: Elaboración propia

- Tipo de muestreo

  Probabilístico, porque la muestra fue obtenida a partir de una fórmula dada, muestreo para una proporción y muestreo estratificado para proporciones.

3.2. Métodos

3.2.1. Tipo de investigación

De acuerdo a la orientación:

Investigación Básica, ya que está orientada a conseguir un nuevo conocimiento con el objetivo de ampliarla.

De acuerdo a la técnica de contrastación:

Descriptiva simple, puesto que se hará un estudio de las variables sin manipulación de las mismas y con datos obtenidos de la realidad en el levantamiento de información. "Pretende medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas".[2]

3.2.2. Metodología de desarrollo

Lo que se pretende con el presente proyecto es dar una solución formal al problema, es por ello que será necesario aplicar una metodología de desarrollo basado en los principios fundamentales de la ingeniería. Tomando en cuenta el punto de la ingeniería del software, ésta nos proporciona varias capas conformadas por procesos, métodos y herramientas, tal como nos señala Pressman (Pressman 2010). La ingeniería del software nos proporciona un enfoque más preciso al momento de aplicar ingeniería a un problema, es por ello que se usará una metodología de desarrollo muy parecido a lo que nos ofrece el "Ciclo de vida del Software", ya que este describe el desarrollo de software desde la fase inicial hasta la fase final, de la misma manera que nos ayudará a describir el desarrollo del presente tesis.

Observando los distintos modelos que nos ofrece el "Ciclo de Vida de Software", podemos obtener la siguiente metodología de desarrollo (ver Gráfico 3.1.) con lo necesario para dar solución al problema de estudio.

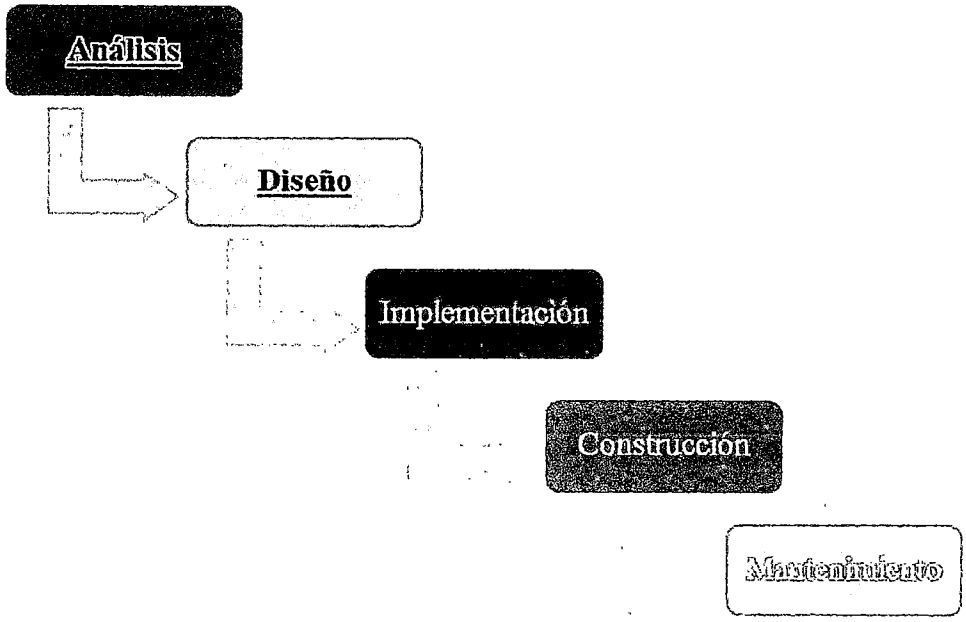
Tener en cuenta que por ser un tipo de investigación descriptiva, se desarrollará principalmente dos etapas las cuales son: Análisis y Desarrollo.

---

[2] Roberto Hernández et al., Metodología de la Investigación (McGraw-Hill, 2010) Pg. 80

En cuanto a las demás etapas, serán abordadas de manera descriptiva y haciendo un planteamiento general de su desarrollo.

Gráfico 3.1. Metodología de desarrollo



Fuente: Elaboración propia

3.2.3. Definición de variables

Objetivo general: Realizar el diagnóstico de la gestión de riesgos para la mejora de los procesos académicos de la Oficina General de Estudios de la UNASAM.

Cuadro 3.8. Definición de variables

Objetivos Específicos	Variable	Definición Conceptual
Diagnosticar el nivel de la Gestión de Riesgos la Oficina General de Estudios.	V1: Diagnóstico de la situación actual	Diagnóstico de la situación actual de la organización en cuanto a gestión de riesgos

Obtener información real sobre la situación actual de la seguridad de la información de la Oficina General de Estudios.	V2: Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información.	De acuerdo al punto 4 de la ISO, se tomará en cuenta las características que esta nos detalla para la seguridad de la información.
Proponer estrategias de mejora para la seguridad de la información de la Oficina General de Estudios.	V3: Propuesta de mejora	Conjunto de propuestas, sugerencias, estrategias o instrucciones para la seguridad de la información.

Fuente: Elaboración propia

3.2.4. Operacionalización de variables

Objetivo general: Realizar el diagnóstico de la gestión de riesgos para la mejora de los procesos académicos de la Oficina General de Estudios de la UNASAM.

Cuadro 3.9. Operacionalización de variables

Objetivos Específicos	Variable	Dimensión	Indicador	Item
Diagnosticar el nivel de la Gestión de Riesgos la Oficina General de Estudios.	V1: Diagnóstico de la situación actual	Gestión de riesgos	Políticas de Seguridad	Entrevistas al personal de la OGE
			Gestión de activo	Entrevistas al personal de la OGE

			Amenazas y Vulnerabilidades	Aplicación MAGERIT
Obtener información real sobre la situación actual de la seguridad de la información de la Oficina General de Estudios.	V2: Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información.	Evaluando los riesgos de seguridad	Conocimientos sobre los riesgos	Encuesta a alumnos, docentes y administrativos: Preguntas 4, 5, 6, 7, 10, 12, 14, 15, 16, 17, 18
				Entrevistas al personal de la OGE
				Observaciones
		Tratamiento de los riesgos de seguridad	Cómo enfrentan los riesgos los usuarios	Encuesta a alumnos, docentes y administrativos: Preguntas 8, 9, 11, 13, 19, 20, 21, 22
				Entrevistas al personal de la OGE
				Observaciones
Proponer estrategias de mejora para la seguridad de la información de	V3: Propuesta de mejora	Definición de controles y estrategias para la seguridad	Políticas, procedimientos y controles	Alineados a la ISO/IEC 27002:2008

la Oficina General de Estudios.		de la información		

Fuente: Elaboración propia

3.2.5. Diseño de la investigación

El diseño de la investigación está dado bajo un enfoque **no experimental** ya que "se realiza sin manipular deliberadamente las variables"[3] y se observan los fenómenos tal como se dan en su contexto natural para su posterior análisis. Dicho esto, el diseño de investigación apropiado, bajo el enfoque anterior, es el **transversal o transeccional,** ya que recopila datos en un momento único y "su propósito es describir variables y analizar su incidencia e interrelación en un momento dado"[4].

3.3. Técnicas

3.3.1. Instrumentos de recolección de datos

Para la obtención de información haremos uso de herramientas como son: entrevista, encuestas y observación (ver Cuadro 3.10).

Cuadro 3.10. Instrumentos de recolección de datos

Instrumento	Justificación	Herramientas	Aplicación
Entrevista	Nos va a permitir conocer más de cerca los procesos	- Grabador de voz - Entrevistas preparadas con	Trabajadores del área en estudio.

[3] Roberto Hernández et al., Metodología de la Investigación (McGraw-Hill, 2010) Pg. 149
[4] Roberto Hernández et al., Metodología de la Investigación (McGraw-Hill, 2010) Pg. 151

	de la OGE, sus problemas, objetivos y requerimientos	una dinámica de preguntas y respuestas abiertas - Cuestionarios	
Observación	Es el método en la cual enfocamos la perspectiva de los problemas que existen en las áreas a trabajar, ya que nos permite observar los hechos tal cual son y ocurren, y sobre todo aquellos que son de interés y significativos para la investigación	- Fichas o guías de observaciones - Cámara fotográfica	Trabajadores de las áreas en estudio, docentes y alumnos
Encuestas	Elaborado especialmente con los ítems y alternativas cerradas con base a las variables e indicadores de estudio. Así mismo comprende las siguientes partes: título, objetivo, instrucción,	- Encuesta estructurada de preguntas abiertas y cerradas	Trabajadores de las áreas en estudio, docentes y alumnos

	preguntas y alternativas de respuesta.		

Fuente: Elaboración propia

3.3.2. Técnicas de procesamiento de información

Las técnicas de procesamiento de información serán:

- Encuestas dirigidas al personal docente, administrativos y alumnos de la UNASAM, procesadas en Microsoft Excel 2010, lo cual nos permitirá obtener un consolidado de los resultados así como gráficos para su interpretación.
- Análisis de las entrevistas realizadas, así como también de los documentos, libros y guías que se estén empleando para la realización de este proyecto.
- Análisis de las observaciones realizadas durante la recopilación de información.

En base a éstas técnicas de procesamiento de información, se establecerá la situación actual de la Oficina General de Estudios y las necesidades a ser resueltas en base al problema planteado.

3.4. Procedimientos

3.4.1. Modelar el negocio

Se realizará una identificación de la importancia que cumple cada una de las unidades que conforman la Oficina General de Estudios, de tal manera que nos un plan para realizar la recolección de información, estableciendo mecanismo para la evaluación de variables cuantitativas y cualitativas si las hubiese.

Se procede a evaluar a la Oficina General de Estudios identificando a cada una de sus unidades así como el personal con el que cuenta. A su vez se también se buscará identificar su interacción con los usuarios de los servicios que ofrece la oficina. Todo ello nos permitirá la recolección de información, permitiéndonos evaluar cada una de las variables identificadas.

3.4.2. Determinar la fórmula de éxito

Procesar la información mediante los indicadores que se han establecido en el mecanismo de evaluación, para después determinar con claridad el cumplimiento de cada uno de los requerimientos establecidos y definición precisa de los objetivos de la investigación.

3.4.3. Comprometer a los actores clave

Una vez que se definen los objetivos y estrategias, se busca el apoyo de los usuarios en general así como el personal responsable del manejo de la información dentro de la Oficina General de Estudios para determinar algunas deficiencias dentro del mismo y así tener una información más real que nos permitirá llegar a los objetivos planteados.

CAPITULO IV: ANÁLISIS

4.1. Análisis de la situación actual

La Universidad Nacional de Ancash Santiago Antúnez de Mayolo, desde sus inicios tuvo una álgida preocupación por permanecer en constante desarrollo tecnológico y científico, con miras a convertirse en una de las mejores universidades nacionales, brindando una educación de calidad y formando profesionales competitivos y acordes a nuestra realidad. Para ello, de manera institucional, ha sido conformada por distintos órganos de apoyo que en conjunto con los altos mandos, se espera que lleven a esta universidad al cumplimiento de sus objetivos. Tal es el caso de la Oficina General de Estudios (OGE), el cual es un Órgano de Apoyo del Vice Rectorado Académico encargada de programar, organizar y evaluar la gestión académica, el archivo y registro central académico, así como de apoyo a las Facultades.

La OGE es uno de los órganos de apoyo que destacan por su papel dentro la gestión académica de la UNASAM, ya que dentro de sus instalaciones manejan una gran cantidad de información considerada de vital importancia para las autoridades universitarias, así como también para alumnos y ex alumnos de esta casa superior de estudios. Para ello y conforme a los objetivos de la UNASAM, ha ido implementando tecnologías de información para el soporte y ayuda de sus procesos y manejo de información, tal es el caso del sistema de información que maneja conocido como: Sistema de Gestión Académica – SIGA UNASAM, a su vez han ido mejorando y adquiriendo equipo informático para complementar y hacer aún más óptimo el manejo de la información.

Pero en la actualidad, en las tecnologías de información que posee la OGE, se pueden apreciar ciertas debilidades, vulnerabilidades y deficiencias. Por ejemplo se puede ver que el SIGA funciona de manera ineficiente presentando problemas

de lentitud al acceder desde la web, esto debido a que la línea de internet de 2 Mb que llega al servidor de la OGE no es suficiente ante las solicitudes de los distintos procesos que realizan los usuarios. Además la base de datos con la que trabaja el SIGA presenta redundancia de información y mala estructura de la misma, debido a que fue desarrollado sin tener en cuenta el crecimiento del sistema y de la información, perjudicando la velocidad de respuesta a las consultas, todo ello por carecer de un orden y por tener datos de más. Otro problema a destacar es la incompatibilidad del servidor web, este problema se presenta debido a que cuando el equipo desarrollador del diseño del SIGA no tuvo una visión del crecimiento del sistema, lo cual origina que en la actualidad el software se encuentre un tanto desactualizado y por ende presentará posibles problemas a los intentos de actualizarlo.

Punto aparte es el tema de la seguridad, ya que actualmente un usuario con conocimientos intermedios puede acceder libremente con todos los permisos de la base de datos y por ende a la data que se maneja en el SIGA UNASAM, creando un problema de alto índole que se debe de tomar en consideración lo antes posible. Este problema también se debe a una falta de configuración del servidor proxy, que si se realizara óptimamente solucionaría problemas de seguridad, rendimiento y hasta conectividad. A su vez cabe mencionar que la base de datos del SIGA no posee un servidor propio, haciendo que este sea vulnerable puesto que está alojado dentro del servidor web.

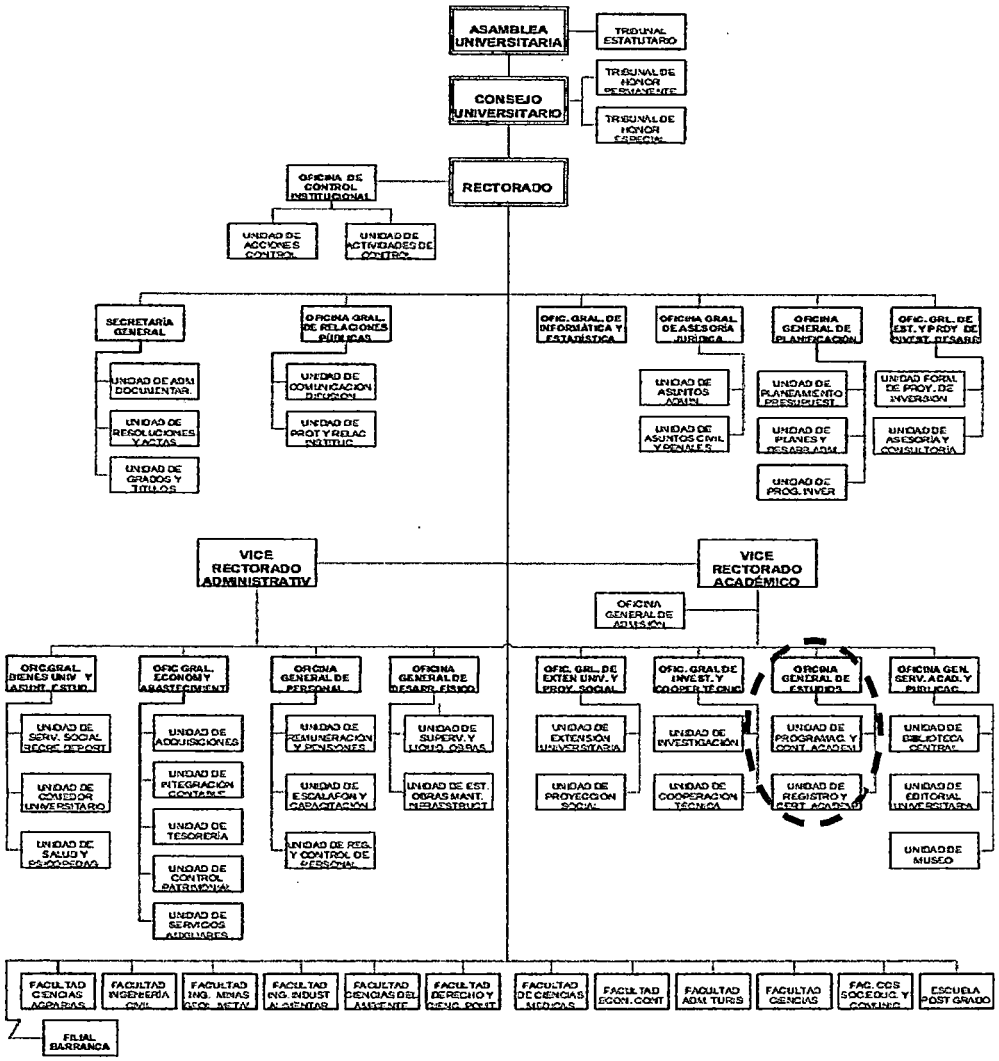
Esta es una breve descripción de la realidad problemática que atraviesa actualmente la OGE, realidad que se espera cambiar con la ayuda del proyecto. Como vemos la UNASAM presenta dificultades en el manejo de información y la seguridad de la misma, estos problemas deben de tener un tratamiento de manera rápida. Para hacer esto posible, la UNASAM debe de tomar en consideración la importancia de la seguridad de la información y los riesgos a los cuales están expuestos y no sólo en la OGE sino también en todas sus dependencias con el

objetivo de impulsar de una manera conjunta y coherente los diferentes elementos que ayudarán a su crecimiento y desarrollo institucional y tecnológico.

4.1.1. Análisis de organigrama funcional – estratégico

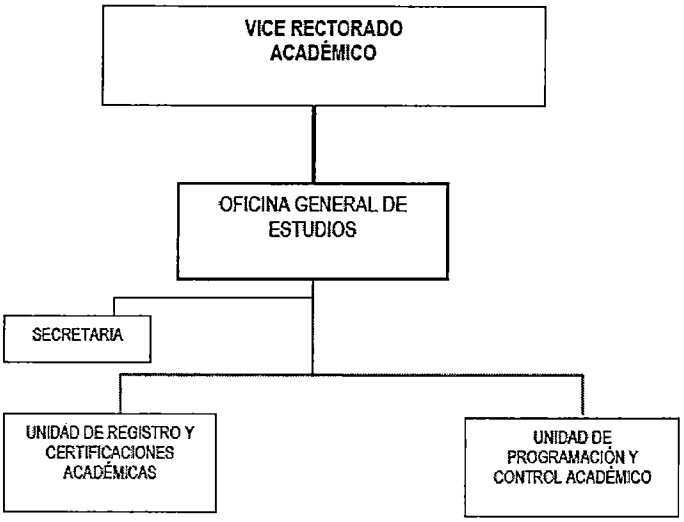
Para hacer un análisis del organigrama funcional, es necesario ubicar a la Oficina General de Estudios dentro del organigrama estructural de la UNASAM, como veremos a continuación:

Gráfico 4.1. Organigrama estructural



Fuente: Manual de Organización y Funciones - UNASAM

Gráfico 4.2. Organigrama estructural de la OGE



Fuente: Manual de Organización y Funciones - UNASAM

La Estructura Orgánica de la Oficina de Estudios es la siguiente:

Órgano de Dirección: Jefatura de la Oficina General de Estudios

Órganos de Línea:

- Unidad de Programación y Control Académico
- Unidad de Registro y Certificaciones Académicas

Órgano de Apoyo: Secretaria

La Oficina General de Estudios, es un Órgano de Apoyo del Vice Rectorado Académico encargada de programar, organizar y evaluar la gestión académica, el archivo y registro central académico, así como de apoyo a las Facultades. Su sigla es OGE. Entre sus funciones específicas encontramos dos puntos importantes que se relacionan directamente con el presente proyecto:

- Administrar la impresión, distribución y archivo de las actas de notas finales de todos los alumnos de la Universidad.

- Organizar y evaluar el proceso de registro del historial académico de todos y cada uno de los alumnos de la Universidad.
- Organizar el registro y control de todos los graduados y titulados, en coordinación con la Secretaría General, así como administrar las estadísticas académicas.

Pasando a sus unidades de línea, sus funciones son las siguientes:

Unidad de Programación y Control Académico: es la encargada de coordinar la evaluación del currículo y planes de estudios de las carreras profesionales, organizar y controlar la matrícula, generar los códigos de cursos, docentes y alumnos; organizar y supervisar el calendario, horarios y carga académica. Su sigla es UPCA

Unidad de Registro y Certificación Académica: es la encargada de llevar el registro historial de los alumnos, administrar las actas de notas finales y expedir los certificados de estudios. Su sigla es URCA.

4.1.2. Evaluación de la capacidad instalada

En el punto 4.1.1., hemos visto cómo se organiza orgánicamente la OGE y algunas de sus funciones más relevantes relacionadas con nuestros objetivos. En este ítem veremos la capacidad de la OGE para dar sostenibilidad a la propuesta de mejora que se plantea.

a. **Personal:** la OGE cuenta con el siguiente personal dentro de sus instalaciones (ver Cuadro 4.1.):

Cuadro 4.1. Cuadro orgánico de cargos

	N°	Denominación de la unidad orgánica y cargos estructurales	Total	Observaciones
JEFATURA	**1.**	Jefe de Oficina	1	Docente
	2.	Secretaria	1	Personal Administrativo
UNIDAD DE PROGRAMACIÓN Y CONTROL ACADÉMICO	**3.**	Jefe de la UPCA	1	Personal Administrativo
	4.	Analista de sistemas / Administrador de base de datos	1	Personal Administrativo
	5.	Alumnos practicantes	3	Alumnos de la UNASAM -
UNIDAD DE REGISTRO Y CERTIFICACIONES ACADÉMICAS	**6.**	Jefe de la URCA	1	Personal Administrativo
		TOTAL	**8**	

Fuente: Manual de Organizaciones y Funciones – UNASAM / Elaboración propia

De acuerdo a esta información, podemos afirmar que los recursos humanos con los que cuenta la OGE son suficientes para dar inicio a una adecuada gestión de riesgos y un mejor control en la información que maneja, ya que proporcionará mecanismos de control para evitar incidentes.

b. **Equipamiento Informático:** El equipamiento con el que cuenta la OGE es el siguiente:

Cuadro 4.2. Equipamiento informático de la OGE

N°	Equipamiento	Cantidad
1	Servidor Proliant ML370 G6	2
2	Computadora Personal Advance Core i7	2
3	Computadora Personal HP - Compaq - Core i7	6
4	Computadora Personal Qualcom - Quad Core	1
5	Computadora Personal - Pentium IV	1
6	Router Cisco 837	1
7	Router D-Link - DGS 1008D	1
8	Switch 3Com BASELINE SWITCH 2816 - 24 ptos 10/100/1000	1
9	Switch HP PRO CURVE 1410 - 24 ptos 10/100/1000	1
10	Switch HP - 16 ptos 10/100	1
11	Switch D-Link DGS 1008D - 8 ptos - 10/100/1000	1
12	Impresora Hp Laserjet P2055DN	3
13	Impresora Hp Laserjet P3015	1
14	Fotocopiadora Ricoh aficio MP 3350	1
15	Scanner Cannon Scanjet 3400C	1
16	HP Scanjet Enterprise 7500	1
17	Disco duro externo Toshiba 1 TB	1

Fuente: Elaboración propia

4.2. Identificación y descripción de requerimientos

Los órganos de Línea son la Unidad de Programación y Control Académico y el segundo órgano de línea es la Unidad de Registros y Certificaciones Académicas. Ambas unidades son las encargadas de llevar un control adecuado de la información académica de todo aquel que ha seguido estudios en la UNASAM.

La unidad en la cual se pondrá mayor énfasis será la Unidad de Programación y Control Académico ya que es en ella donde encontraremos al administrador de la base de datos del SIGA WEB, factor clave para ubicar los riesgos debido al grado de importancia de la información que maneja.

No menos importante es la Unidad de Registro y Control Académico, ya que la que tiene a su cargo las actas de notas de la universidad desde sus inicios, siendo un activo importante para la gestión de riesgos y un punto clave para tomar en cuenta la seguridad de la información.

4.2.1. Identificación de fuentes de información

a. **Encuestas a alumnos, personal docente y administrativo:** se aplicó una encuesta estructurada brindando las alternativas que nos ayuden a medir las variables definidas en el capítulo III. La muestra a aplicar es la siguiente:

Cuadro 4.3. Muestra total

N°	Descripción	Muestra
1	Alumnos	362
2	Personal docente	212
3	Personal administrativo	50
TOTAL		**624**

Fuente: Elaboración propia

De la encuesta que se aplicó (ver anexos), ésta se basó en el punto 4 de la ISO 27002:2008, lo cual nos ayuda a conseguir el segundo objetivo planteado y medir la V2: Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información. Además también se apoyará en las observaciones realizadas y en algunas acotaciones que puedan brindar las entrevistas efectuadas.

Cuadro 4.4. Preguntas de la encuesta alineadas al punto 4 de la ISO

Evaluación y Tratamiento del Riesgo	**Preguntas de la Encuesta**	
	Alumnos	**Docentes y Administrativos**
Evaluando los Riesgos de Seguridad	Pregunta 4	Pregunta 4
	Pregunta 5	Pregunta 5
	Pregunta 6	Pregunta 6
	Pregunta 7	Pregunta 7
	Pregunta 10	Pregunta 10
	Pregunta 12	Pregunta 12
	Pregunta 14	Pregunta 14
	Pregunta 15	Pregunta 15
	Pregunta 16	Pregunta 16
	Pregunta 17	Pregunta 17
	Pregunta 18	Pregunta 18
Tratamiento de los Riesgos de Seguridad	Pregunta 8	Pregunta 8
	Pregunta 9	Pregunta 9
	Pregunta 11	Pregunta 11
	Pregunta 13	Pregunta 13
	Pregunta 19	Pregunta 19
	Pregunta 20	Pregunta 20
	Pregunta 21	Pregunta 21
		Pregunta 22

Fuente: Elaboración propia

b. **Entrevistas al personal de la OGE:** entrevista al personal de la OGE (ver anexo), teniendo mayor ahínco en el Jefe de la Oficina y al Administrador de la Base de Datos. Estas entrevistas conjuntamente con las observaciones ayudará a tener un mayor conocimiento de la situación actual de la OGE en cuanto a su nivel de seguridad de la información y ver qué medidas han optado hasta el momento y que controles se deberán de seguir a partir de ello. Las entrevistas nos ayudarán a conseguir los objetivos 1 y 2, además de proporcionarnos datos suficientes para la medición de las variables V1 y V2.
   V1: Diagnóstico de la situación actual
   V2: Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información.

c. **Inventario de activos y controles en la OGE (Magerit):** Los activos son importantes en toda organización, y en esta oficina no es la excepción. Tener un listado de activos nos permitirá obtener el riesgo al que están expuestos ellos. Una vez entendido esto nos permitirá proponer los controles y las medidas necesarias a tomar en cuenta para disminuir el riesgo. Todo ello nos ayuda a conseguir el objetivo 1 y además nos dará los datos para la medición de la variable V1.
   V1: Diagnóstico de la situación actual

Cuadro 4.5. Activos OGE

Tipo	Código	Activo
Bienes de información	BI-01	Actas
	BI-02	Resoluciones
	BI-03	Oficios
Bienes físicos	BF-01	SERVIDOR Proliant ML370 G6-SQL Server (BD y Aplicación)

	BF-02	SERVIDOR Proliant ML370 G6- Firewall - ClearOs
	BF-03	Computadora Personal Advance Core i7
	BF-04	Computadora Personal HP - Compaq - Core i7
	BF-05	Computadora Personal HP - Compaq - Core i7
	BF-06	Computadora Personal HP - Compaq - Core i7
	BF-07	Computadora Personal Qualcom - Quad Core
	BF-08	Computadora Personal - Pentium IV
	BF-09	Computadora Personal HP - Compaq - Core i7
	BF-10	Computadora Personal HP - Compaq - Core i7
	BF-11	Computadora Personal HP - Compaq - Core i7
	BF-12	Computadora Personal Advance Core i7
	BF-13	Router Cisco 837
	BF-14	Router D-Link - DGS 1008D
	BF-15	Switch 3Com BASELINE SWITCH 2816 - 24 ptos 10/100/1000
	BF-16	Switch HP PRO CURVE 1410 - 24 ptos 10/100/1000
	BF-17	Switch HP - 16 ptos 10/100
	BF-18	Switch D-Link DGS 1008D - 8 ptos - 10/100/1000
	BF-19	Impresora Hp Laserjet P2055DN
	BF-20	Impresora Hp Laserjet P2055DN
	BF-21	Impresora Hp Laserjet P2055DN
	BF-22	Impresora Hp Laserjet P3015
	BF-23	Fotocopiadora Ricoh aficio MP 3350
	BF-24	Scanner Cannon Scanjet 3400C
	BF-25	HP Scanjet Enterprise 7500
	BF-26	Disco duro externo Toshiba 1 TB
Bienes de Software	BS-01	SIGA - Web
	BS-02	SQL Server 2008 R2

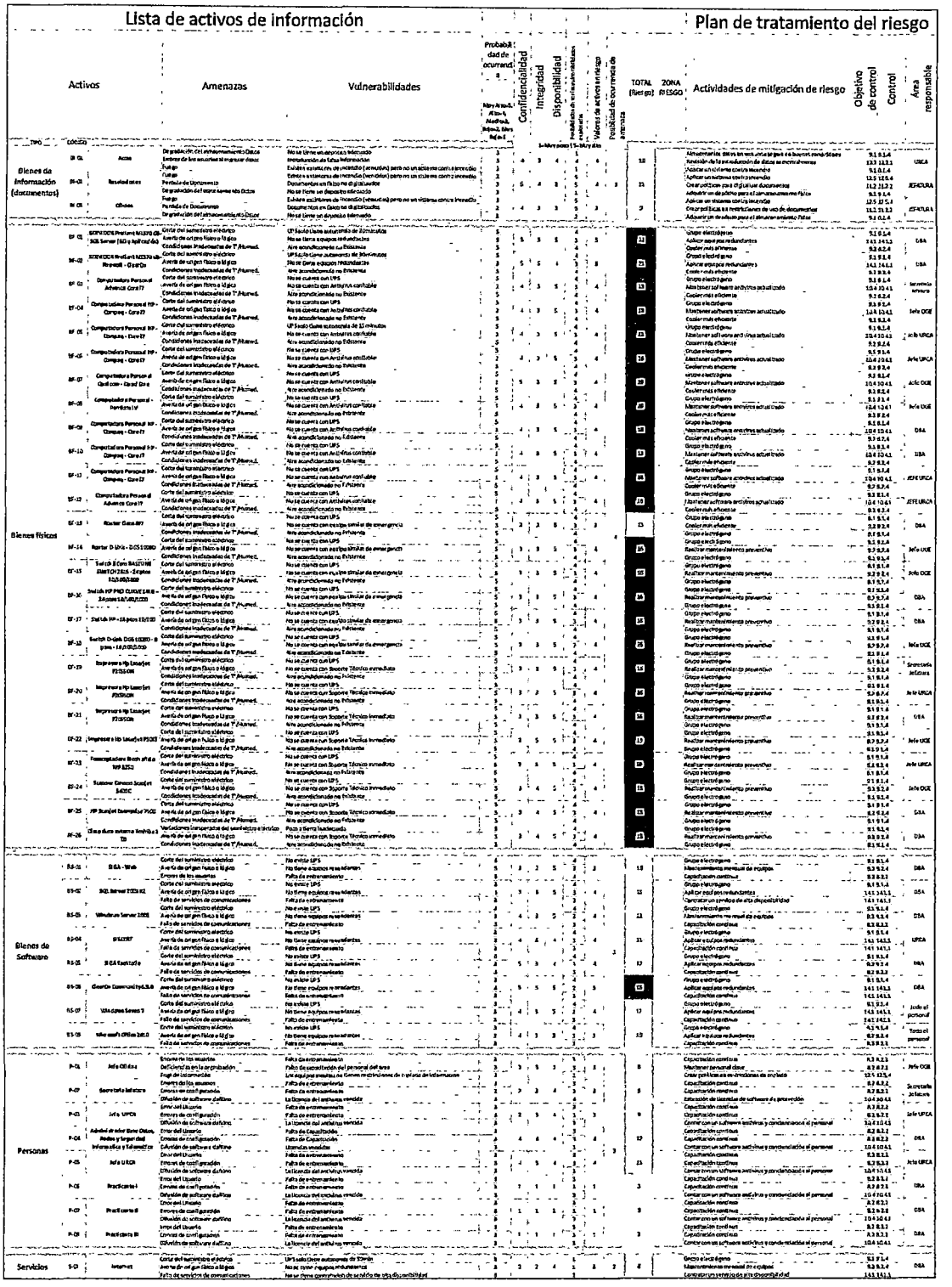
	BS-03	Windows Server 2008
	BS-04	SISCERT
	BS-05	SIGA
	BS-06	ClearOs Community 6.5.0
	BS-07	Windows Seven 7
	BS-08	Microsoft Office 2010
Personas	P-01	Jefe Oficina
	P-02	Secretaria Jefatura
	P-03	Jefe UPCA
	P-04	Administrador Base Datos, Redes y Seguridad Informática y Telemática
	P-05	Jefe URCA
	P-06	Practicante I
	P-07	Practicante II
	P-08	Practicante III
Servicios	S-01	Internet

Fuente: Elaboración propia

Una vez identificados los activos relevantes con los que cuenta la OGE, se realiza un análisis y evaluación de los mismos para poder determinar a qué amenazas están expuesto y posteriormente determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo. Todo ello nos lleva a estimar el riesgo (definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza).

En el siguiente cuadro podremos visualizar todo esto que nos propone MAGERIT para gestionar el riesgo, ya aplicado a los activos de la OGE.

Cuadro 4.6. Tasación de activos de OGE (Consultar CD adjunto para una mejor visualización. Archivo: Inventario de activos y controles – OGE o ver Anexo 10)



Fuente: Elaboración propia

4.3. Diagnóstico de la situación actual

4.3.1. Informe de diagnóstico

De los análisis de la situación actual que enfrenta la OGE, observamos deficiencias en la seguridad de la información por lo que es necesario y urgente dar los controles necesarios que ayuden a mitigar los incidentes y dar frente a las amenazas y vulnerabilidades que se presenten. Cabe recalcar que la información que maneja esta oficina es de importancia para toda la comunidad universitaria así que cualquier amenaza podría tener un enorme impacto en cuanto a la realización de las actividades académicas con normalidad. Además se deberá de tener en cuenta también mejoras en equipamiento y software, como también en las instalaciones donde se encuentra.

Punto aparte está mencionar el papel que cumplen los usuarios en todo esto, como veremos en el Capítulo V, el nivel de conocimiento de los usuarios sobre seguridad de la información es vago o escaso y no le toman la importancia del caso. En base a esto también se debe considerar educar al usuario en estos temas y así podamos reducir los riesgos no solo para la OGE sino para toda la UNASAM.

4.3.2. Medidas de mejoramiento

Lo que se propone ante la situación actual de la Oficina General de Estudios es un diagnóstico y una propuesta de mejora para la gestión de riesgos tomando en cuenta estándares que nos permitan seguir ciertos criterios para enfrentar las amenazas, tal es el caso de la ISO/IEC 27002:2008 y MAGERIT. En cuanto a la ISO, aun no es certificado pero propone alternativas ante las amenazas a la seguridad de la información de cualquier

entidad, alternativa y medida que permitirán dar mayor seguridad a los usuarios y a la comunidad Santiaguina en general.

En cuanto al equipamiento informático de la oficina, se recomienda actualizar sus equipos de cómputo, especialmente para aquellos que serán los administradores del sistema, así como también tomarle la atención necesaria a los activos que posee la OGE ya que como vemos en el siguiente gráfico el nivel de riesgo es alto, especialmente en lo que concierne a los bienes físicos que posea. Las medidas a tomar se verán en el siguiente capítulo.

Riesgo=Probabilidad*Impacto

Cuadro 4.7. Niveles de Riesgo

Riesgo			
1	2	1	Aceptable
3	7	2	Tolerable
8	14	3	Intolerable
15	25	4	Extremo

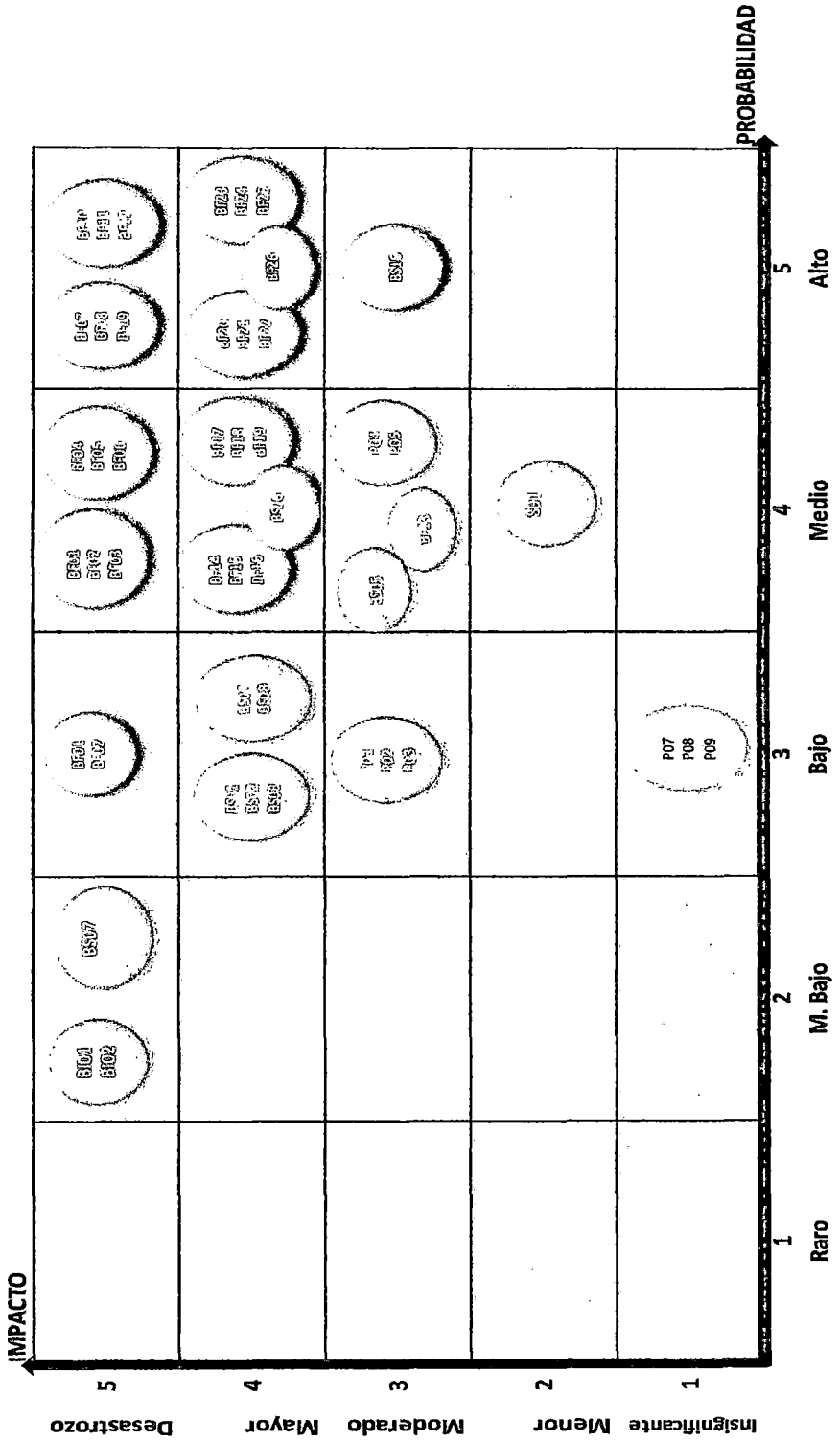
Fuente: MAGERIT versión 3.0

Cuadro 4.8. Matriz de calificación de riesgo

Desastrozo	Impacto	5		5	10	15	20	25
Mayor		4		4	8	12	16	20
Moderado		3		3	6	9	12	15
Menor		2		2	4	6	8	10
Insignificante		1		1	2	3	4	5
	Riesgos			1	2	3	4	5
				Probabilidad				
				Raro	M. Bajo	Bajo	Medio	Alto

Fuente: MAGERIT versión 3.0

Gráfico 4.3. Mapa de riesgos de la OGE (Consultar CD adjunto para una mejor visualización. Archivo: Mapa de Riesgo)



Fuente: Elaboración propia

CAPITULO V: DISEÑO DE LA SOLUCIÓN

5.1. Controles de seguridad

Los controles de seguridad son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos. El objetivo de control en tecnologías de información se define como una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de tecnología de información particular.

El gobierno de las tecnologías de información se define como una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre las tecnologías de información y sus procesos.

Lo que es necesario recalcar aquí es que los controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo. Es der, que de esta actividad surgirá la primera decisión acerca de los controles que se deberán abordar.

Cabe aclarar que la ISO 27002:2008 proporciona una buena base de referencia, no siendo exhaustivo, por lo tanto se pueden seleccionar más aún. Es decir, estos controles que proporciona son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control. Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, deberán de ser incluidas.

Los controles que propone la norma son los siguientes:

A.5 Política de seguridad

A5.1 Política de seguridad de la información

A.6 Organización de la información de seguridad

A.6.1 Organización interna

A.6.2 Terceros

A.7 Administración de recursos

A.7.1 Responsabilidad por los activos

A.7.2 Clasificación de la información

A.8 Seguridad de los recursos humanos

A.8.1 Antes del empleo

A.8.2 Durante el empleo

A.8.3 Terminación o cambio de empleo

A.9 Seguridad física y del entorno

A.9.1 Áreas aseguradas

A.9.2 Seguridad del equipo

A.10 Administración de las comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades operativas

A.10.2 Gestión de servicios de terceros

A.10.3 Planeamiento y aceptación de sistemas

A.10.4 Protección contra código malicioso y código móvil

A.10.5 Respaldo

A.10.6 Gestión de seguridad de redes

A.10.7 Manipulación de medios

A.10.8 Intercambio de información

A.10.9 Sistemas de información de negocios

A.10.10 Monitoreo

A.11 Control de accesos

A.11.1 Requisito de negocios para el control de acceso

A.11.2 Gestión del acceso de usuarios

A.11.3 Responsabilidades de los usuarios

A.11.4 Control del acceso a redes

A.11.5 Control de acceso al sistema operativo

A.11.6 Control del acceso a aplicación e información

A.11.7 Computación móvil y teletrabajo

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.12.1 Requisitos de seguridad para sistemas de información

A.12.2 Procesamiento correcto en aplicaciones

A.12.3 Controles criptográficos

A.12.4 Seguridad de archivos del sistema

A.12.5 Seguridad en los procesos de desarrollo y soporte

A.12.6 Gestión de vulnerabilidades técnicas

A.13 Administración de los incidentes de seguridad

A.13.1 Reportes de eventos y debilidades de seguridad de la información

A.13.2 Gestión de incidentes y mejoras de seguridad de la información

A.14 Administración de la continuidad de negocio

A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocios

A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)

A.15.1 Cumplimiento de requisitos legales

A.15.2 Cumplimiento de las políticas y normas de seguridad, y cumplimiento técnico

A.15.3 Consideraciones de auditoria de sistemas de información

Ver Anexo 01 para observar con mayor detenimiento cada uno de estos controles que propone la ISO 27002:2008.

5.2. Diseño de la funcionalidad de la solución

La solución que usaremos ante nuestro problema será la metodología MAGERIT es una metodología de análisis y gestión de riesgos, la cual permite llevar a cabo:

- El análisis de riesgos de cualquier tipo de sistema de información o de sus elementos, conjuntando en un índice único (el "riesgo") las estimaciones de sus vulnerabilidades ante las amenazas y del impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización.
- La gestión de los riesgos, basada en los resultados obtenidos en el análisis anterior, seleccionando las medidas o "salvaguardas" (controles) de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles prejuicios.

Esta metodología propone para el análisis de riesgos las 4 etapas siguientes:

- La etapa 1, Planificación del análisis y gestión de riesgos, establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos. (Capítulo 1)
- La etapa 2, Análisis de riesgos, permite identificar y valorar las entidades que intervienen en el riesgo. (Capítulo 4)
- La etapa 3, Gestión de riesgos, permite identificar las funciones o servicios de salvaguarda reductores del riesgo detectado. (Capítulo 4)
- La etapa 4, Selección de salvaguardas, permite seleccionar los mecanismos de salvaguarda que hay que implementar.

El análisis de riesgos de este proyecto abarco las etapas 2, 3 y 4. La etapa 1 fue desarrollada en cierta manera en el capítulo 1 de este proyecto.
En el caso de la Etapa 4, a continuación veremos algunas salvaguardas a tomar en cuenta para contrarrestar las amenazas:

5.2.1. Identificación de salvaguardas

- **Protecciones Generales**: A continuación las salvaguardas que fueran escogidas::
  - Se requiere autorización previa: Pertenece al grupo de Restricción de acceso a la información que a su vez pertenece al Control de Acceso Lógico. La razón se escogió esta salvaguarda ya que las personas pueden acceder a los activos inclusive los más importantes. La misma por que hace frente a las amenazas a las que están expuestos los activos. Y esta pueda ser aplicada a estas clases de activos: Datos/ Información, Servicios, Aplicaciones (software), Equipamiento informático(hardware), Redes de comunicaciones y Soportes de información
  - Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad
  - Hace frente a las siguientes amenazas: Errores de los usuarios, Errores del administrador del sistema/ de la seguridad, Difusión de software dañino, Errores de secuencia, Alteración de la información, Fugas de información, Vulnerabilidad de los programas (software), Errores de mantenimiento /actualización de programas (software), Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Uso no previsto, Alteración de secuencia, Acceso no autorizado, Modificación de la información, Revelación de información y Manipulación de hardware
  - Herramienta contra código de dañino: La OGE no posee una herramienta contra código dañino, pero toma como medida a esto la prueba de código antes de ser implantada alguna modificación en la base de datos o el sistema. Además de ello también se plantean las siguientes salvaguardas:
    - El programa se actualiza regularmente
    - La base de datos de virus se actualiza regularmente

- Se revisan los programas y servicios de arranque del sistema

Estas salvaguardas solo pueden ser aplicado a la capa de: Aplicaciones (software), y hacen frente al siguiente amenaza: Difusión de software dañino

- **Protecciones de las Aplicaciones Informáticas:** Se seleccionó las siguientes salvaguardas ya que la OGE no posee estas normas de seguridad como son:
  - Se dispone de normativa sobre el uso autorizado de las aplicaciones
  - Se dispone de normativa relativa al cumplimiento de los derechos
  - Se controla la instalación de software autorizado y productos con licencia
  - Se dispone de procedimientos para realizar copias de seguridad
  - Se aplican perfiles de seguridad: esta salvaguarda se encuentra a medias porque existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema pero gracias a esta salvaguarda podemos hacer frente a estas amenazas : Errores de los usuarios , Difusión de software dañino, Vulnerabilidad de los programas (software),Errores de mantenimiento/actualización de programas (software) y Uso no previsto Se debería tratar de cumplir con lo siguiente:
    - Seguridad de los ficheros de datos de la aplicación
    - Se protegen los ficheros de configuración
    - Seguridad de los mecanismos de comunicación entre procesos

  Donde se asegura las dimensiones de seguridad como confidencialidad e integridad
  - Además de que se debe de llevar un Control de versión de toda actualización de software, ayuda a saber que cualquier software que posea la empresa esté libre de errores y hacer frente amenazas como son: Vulnerabilidades de los programas (software) y Errores de

mantenimiento /actualización de programas (software).

- **Protección de los Equipos Informáticos (HW):** A continuación las salvaguardas adecuadas para la protección de los equipos.
  - Se dispone de normativa sobre el uso correcto de los equipos
  - Se dispone de procedimientos de uso de equipamiento
  - Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la OGE minimiza amenazas como son: Errores del administrados del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

  Además se debe de tener en cuenta con estas salvaguardas al momento de utilizar los equipos como son:
  - Protección física de los equipos: son mecanismos que la empresa no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el Servidor de Datos
    - Para evitar accesos innecesarios
    - Para evitar acceso no autorizados
  - Seguridad del equipamiento de oficina

  Después de evaluar las salvaguardas antes mencionadas se debe implantar las siguientes salvaguardas:
  - Se evalúa el impacto en la confidencialidad de los datos
  - Se evalúa el impacto en la integridad de los datos

  Ninguna de estas salvaguardas posee la OGE como son:
  - Se priorizan las actuaciones encaminadas corregir riesgos elevados
  - Se mantiene en todo momento la regla de "seguridad por defecto"
  - Se debe de controlar: Reproducción de documentos

- **Protección de las comunicaciones:** se han escogido las siguientes salvaguardas para minimizar riesgos:

- Se deben de aplicar perfiles de seguridad : para garantizar la comunicación en la empresa y para hacer frente amenazas como:, Errores de secuencia, Alteración de la información, Uso no previsto, Alteración de secuencia y Acceso no autorizado, además proteger las dimensiones de seguridad : integridad , confidencialidad y autenticidad.
- La empresa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado
- Ni siquiera de mecanismos como son :
  - Comprobación de origen y destino
  - Mecanismos de control
- No tiene ninguna: Seguridad de los servicios de red

Todas las salvaguardas anteriormente desplegadas hacen frente a la amenaza de Acceso no autorizado.

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear siguiente salvaguardas:

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas anti spyware
- Se deshabilitan las "cookies" en los navegadores
- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del trafico
- Se toman medidas frente a la inyección de información espuria
- Se aplica la regla de "seguridad por defecto"
- Se requiere autorización para que medios y dispositivos que tengan acceso a redes y servicios

- **Protección de los Soportes de Información:** para proteger el único activo se han escogido las salvaguardas más apropiadas:
  - Proteger en uso de contenedores cerrados
  - Disponer de normativa de relativa a la protección criptográfica de los contenidos

- **Elementos Auxiliares :**
  - Se asegura la disponibilidad como:
    - ✓ Siguiendo las recomendaciones del fabricante o proveedor
    - ✓ Continuidad de operaciones: para asegurar las disponibilidad de los equipos auxiliares además para contrarrestar la amenaza de contaminación medioambiental
    - ✓ Climatización: La adecuada climatización de cada equipo ayuda a enfrentar la amenaza que tiene la mayoría de estos componentes que es: Condiciones inadecuadas de temperatura o humedad.

- **Protección de las Instalaciones:**
  - Se dispone de normativa de seguridad para la seguridad de las instalaciones.
  - Se dispone de áreas específicas para equipos informáticos , para protegerlos de la Ocupación enemiga
  - Además de la Protección del perímetro y reforzar la Vigilancia en las instalaciones de la OGE.
  - Protección frente a siniestros

- **Gestión del Personal:** Se deben de crear las siguientes normas de seguridad:
  - Se dispone de normativa relativa a la gestión de personal(materia de seguridad)

- Se dispone de procedimientos para la gestión de personal(materia de seguridad)
- Creación de normas del personal: Propio y Subcontratado
- Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
- Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos, frente ataques de cómo Extorsión y Ataque desde el interior
- Procedimientos relevantes de seguridad: Emergencias, incidencias.

Después de haber realizado esta tarea tendremos la Declaratoria de Aplicabilidad que es documento formal donde constan las salvaguardas necesarias para proteger los activos de la OGE.

CAPITULO VI: CONSTRUCCIÓN DE LA SOLUCIÓN

6.1. Construcción

6.1.1. Gestión de Riesgos

Después de haber realizado el análisis de riesgos queda a la vista los impactos y los riesgos a los que está expuesta la OGE.

Lo que ha llegado a una calificación de cada riesgo significativo, determinándose si:

- ✓ Es extremo en el sentido de que requiere atención urgente.
- ✓ Es intolerable en el sentido de que requiere atención.
- ✓ Es tolerable en el sentido de que pueda ser objeto de estudio para su tratamiento.
- ✓ Es aceptable en el sentido de que no se van a tomar acciones para atajarlo.

El resultado de análisis es solo un análisis. A partir de que disponemos de información para tomar decisiones conociendo lo que se quiere proteger (activos valorados, de qué lo queremos proteger – amenazas valoradas) y que demos por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.[5]

6.1.2. Plan de Seguridad

Trata de cómo llevar a cabo planes de seguridad, con el fin de materializar las decisiones adoptadas para el tratamiento de los riesgos.

---

[5] *Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 45*

Para ello se identifican 3 tareas:

- Identificación de proyectos de seguridad
- Plan de ejecución
- Ejecución

a. Identificación de proyectos de Seguridad

El objetivo de esta tarea es:

Elaborar un conjunto integral de programas de seguridad

"Un programa seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con objetivo en común, bien porque se trata de tareas que competen a una única unidad acción"[6]

Esta tarea se va a realizar 3 actividades:

- Normativas de Seguridad
- Eliminar fallos de seguridad evidentes
- Clasificación del inventario (SW,HW, Soportes de Información, Elementos auxiliares)[7]

i. Normativas de Seguridad

- ✓ Documentación del uso autorizado de las aplicaciones

---

[6] *Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método*, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 74

[7] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua*, Tesis Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato , julio del 2012 ,p .138

- Se considerara una falta que el personal instale cualquier tipo de programa (Software) en sus computadoras, que sea para fines personales o de recreación.
- Para prevenir infecciones por virus informáticos, el personal deberá evitar hacer uso de cualquier clase de software no proporcionado por la OGE.
- El personal está obligado a verificar que la información y que los medios de almacenamiento, considerando memorias USB, CDs, estén libres de cualquier tipo de software dañino, para ello deben ejecutar el software antivirus.

✓ Documentación del uso correcto de equipos de equipos informáticos

- Al personal que se le asigne un equipo informático deberá hacerse cargo del mismo
- Los empleados no deberán mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos. Solo el personal adecuado podrá realizarlo.
- Mientras se utilizan los equipos de cómputo, no se podrá consumir alimentas o ingerir líquidos, solo si son botellas de plástico.
- Evitar colocar objeto encima del equipo o cubrir los orificios de ventilación.
- Mantener el equipo informático en un entorno limpio y sin humedad.
- Solo el personal apropiado podrá llevar a cabo los servicios y reparaciones al equipo informático.
- En caso de que existe descompostura por maltrato por descuido negligencia por parte del responsable, estará

obligado a cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

- ✓ Documentación del resguardo y protección de la información
  - El uso de CDs, memorias USB o disco duro eterno, es exclusivo para respaldos de información. El personal encargado es el responsable de su resguardo.
  - El personal encargado deberá respaldar de manera periódica la información sensible y critica que se encuentren en sus equipos de cómputo del que hagan uso.

- ✓ Documentación del uso de servicios de internet
  - Para el uso del correo electrónico el personal de la OGE no debe de usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.
  - Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos (concernientes a la OGE) como información que es de propiedad de la OGE.
  - Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
  - El acceso a internet es exclusivamente para actividades relacionadas con las necesidades del puesto y función que desempeña.

- ✓ Documentación de protección de las instalaciones
  - Establecer normas de conducta cuando estén cerca del servidor, lugares de trabajo, etc. además de cumplir todas las normas de sanidad y seguridad existentes para las instalaciones de la OGE.

- ✓ Documentación de la gestión del personal
  - En cada contrato de trabajo se deberá incluir cláusulas de confidencialidad para asegurar la información de la OGE.
  - Aquel personal que utilice los bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información.
  - Que cada empleado deberá cumplir con un horario de trabajo.
  - Establecer normas de conducta de los empleados para formar un ambiente laboral adecuado y respetuoso entre todos.

ii. Eliminar fallos de seguridad evidentes

El lugar donde se encuentra los servidores de base de datos no cuenta con una instalación adecuada ya que no han seguido ninguna estándar de seguridad. Por lo que se puedo observar, no cuenta con una ventilación adecuada además que el UPS solo brinda 30 minutos de carga. Se encuentra ubicados en la oficina del administrador de la base de datos, la cual no posee muchos controles de seguridad para el ingreso al mismo. Además si hubiera un incendio no cuenta extinguidores y no maneja redundancia del equipo.

Las contraseñas que son empleadas, solo son de conocimiento del administrador de la base de datos, las cuales se sugiere que sean cambiadas en periodos determinados.

iii. Clasificación del inventario (SW, HW, Soportes de Información, Elementos auxiliares)

La OGE no contaba con un inventario donde se clasificaba a cada uno de sus activos de una manera más detallada como se lo ha realizado en este proyecto, ya que el único inventario con el que cuentan a la mano es el Inventario Físico de Bienes el cual se realiza de manera anual y está a cargo de la Oficina de Patrimonio.

b. Plan de Ejecución

El objetivo de esta tarea es:

Ordenar temporalmente los programas de seguridad

Para llegar un plan de seguridad optimo se ha llegado a lo siguiente orden de los programas de seguridad.

- Eliminar fallos de seguridad evidentes
- Clasificación del inventario(SW,HW, Soportes de Información, Elementos auxiliares)
- Normativas de Seguridad[8]

c. Ejecución

Esta actividad recoge la serie de proyectos que materializan el plan de seguridad y que se van realizando según dicho plan de acuerdo a lo analizado.[9]

---

[8] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua*, Tesis Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato , julio del 2012 ,p .140

[9] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas*

6.2. Pruebas

Como parte de este punto de la solución a plantear para la Gestión de Riesgos dentro de la OGE, es hacer uso de la herramienta P.I.L.AR., que nos puede ayudar a efectuar las pruebas pertinentes.

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología Magerit.

Esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un Análisis de Riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

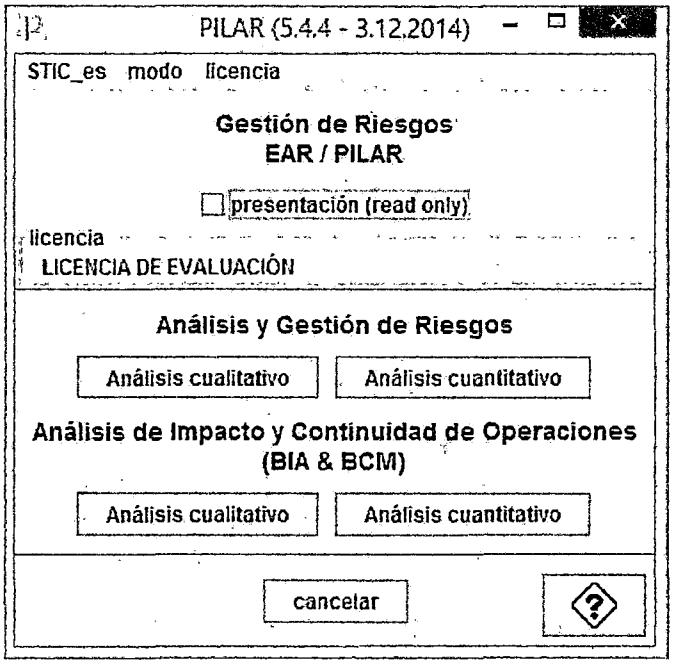
---

de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua, Tesis Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato , julio del 2012 ,p .140

"Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema."[10]

PILAR puede hacer análisis cuantitativo y cualitativo.

Gráfico 6.1. Herramienta PILAR 5.4.4



Fuente: Captura de pantalla del software

Los resultados se presentan en diversos formatos como son: gráficas y tablas donde se pueden incorporar hojas de cálculo.

Como vemos esta herramienta nos brinda una solución práctica para la gestión de riesgos, además podrá ser utilizada por la misma oficina para obtener datos necesarios conforme va cambiando su situación actual y las salvaguardas necesarias para la protección de sus activos.

---

[10] *Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 125*

CAPITULO VII: IMPLEMENTACIÓN

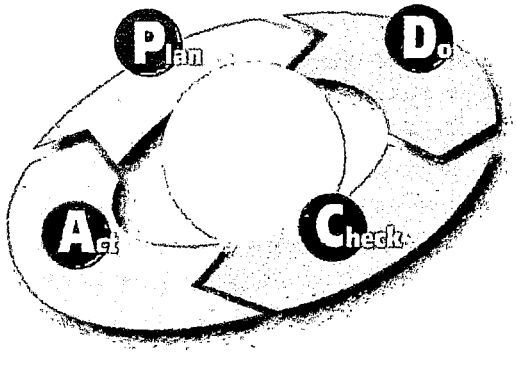
7.1. Monitoreo y Evaluación de la Solución

7.1.1. Elementos del Monitoreo y Evaluación

Las acciones de monitoreo se realizarán más eficientemente cuando las actividades, recursos y activos relacionados se gestionen como un proceso, para ello se debe tener identificado la interacción entre los mismos. Además se deberá tener en cuenta las medidas preventivas a tomar y llevar un registro de los mismos. Para llevar un control de todo esto, se propone realizarlo a través del ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, = planificar-hacer-verificar-actuar). Es una estrategia de mejora continua de la calidad en cuatro pasos, que tienen por función:

a. Toma de datos y registro en las tablas respectivas
b. Contrastación de los datos contra el nivel esperado de cumplimiento
c. Decisión respecto de las acciones correctivas o de retroalimentación necesarias de acuerdo a la información obtenida
d. Implementación de las acciones correctivas o de retroalimentación

Gráfico 7.1. Ciclo de Deming



Fuente: http://es.wikipedia.org/wiki/Archivo:PDCA_Cycle.svg

7.1.2. Plan de Monitoreo y Evaluación

El Plan de monitoreo y evaluación debe necesariamente dar respuesta al menos a las siguientes interrogantes: ¿Cómo se va a recoger la información?, ¿Quién va a recogerla?, ¿Cuándo se va a obtener?, ¿Cómo se va a analizar la información recogida?, ¿Quién la va a analizar?, ¿Cuándo se va a hacer el análisis?, ¿Quién va a recibir los resultados?, ¿En qué formato se van a distribuir?

7.2. Bitácora y puesta a punto

Para el registro de las observaciones, ideas, datos, avances y obstáculos en el desarrollo de las actividades que se llevan a cabo durante el proyecto, se empleó el siguiente cuadro para consolidar las condiciones bajo las cuales se desarrolló el proyecto.

Cuadro 7.1. Bitácora para el desarrollo del proyecto

Fecha	Etapa	Actividad	Observación
Del 01/09/2014 Al 28/11/2014	Análisis	Identificar fuentes de información	Se realizó de acuerdo a lo planificado
		Recopilar información	Se realizó de acuerdo a lo planificado
		Organizar información	Se realizó de acuerdo a lo planificado
		Analizar la información	Se realizó de acuerdo a lo planificado

Del 01/12/2014 Al 31 /12/2014	Diseño	Plantear controles de seguridad	Se realizó de acuerdo a lo planificado
		Identificar Salvaguardas	Se realizó de acuerdo a lo planificado
	Construcción	Gestión de Riesgos	Se realizó de acuerdo a lo planificado
		Establecer un Plan de seguridad	Se realizó de acuerdo a lo planificado

Fuente: Elaboración propia

Una vez implementada la propuesta de mejora para la gestión de riesgos, haberse hecho el monitoreo correspondiente y realizadas las pruebas necesarias, la puesta en operatividad dependerá de la adaptación al cambio de los actores principales y a las consideraciones del jurado calificador.

CAPITULO VIII: RESULTADOS

Después de haber aplicado nuestros instrumentos para la recolección de información y nuestras herramientas en el procesamiento de la misma, notamos por medio de los resultados la realidad que vive la OGE en cuanto refiere al tema de seguridad de la información.

La muestra a trabajar estadísticamente está dividida en tres sectores, Docentes y/o Administrativos, Alumnos. Además se realizaron entrevistas al jefe de la OGE y al administrador de la base de datos; de la cual mostramos resultados de manera detallada obtenidos al procesar la información:

8.1. Docentes y/o Administrativos, descripción de resultados

Datos obtenidos de docentes y/o administrativos de la encuesta realizada en las diversas facultades de la UNASAM. Modelo de encuesta, (Ver Anexo 3).

- ✓ En la pregunta 2, notamos que del 100% de nuestra muestra encuestada el 70% fueron varones y los otros 30% restantes fueron mujeres.
- ✓ En la pregunta 4, notamos que el 88 % de los encuestados apagan debidamente los equipos informáticos después de utilizarlos, mientras que un 12% no realiza adecuadamente esta acción. Del porcentaje que respondieron SI, el 71% de ellos efectúa esta acción de manera correcta la cual es dirigiéndonos al botón de inicio.
- ✓ En las preguntas 5, 6, 7, 8 y 9, apreciamos que el 75% no se siente seguro en los ambientes donde se encuentran los equipos informáticos, el 75% no observo extintor cerca de los equipos informáticos, el 69% no observo ninguna señalización, el 73% no tiene conocimiento de un adecuado manejos del extintor, el 88% no participo de ningún simulacro frente a desastres específicamente en áreas donde hay equipos informáticos, quedando así la diferencia porcentual por cada una de las preguntas.

- ✓ En la pregunta 10, notamos que el 71% manipuló alguna vez los componentes del equipo asignado a su persona de manera que si este sufrió algún inconveniente, busco hacerlo funcionar correctamente y el 29% restante no intento por ningún motivo manipular los componentes de su equipo asignado.
- ✓ En la pregunta 11, vemos que el 88% asumiría una responsabilidad si se le detecta realizando actividades sospechosas como el ingreso a lugares restringidos, y el 12% restante no asumiría responsabilidad alguna.
- ✓ En la preguntas 12, pudimos notar que el 57% siempre hace uso de los antivirus, ya sea ingresando o extrayendo información en algún dispositivo de almacenamiento, el 32% lo hace a veces y el 10% restante nunca los hace.
- ✓ En la pregunta 13, percibimos que el 50% activa el antivirus, el 31% lo activa, detecta y elimina, el 15% hace otras cosas menos las acciones correctas y el 4% restante no sabe qué hacer.
- ✓ En la pregunta 14, nótese que el 79% notó que el antivirus no funciona adecuadamente ya que no se encuentra actualizado, y el 21% restante observo que tiene un buen funcionamiento y una adecuada actualización.
- ✓ En la pregunta 15, vemos que el 86% hace uso del SIGA WEB UNASAM, en la pregunta 16, vemos que un 16% siempre hace uso del SIGA, el 66% casi siempre lo usa y un 3% no hace uso de él.
- ✓ En las preguntas 17, 18 y 19, vemos que el 41% tiene por clave valores poco frecuentes, y un 69% no comparte con nadie su clave y un 53% no cambia su clave de acceso.
- ✓ En la pregunta 20, percibimos que nadie considera que el acceso al SIGA WEB UNASAM es más rápido dentro de la universidad que dentro de ella, un 68% señala que es más lento dentro de la universidad que fuera de ella y un 18% indica que la velocidad para acceder al SIGA es la misma ya sea dentro o fuera de la universidad.
- ✓ En la pregunta 21, observamos que el 87% no cuenta con ningún tipo de capacitación acerca de seguridad de la información, el 13% restante si no se capacito tiene algún conocimiento acerca del tema.

- ✓ En la pregunta 22, notamos que al 100% de los encuestados les gustaría tener mayor conocimiento acerca de seguridad de la información, de los cuales el 57% le gustaría conocer acerca del tema por medio de charlas y conferencias, el otro 43% a través de otros medios como folletos, foros por el portal y como parte de algún curso.
  (Ver Anexo 7 para visualizar las tablas y gráficos estadísticos)

8.2. Alumnos, descripción de resultados

Datos obtenidos de los alumnos de la encuesta realizada en las diversas facultades de la UNASAM. Modelo de encuesta, (Ver Anexo 2).

- ✓ En la pregunta 1, notamos que del 100% de nuestra muestra encuestada el 48% fueron mujeres y los otros 52% restantes fueron varones.
- ✓ En la pregunta 4, notamos que el 89 % de los encuestados apagan debidamente los equipos informáticos después de utilizarlos, mientras que un 11% no realiza adecuadamente esta acción. Del porcentaje que respondieron SI, el 59% de ellos efectúa esta acción de manera correcta la cual es dirigiéndonos al botón de inicio.
- ✓ En las preguntas 5, 6, 7 y 8, pudimos notar que el 67% no se siente seguro en los ambientes donde se encuentran los equipos informáticos, el 76% no observo extintor cerca de los equipos informáticos, el 73% no observo ninguna señalización, el 75% no participo de ningún simulacro frente a desastres específicamente en áreas donde hay equipos informáticos, quedando así la diferencia porcentual por cada una de las preguntas.
- ✓ En la pregunta 9, notamos que el 61% manipulo alguna vez los componentes del equipo informático de manera que si este sufrió algún inconveniente, busco hacerlo funcionar correctamente y el 39% restante no intento por ningún motivo manipular los componentes del equipo asignado.
- ✓ En las preguntas 10 y 11, vemos que un 89% a 80% se siente responsable y/o identifica con el equipo informático que usa o usarán en algún momento

dentro de la UNASAM, y de un 11% a 20% restante no se identifica, menos asumiría responsabilidad alguna.

- ✓ En la preguntas 12, pudimos notar que un 28% siempre hace uso de los antivirus, ya sea ingresando o extrayendo información en algún dispositivo de almacenamiento, el 53% lo hace a veces y el 19% restante nunca los hace.
- ✓ En la pregunta 13, percibimos que un 18% activa el antivirus, mientras que un 43% activa el antivirus, lo detecta y elimina, el 19% hace otras cosas menos las acciones correctas y el 16% restante no sabe qué hacer.
- ✓ En la pregunta 14, nótese que el 86% notó que el antivirus no funciona adecuadamente, ya que, no se encuentra actualizado y/o activado, y el 14% restante observo que tiene un buen funcionamiento y una adecuada actualización.
- ✓ En la pregunta 15, vemos que el 4% siempre accede a la información que proporciona el SIGA WEB UNASAM, mientras que el 77% lo hace casi siempre y un 20% no accede.
- ✓ En las preguntas 16, 17 y 18, vemos que el 31% de los encuestados tienen como referencia su nombre y apellido para acceder al SIGA WEB UNASAM, un 71% no comparte con nadie su clave y un 70% nunca cambia su clave de acceso ya que no lo veían como una acción importante.
- ✓ En la pregunta 19, percibimos que un 12% considera que el acceso al SIGA WEB UNASAM es más rápido dentro de la universidad que dentro de ella, un 45% señala que es más lento dentro de la universidad que fuera de ella y un 43% indica que la velocidad para acceder al SIGA es la misma ya sea dentro o fuera de la universidad.
- ✓ En la pregunta 20, observamos que el 97% no cuenta con ningún tipo de capacitación acerca de seguridad de la información, el 3% restante si no se capacito tiene algún conocimiento acerca del tema.
- ✓ En la pregunta 21, notamos que el 87% le gustaría tener mayor conocimiento acerca de seguridad de la información, de los cuales el 39% le gustaría conocer acerca del tema por medio de charlas y conferencias, el otro 54% a

través de otros medios como folletos, foros por el portal y como parte de algún curso.

(Ver Anexo 7 para visualizar las tablas y gráficos estadísticos)

8.3. Jefe de la Oficina General de Estudios

Datos obtenidos de la entrevista realizada al jefe de la Oficina General de Estudios de la UNASAM. Modelo de entrevista, (Ver Anexo 4)

Según los datos obtenidos en la entrevista realizada al Ing. Einer Espinoza Muñoz, jefe de la Oficina General de Estudios, se obtuvo lo siguiente:

Indicó que la UNASAM no cuenta con un comité encargado de la seguridad de la información. Se reveló que a la necesidad de proteger los activos de la OGE ha establecido algunas normas, procedimiento y mecanismos de control elaborados en base a sus conocimientos conseguidos a través de su larga experiencia, y según sus análisis previos serían los más apropiados para salvaguardar los equipos y los activos de información que se transmiten por la red de la universidad, todo ello en un trabajo coordinado con el administrador de la base de datos, ya que es él quien tiene mayor conocimiento al respecto al ser de la especialidad de Ingeniería de Sistemas e Informática.

Referente a los mecanismos de control nos dijo que no existen documentos formales por lo que lo han estado manejando conforme se presentaba alguna incidencia. En cuanto al control de los trabajadores con respecto al tema de seguridad de la información, ha proporcionado cuentas de usuarios pero con acceso restringido, esto se hace posible de manera coordinada con el administrador de la base de datos ya que es él quien genera esos permisos. Con lo que respecta al acceso al área donde se encuentran los servidores no hay un registro del mismo, pero a ésa área acceden solo personas autorizadas y

previamente identificadas ya que hay usuarios que hacen solicitud de información y se dirige ahí mediante previa presentación de oficios.

Con lo concerniente a las políticas de seguridad de la información, no hay un documento donde éstas estén especificadas, esto lo atribuye a un factor presupuestal y a una falta de cultura institucional dentro de la UNASAM. Pese a ello manifiesta que es de suma urgencia la elaboración de dicha políticas de seguridad de la información dentro de la UNASAM y que se priorice la oficina a su cargo ya que la información que maneja es de suma importancia para la comunidad universitaria.

En cuanto al nivel de conocimiento de seguridad de la información por parte de su personal, nos indica que ellos no tienen conocimiento de cuáles son los activos más importante que se deben de proteger en relación a la información ante cualquier desastre natural, provocado o humano. Hasta ahora no lo había considerado como un factor importante, dando prioridad a otras actividades que competen a la dependencia que dirige. A pesar de ello hay iniciativa de realizarlo en un futuro.

Los problemas más frecuentes que se presentan en la OGE son con respecto al SIGA WEB UNASAM, ya que los usuarios hacen pedidos de modificaciones pasada la fecha establecida. La mayoría de los cambios de datos dentro del sistema que se maneja, son registrados en oficios, resoluciones y archivos genéricos. En el caso de cambios que se realizan en la estructura o codificación del sistema no son registrados pero si hay procedimientos para efectuar estos cambios (se prueban los cambios de manera local).

Sobre el mantenimiento de los equipos, no hay un plan de mantenimiento y este se efectúa únicamente cada vez que se requiere y en el caso del tema del antivirus es visto directamente por la Oficina General de Informática y Estadística, y en el

caso de que se desee adquirir software o hardware también lo trabajan directamente con esta oficina.

8.4. Administrador de la Base de Datos

Datos obtenidos de la entrevista realizada al Administrador de la Base de Datos. Modelo de entrevista, (Ver Anexo 5)

Según los datos obtenidos en la entrevista realizada al Ing. Paul Elbin Pohl Cáceres, administrador de la base de datos, se obtuvo lo siguiente:

Él es el único responsable directo de ésa área, trabaja de manera coordinada con el jefe de la oficina y con los practicantes que ingresan por cada semestre.

Con lo que respecta al uso del antivirus dentro de esta dependencia, hacen uso del antivirus Kaspersky el cual es actualizado anualmente y esta tarea corresponde directamente a la Oficina General de informática y Estadística ya que es la encargada de velar que todas las oficinas de la UNASAM cuenten con ello.

En cuanto a los inconvenientes que se puedan presentar en esta área, solo se presentan inconvenientes informáticos los cuales son informados inmediatamente al jefe de la oficina y el tiempo en darles solución depende de la magnitud del problema.

La capacitación a usuarios para que hagan un buen uso de la información que maneja el SIGA WEB UNASAM, estaba a cargo de la UPCA – OGE, pero esto ya no se realiza hace dos años porque no ha habido cambios bruscos en el sistema. En el caso de los nuevos usuarios no presentan mayor problema para hacer uso del sistema y quizás el único problema que tienen ellos es sobre la clave de acceso.

La UNASAM, no se ha preocupado por capacitarlo en temas concernientes a la seguridad de la información. Ante este hecho el administrador de la base de datos se ha visto en la obligación de capacitarse por sus propios medios a manera de autoaprendizaje. Para afrontar desastres naturales o humanos ha adquirido los conocimientos necesarios por su propia cuenta y mediante la experiencia en trabajos anteriores. No hay proyectos o mejoras en mente con respecto a la seguridad de la información, pero si los hay de otra envergadura como es la incorporación de nuevos sistemas.

No existen manuales o documentos donde se especifiquen los controles para la seguridad de la información así como tampoco hay documentación sobre políticas de seguridad, pero considera necesario e importante el establecimiento de todo ello para evitar la pérdida o corrupción de la información que maneja.

En cuanto al manejo de la base de datos, lo administra únicamente él, ya que este acceso de nivel administrador, por seguridad debe ser de conocimiento de una sola persona y así también evita el acceso a personas ajenas que pueden ocasionar colapsos en el sistema. El acceso por parte de otras personas se maneja a través de claves de autenticación. Es importante también la realización de backups siendo esta realizada de manera manual, diario (dentro del mismo servidor) y semanal (en un disco duro externo). Esta información no sale de las instalaciones de la UNASAM. No hay un procedimiento documentado para realizar esta acción.

Los problemas más frecuentes a los cuales se enfrenta son: instalaciones inadecuadas que dificultad el trabajo, cortes de internet, cortes de fluido eléctrico. No hay un archivo para el registro de estos problemas y tampoco hay estrategias establecidas para afrontarlas, siendo cada problema manejado al instante y con los medios que cuenten en ese momento.

Las modificaciones que se hacen a los servicios que otorga el sistema a los usuarios no son registrados, pero si hay un procedimiento interno para efectuarlas,

primero se realizan pruebas internas y una vez se compruebe su funcionalidad se efectúan los cambios en el sistema de manera general para todos los usuarios.

Cuenta con el apoyo de los practicantes para proponer mejoras al sistema, cada uno de ellos es responsable del software que desarrolla. No hay un control de calidad para la producción del software que se aplique, lo cual puede ocasionar que el software no cumpla con las expectativas de los usuarios. Cada miembro del equipo posee una copia del software que desarrolla y se les orienta sobre su responsabilidad, ética y confiabilidad al poseer esta información.

Por último nos indica que sí cuenta con los equipos necesarios para realizar sus actividades así como también con el software adecuado, éste último es proporcionado por la Oficina General de Informática y Estadística. Además para evitar la posible intrusión de algún agente malicioso externo, se maneja restricciones a través de la red, evitando el acceso a cierto tipo de contenidos.

8.5. Resultados y variables:

a. Variable 1: Diagnóstico de la situación actual

Cuadro 8.1. Operacionalización variable 1

Objetivos Específicos	Variable	Dimensión	Indicador	Item
Diagnosticar el nivel de la Gestión de Riesgos la Oficina	V1: Diagnóstico de la situación actual	Gestión de riesgos	Políticas de Seguridad	Entrevistas al personal de la OGE
			Gestión de activo	Entrevistas al personal de la OGE

General de Estudios.			Amenazas y Vulnerabilidades	Aplicación MAGERIT

Fuente: Elaboración propia

Como podemos observar la dimensión de la V1 es la gestión de riesgos, dentro de la cual tenemos 3 indicadores los cuales fueron puestos a prueba con la ayuda de cada uno de los ítems. Ahora veremos los resultados reflejados por cada indicador de la variable:

Cuadro 8.2. Resultados variable 1

Indicador	Resultados
Políticas de Seguridad	De las entrevistas realizadas al personal de la OGE, especialmente al Jefe de Oficina y al Administrador de la Base de Datos, se puede observar que no hay políticas de seguridad claras, es decir si bien es cierto toman algunas medidas de seguridad, éstas se dan conforme se presentan situaciones o según sus propios conocimientos se los determinen. No hay una política establecida y por ende no hay un documento que especifique la misma.
Gestión de activo	De las entrevistas realizadas al personal de la OGE, se pudo obtener que no hay una adecuada gestión de activos con los que cuenta. Aún presenta deficiencias, entre las que se puede señalar que hay una inadecuada distribución de los mismos, hay carencia de señalización en los ambientes en los que se encuentran los activos, no hay capacitación a los empleados respecto a la gestión de activos, etc.

Amenazas y Vulnerabilidades	Para este indicador se aplicó MAGERIT a los activos con los que cuenta la OGE. Los resultados obtenidos del mismo reflejan que una gran cantidad de sus activos, especialmente los bienes físicos, están en un nivel alto de riesgo siendo considerado este como Extremos. Esto nos muestra claramente que las amenazas están presentes y por ende los activos son vulnerables ante cualquier incidencia, pudiendo ocasionar que la oficina no brinde un adecuado servicio a los usuarios o que este falle en cualquier momento.

Fuente: Elaboración propia

b. **Variable 2:** Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información

Cuadro 8.3. Operacionalización de la variable 2

Objetivos Específicos	Variable	Dimensión	Indicador	Item
Obtener información real sobre la situación actual de la seguridad de la información de la Oficina General de Estudios.	V2: Controles contenidos en la ISO/IEC 27002:2008 para la seguridad de la información.	Evaluando los riesgos de seguridad	Conocimientos sobre los riesgos	Encuesta a alumnos, docentes y administrativos: Preguntas 4, 5, 6, 7, 10, 12, 14, 15, 16, 17, 18
				Entrevistas al personal de la OGE
				Observaciones

		Tratamiento de los riesgos de seguridad	Cómo enfrentan los riesgos los usuarios	Encuesta a alumnos, docentes y administrativos : Preguntas 8, 9, 11, 13, 19, 20, 21, 22
				Entrevistas al personal de la OGE
				Observaciones

Fuente: Elaboración propia

Como podemos observar en el caso de la V2 encontramos dos dimensiones y cada uno con su respectivo indicador los cuales fueron puestos a prueba con la ayuda de cada uno de los ítems. Ahora veremos los resultados reflejados por cada dimensión en indicados correspondiente:

Cuadro 8.4. Resultados variable 2

Dimensión	Indicador	Resultados
Evaluando los riesgos de seguridad	Conocimientos sobre los riesgos	En el caso de los usuarios encuestados (alumnos, docentes y administrativos), los resultados reflejaron que en su mayoría tienen poco conocimiento de los riesgos a los cuales se enfrenta la información. Fue importante obtener este resultado, ya que para mantener la integridad de la información que maneja la OGE, también

		se debe de involucrar en cierta medida a los usuarios. En el caso del personal de la OGE entrevistado, si son conscientes de los riesgos a los cuales está expuesta la información que manejan. De las observaciones que se pudo realizar, hay mucho que hacer para que tanto los usuarios como el personal de la OGE tengan los conocimientos necesarios de los riesgos.
Tratamiento de los riesgos de seguridad	Cómo enfrentan los riesgos los usuarios	En el caso de los usuarios (alumnos, docentes y administrativos), si bien es cierto no todos han sido capacitados pero gran parte de ellos hace frente a los riesgos que se puedan presentar pero todo ello lo hacen de manera empírica. En el caso del personal de la OGE que fue entrevistado, han tomado algunas medidas preventivas ante las amenazas que se han presentado. Pero como mencionamos en el cuadro anterior, todo ello no está debidamente documentado o estandarizado. De las observaciones que se realizaron, tanto los usuarios como el personal de la OGE hacen frente a los riesgos dependiendo como se presenten y muchos de ellos se valen de conocimientos adquiridos de la propia experiencia.

Fuente: Elaboración propia

c. **Variable 3:** Propuesta de mejora

Cuadro 8.5. Operacionalización de variable 3

Objetivos Específicos	Variable	Dimensión	Indicador	Item
Proponer estrategias de mejora para la seguridad de la información de la Oficina General de Estudios.	V3: Propuesta de mejora	Definición de controles y estrategias para la seguridad de la información	Políticas, procedimientos y controles	Alineados a la ISO/IEC 27002:2008

Fuente: Elaboración propia

En el caso de la V3, se proponen mejoras para la seguridad de la información de la OGE, así como también para una adecuada gestión de riesgos. Estos controles y medidas se trataron en el capítulo V de la tesis.

CAPITULO IX: DISCUSIÓN DE RESULTADOS

Este proyecto abarcó lo que es gestión de riesgos de la Oficina General de Estudios de la UNASAM, por ser una de las dependencias con activos de información importantes para la institución, que si fallan en cualquier momento pueden ocasionar problemas e inconvenientes en el desarrollo normal de los procesos académicos. A pesar de ello se ha observado que hasta el momento no se ha puesto mayor esfuerzo en lo que respecta la gestión de riesgos.

A lo largo de este trabajo se han observado estudios e información sobre el tema en cuestión, pero generalmente una gestión de riesgo viene desde uno de las dependencias que no deben de faltar en cualquier organización o institución que este en crecimiento, esta dependencia es conocida mayormente como Área de Informática o Taller de Informática, siendo esta un actor clave para la gestión de riesgos ya que no solo abarca una oficina, sino toda la organización en general, además debe ser ella la encargada de proponer las políticas y controles necesarios. A pesar que nos encontramos en una etapa donde la información es importante, poco o nada se hace para salvaguardarlo y protegerla de los riesgos y amenazas a los que se ven expuestos diariamente. La función de un el área mencionada no se limita solo a reparar computadoras o actualizar antivirus, sino va mucho más allá de ello, es un actor clave para proponer el cambio en las organizaciones y concientizar a proteger uno de los bienes más preciados el cual es la información.

Se espera que a partir de este proyecto se tome conciencia sobre las amenazas, vulnerabilidades y riesgos a los que están expuestos los activos y se empiece por implantar políticas de seguridad, salvaguardas y controles, empezando por cosas que pueden parecer pequeñas pero que pueden formar parte de un cambio.

CONCLUSIONES

- ✓ La mejora de los procesos académicos de la OGE se verán evidenciadas una vez se apliquen las medidas para una correcta gestión de riesgos la cual abarca las salvaguardas elegidas, controles establecidos y el plan de seguridad para la OGE.

- ✓ Al evaluar el nivel de riesgo de los activos de la OGE, se aprecia que en su mayoría de ellos están entre un estado de intolerable y extremo riesgo. Gracias a la metodología Magerit se siguió una serie de puntos para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la OGE donde se supo escoger que medidas serán necesarias para mitigar el riesgo.

- ✓ La situación actual de la seguridad de la información de la Oficina General de Estudios se podría catalogar como deficiente, ya que hasta el momento no ha tomado controles o medidas alineadas a algún estándar o metodología. No tiene medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro. Además se considera que también se debe hacer partícipes a los usuarios de estas medidas que puedan adoptar.

- ✓ Después de haber realizado este proyecto, la OGE obtendrá un documento encaminado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para el personal que labora en sus instalaciones, así como también se incluirá la participación de los usuarios.

RECOMENDACIONES

- ✓ Se recomienda que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.

- ✓ Se sugiere al jefe de la OGE, que conjuntamente con el personal a su cargo, implementen las salvaguardas que fueron escogidas.

- ✓ Para reducir los riesgos que existen en los activos de la OGE se debería de pensar en trabajar conjuntamente con la Oficina General de Informática y Estadística, ya que ésta posee un taller de cómputo capaz de atender estas necesidades.

- ✓ Asimismo de capacitar al personal para que se cumplan las normas de seguridad establecidas en el plan que se emplearon en la gestión de riesgos.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Bautista, José de Jesús. «Auditoría en informática.» *Universidad Nacional Autónoma de México Web site.* 2005. http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/6/1664.pdf (último acceso: 18 de Mayo de 2014).

Alvarez Basaldúa, Luis Daniel. *Seguridad en informática (Auditoría de sistemas).* Tesis de maestría, México D.F.: Universidad Iberoamericana, 2005.

Ampuero Chang, Carlos Enrique. *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros.* Tesis de grado, Lima: Pontificia Universidad Católica del Perú, 2011.

Barranco de Areba, Jesús. *Metodología del análisis estructurado de sistemas.* España: Universidad Pontificia Comillas, 2001.

Camacho Gomez, Pedro Daniel, y Wilmer Nilton Ramos Arrieta. *Metodología táctica para la implantación de sistemas de información basado en métrica y COBIT.* Tesis de grado, Lima: Universidad Nacional Mayor de San Marcos, 2010.

Cano, Jeimy J. «La gerencia de la seguridad de la información: evolución y retos emergentes.» *ISACA Web site.* Octubre de 2011. http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx (último acceso: Diciembre de 2014).

Cedillo Viera, Franklin Manuel, Carlos Alberto Desiderio Calderón, y Douglas Junior Quintero Vinces. *Análisis, diseño e implementación del módulo de control de procesos de gestión y apoyo del sistema estratégico de calidad de compulead S.A.* Tesis de grado, Guayaquil: Escuela Superior Politécnica del Litoral, 2009.

Consejo Nacional de Ciencia y Tecnología - CONACYT. «Definición de auditoría y revisión de control.» *Consejo Nacional de Ciencia y Tecnología - CONACYT Web site.* 2012. http://www.conacyt.gob.mx (último acceso: 18 de Mayo de 2014).

Córdova Rodríguez, Norma Edith. *Plan de seguridad informática para una entidad financiera.* Trabajo monográfico para titulación, Lima: Universidad Nacional Mayor de San Marcos, 2003.

CSIRT - CV Centre de Seguretat TIC de la Comunitat Valenciana. «Doce medidas básicas para la seguridad informática.» *CSIRT - CV.* 2010. http://www.csirtcv.gva.es (último acceso: Setiembre de 2014).

Duque Ochoa, Blanca Rubiela. *Metodologías de Gestión de Riesgos (Octave, Magerit, DAFP).* Tesis de grado, Caldas: Universidad de Caldas, 2010.

Erb, Markus. «Gestión de riesgo en la seguridad informática.» *Protejete Web Site.* 2010. https://protejete.wordpress.com (último acceso: 18 de Mayo de 2014).

Espinoza Aguinaga, Hans Ryan. *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Tesis de grado, Lima: Pontificia Universidad Católica del Perú, 2013.

Ferrero Recaséns, Eduardo. *Análisis y gestión de riesgos del servicio IMAT del sistema de formación de I.C.A.I.* Proyecto fin de carrera, Madrid: Universidad Pontificia Comillas, 2006.

Hernández Sampieri, Roberto, Carlos Fernández Collado, y María del Pilar Baptista Lucio. *Metodología de la investigación.* México D.F.: McGraw-Hill/Interamericana Editores, S.A. de C.V., 2010.

ITERA It & business process. «¿Qué es COBIT?» *ITERA Web site.* 2010. http://www.itera.com.mx/itinstitute/mails/chile/cobit.htm (último acceso: 18 de Mayo de 2014).

Larrondo Quirós, Agustín. *Uso de la norma ISO/IEC 27004 para auditoría informática.* Proyecto fin de carrera, Madrid: Universidad Carlos III de Madrid, 2010.

Mañas, José Antonio. *Gestión de riesgos, análisis y tratamiento. Diapositivas.* Madrid, Marzo de 2006.

Martínez Saravia, Víctor Enrique. *Concienciación en seguridad de la información, la estrategia para fortalecer el eslabón más débil de la cadena.* Tesis de maestría, Bogotá D.C.: Fundación Universitaria Iberoamericana, 2010.

Ministerio de Hacienda y Administraciones Públicas. «MAGERIT - versión 3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).» *Portal de Administración Electrónica.* Octubre de 2012. http://administracionelectronica.gob.es (último acceso: Setiembre de 2014).

Pallas Mega, Gustavo. *Metodología e implantación de un SGSI en un grupo empresarial jerárquico.* Tesis de maestría, Montevideo: Universidad de la República, 2009.

Pressman, Roger S. *Ingeniería del software.* México D.F.: McGraw-Hill Interamericana Editores, S.A. de C.V., 2010.

Quees.info. «¿Qué es la informática?» *Quees.info Web Site.* 2013. http://www.quees.info/que-es-la-informatica.html (último acceso: 18 de Mayo de 2014).

Ripoll Ripoll, José Ismael. «Unidad Docente de Sistemas Operativos del Departamento de Informática de Sistemas y Computadores de la Universidad Politécnica de Valencia.» *Unidad Docente de Sistemas Operativos del Departamento de Informática de Sistemas y Computadores de la Universidad Politécnica de Valencia Web site.* 3 de Noviembre de 2014. http://web-sisop.disca.upv.es/gii-ssi/seguridad_es.pdf (último acceso: 5 de Noviembre de 2014).

Tirado Goyeneche, Erickson Jesús. *Análisis de riesgos Universidad Francisco de Paula Santander.* Plan de Gestión de Riesgos, Cúcuta: Universidad Francisco de Paula Santander, 2012.

United States Computer Emergency Readniness Team (US - CERT). «Consejos y pautas para la seguridad informática (Cyber Securoty Tips).» *United States Computer Emergency Readniness Team.* Agosto de 2013. https://www.us-cert.gov/ncas/tips (último acceso: Noviembre de 2014).

Universidad Francisco de Paula Santander. «Seguridad Informática - MAGERIT.» *Universidad Francisco de Paula Santander Wikispaces.* 2014. http://seguridadinformaticaufps.wikispaces.com/MAGERIT (último acceso: 18 de Mayo de 2014).

Universidad Nacional Autónoma de México. *Auditoría en informática.* Apuntes, México: Universidad Nacional Autónoma de México, 2010.

Universidad Nacional del Nordeste. «¿Qué es seguridad?» *Universidad Nacional del Nordeste Web Site.* 2002. http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm (último acceso: 18 de Mayo de 2014).

Villena Aguilar, Moisés Antonio. *Sistema de gestión de seguridad de información para una institución financiera.* Tesis de grado, Lima: Pontificia Universidad Católica del Perú, 2006.

ANEXOS

Anexo 1

A.5 Política de seguridad		
A.5.1 Política de seguridad de la información Objetivo: Proveer dirección y soporte de la dirección para la seguridad de la información conforme a los requisitos del negocio, las leyes y reglamentos pertinentes.		
A.5.1.1	Documento de política de seguridad de la Información	Control El documento de política de seguridad de la información deberá ser aprobado por Gerencia, y publicado y comunicado a todos los empleados y terceros pertinentes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información deberá revisarse a intervalos planeados o si ocurren cambios significativos, para asegurar la continuidad de su propiedad, adecuación y efectividad
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la Gerencia con la seguridad de la Información.	Control La Gerencia deberá apoyar activamente la seguridad dentro de la organización mediante una dirección clara, compromiso demostrado, delegación explícita, y reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de seguridad de la información	Control Las actividades de seguridad de la información deberán coordinarse con los representantes de diferentes partes de la organización que tengan funciones y trabajos pertinentes.
A.6.1.3	Aplicación de responsabilidades de seguridad de la información	Control Todas las responsabilidades de seguridad de la información deben definirse claramente.
A.6.1.4	Proceso de autorización para instalaciones de procesamiento de información.	Control Deberá definirse e implementarse un proceso de autorización de gerencia para nuevas instalaciones de procesamiento de la información.

A.6.1.5	Convenios de confidencialidad	Control Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la información deberán ser identificados y revisados periódicamente.
A.6.1.6	Contacto con las autoridades	Control Deberán mantenerse contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con los grupos de interés especial	Control Deberán mantenerse contactos apropiados con los grupos de interés especial u otros foros especializados de seguridad y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización a la gestión de la seguridad de la información (objetivos de control, controles, políticas, procesos, y procedimientos de seguridad de la información) deberá revisarse independientemente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.
A.6.2 Terceros Objetivo: Mantener la seguridad de la información y de las instalaciones de procesamiento de información de la organización, que son accesadas, procesadas, comunicadas a terceros, o administradas por terceros.		
A.6.2.1	Identificación de los riesgos relacionados con terceros.	Control Deberán identificarse los riesgos para la información e instalaciones de procesamiento de información de la organización, provenientes de procesos de negocios que involucran a terceros, e implementarse controles adecuados antes de conceder acceso.
A.6.2.2	Enfocar la seguridad en el trato con los clientes	Control Deberán enfocarse todos los requisitos de seguridad identificados antes de darles a los clientes acceso a la información o activos de la organización.
A.6.2.3	Enfocar la seguridad en los convenios con terceros.	Control Los convenios con terceros que involucren acceder, procesar, comunicar o administrar la información o instalaciones de procesamiento de información de la organización, o agregar productos o

		servicios a dichas instalaciones, deberán abarcar todos los requisitos de seguridad pertinentes
A.7 Gestión de activos		
A.7.1 Responsabilidad por los activos Objetivo: Alcanzar y mantener una protección adecuada de los activos de la organización.		
A.7.1.1	Inventario de activos	Control Todos los activos deberán identificarse claramente y efectuarse y mantenerse un inventario de todos los activos importantes.
A.7.1.2	Propiedad de activos	Control Toda la información y activos relacionados con instalaciones de procesamiento de información deberán tener un 'dueño'2 que sea un miembro designado de la organización.
A.7.1.3	Uso aceptable de los activos	Control Deberán identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos relacionados con las instalaciones de procesamiento de información.
A.7.2 Clasificación de la información Objetivo: Asegurar que la información reciba el nivel de protección adecuado.		
A.7.2.1	Pautas de clasificación	Control La información deberá clasificarse en función de su valor, requisitos legales, sensibilidad y criticabilidad para la organización.
A.7.2.2	Rotulación y manipulación de la información	Control Deberá prepararse e implementarse un conjunto de procedimientos adecuados para la rotulación y manipulación de la información, de acuerdo al esquema de clasificación adoptado por la organización.
A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros entiendan sus responsabilidades y sean adecuados para las funciones en las que se les ha considerado, así como reducir el riesgo de robo, estafa o mal uso de las instalaciones		
A.8.1.1	Funciones y responsabilidades	Control Las funciones y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceros deberán definirse y documentarse de acuerdo a la política de seguridad de información de la organización.
A.8.1.2	Tamizaje	Control

		Deberá efectuarse la verificación de antecedentes de todos los candidatos a empleo, contratistas, y usuarios de terceros, conforme a las leyes, reglamentos y ética pertinentes, y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y a los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceros deberán aceptar y firmar los términos y condiciones de su contrato de empleo, el cual deberá indicar sus responsabilidades de seguridad de la información así como las de la organización.
A.8.2 Durante el empleo		
Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceros conozcan las amenazas y problemas de seguridad de la información, así como sus responsabilidades y obligaciones, y estén capacitados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano.		
A.8.2.1	Responsabilidades de la Gerencia	Control La Gerencia exigirá que los empleados, contratistas y usuarios de terceros apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos por la organización.
A.8.2.2	Concientización, educación y entrenamiento de seguridad de la información	Control Todo el personal de la organización y, cuando sea pertinente, los contratistas y usuarios de terceros, deberán recibir el entrenamiento de concientización adecuado y actualizaciones periódicas de políticas y procedimientos de la organización, según corresponda a sus funciones de trabajo.
A.8.2.3	Proceso disciplinario	Control Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
A.8.3 Terminación o cambio de empleo Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros salgan de una organización o cambien de empleo en forma ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Deberán definirse y asignarse claramente las responsabilidades para efectuar la terminación del empleo o cambio de empleo.
A.8.3.2	Devolución de activos	Control

		Todos los empleados, contratistas y usuarios de terceros deberán devolver todos los activos de la organización en su poder al terminar su empleo, contrato o convenio.
A.8.3.3	Retiro de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a la información y a las instalaciones de procesamiento de información deberán retirarse al terminar su empleo, contrato o convenio, o modificarse según el cambio.
A.9 Seguridad física y ambiental		
A.9.1 Áreas aseguradas Objetivo: Impedir el acceso físico no autorizado, daños e interferencias en los locales y la información de la organización.		
A.9.1.1	Perímetro de seguridad físico	Control Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información.
A.9.1.2	Controles de ingreso físico	Control Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado.
A.9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Control Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones.
A.9.1.4	Protección contra amenazas exteriores y ambientales	Control Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
A.9.1.5	Trabajo en áreas aseguradas	Control Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado.
A.9.1.6	Acceso público, áreas de entrega y carga	Control Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de

		procesamiento de información para evitar el acceso no autorizado.
A.9.2 Seguridad del equipo Objetivo: Impedir la pérdida, daño, robo o compromiso de activos así como interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección del equipo	Control El equipo deberá ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
A.9.2.2	Servicios de soporte	Control El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte.
A.9.2.3	Seguridad del cableado	Control El cableado de energía y telecomunicaciones que conduzca datos o soporte los servicios de información deberá estar protegido de intercepción o daño.
A.9.2.4	Mantenimiento del equipo	Control El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera de las instalaciones	Control Deberá aplicarse seguridad al equipo fuera de las instalaciones, teniendo en cuenta los diversos riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Eliminación o reutilización segura del equipo	Control Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre escritura apropiada de cualquier información sensible y "software" autorizado antes de su eliminación.
A.9.2.7	Remoción de propiedad	Control No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.
A.10 Gestión de comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operativas Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información.		
A.10.1.1	Procedimientos operativos documentados	Control Los procedimientos operativos deberán documentarse, mantenerse y ponerse a

		disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de los cambios	Control Se controlarán los cambios en las instalaciones y sistemas de procesamiento de información.
A.10.1.3	Separación de deberes	Control Los deberes y áreas de responsabilidad deberán separarse para reducir las oportunidades de modificación no autorizada o inadvertida o mal uso de los activos de la organización.
A.10.1.4	Separación de instalaciones de desarrollo, prueba y operaciones	Control Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo.
A.10.2 Gestión de servicios de terceros Objetivo: Implementar y mantener el nivel adecuado de seguridad de información y servicios en línea con los convenios de servicios por terceros.		
A.10.2.1	Entrega de servicios	Control Se deberá asegurar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el convenio de servicios por terceros, sean implementados, operados y mantenidos por el tercero.
A.10.2.2	Monitoreo y revisión de servicios de terceros	Control Los servicios, informes y registros suministrados por terceros deberán monitorearse y revisarse periódicamente, y efectuarse auditorias regularmente.
A.10.2.3	Gestión de cambios en terceros	Control Deberá gestionarse los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, tomando en cuenta la criticabilidad de los sistemas y procesos de negocios involucrados y la reevaluación de los riesgos.
A.10.3 Planeamiento y aceptación de sistemas Objetivo: Minimizar el riesgo de fallas de sistemas.		
A.10.3.1	Gestión de la capacidad	Control El uso de los recursos debe monitorearse y refinarse, y deben hacerse proyecciones de las necesidades de capacidad futuras para asegurar el desempeño requerido del sistema.
A.10.3.2	Aceptación de sistemas	Control

		Deberán establecerse criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones, y realizarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación.
A.10.4 Protección contra código malicioso y código móvil Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra código malicioso	Control Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios.
A.10.4.2	Controles contra código móvil	Control Cuando el uso de código móvil está autorizado, la configuración deberá asegurar que el código móvil autorizado opere según una política de seguridad claramente definida, y se impedirá la ejecución de código móvil no autorizado.
A.10.5 Respaldo Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de información.		
A.10.5.1	Respaldo de la información	Control Deberán hacerse copias de respaldo de la información y el "software", y probarse periódicamente según la política de respaldo convenida.
A.10.6 Gestión de seguridad de redes Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de redes	Control Las redes deberán manejarse y controlarse debidamente, a fin de protegerse de amenazas, y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Las características de seguridad, niveles de servicio, y requisitos de gestión de todos los servicios de red deberán identificarse e incluirse en cualquier convenio de servicios de red, ya sea que los servicios se provean internamente o del exterior.
A.10.7 Manipulación de medios		

Objetivo: Impedir la divulgación, modificación, remoción o destrucción no autorizadas de activos, y la interrupción de las actividades de negocios.		
A.10.7.1	Manejo de medios removibles	Control Deberá haber procedimientos para el manejo de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deberán eliminarse de modo seguro y sin riesgo de accidente cuando no se les necesite más, usando procedimientos formales.
A.10.7.3	Procedimientos de manipulación de información	Control Deberán establecerse procedimientos para la manipulación y almacenamiento de información, a fin de protegerla de la divulgación no autorizada o del mal uso.
A.10.7.4	Seguridad de la documentación del sistema	Control Deberá protegerse la documentación del sistema contra el acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y "software" que se intercambian dentro de una organización y con cualquier organización exterior.		
A.10.8.1	Políticas y procedimientos de intercambio de información	Control Deberán existir políticas, procedimientos y controles formales de intercambio de información para protegerlo mediante el uso de todo tipo de facilidades de comunicación.
A.10.8.2	Convenios de intercambio	Control Deberán establecerse convenios para el intercambio de información y "software" entre la organización y organismos externos.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contengan información deberán protegerse contra el acceso no autorizado, el mal uso o corrupción durante su transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajería electrónica	Control La información contenida en la mensajería electrónica deberá protegerse debidamente.
A.10.8.5	Sistemas de información de negocios	Control Deberán prepararse e implementarse políticas y procedimientos para proteger la información relacionada con la interconexión de los sistemas de información de negocios.
A.10.9 Servicios de comercio electrónico Objetivo: Verificar la seguridad de los servicios de comercio electrónico y su uso seguro.		

A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que circula por redes públicas, deberá protegerse de la actividad fraudulenta, objeción de contrato y de la divulgación y modificación no autorizadas.
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración no autorizada del mensaje, divulgación no autorizada, y duplicación o reproducción no autorizadas del mensaje.
A.10.9.3	Información disponible públicamente	Control Deberá protegerse la integridad de la información colocada en un sistema de disponibilidad pública para impedir su modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas		
A.10.10.1	Registros de auditoria	Control Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso.
A.10.10.2	Monitoreo del uso del sistema	Control Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente.
A.10.10.3	Protección de la información de registro	Control Las instalaciones de registro y la información de registro deberán protegerse contra las alteraciones y el acceso no autorizado.
A.10.10.4	Registros de Administrador y operador	Control Se deberán registrar las actividades del administrador del sistema y del operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas.
A.10.10.6	Sincronización de reloj	Control

		Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad, deberán sincronizarse con una fuente de tiempo exacto convenida.
A.11 Control de acceso		
A.11.1 Requisito de negocios para el control de acceso Objetivo: Controlar el acceso a la información		
A.11.1.1	Política de control del acceso	Control Se deberá establecer, documentar, y revisar una política de control del acceso basada en los requisitos de negocios y de seguridad para el acceso.
A.11.2 Gestión del acceso de usuarios Objetivo: Asegurar el acceso de usuarios autorizados e impedir el acceso no autorizado a los sistemas de información.		
A.11.2.1	Inscripción de usuarios	Control Deberá haber un procedimiento formal de inscripción y des-inscripción de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Deberá restringirse y controlarse la asignación y uso de privilegios.
A.11.2.3	Manejo de contraseña de usuarios	Control La asignación de contraseñas deberá controlarse mediante un proceso de manejo formal.
A.11.2.4	Revisión de derechos de acceso de usuarios	Control La gerencia deberá revisar los derechos de acceso de usuarios a intervalos regulares utilizando un procedimiento formal.
A.11.3 Responsabilidades de los usuarios Objetivo: Impedir el acceso de usuario no autorizado, así como el compromiso o robo de información o de instalaciones de procesamiento de información.		
A.11.3.1	Uso de contraseñas	Control Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.
A.11.3.2	Equipo de usuario no atendido	Control Los usuarios deberán asegurar que el equipo no atendido tenga protección adecuada.
A.11.3.3	Política de escritorio limpio y pantalla limpia	Control Deberá adoptarse una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para

		instalaciones de procesamiento de información.
A.11.4 Control del acceso a redes Objetivo: Prevenir el acceso no autorizado a los servicios de redes.		
A.11.4.1	Política sobre uso de servicios de redes	Control A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar.
A.11.4.2	Autenticación de usuarios para conexiones remotas	Control Deberán usarse métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación de equipo en redes	Control La identificación automática de equipo deberá considerarse como un medio de autenticar las conexiones desde lugares y equipo específicos.
A.11.4.4	Protección de puertos de diagnóstico y configuración remotos.	Control Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Separación en las redes	Control En las redes deberán separarse los grupos de servicios de información, usuarios y sistemas de información.
A.11.4.6	Control de conexión a redes	Control En redes compartidas, especialmente aquellas que se extienden más allá de los límites de la organización, deberá restringirse la capacidad de los usuarios para conectarse a la red, conforme a la política de control de acceso y a los requisitos de las aplicaciones de negocios (ver 11.1).
A.11.4.7	Controles de ruteo de redes	Control Deberá implementarse el control de ruteo de redes para asegurar que las conexiones y los flujos de información de computadores no violen la política de control de acceso de las aplicaciones de negocios.
A.11.5 Control de acceso al sistema operativo Objetivo: Impedir el acceso no autorizado a los sistemas operativos		
A.11.5.1	Procedimientos seguros de inicio de sesión	Control El acceso a los sistemas operativos deberá controlarse mediante un procedimiento seguro de inicio de sesión.
A.11.5.2	Identificación y autenticación de usuario	Control

		Todos los usuarios deberán tener un código de idorganización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la idorganización reclamada por un usuario.
A.11.5.3	Sistema de manejo de contraseñas	Control Los sistemas de manejo de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad.
A.11.5.4	Uso de utilitarios de sistema	Control El uso de programas utilitarios que podrían ser capaces de cancelar los controles de sistema y de aplicación deberá restringirse y controlarse estrictamente.
A.11.5.5	Expiración de sesión	Control Las sesiones inactivas deberán cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación del tiempo de conexión	Control Deberá usarse restricciones del tiempo de conexión para proveer seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control del acceso a aplicación e información Objetivo: Impedir el acceso no autorizado a la información contenida en los sistemas de aplicaciones		
A.11.6.1	Restricción del acceso a la información	Control El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas sensibles	Control Los sistemas sensibles deberán tener un ambiente de computación dedicado (aislado).
A.11.7 Computación móvil y teletrabajo Objetivo: Asegura la seguridad de la información cuando se utilice computación móvil y actividades de teletrabajo		
A.11.7.1	Computación y comunicaciones móviles	Control Deberá existir una política formal y adoptarse medidas de seguridad adecuadas para protegerse contra los riesgos de usar facilidades móviles de computación y comunicación.
A.11.7.2	Teletrabajo	Control Deberá prepararse e implementarse una política, planes y procedimientos

		operativos para las actividades de teletrabajo.
A.12 Adquisición, desarrollo y mantenimiento de sistemas de información		
A.12.1 Requisitos de seguridad para sistemas de información Objetivo: Exigir que la seguridad sea parte integral de los sistemas de información		
A.12.1.1	Análisis y especificación de requisitos de seguridad	Control Los enunciados de requisitos de negocios para nuevos sistemas de información, o para mejoras de sistemas de información existentes, deberán especificar los requisitos para controles de seguridad.
A.12.2 Procesamiento correcto en aplicaciones Objetivo: Prevenir errores, pérdidas, modificación no autorizada o mal uso de la información en aplicaciones		
A.12.2.1	Validación de datos de entrada	Control Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados.
A.12.2.2	Control de procesamiento interno	Control Deberán incorporarse comprobaciones de validación en las aplicaciones, para detectar cualquier corrupción de información debido a errores de proceso o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Deberán identificarse los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificarse e implementarse los controles apropiados.
A.12.2.4	Validación de datos de salida	Control Los datos de salida de las aplicaciones deberán validarse para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Deberá prepararse e implementarse una política sobre el uso de controles criptográficos para protección de la información.
A.12.3.2	Administración de claves	Control Deberá efectuarse la administración de claves para apoyar el uso de técnicas criptográficas en la organización.
A.12.4 Seguridad de archivos del sistema Objetivo: Establecer la seguridad de los archivos del sistema		

A.12.4.1	Control del "software" operativo	Control Deberán existir procedimientos para controlar la instalación de "software" en los sistemas operativos.
A.12.4.2	Protección de datos de prueba del sistema	Control Los datos de prueba deberán seleccionarse cuidadosamente, y ser protegidos y controlados.
A.12.4.3	Control del acceso a código fuente de programas	Control Deberá restringirse el acceso al código fuente de programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del "software" e información del sistema de aplicaciones		
A.12.5.1	Procedimientos de control de cambios	Control La implementación de cambios deberá controlarse mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema operativo	Control Cuando se cambien los sistemas operativos, deberán revisarse y probarse las aplicaciones de negocios críticas para asegurar que no existe impacto negativo en las operaciones o seguridad de la organización.
A.12.5.3	Restricciones a cambios en paquetes de "software"	Control Deberá desalentarse las modificaciones a los paquetes de "software", limitarse a los cambios necesarios, y todos los cambios deberán controlarse estrictamente.
A.12.5.4	Filtraciones de información	Control Deberá evitarse las ocasiones de filtración de información.
A.12.5.5	Desarrollo de programas por terceros	Control La organización deberá supervisar y monitorear el desarrollo de programas por terceros.
A.12.6 Gestión de vulnerabilidades técnicas Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Deberá obtenerse información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a esas vulnerabilidades, y tomarse medidas

		adecuadas para resolver el riesgo relacionado.
A.13 Gestión de incidentes de seguridad de la información		
A.13.1 Reportes de eventos y debilidades de seguridad de la información Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociadas con los sistemas de información sean comunicados de tal manera que se tomen las acciones correctivas oportunamente.		
A.13.1.1	Reportes de eventos de seguridad de la información	Control Los eventos de seguridad de la información deberán reportarse por medio de los canales de gerencia apropiados tan pronto como sea posible.
A.13.1.2	Reportes de debilidades de seguridad	Control Los eventos de seguridad de la información deberán reportarse por medio de los canales de gerencia apropiados tan pronto como sea posible.
A.13.2 Gestión de incidentes y mejoras de seguridad de la información Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendiendo de los incidentes de seguridad de la información	Control Deberán existir mecanismos en ejecución que permitan cuantificar y monitorear los tipos, volúmenes, y costos de los incidentes de seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona o organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civiles o penales), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente.
A.14 Gestión de la continuidad de negocios		
A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocios Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación.		
A.14.1.1	Incluir seguridad de la información en el proceso de	Control Deberá desarrollarse y mantenerse un proceso gestionado de continuidad del

	gestión de la continuidad de negocios	negocio en toda la organización, que se encargue de los requerimientos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad de negocios y evaluación de riesgos	Control Deberá identificarse los eventos que pueden causar interrupciones a los procesos de negocios, junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información.	Control Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos.
A.14.1.4	Marco de planeamiento de la continuidad de los negocios	Control Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento.
A.14.1.5	Prueba, mantenimiento y reevaluación de planes de continuidad de los negocios	Control Los planes de continuidad de los negocios deberán probarse y actualizarse regularmente para asegurar que estén al día y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento de requisitos legales Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito de seguridad.		
A.15.1.1	Identificación de la legislación aplicable	Control Deberá definirse, documentarse y mantenerse al día explícitamente todos los requisitos estatutarios, de regulación y contractuales pertinentes y el enfoque de la organización Para cumplirlos, para cada sistema de información en la organización.
A.15.1.2	Derechos de propiedad intelectual (DPI)	Control Deberá implementarse procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de regulación y contractuales sobre el uso del

		material respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de "software" propietario.
A.15.1.3	Protección de los registros de la organización	Control Los registros importantes deberán protegerse de pérdida, destrucción y falsificación, de conformidad con los requisitos estatutarios, de regulación, contractuales y de negocios.
A.15.1.4	Protección de datos y privacidad de la información personal	Control La protección y privacidad de los datos deberá asegurarse como sea necesario mediante la legislación y reglamentos pertinentes y, si corresponde, mediante las cláusulas contractuales.
A.15.1.5	Prevención del mal uso de las instalaciones de procesamiento de información	Control A los usuarios se les deberá disuadir de utilizar las instalaciones de procesamiento de información para fines no autorizados.
A.15.1.6	Reglamentación de los controles criptográficos	Control Los controles criptográficos deberán usarse cumpliendo con todos los convenios, leyes, y reglamentos pertinentes.
A.15.2 Cumplimiento de las políticas y normas de seguridad, y cumplimiento técnico Objetivo: Asegurar que los sistemas cumplan con las políticas y normas de seguridad de la organización		
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	Control Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico	Control Deberá comprobarse regularmente el cumplimiento de las normas de implementación de seguridad en los sistemas de información.
A.15.3 Consideraciones de auditoria de sistemas de información Objetivo: Maximizar la efectividad del proceso de auditoría de sistemas de información y minimizar la interferencia de dicho proceso.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Los requerimientos y actividades de auditoria que involucren comprobaciones de los sistemas operativos deberán planearse y acordarse cuidadosamente para minimizar el riesgo de perturbaciones a los procesos de negocios.

A.15.3.2	Protección de las herramientas de auditoria de sistemas de información	Control Deberá protegerse el acceso a las herramientas de auditoria de sistemas de información para impedir cualquier posible mal uso o compromiso.

Anexo 2

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Dirigido a los **alumnos** de las diferentes facultades que conforman la UNASAM

Objetivos:

- Conocer que tan involucrados se encuentran los alumnos en el resguardo de la Tecnología de Información.
- Identificar si los alumnos utilizan de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

1. Sexo:
   Masculino ( ) Femenino ( )

2. Escuela profesional a la que perteneces: .....

3. Ciclo de estudios en el que te encuentras:.....

4. Usted apaga los equipos informáticos debidamente después de utilizarlos
   SI ( ) NO ( )
   Si tu respuesta es **Sí,** Cómo apagas tu equipo después de trabajar
   a. Apagando directamente el estabilizador. ( )
   b. Desenchufando el cable de energía de la computadora. ( )
   c. Manteniendo presionando el botón de apagado del CPU. ( )
   d. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )
   e. Bajando la llave de energía. ( )
   f. Otros, Especificar..... ( )
   g. Ninguno. ( )

5. Te sientes seguro en los ambientes donde se encuentran los equipos informáticos dentro de la universidad frente a cualquier desastre natural o humano
   SI ( ) NO ( )

6. Has observado algún extinguidor cerca de los equipos informáticos
   SI ( ) NO ( )

7. Has observado algún tipo de señalización de emergencia en los ambientes donde existen equipos informáticos
   SI ( ) NO ( )

8. Has participado de algún simulacro frente a cualquier desastre natural, especialmente en áreas donde hay equipos informáticos
   SI ( ) NO ( )
   Si tu respuesta es **No;**
   Como nos sugieres que se realice y cada que tiempo:
   .....

9. Has manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, Mouse y conexiones de red que conectan al CPU para hacerlos funcionar
   SI ( ) NO ( )

10. Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la UNASAM
    SI ( ) NO ( )

11. Si en el transcurso del uso de un equipo informático se te detecta realizando alguna actividad sospechosa como ingresando a lugares restringidos, usted sería capaz de afrontarla (por la responsabilidad que asume en ese determinado momento sobre el equipo asignado)
    SI ( ) NO ( )

12. Hace usted uso de los antivirus en los equipos informáticos de la UNASAM cuando ingresa o saca información en algún dispositivo de almacenamiento
    Si ( ) A veces ( ) Nunca ( )

13. Que hace cuando detecta un virus en la computadora de la UNASAM
    a. Activa el antivirus ( )
    b. Activa el antivirus, detecta los virus y los elimina ( )
    c. Borra el archivo ( )
    d. Formatea el dispositivo de almacenamiento ( )
    e. No hago nada (Por que no sé) ( )
    f. Otros, Especificar..... ( )

14. Usted ha detectado que el antivirus que utiliza la UNASAM funciona adecuadamente y que se encuentra actualizado
    SI ( ) NO ( )

15. Que tan frecuente es su acceso a la información que proporciona el SIGA WEB UNASAM.
    Siempre ( ) Casi siempre ( ) Nunca ( )

16. Normalmente su clave de acceso al SIGA WEB UNASAM hace referencia a:
    a. Su nombre y apellido ( )
    b. Su fecha de nacimiento ( )
    c. Teléfono (de casa o móvil) ( )
    d. Número de DNI ( )
    e. Otro ( )

17. La Clave con la cual ingresa al SIGA WEB UNASAM es conocida también por:
    a. Un compañero de estudios ( )
    b. Familiares ( )
    c. Otros, Especifica..... ( )
    d. No comparte con nadie su clave ( )

18. Cada que tiempo cambia su clave de acceso al SIGA WEB UNASAM
    Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

    Y si nunca cambio su clave, cuál es y porque motivo no lo hizo .....
.....

19. Qué tan veloz es el acceso al portal WEB dentro o fuera de la UNASAM
    a. Es más rápido dentro de la universidad que fuera de ella ( )
    b. Es más lenta dentro de la universidad que fuera de ella ( )
    c. Es igual en ambos lugares ( )

20. Usted recibió alguna capacitación acerca de Seguridad de la Información en la UNASAM
    SI ( ) NO ( )

21. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información
    SI ( ) NO ( )
    Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:
    a. Folletos y boletines ( )
    b. Charlas o conferencias ( )
    c. Foros a través del portal WEB de la UNASAM ( )
    d. Como parte de algún curso en tu carrera ( )
    e. Otros, Especifique: ..... ( )

Anexo 3

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Dirigido a los **Docentes y/o Administrativos** de la UNASAM

Objetivos:

- Conocer que tan involucrados se encuentran los docentes y/o administrativos en el resguardo de la Tecnología de Información.
- Saber si los docentes y/o administrativos utilizan de manera óptima las tecnologías de información y de que manera ayudarían a salvaguardar la misma.

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

1. Sexo:
   Masculino ( ) Femenino ( )

2. Cargo del Informante: .....

3. A qué facultad pertenece: .....

4. Usted apaga los equipos informáticos debidamente después de utilizarlos
   SI ( ) NO ( )
   Si tu respuesta es **SÍ,** Cómo apagas tu equipo después de trabajar
   a. Apagando directamente el estabilizador. ( )
   b. Desenchufando el cable de energía de la computadora. ( )
   c. Manteniendo presionando el botón de apagado del CPU. ( )
   d. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )
   e. Bajando la llave de energía. ( )
   f. Otros, Especificar..... ( )
   g. Ninguno. ( )

5. Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro de la universidad frente a cualquier desastre natural o humano
   SI ( ) NO ( )

6. Ha observado algún extinguidor cerca de los equipos informáticos
   SI ( ) NO ( )

7. Ha observado algún tipo de señalización de emergencia en los ambientes donde existen equipos informáticos
   SI ( ) NO ( )

8. Sabe utilizar de forma adecuada un extintor
   SI ( ) NO ( )
   Si la respuesta es **SÍ;** Lo aprendió a utilizar a través de:
   a. Charlas y capacitaciones fuera de la Universidad ( )
   b. Charlas y capacitaciones dentro de la Universidad ( )
   c. Manuales de extintor ( )
   d. Internet ( )

9. Ha participado de algún simulacro frente a cualquier desastre natural o humano, especialmente en áreas donde hay equipos informáticos
   SI ( ) NO ( )
   Si tu respuesta es **No;**
   Como nos sugieres que se realice y cada que tiempo:
   .....

10. Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar
    SI ( ) NO ( )

11. Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la UNASAM
    SI ( ) NO ( )

12. Hace usted uso de los antivirus en los equipos informáticos de la UNASAM cuando ingresa o saca información en algún dispositivo de almacenamiento
    Si ( ) A veces ( ) Nunca ( )

13. Que hace cuando detecta un virus en la computadora que le proporciona la UNASAM
    a. Activa el antivirus ( )
    b. Activa el antivirus, detecta los virus y los elimina ( )
    c. Borra el archivo ( )
    d. Formatea el dispositivo de almacenamiento ( )
    e. No hago nada (Porque no sé) ( )
    f. Otros, Especificar..... ( )

14. Usted ha detectado que el antivirus del que hace uso la UNASAM funciona adecuadamente y que se encuentra actualizado
    SI ( ) NO ( )

15. Usted hace uso del SIGA WEB UNASAM
    SI ( ) NO ( )
    Si su respuesta es NO pasar a la pregunta 21.

16. Que tan frecuente es su acceso a la información que proporciona el SIGA WEB UNASAM.

Siempre ( ) Casi siempre ( ) Nunca ( )

17. Normalmente su clave de acceso al SIGA WEB UNASAM hace referencia a:
    b. Su nombre y apellido ( )
    c. Su fecha de nacimiento ( )
    d. Teléfono (de casa o móvil) ( )
    e. Nombre de su esposo(a) o hijo(a) ( )
    f. Otro ( )

18. La Clave con la cual ingresa al SIGA WEB UNASAM es conocida también por:
    b. Un compañero de trabajo ( )
    c. Mi esposo(a) o hijo(a) ( )
    d. Algún alumno ( )
    e. Otros, Especifica..... ( )
    f. No comparte con nadie su clave ( )

19. Cada que tiempo cambia su clave de acceso al SIGA WEB UNASAM
    Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

    Y si nunca cambio su clave, cuál es y porque motivo no lo hizo .....

20. Qué tan veloz es el acceso al portal WEB dentro o fuera de la UNASAM
    b. Es más rápido dentro de la universidad que fuera de ella ( )
    c. Es más lenta dentro de la universidad que fuera de ella ( )
    d. Es igual en ambos lugares ( )

21. Usted recibió alguna capacitación acerca de Seguridad de la Información en la UNASAM
    SI ( ) NO ( )

22. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información
    SI ( ) NO ( )
    Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:
    f. Folletos y boletines ( )
    g. Charlas o conferencias ( )

h. Foros a través del portal WEB de la UNASAM ( )

i. Como parte de algún curso en tu carrera ( )

j. Otros, Especifique: ..... ( )

Anexo 4

ENTREVISTA

Las empresas de hoy en día manejan su información por medio de sistemas integrados u otros, los cuales muchos de ellos ven reflejado la vulnerabilidad de su información frente a cualquier peligro que se les presente. Es por ello que este proyecto de investigación busca encontrar los puntos débiles con respecto a todo lo que es la tecnología de información y comunicación de la Oficina General de Estudios de la UNASAM, motivo por el cual está entrevista va dirigido al **Jefe de la Oficina General de Estudios** como agente beneficiario de la Seguridad de la Información.

Para saber quiénes son las personas que toman las decisiones con respecto a la seguridad de la información se listo las siguientes preguntas:

¿La UNASAM cuenta con un comité de seguridad de la información?
SI ( )
Las funciones del comité se encuentran detalladas en el manual de funciones y organización u otro
documento_____
Quién conforma ese
comité_____
Ese comité es plenamente identificable por la comunidad
universitaria_____

NO ( )
Si no cuentan con ese comité, quienes son los encargados de establecer las políticas de seguridad de la información

_____
O, sólo las políticas son establecidas por si mismo como jefe de la Oficina General de Estudios _____
Estas políticas son conocidas por todos los
usuarios_____
A través de que medio se les dió a
conocer_____

Preguntas sobre mecanismos de control con respecto a la seguridad de la información

¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la
información?_____
¿De qué manera controla a sus trabajadores, con respecto al tema de seguridad de la información?_____
__
¿De qué forma controla los accesos a la red y quién ordena que se genere esos permisos?_____
—

¿Existen bitácoras donde se registran los sucesos de todos los usuarios que ingresan a la
red?_____
__

Detecto en alguna ocasión algo indebido_____

¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?_____
__

Preguntas sobre políticas de seguridad

¿Existe un documento donde se especifique las políticas de seguridad de la información?

SI ( )

¿Quién elaboró ese documento y por quién fue aprobado?_____
_____
__

¿Sus trabajadores y usuarios conocen este documento?_____

¿Se aplican estas políticas a toda la comunidad universitaria?_____

¿Cada que tiempo se revisan esas políticas?_____

NO ( )

¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información en la UNASAM?_____

¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información para la UNASAM?_____

Porqué_____
___

Y para su área_____

Preguntas sobre el nivel conocimiento de seguridad de la información por parte de su personal

Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

SI ( )

¿Para ello existen procedimientos documentados para actuar antes, durante y después del
desastre?_____
¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?

_____
__
Lo cree necesario hacerlo con esta
organización_____
¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para
elaborarlo?_____

NO ( )
¿A qué se
debe?_____

Preguntas sobre backups y claves

La administración de todos los servicios de tecnología de información que están a su cargo se manejan a través de claves de
autenticación_____
Cree usted necesario que la alta dirección deba poseer las claves (y su actualización de las mismas)

_____
Porqué_____
___

¿Existe algún procedimiento para realizar backups, de la información que usted maneja?
SI ( )
¿Están descritos en algún
documento?_____
¿Se cumplen conforme están
descritos?_____
¿Son depositados en algún lugar especial dentro de la UNASAM o fuera de ella?

_____
__
Porqué_____
___
Cada que tiempo se hace y quién los
realiza_____

NO ( )
Porqué_____

Preguntas sobre problemas frecuentes

¿Cuáles son los problemas más frecuentes con los que se enfrenta el área que Usted tiene a cargo?
Frente a las actividades de su área_____
Frente a los servicios que le brinda a los usuarios_____
¿Se encuentran archivados esos problemas? ¿Qué estrategia usa para disminuir esos problemas frecuentes? Existe alguna estadística de la evolución de esos problemas
_____
__
Emplean tarjetas o fichas de seguimiento de los equipos que se les brinda a los usuarios_____
___

Preguntas sobre modificaciones en los servicios que se le presta a los usuarios

¿Todas las modificaciones que se haga a los servicios que se le presta a los usuarios es
registrado?_____
_
Existe algún procedimiento interno para
efectuarlos_____

Preguntas sobre mantenimiento de los equipos

¿Existe un plan de mantenimiento para todos los equipos de la UNASAM?
SI ( )
Cada qué tiempo lo
realizan_____
¿Qué aspectos son los que toman en cuenta para ese mantenimiento?
_____
__
Cómo se trata el tema de los antivirus dentro de la
UNASAM_____
_____
__

Preguntas sobre adquisición de software y hardware

¿Cuál es el procedimiento para la adquisición de un SW o
HW?_____
_____
__
Este procedimiento se encuentra debidamente identificado en un
documento_____

Porqué_____

¿Quién justifica la adquisición?_____

¿Quién evalúa la adquisición?_____

¿Quién evalúa los proveedores?_____

Anexo 5

ENTREVISTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Las empresas de hoy en día manejan su información por medio de sistemas integrados u otros, los cuales muchos de ellos ven reflejado la vulnerabilidad de su información frente a cualquier peligro que se les presente. Es por ello que nuestro proyecto de investigación busca encontrar los puntos débiles con respecto a todo lo que es la Tecnología de Información y Comunicación de la Oficina General de Estudios, motivo por el cual está entrevista estará dirigido al **personal encargado de la administración de base de datos de la OGE** como principal agente encargados de la Seguridad de la Información que resguarda ésta.

Nombre:

Cargo del informante:

¿Qué tipo de relación laboral tiene Ud. con la UNASAM?

a. Contratado por horas ( )

b. Contratado tiempo Completo( )

c. Otras ( ), especifique:
.....

¿Cuántas personas laboran en el área de administración de base de datos? ¿Quién es el responsable?

.....
.....
.....

¿Utilizan antivirus?

Si ( ) No ( )

Si la respuesta es **Sí,**

¿Tipo de antivirus que utiliza?

a. Norton ( )

b. Kaspersky ( )

c. Nod 32 ( )

d. Panda ( )

e. Otros ( ), especifique:
.....

Cada que tiempo cambian o actualizan la versión del antivirus

a. Mensual ( )

b. Trimestral ( )

c. Semestral ( )

d. Anual ( )

e. Otros periodos ( ), especifique:
.....

¿Quién se encarga de la actualización del antivirus?
.....
.....
.....
¿Se registran los inconvenientes? ¿Cuál es el tiempo promedio que demoras para solucionar dichos inconvenientes?
.....
.....
.....
¿Quiénes le brindan capacitación a usuarios (profesores, administrativos, alumnos, etc.) antes que hagan uso o "buen uso" de la información que maneja el SIGA WEB UNASAM?
.....
.....
.....

A Usted se le brinda capacitación por parte de la UNASAM acerca de seguridad de la información
Si ( ) No ( )
Si la respuesta es **Si;** Cada que tiempo y quien se encarga de hacerlo
.....
.....
.....
En caso contrario, ¿cómo se capacitan?
.....
...

Usted cuenta con los medios y capacidad para afrontar cualquier desastre natural o humano como:

Aplacar un incendio utilizando un extintor	Si ( )	No ( )
Desplazar a los usuarios correctamente guiándose por señalizaciones	Si ( )	No ( )
Utilización de primeros auxilios (existencia u utilidad de un botiquín)	Si ( )	No ( )
Otros, Especifique _____	( )	
Ninguno	( )	

Usted sabe utilizar correctamente un extintor ¿Si lo sabe, se le capacito dentro de la UNASAM, o lo aprendió fuera?

.....
.....
.....

¿Cuáles son los problemas más frecuentes que se atienden con respecto a los usuarios?

Hardware:

.....

Software:

.....

¿Cómo se podrían evitar?

.....
...

¿Existen proyectos o mejoras con respecto a la seguridad de la información en el área que laboras?

.....
.....
.....

¿De quién y de donde surgen estas iniciativas?

.....
.....
.....

Preguntas sobre mecanismos de control con respecto a la seguridad de la información

¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información?_____

¿De qué manera controla a los trabajadores, con respecto al tema de seguridad de la información?_____

¿Cómo se controla la creación de usuarios para acceder al sistema y quién solicita esa creación?_____

¿Quién se encarga de aplicar las restricciones al usuario del sistema?

¿Existen bitácoras donde se registran los sucesos de todos los usuarios que ingresan a la

red?_____
_____

Detecto en alguna ocasión algo indebido_____
¿Se registran los accesos de personas al área que tiene a cargo?_____
¿Se registran los sucesos o incidentes que suceden dentro del área?_____
¿Cada qué tiempo solicitan que se les de mantenimiento a sus equipos?_____

Preguntas sobre políticas de seguridad

¿Existe un documento donde se especifique las políticas de seguridad de la información?

SI ( )
¿Quién elaboró ese documento y por quién fue aprobado?_____
¿Sus trabajadores y usuarios conocen este documento?_____
¿Se aplican estas políticas a toda la comunidad universitaria?_____
¿Cada que tiempo se revisan esas políticas?_____

NO ( )
¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información en la UNASAM?_____
¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información para la UNASAM?_____

Porqué_____
_____
Y para su área (lo cree necesario)
_____

Preguntas sobre el nivel conocimiento de seguridad de la información por parte de su personal

Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

SI ( )
¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre?_____

¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?

_____

Lo cree necesario hacerlo con esta organización_____

¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo?_____

NO ( )

¿A qué se debe?_____

Preguntas sobre backups y claves

La administración del sistema que está a su cargo, se manejan a través de claves de autenticación_____

Cree usted necesario que la alta dirección deba poseer las claves (y su actualización de las mismas)

_____

Porqué_____

¿Existe algún procedimiento para realizar backups, de la información que usted maneja?

SI ( )

¿Están descritos en algún documento?_____

¿Se cumplen conforme están descritos?_____

¿Son depositados en algún lugar especial dentro de la UNASAM o fuera de ella?_____

Porqué_____

Cada que tiempo se hace y quién los realiza_____

NO ( )

Porqué_____

Preguntas sobre problemas frecuentes

¿Cuáles son los problemas más frecuentes con los que se enfrenta el área que Usted tiene a cargo?

En las actividades de su área_____
En los servicios que le brinda a los usuarios_____
¿Se encuentran archivados esos problemas? ¿Qué estrategia usa para disminuir esos problemas frecuentes? Existe alguna estadística de la evolución de esos problemas

_____
__
Emplean tarjetas o fichas de seguimiento de los problemas en el uso del sistema por parte
usuarios_____

Preguntas sobre modificaciones en los servicios que se le presta a los usuarios

¿Todas las modificaciones que se haga a los servicios que otorga el sistema a los usuarios son
registrados?_____
Existe algún procedimiento interno para
efectuarlos_____

Preguntas sobre responsabilidad de software a desarrolla

¿Cada integrante del equipo de desarrollo de sistemas es responsable del software que desarrolla?
SI ( )
¿Qué control de calidad para la producción del software se le
aplica?_____
¿Esto le permite tener una copia de resguardo en su
casa?_____
¿Acata las políticas que se le impone?

NO ( )
Porqué

_____

Preguntas sobre manejo de base de datos

¿Quién es el primer responsable en el manejo de la base de
datos?_____
¿Toda actividad que se realice en ella es
documentada?_____
¿Aparte del departamento que tiene a cargo, existe otra persona que cada cierto tiempo realice una evaluación del nivel de desarrollo de su
área?_____
¿Cualquier trabajador que tenga a su cargo puede modificar la base de datos en el momento que
desee?_____

¿A tenido algún inconveniente con la base de datos en algún momento?_____

Preguntas sobre software y hardware

¿Cuentan con los equipos necesarios para realizar sus actividades?_____

¿Cuentan con el software necesario para realizar sus actividades?_____

¿Todo el software que se utilizan sea SW con licencia o SW libre, son solicitado al área de taller de cómputo?_____

¿Su área maneja restricciones a través de la red, igual como cualquier otra área?_____

Anexo 6

CUESTIONARIO SOBRE SEGURIDAD DE LA INFORMACIÓN

Hacia: Trabajadores de la OGE - Administración de la Base de Datos
Objetivo:
Identificar el grado de conocimiento que cuentan los Trabajadores en el resguardo de la Tecnología de Información, sus Aplicaciones y en el desarrollo, mantenimiento del software que elaboran y como se han involucrado.
Instrucciones:
Lea cada pregunta y responda a c/u de ellas sobre las líneas punteadas, en algunos casos señale con una X en las alternativas propuestas con paréntesis

¿Cuántas llamadas de usuarios al día recibe por inconvenientes técnicos en el software que han desarrollado? ¿Describa el inconveniente más frecuente que sucede en la mayoría de usuarios?
Número de llamadas (....)
Inconveniente más frecuente:
.....
...
.....
...

¿Se registran dichos inconvenientes? ¿Cuál es tiempo promedio que demoras para solucionar dichos inconvenientes?
.....
...
.....
...

¿Guarda una copia de seguridad del código que desarrollan por seguridad en un lugar distinto a sus instalaciones?
A veces ( ) Casi siempre ( ) Siempre ( ) Nunca ( )

¿Usted brinda soporte y mantenimiento al equipo que le fue asignado en desarrollo de sistemas? Y si no lo hace ¿A quién acude o informa? ¿A través de que medio (si es correo electrónico, cuál es)?
.....
.....
.....

Usted cuenta con los medios y la capacidad para afrontar cualquier desastre natural o humano como:
El área posee un extintor. SI ( ) NO ( )

El área posee señales de seguridad.	SI ( )	NO ( )
Me capacitan constantemente para afrontar este tipo de problema	SI ( )	NO ( )
Se posee una lista de número de emergencia a la mano	SI ( )	NO ( )
Existe un botiquín de primeros auxilios	SI ( )	NO ( )
Otros, Especificar.....	( )	
Ninguno	( )	

Usted sabe utilizar el extintor ¿Si lo sabe, donde lo aprendió?

.....
....
.....
....

Existe alguna persona encargada de guardar el backup del sistema general con su respectiva base de datos de la UNASAM (desarrollada y en desarrollo) ¿Cómo se llama? ¿Qué cargo ocupa en el área? ¿Cada cuánto tiempo lo hace?

.....
.....
.....

¿De qué forma se realiza el seguimiento de actividades en relación a la producción de desarrollo del software de la UNASAM?

.....
.....
.....

Existe algún mecanismo de control de calidad en la producción del software de la UNASAM ¿Si existe, cuál es (descríbalo)?

.....
.....
.....

¿Quién asigna a la persona para que realice el control de calidad? ¿La persona(s) encargada(s) de llevar el control de calidad se llama(n)? ¿Son internos o externos al área? ¿Son personas ajenas a la universidad? ¿Y cada cuanto tiempo lo realizan?

.....
.....
.....

¿Existe un comité de seguridad de la información que está informado constantemente sobre el desarrollo, inconvenientes, ocurrencias, fallas, etc. con respecto a la producción del software?

.....
.....
.....

¿Cree que sus equipos informáticos se encuentran completamente seguros dentro de su área, cómo?

Todos mis accesos al equipo son a través de claves	SI ( )	NO ( )
Se posee un buen antivirus y siempre está actualizado	SI ( )	NO ( )
El área de trabajo es completamente segura	SI ( )	NO ( )
Se registra los ingresos de cada persona dentro del área	SI ( )	NO ( )
Se posee una caja fuerte en el área	SI ( )	NO ( )
El área es vigilada por una cámara de video	SI ( )	NO ( )
Otros, Especificar.....	( )	
Ninguna	( )	

Sus claves de acceso a las diferentes aplicaciones, cada qué tiempo los cambia
Mensualmente ( ) Trimestralmente ( ) Semestralmente ( ) Anualmente ( )

Existe alguna clave acceso que se comparta entre los trabajadores de está área (Si existe Porqué razón)

.....
.....
.....

En alguna ocasión, la alta Dirección te ha solicitado modificar data de la Base de Datos de la universidad
A veces ( ) Casi siempre ( ) Siempre ( ) Nunca ( )

Al realizar alguna modificación en la Base de Datos, cuál es el procedimiento que realiza el área para realizarlo ¿se registra está incidencia en archivos?
A veces ( ) Casi siempre ( ) Siempre ( ) Nunca ( )

¿Usted cree que es responsable de su equipo informático y de cada actividad que realice usted o terceras personas sobre ella?
A veces ( ) Casi siempre ( ) Siempre ( ) Nunca ( )

Qué recomendaría Usted para mejorar el área donde se trabaja y también que ¿recomendaría para la parte de desarrollo de software (producción del mismo)?

.....
.....
.....

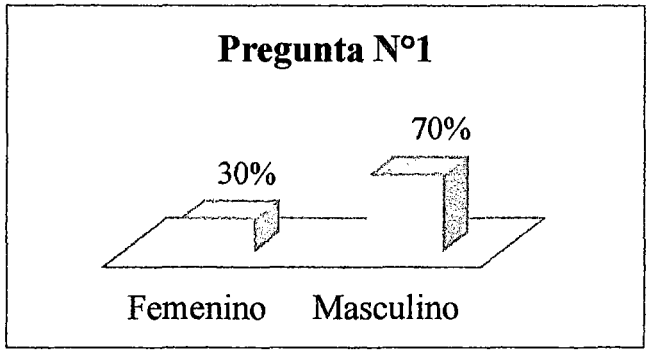
Anexo 7

Resultados de procesamiento de información de docentes y administrativos

Distribución porcentual de los docentes y administrativos de la UNASAM, según sexo

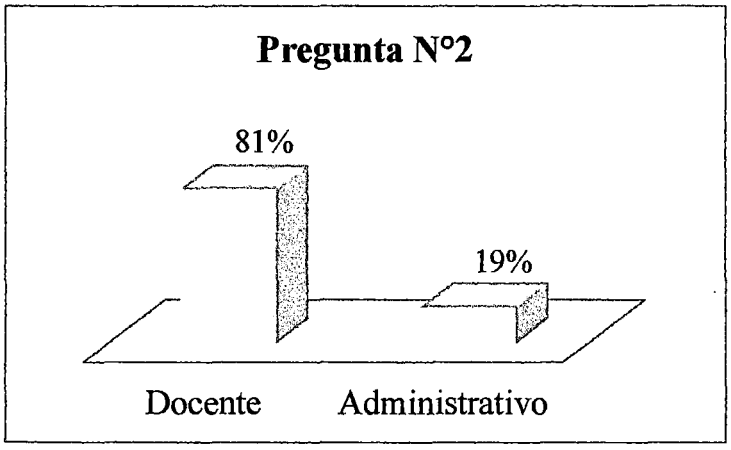
	Frecuencia	Porcentaje
Femenino	79	30%
Masculino	183	70%
TOTAL	262	100%

Fuente (Elaboración propia)



Distribución porcentual de los docentes y administrativos de la UNASAM, según cargo del informante

Cargo	Frecuencia	Porcentaje
Docente	212	81%
Administrativo	50	19%
TOTAL	262	100%

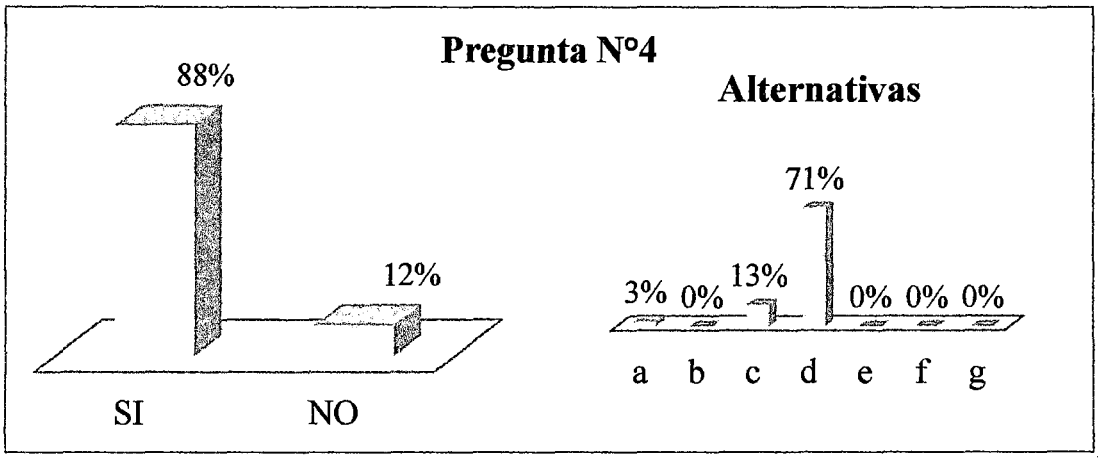


Distribución porcentual de los docentes y administrativos de la UNASAM, según el apagado debido de los equipos informáticos después de utilizarlos

Alternativa	Frecuencia	Porcentaje
SI	230	88%
NO	32	12%
TOTAL	262	100%

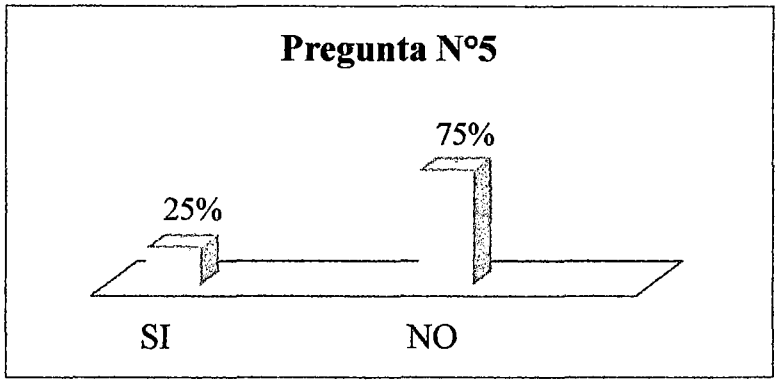
Si la respuesta fue SI:

Alternativa	Frecuencia	Porcentaje
a	7	3%
b	0	0%
c	34	13%
d	187	71%
e	0	0%
f	0	0%
g	0	0%
TOTAL	228	87%



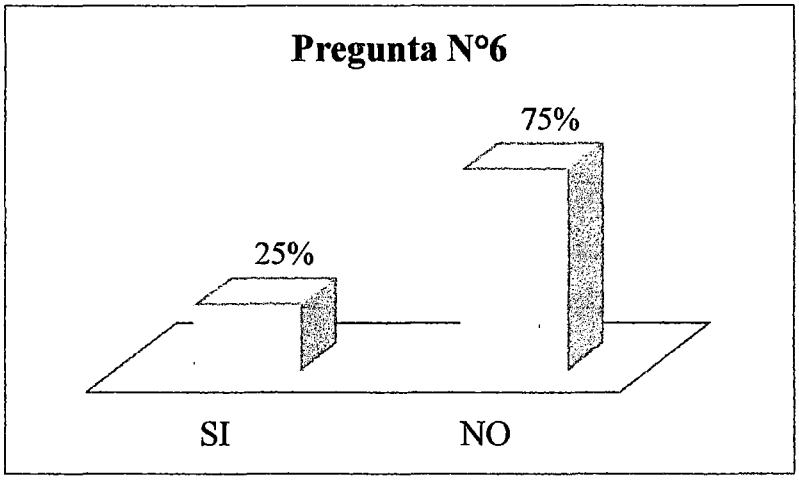
Distribución porcentual de los docentes y administrativos de la UNASAM, según la seguridad que tiene en los ambientes en los que se encuentran los equipos informáticos frente a un desastre natural o humano.

Alternativa	Frecuencia	Porcentaje
SI	65	25%
NO	197	75%
TOTAL	262	100%



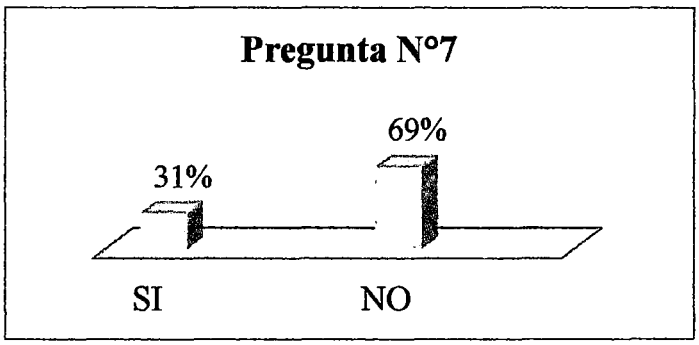
Distribución porcentual de los docentes y administrativos de la UNASAM, según observó existe algún extintor cerca de los equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	65	25%
NO	197	75%
TOTAL	262	100%



Distribución porcentual de los docentes y administrativos de la UNASAM, según observó existe alguna tipo de señalización de emergencias en los ambientes que se encuentran los equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	80	31%
NO	182	69%
TOTAL	262	100%

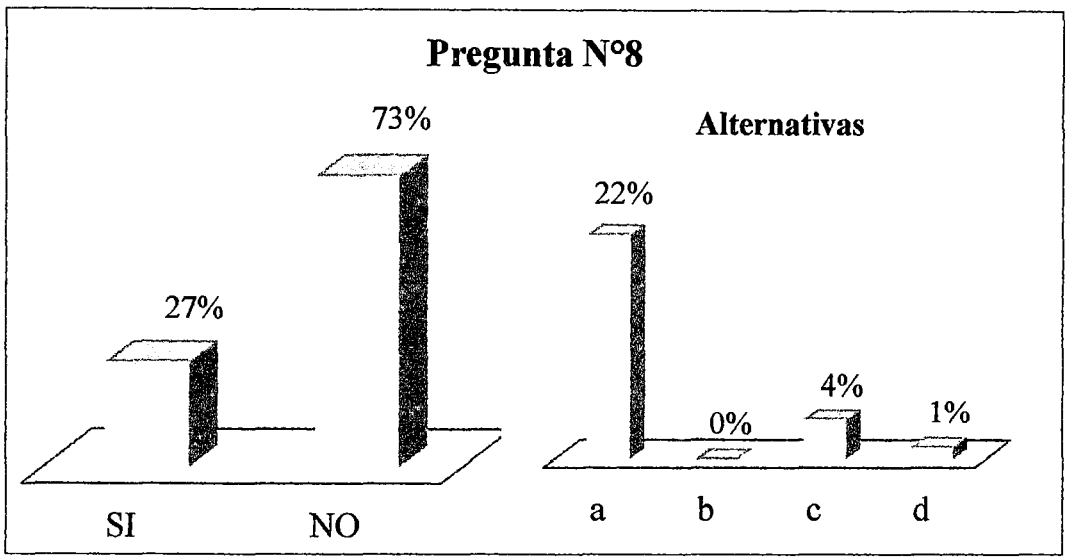


Distribución porcentual de los docentes y administrativos de la UNASAM, según observó su conocimiento del uso adecuado de un extintor

Alternativa	Frecuencia	Porcentaje
SI	70	27%
NO	192	73%
TOTAL	262	100%

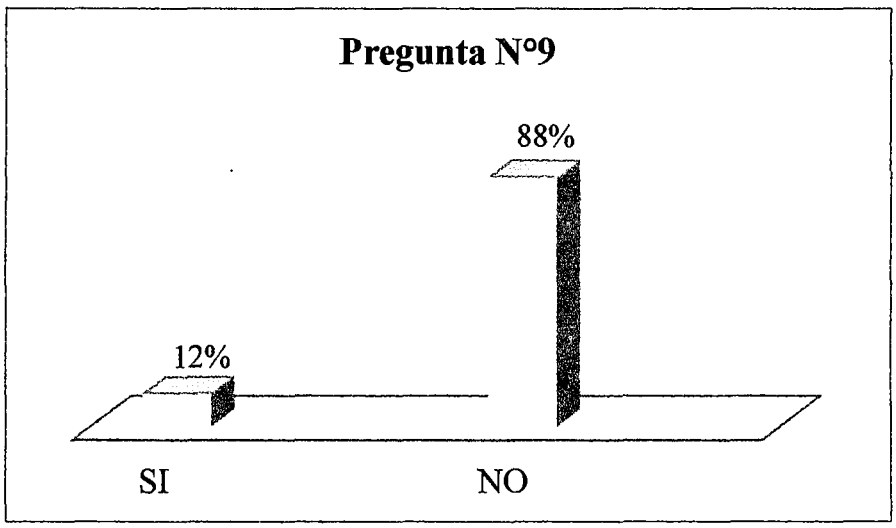
Si la respuesta es SI, de qué manera lo aprendió a utilizar

Alternativa	Frecuencia	Porcentaje
a	57	22%
b	0	0%
c	10	4%
d	3	1%
TOTAL	70	27%



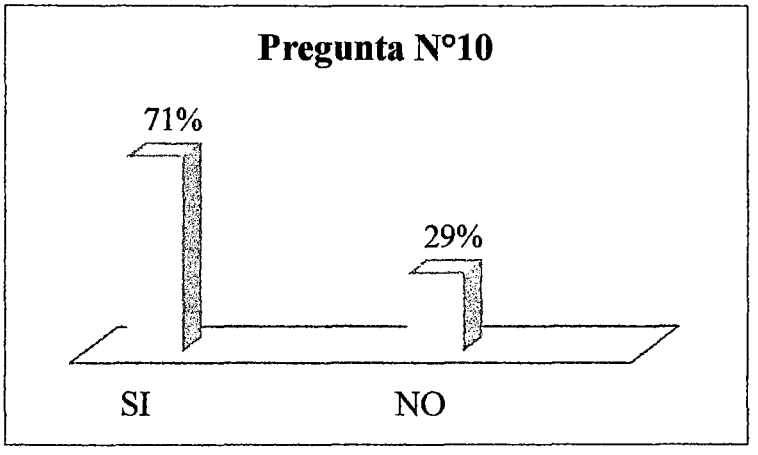
Distribución porcentual de los docentes y administrativos de la UNASAM, según la participación de simulacros frente a cualquier desastre específicamente en áreas donde hay equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	31	12%
NO	231	88%
TOTAL	262	100%



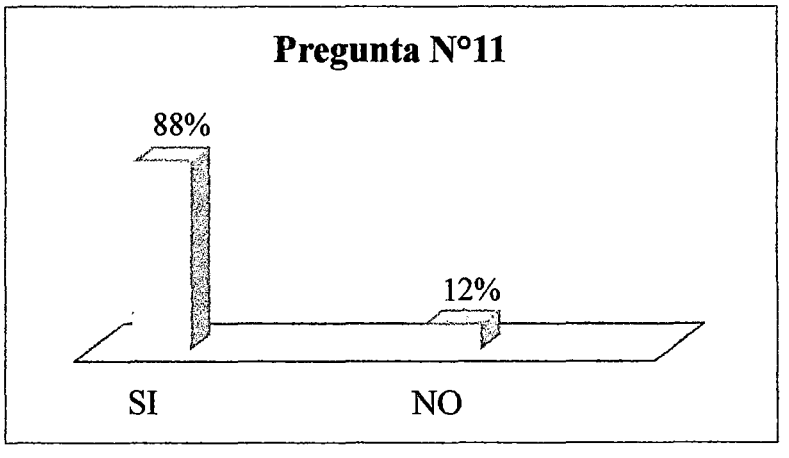
Distribución porcentual de los docentes y administrativos de la UNASAM, según la manipulación de componentes del equipo informático de manera que si sufrió algún inconveniente este funcione.

Alternativa	Frecuencia	Porcentaje
SI	187	71%
NO	75	29%
TOTAL	262	100%



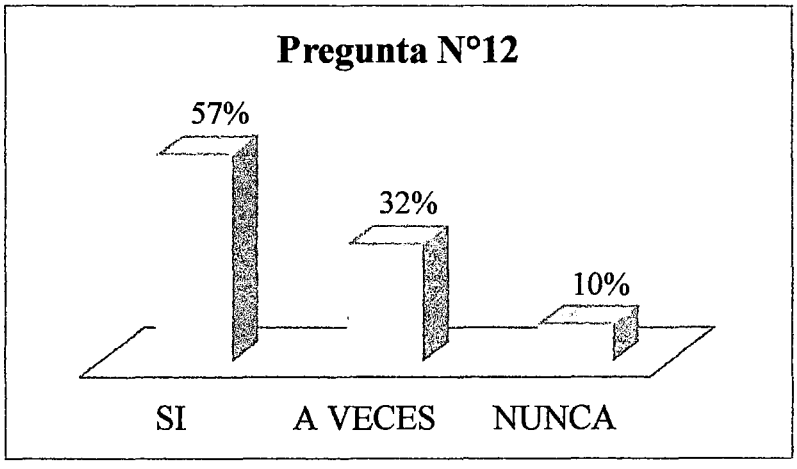
Distribución porcentual de los docentes y administrativos de la UNASAM, según la responsabilidad que asume al utilizar un equipo informático.

Alternativa	Frecuencia	Porcentaje
SI	231	88%
NO	31	12%
TOTAL	262	100%



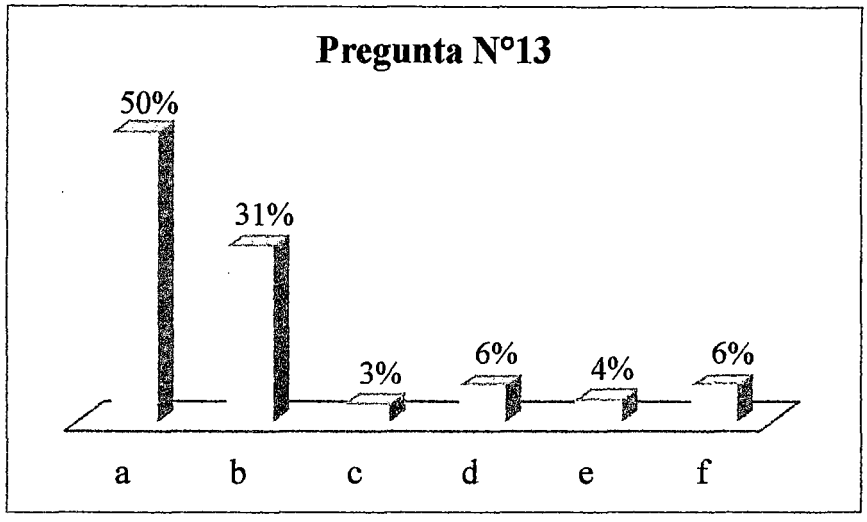
Distribución porcentual de los docentes y administrativos de la UNASAM, según el uso de los antivirus en los equipos informáticos cuando ingresa o saca información en algún dispositivo de almacenamiento

Alternativa	Frecuencia	Porcentaje
SI	150	57%
A VECES	85	32%
NUNCA	27	10%
TOTAL	262	100%



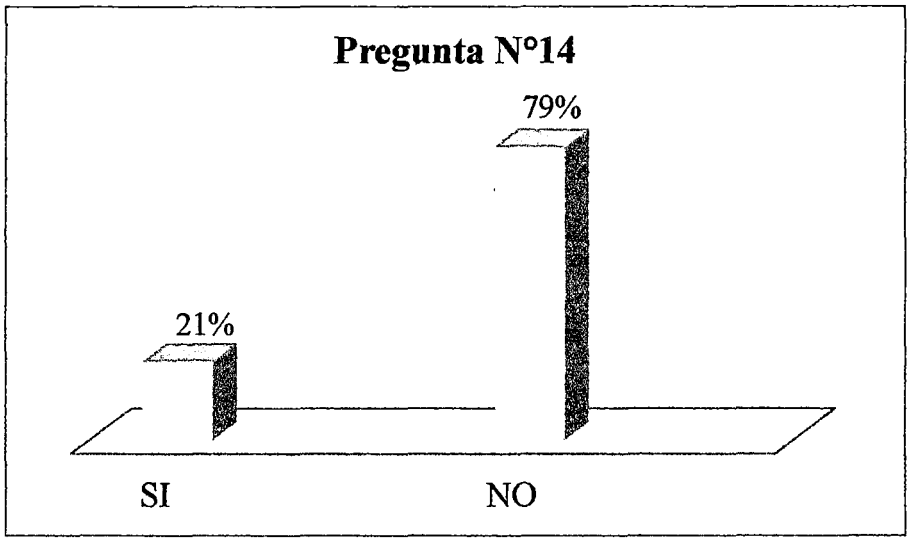
Distribución porcentual de los docentes y administrativos de la UNASAM, según lo que realiza cuando detecta un virus en los equipos informáticos

Alternativa	Total	100%
a	130	50%
b	80	31%
c	8	3%
d	17	6%
e	10	4%
f	17	6%
TOTAL	262	100%



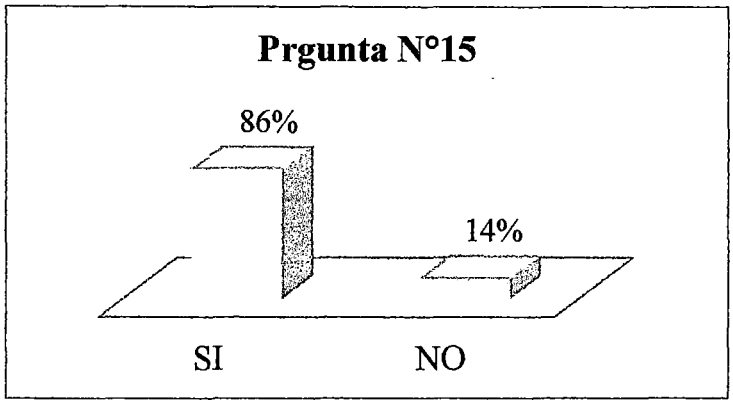
Distribución porcentual de los docentes y administrativos de la UNASAM, según el buen funcionamiento de los antivirus instalados y su adecuada actualización

Alternativa	Frecuencia	Porcentaje
SI	231	88%
NO	31	12%
TOTAL	262	100%



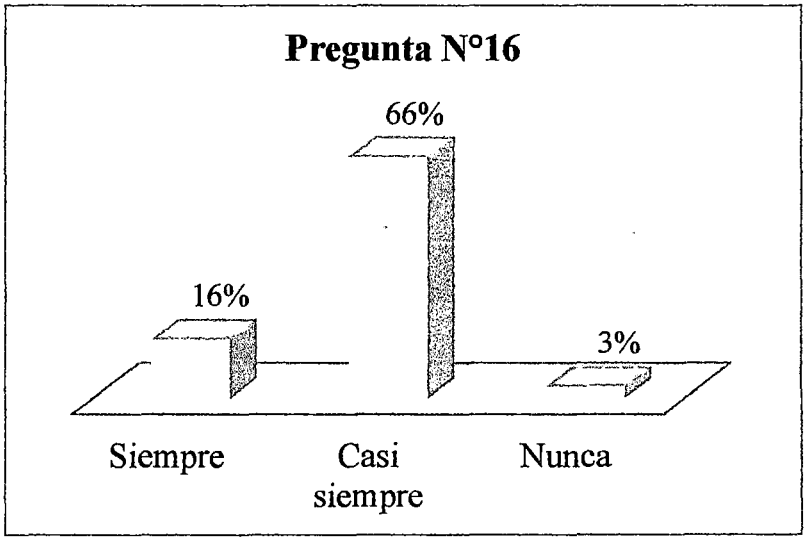
Distribución porcentual de los docentes y administrativos de la UNASAM, según si hacen o no uso del SIGA

Alternativa	Frecuencia	Porcentaje
SI	226	86%
NO	36	14%
TOTAL	226	86%



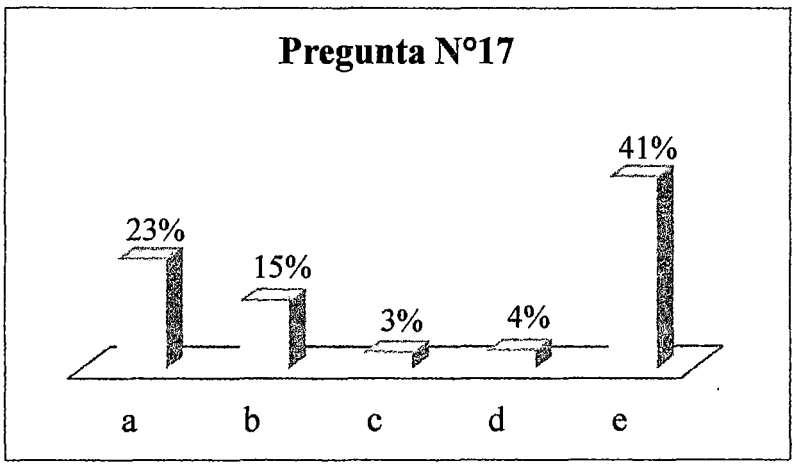
Distribución porcentual de los docentes y administrativos de la UNASAM, según qué tan frecuente es su acceso a la información del SIGA

Alternativa	Frecuencia	Porcentaje
SIEMPRE	43	16%
CASI SIEMPRE	174	66%
NUNCA	9	3%
TOTAL	226	86%



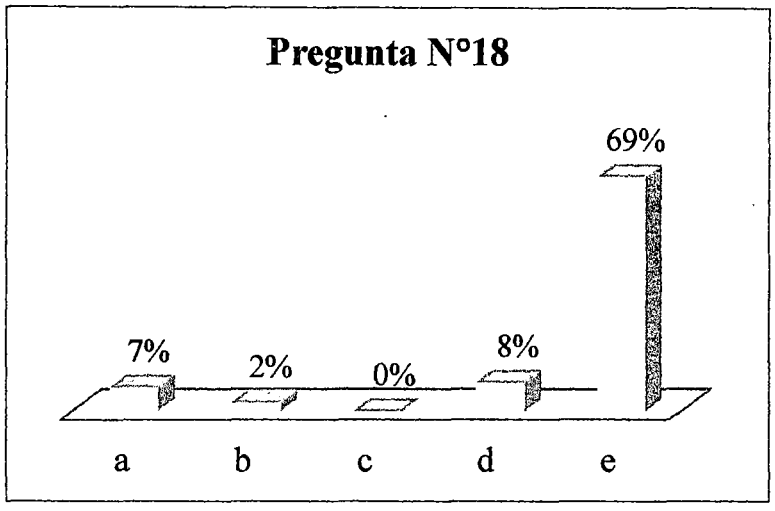
Distribución porcentual de los docentes y administrativos de la UNASAM, según a la referencia que hace la clave de acceso al SIGA que maneja

Alternativa	Frecuencia	Porcentaje
a	61	23%
b	38	15%
c	9	3%
d	10	4%
e	107	41%
TOTAL	226	86%



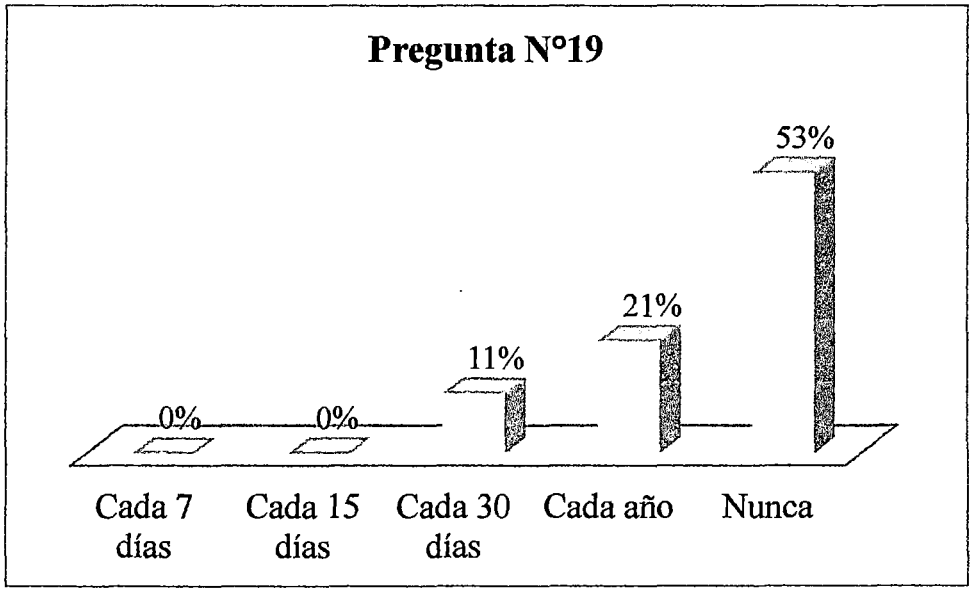
Distribución porcentual de los docentes y administrativos de la UNASAM, según el conocimiento por parte de otras personas respecto a su clave de acceso

Alternativa	Frecuencia	Porcentaje
a	61	23%
b	38	15%
c	9	3%
d	10	4%
e	107	41%
TOTAL	226	86%



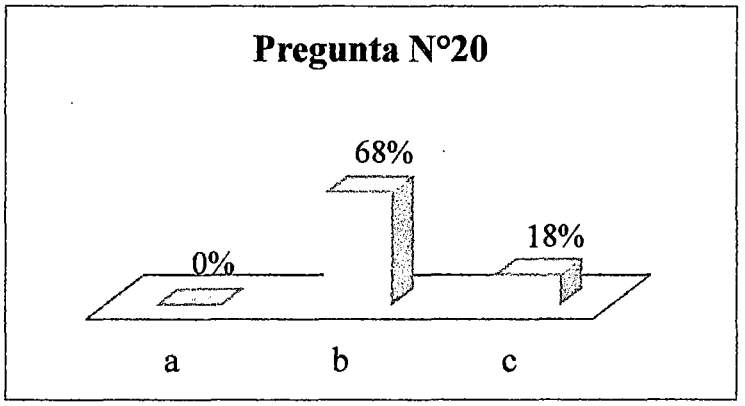
Distribución porcentual de los docentes y administrativos de la UNASAM, según la frecuencia con la que cambia su clave de acceso

Alternativa	Frecuencia	Porcentaje
Cada 7 días	0	0%
Cada 15 días	0	0%
Cada 30 días	30	11%
Cada año	56	21%
Nunca	140	53%
TOTAL	226	86%



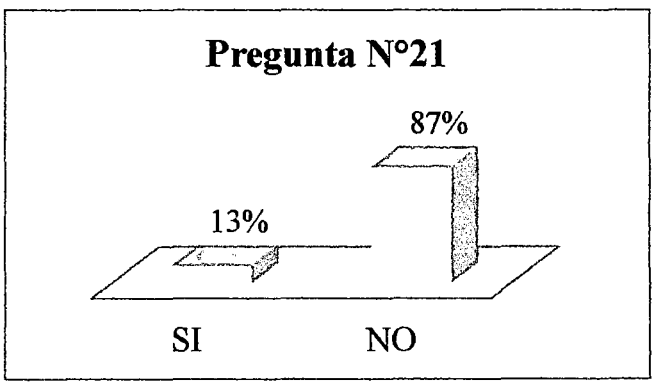
Distribución porcentual de los docentes y administrativos de la UNASAM, según la velocidad de acceso que experimental al ingresar al portal del SIGA WEB dentro y fuera de la UNASAM

Alternativa	Frecuencia	Porcentaje
a	0	0%
b	178	68%
c	48	18%
TOTAL	226	86%



Distribución porcentual de los docentes y administrativos de la UNASAM, según la capacitación recibida acerca de seguridad de la información en la UNASAM

Alternativa	Frecuencia	Porcentaje
SI	34	13%
NO	228	87%
TOTAL	262	100%

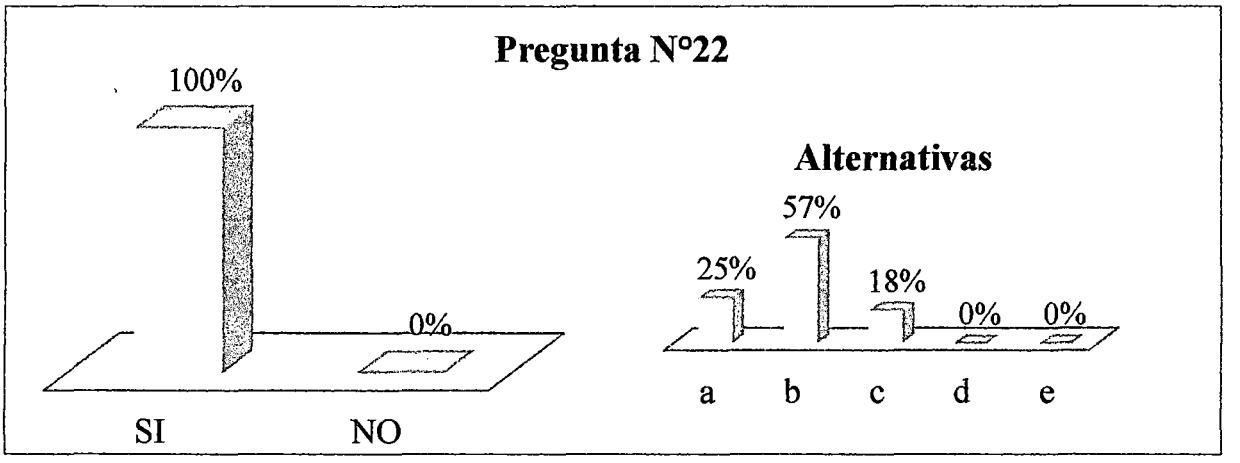


Distribución porcentual de los docentes y administrativos de la UNASAM, según el interés que muestra por adquirir mayor conocimiento sobre seguridad de la información

Alternativa	Frecuencia	Porcentaje
SI	262	100%
NO	0	0%
TOTAL	262	100%

Si la respuesta fue SI, eligió un medio por el cual le interesaría conocer más sobre el tema

Alternativa	Frecuencia	Porcentaje
a	65	25%
b	150	57%
c	47	18%
d	0	0%
e	0	0%
TOTAL	262	100%



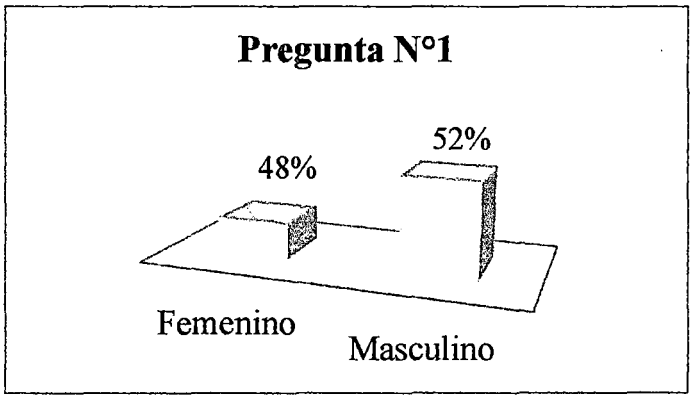
Anexo 8

Resultados de procesamiento de información de alumnos

Distribución porcentual de los alumnos de la UNASAM, según sexo

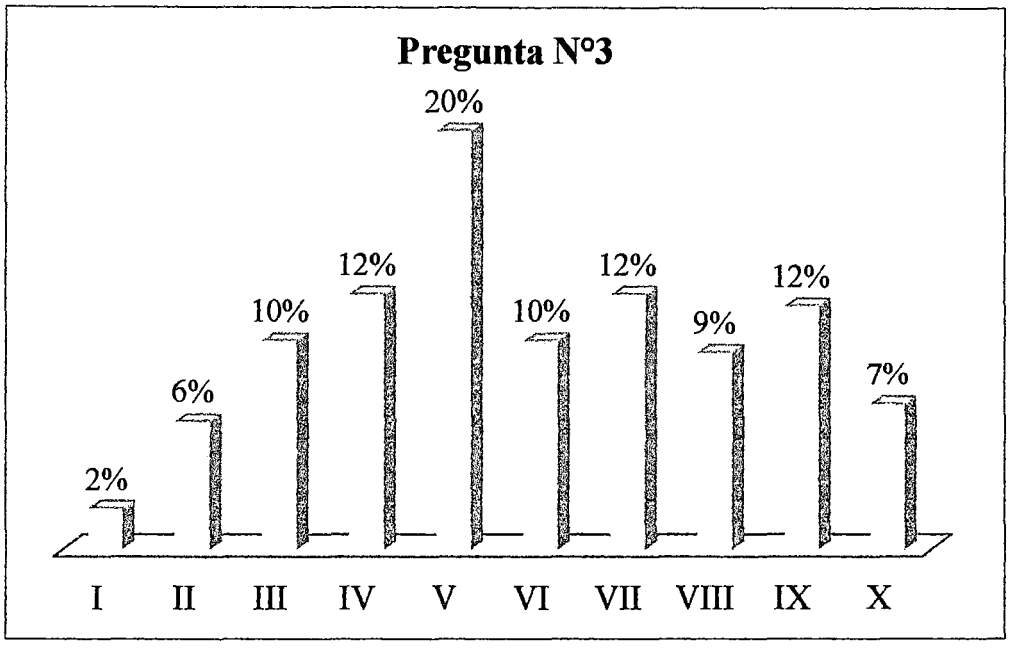
	Frecuencia	Porcentaje
Femenino	173	48%
Masculino	189	52%
TOTAL	362	100%

Fuente (Elaboración propia)



Distribución porcentual de los alumnos de la UNASAM, según el ciclo que está cursando

Ciclo	Frecuencia	Porcentaje
I	7	2%
II	22	6%
III	36	10%
IV	44	12%
V	72	20%
VI	36	10%
VII	44	12%
VIII	34	9%
IX	42	12%
X	25	7%
TOTAL	362	100%

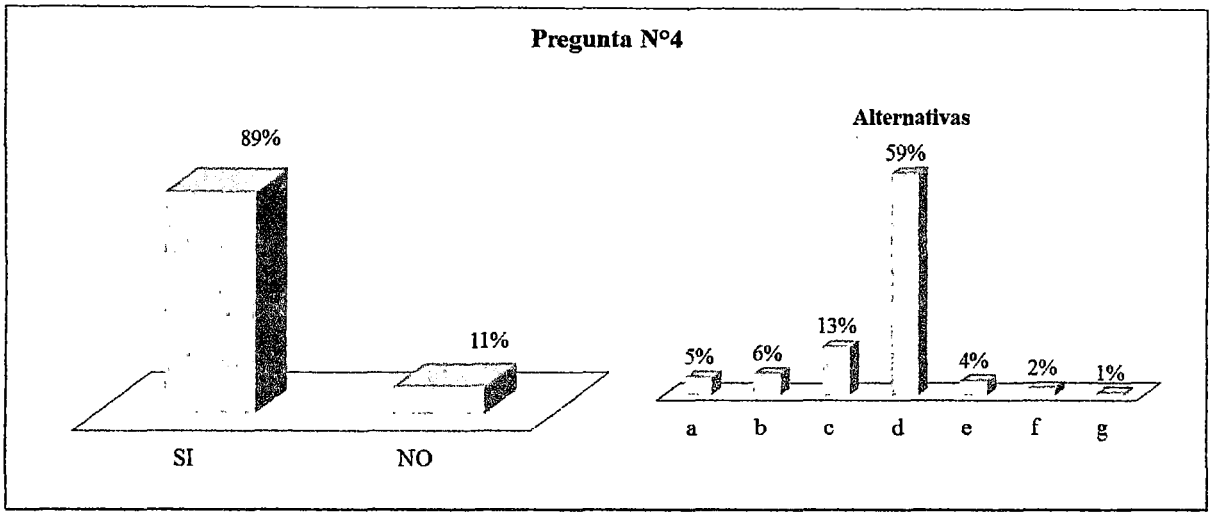


Distribución porcentual de los alumnos de la UNASAM, según el apagado debido de los equipos informáticos después de utilizarlos

Alternativa	Frecuencia	Porcentaje
SI	322	89%
NO	40	11%
TOTAL	362	100%

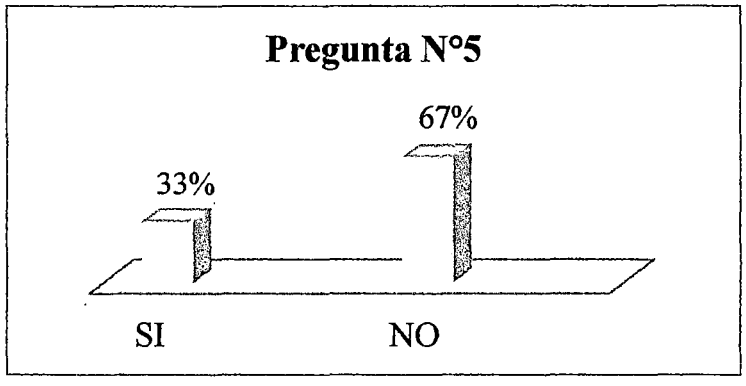
Si la respuesta fue SI:

Alternativa	Frecuencia	Porcentaje
a	17	5%
b	21	6%
c	47	13%
d	215	59%
e	14	4%
f	7	2%
g	2	1%
TOTAL	322	89%



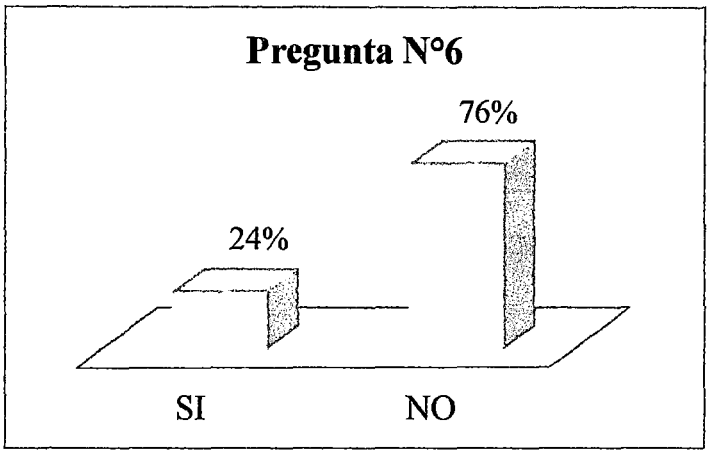
Distribución porcentual de los alumnos de la UNASAM, según la seguridad que tiene en los ambientes en los que se encuentran los equipos informáticos frente a un desastre natural o humano.

Alternativa	Frecuencia	Porcentaje
SI	119	33%
NO	243	67%
TOTAL	362	100%



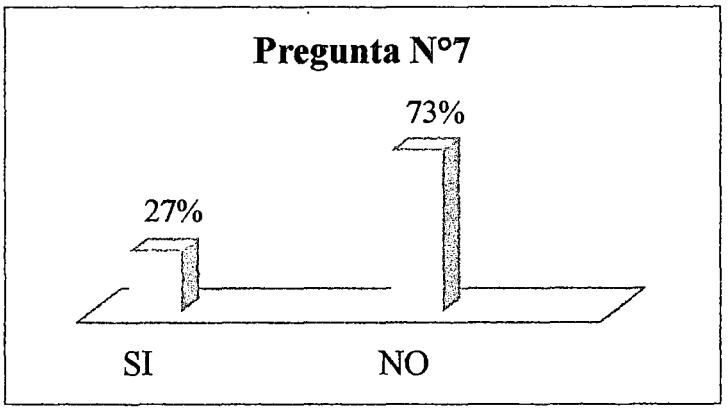
Distribución porcentual de los alumnos de la UNASAM, según observó existe algún extintor cerca de los equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	86	24%
NO	276	76%
TOTAL	362	100%



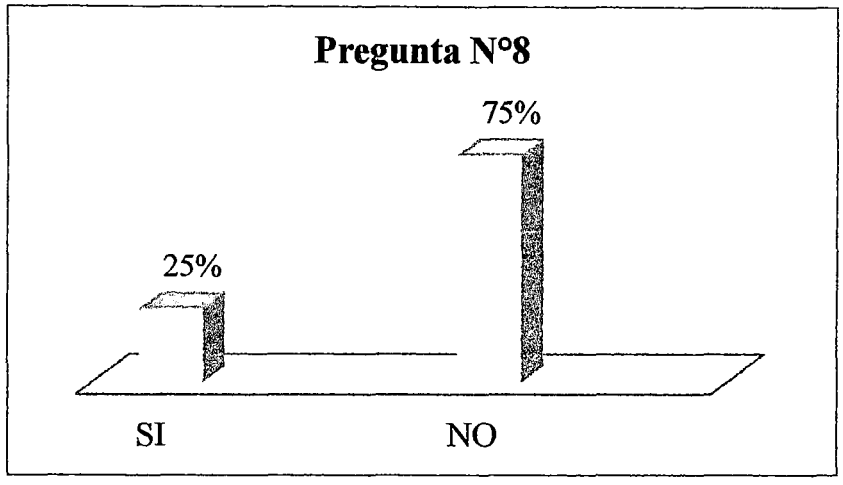
Distribución porcentual de los alumnos de la UNASAM, según observó existe alguna tipo de señalización de emergencias en los ambientes que se encuentran los equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	99	27%
NO	263	73%
TOTAL	362	100%



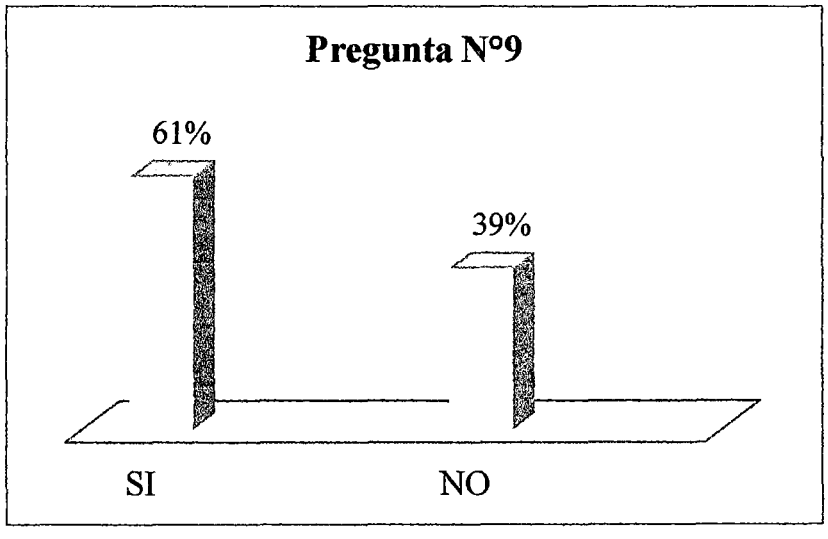
Distribución porcentual de los alumnos de la UNASAM, según la participación de simulacros frente a cualquier desastre específicamente en áreas donde hay equipos informáticos.

Alternativa	Frecuencia	Porcentaje
SI	89	25%
NO	273	75%
TOTAL	362	100%



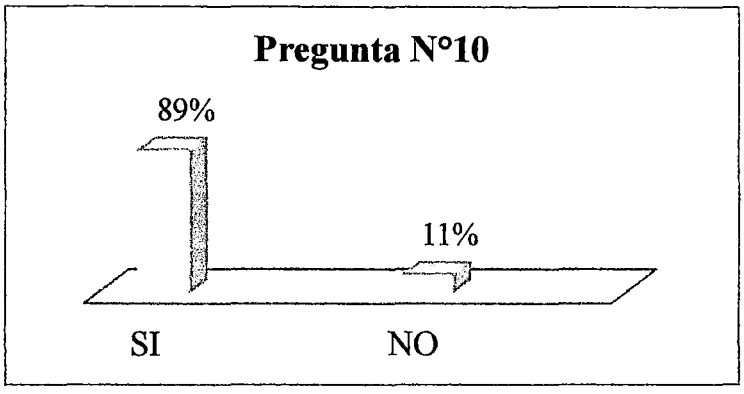
Distribución porcentual de los alumnos de la UNASAM, según la manipulación de componentes del equipo informático de manera que si sufrió algún inconveniente este funcione.

Alternativa	Frecuencia	Porcentaje
SI	221	61%
NO	141	39%
TOTAL	362	100%



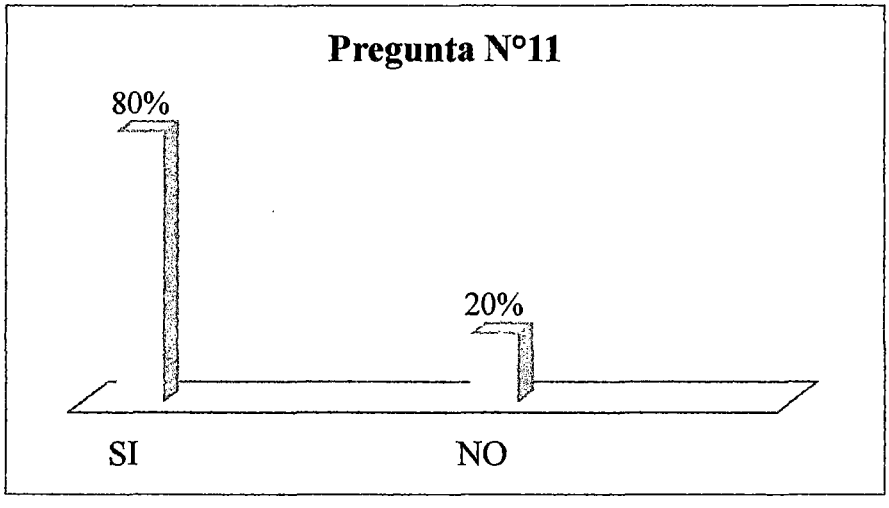
Distribución porcentual de los alumnos de la UNASAM, según la responsabilidad que asume al utilizar un equipo informático.

Alternativa	Frecuencia	Porcentaje
SI	321	89%
NO	41	11%
TOTAL	362	100%



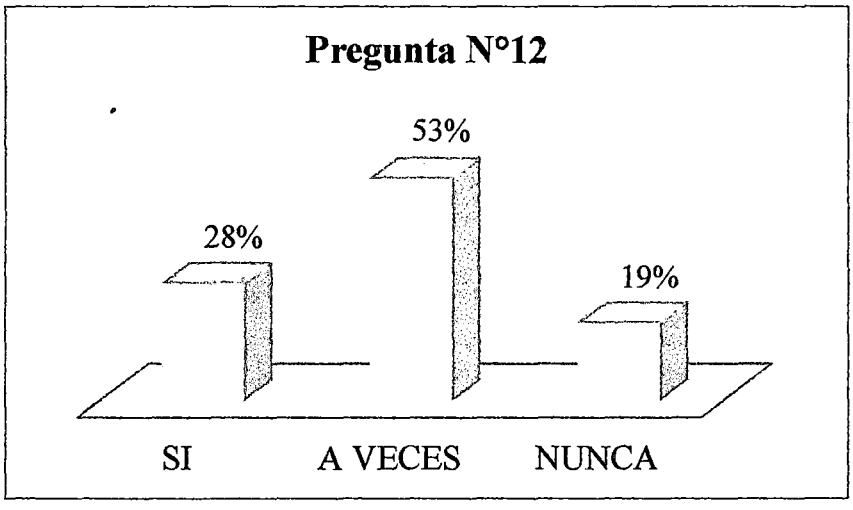
Distribución porcentual de los alumnos de la UNASAM, según la responsabilidad que asumiría si se le detecta realizando actividad sospechosas como el ingreso a lugares restringidos.

Alternativa	Frecuencia	Porcentaje
SI	288	80%
NO	74	20%
TOTAL	362	100%



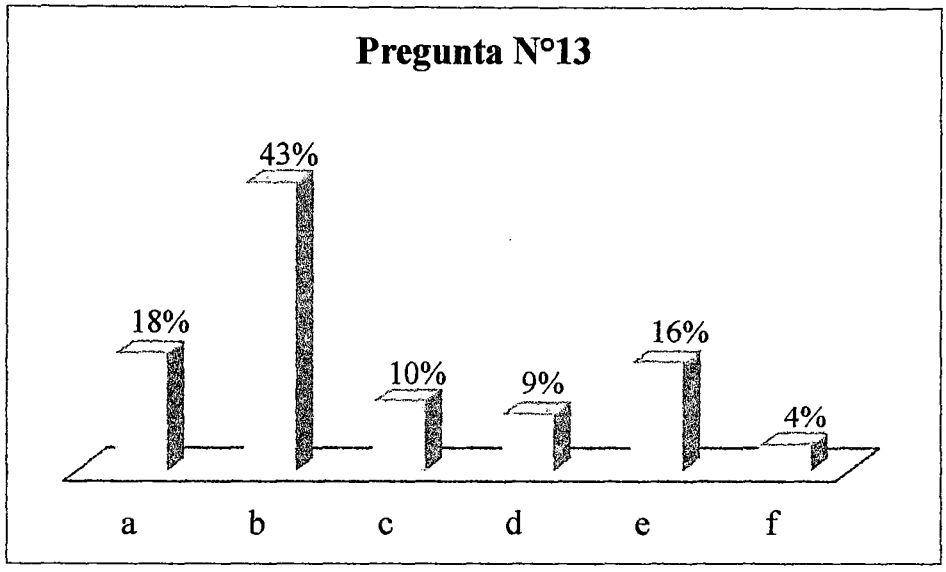
Distribución porcentual de los alumnos de la UNASAM, según el uso de los antivirus en los equipos informáticos cuando ingresa o saca información en algún dispositivo de almacenamiento

Alternativa	Frecuencia	Porcentaje
SI	102	28%
A VECES	192	53%
NUNCA	68	19%
TOTAL	362	100%



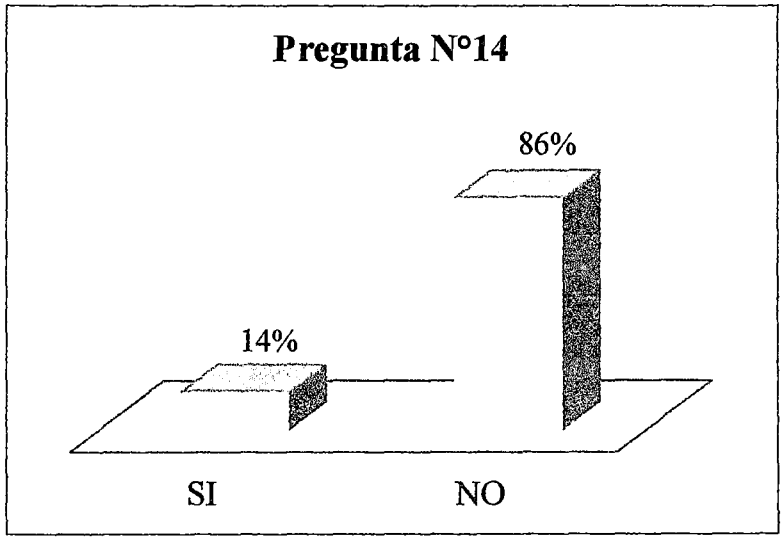
Distribución porcentual de los alumnos de la UNASAM, según lo que realiza cuando detecta un virus en los equipos informáticos

Alternativa	Total	100%
a	64	18%
b	156	43%
c	38	10%
d	31	9%
e	59	16%
f	14	4%
TOTAL	362	100%



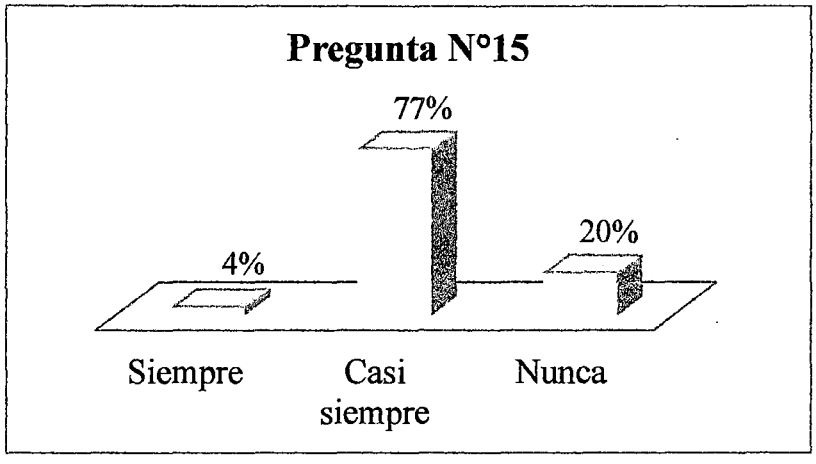
Distribución porcentual de los alumnos de la UNASAM, según el buen funcionamiento de los antivirus instalados y su adecuada actualización

Alternativa	Frecuencia	Porcentaje
SI	52	14%
NO	310	86%
TOTAL	362	100%



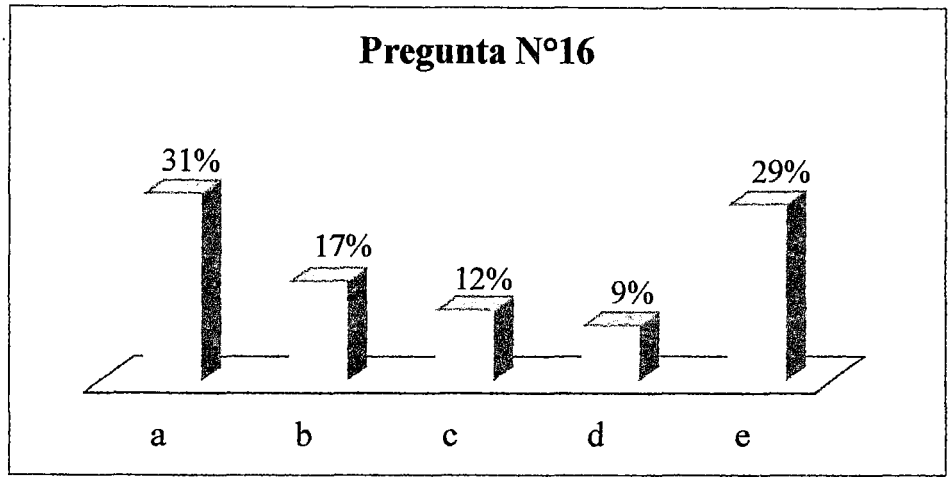
Distribución porcentual de los alumnos de la UNASAM, según qué tan frecuente es su acceso a la información del SIGA

Alternativa	Frecuencia	Porcentaje
SIEMPRE	14	4%
CASI SIEMPRE	277	77%
NUNCA	71	20%
TOTAL	362	100%



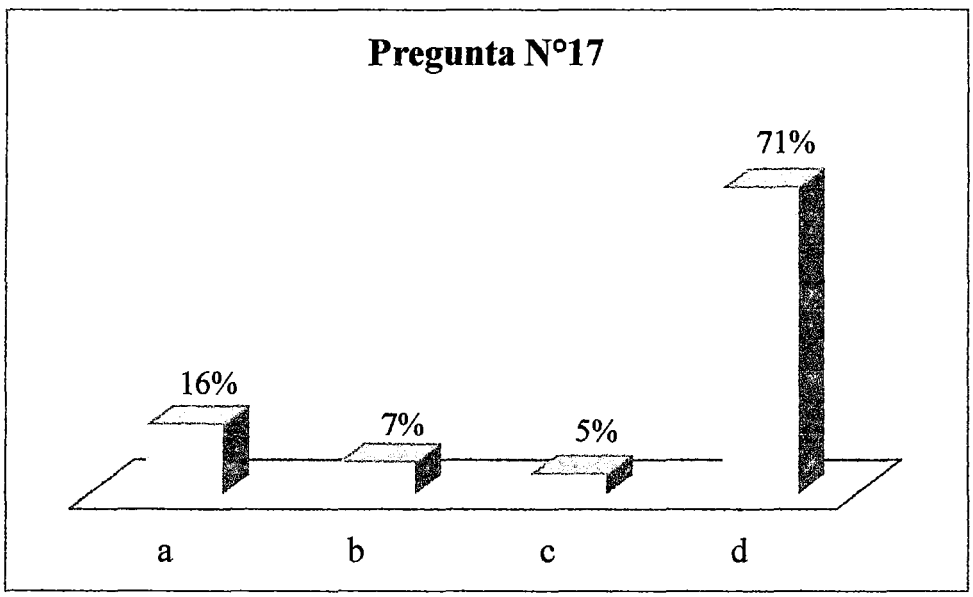
Distribución porcentual de los alumnos de la UNASAM, según a la referencia que hace la clave de acceso al SIGA que maneja

Alternativa	Frecuencia	Porcentaje
a	112	31%
b	60	17%
c	43	12%
d	34	9%
e	106	29%
TOTAL	355	98%



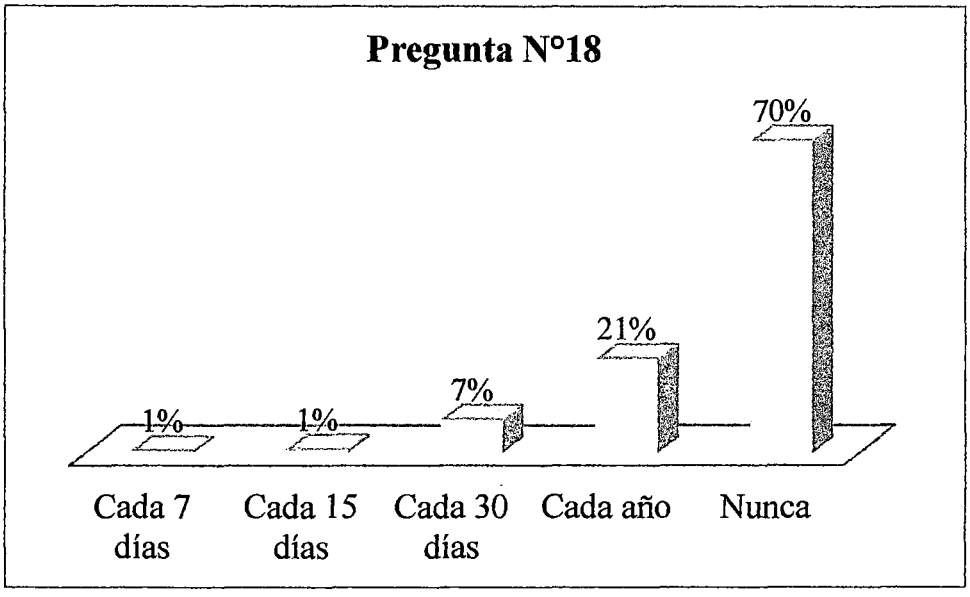
Distribución porcentual de los alumnos de la UNASAM, según el conocimiento por parte de otras personas respecto a su clave de acceso

Alternativa	Frecuencia	Porcentaje
a	59	16%
b	27	7%
c	17	5%
d	257	71%
TOTAL	360	99%



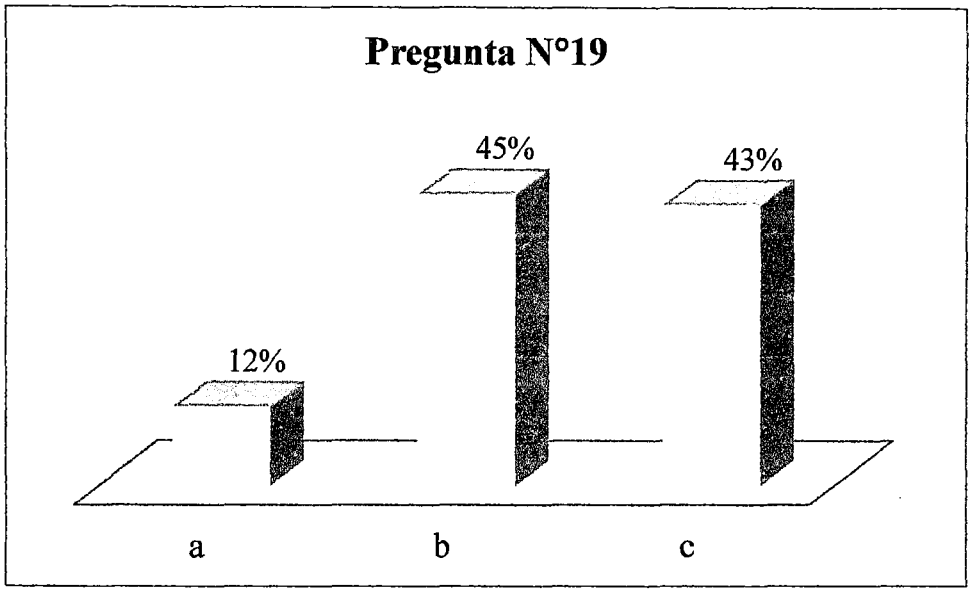
Distribución porcentual de los alumnos de la UNASAM, según la frecuencia con la que cambia su clave de acceso

Alternativa	Frecuencia	Porcentaje
Cada 7 días	2	1%
Cada 15 días	3	1%
Cada 30 días	27	7%
Cada año	76	21%
Nunca	252	70%
TOTAL	360	99%



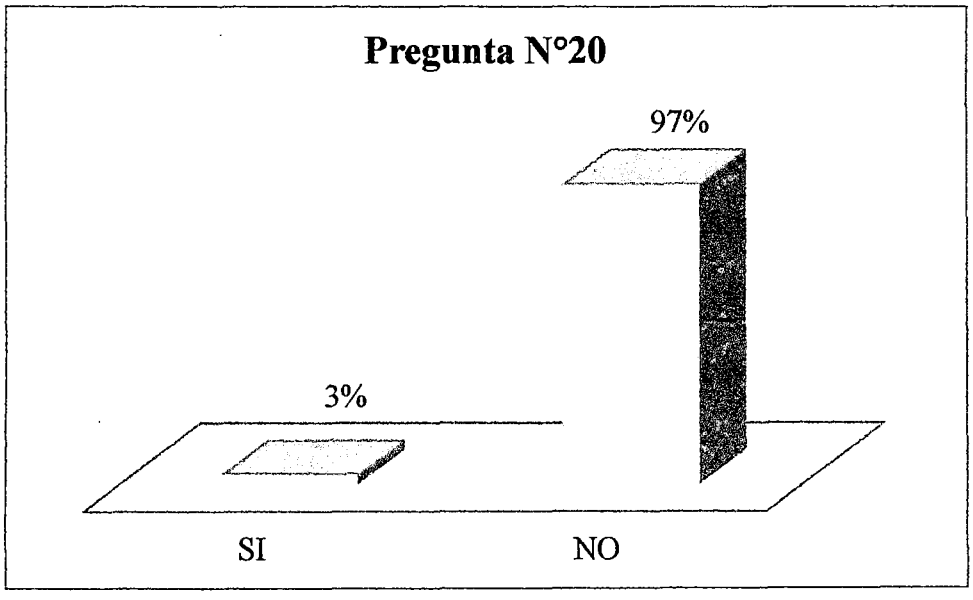
Distribución porcentual de los alumnos de la UNASAM, según la velocidad de acceso que experimental al ingresar al portal del SIGA WEB dentro y fuera de la UNASAM

Alternativa	Frecuencia	Porcentaje
a	44	12%
b	162	45%
c	156	43%
TOTAL	362	100%



Distribución porcentual de los alumnos de la UNASAM, según la capacitación recibida acerca de seguridad de la información en la UNASAM

Alternativa	Frecuencia	Porcentaje
SI	12	3%
NO	350	97%
TOTAL	362	100%

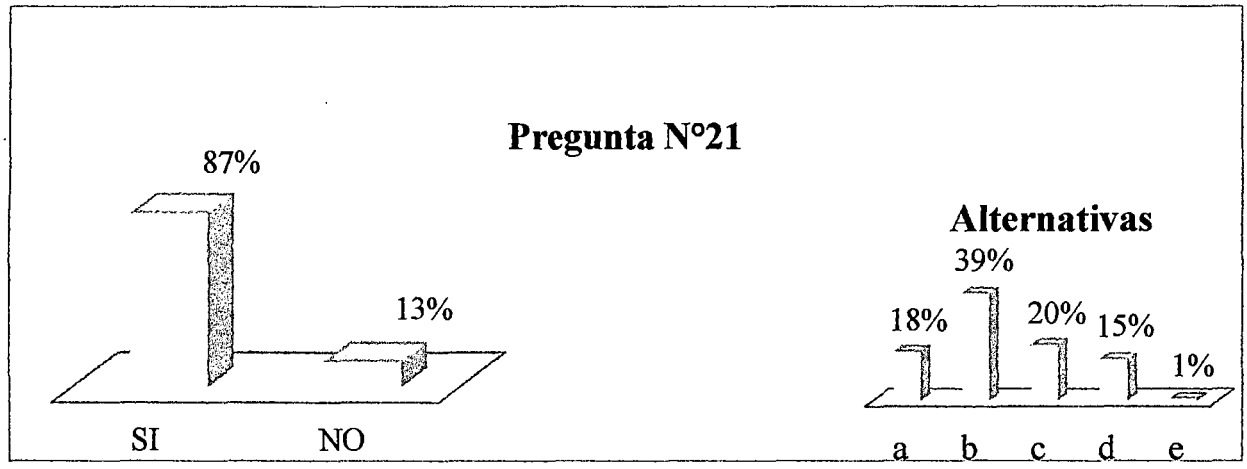


Distribución porcentual de los alumnos de la UNASAM, según el interés que muestra por adquirir mayor conocimiento sobre seguridad de la información

Alternativa	Frecuencia	Porcentaje
SI	315	87%
NO	47	13%
TOTAL	262	100%

Si la respuesta fue SI, eligió un medio por el cual le interesaría conocer más sobre el tema

Alternativa	Frecuencia	Porcentaje
a	65	18%
b	142	39%
c	74	20%
d	55	15%
e	3	1%
TOTAL	339	95%



Anexo 9

Imágenes de la Oficina General de Estudios

Foto1: Ing° Einer Espinoza Muñoz – Jefe de la OGE

Foto2: Lic. Enedina Alejo Pérez –Jefe de URCA

Foto3: Área de los servidores de la base de datos

Foto 4: Equipos mal distribuidos 1

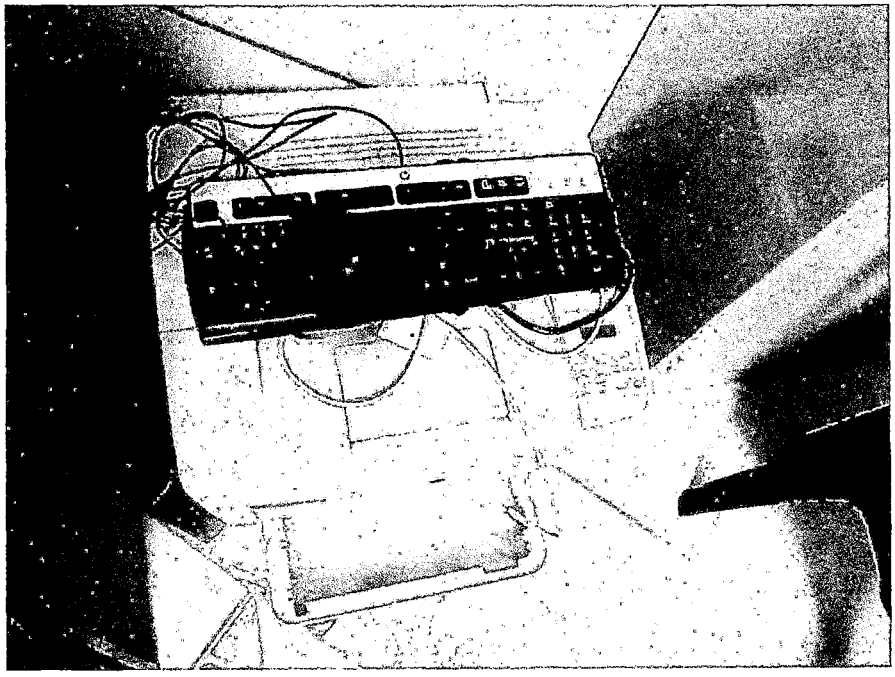
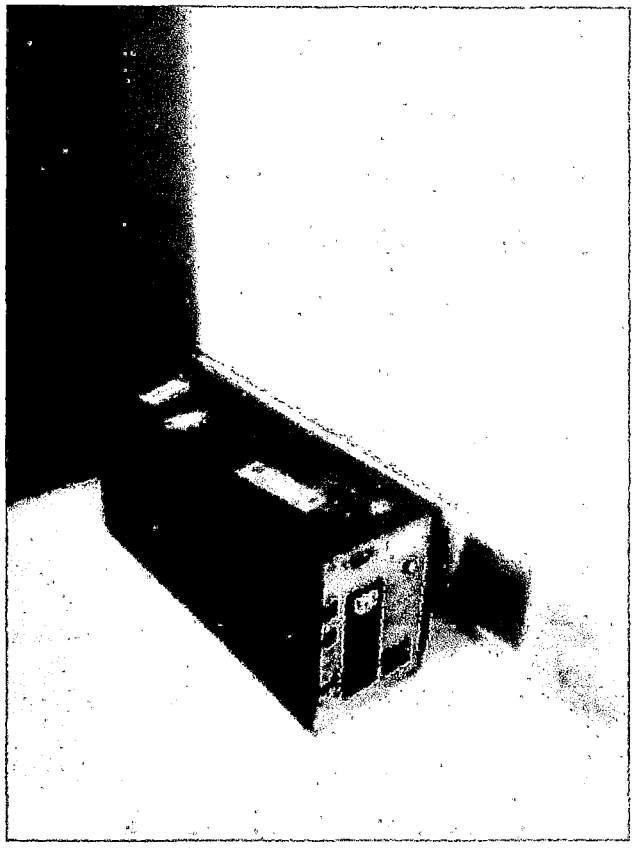


Foto 5: Equipos mal distribuidos 2



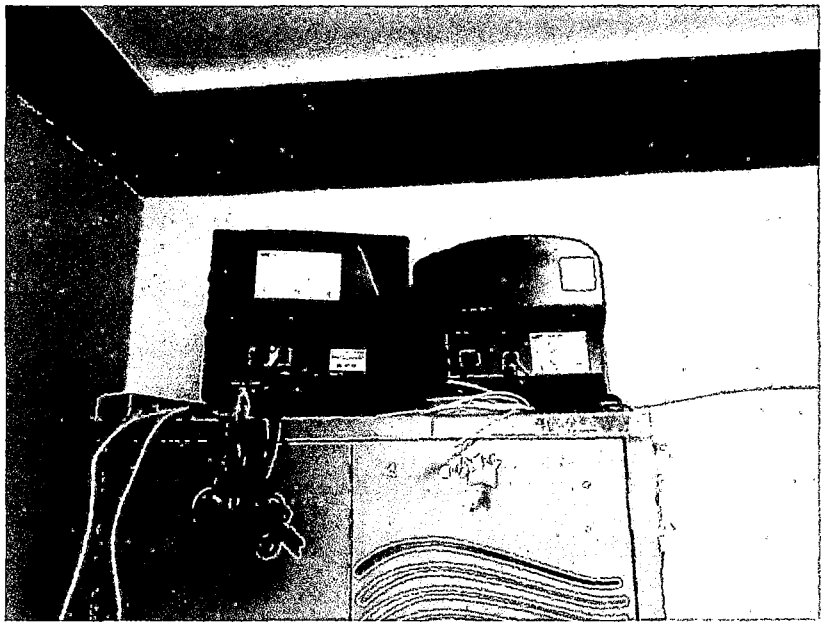
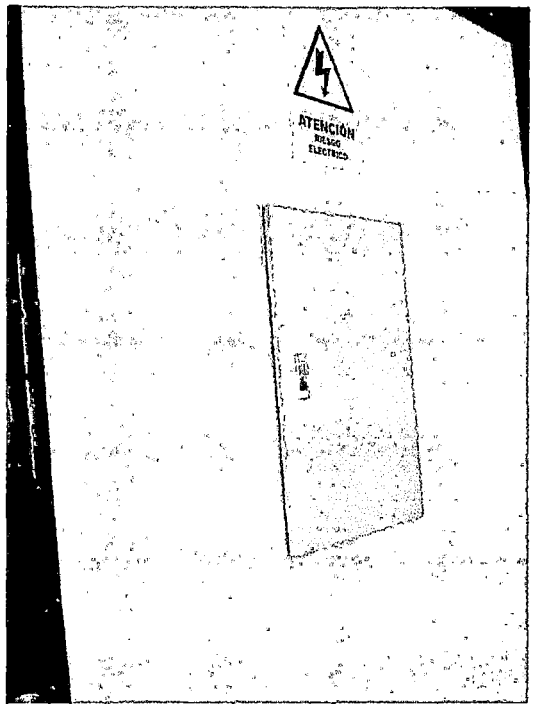


Foto 5: Algunas señalizaciones



Anexo 10