UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

ESCUELA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN ESTRATÉGICA
DE NEGOCIOS CON MENCIÓN EN GESTIÓN EMPRESARIAL

PROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE ADMISIÓN Y REGISTRO ACADÉMICO DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO, 2016

Oscar Atalaya Vásquez

Asesor: Víctor Hugo Delgado Céspedes

Cajamarca, Perú

Junio – 2016

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

ESCUELA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN ESTRATÉGICA
DE NEGOCIOS CON MENCIÓN EN GESTIÓN EMPRESARIAL

PROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE ADMISIÓN Y REGISTRO ACADÉMICO DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO, 2016

—Tesis presentada en cumplimiento parcial de los requerimientos para el Grado Académico de Magíster en Administración Estratégica de Negocios, mención en Gestión Empresarial

Oscar Atalaya Vásquez

Asesor: Víctor Hugo Delgado Céspedes

Cajamarca, Perú

Junio - 2016

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

ESCUELA DE POSGRADO

APROBACIÓN DE MAESTRÍA

PROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE ADMISIÓN Y REGISTRO ACADÉMICO DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO, 2016

Presidente: _____

Secretario: _____

Vocal: _____

Asesor: **Víctor Hugo Delgado Céspedes**

A:

Mi familia, en especial a mi madre y al ser que es mi razón de superación día a día, mi pequeño hijo Oscar Joaquín

AGRADECIMIENTOS

- A la institución en donde me he venido desarrollado laboral y profesionalmente, la UPAGU, especialmente a las autoridades y compañeros que me impulsaron en este reto.
- A los integrantes del Departamento de Admisión y registro Académico de la UPAGU, quienes me brindaron el apoyo incondicional para la finalización del presente trabajo.
- A los amigos y familiares que colaboraron de una u otra forma en la consolidación de este trabajo con la orientación y los consejos pertinentes.
- Al Dr. Víctor Hugo Delgado Céspedes por el continuo asesoramiento para que este trabajo se convierta en un trabajo profesional de calidad.

ÍNDICE DE CONTENIDOS

Items **Pág.**

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente informe de investigación, se pretende verificar la existencia de riesgos en la seguridad de la información que corresponde al Departamento de Admisión y Registro Académico (DARA) de la Universidad Privada Antonio Guillermo Urrelo. Específicamente se trata de la preocupación por los riesgos que puedan encontrar. Esto impulsa a proponer una alternativa para proteger los activos de la información con base en la preservación de los tres principios básicos: la integridad, la confidencialidad y la disponibilidad de la información. Para ello se propone un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como metodología lo señalado en la norma internacional ISO/IEC 27000, que nos provee las estrategias a seguir, teniendo en cuenta la aplicación de los instrumentos de investigación, estas estrategias son: a) definir los procesos core del DARA, b)definir los activos de información que son utilizados en los procesos hallados, los cuales fueron clasificados en tres grupos fundamentales que son la misma información, los equipos e infraestructura que la soportan y las personas que la utilizan; c)identificación de los riesgos que pueden afectar a los activos, d)valoración de los elementos antes mencionados. Concluido el trabajo se concluyó en que los activos del DARA tienen riesgos que podrían afectar la continuidad de los procesos; por ello es necesario definir la propuesta. Se sugiere, además, la implementación inmediata del SGSI, así como la utilización de un software especializado que soporte al SGSI y este adecuado a la norma para un efectivo control.

ABSTRACT

The purpose of this research report is to verify the existence of security risks on the information regarding the Department of Admission and Academic Registry (DAAR) of the Antonio Guillermo Urrelo Private University. It is specifically the concern about the risks they may occur. It drives to propose an alternative to protect the information assets, always trying to maintain the three basic principles: integrity, confidentiality and information availability. This requires an Information Security Management System (ISMS), whit the use of methodology stated by the international norm ISO / IEC 27000, which provides us with the strategies to follow, considering the applications of research instruments, such strategies are: a) define the core processes of DAAR, b) define the information assets used on the processes found, which were classified into three main groups the information itself, the equipment and infrastructure that support it and people that use it; c) identification of risks that may affect the assets, d) assessment of the former elements. After finishing the work it was concluded that the DAAR assets take on risks that may affect the continuity of the processes; this is why it is necessary to evaluate the proposal. It also suggests the immediate implementation of ISMS, as well as the use of a specialized software that can supports ISMS which must be adequate to the norm for an effective control.

INTRODUCCIÓN

El presente trabajo se fundamentó por la problemática que se pudo apreciar en los procesos de tratamiento de la información, dentro de la Universidad Privada Antonio Guillermo Urrelo (UPAGU), específicamente en el Departamento de Admisión y Registro Académico.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y, en muchos casos, llegando a tener un valor superior. Por esto y otros motivos, la seguridad de la información es un asunto tan importante para todos, pues afecta directamente a los negocios de una empresa o de un individuo. Además tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que las conocen.

En esta investigación, se propuso identificar la existencia de riesgos en la seguridad que pueda tener la información dentro del Departamento de Admisión y registro Académico (DARA) de la UPAGU y a partir de los resultados proponer un sistema de seguridad de la información, mismo que buscará asegurar los principios básicos de la información y los elementos con los que interactúa.

El informe de investigación está estructurado en cinco capítulos. El primer capítulo presenta el problema de investigación, en él se encuentra la formulación del problema, los objetivos y justificación de los mismos, que son las directrices del presente trabajo; además se evaluaron las limitantes y los aspectos que dan la viabilidad de esta investigación, centrándonos más que todos en los aspectos tecnológicos, económicos, legales.

En el segundo capítulo se establece el marco teórico, que dio el soporte al presente trabajo, se desarrolla una recopilación de los temas centrales que fundamentaron la seguridad de la información. Además se detallan las definiciones más importantes para comprender la terminología bases de esta investigación.

El procedimiento metodológico se detalla en el capítulo tres, en donde se describen los elementos que norman a este trabajo de investigación. Se ha dimensionado las variables de acuerdo al problema establecido, puesto que este trabajo se enfocó en tres aspectos generales, que permite tener una visión más clara. La seguridad de la información de acuerdo a la teoría se puede abarcar de tres puntos, la seguridad de la información propiamente dicha, la seguridad en los equipos que soportan la información incluida la infraestructura y también se incluye los aspectos de seguridad en las personas que usan a la información, es así que en base a estos tres puntos se ha dimensionado la investigación que se detallan en el capítulo indicado; además se describe la investigación que se utilizó para este trabajo, el tipo, diseño y también los métodos y técnicas.

Posteriormente en el capítulo cuatro se realiza la evaluación respecto a los resultados obtenidos luego de la aplicación de los instrumentos y el análisis

correspondiente, para este caso se aplicaron encuestas, entrevistas y la observación directa, lo que permitió alcanzar resultados que sirvieron para corroborar la hipótesis planteada y poder realizar la propuesta de un sistema de gestión de seguridad de la información. Justamente, los resultados de esta investigación son los que permitieron realizar una adecuada propuesta, pues es de aquí, de los resultados obtenidos en donde se plasma la base para realizar la propuesta consistente para la institución, hoy en día se cuentan con normas y estándares que pueden orientar este tipo de trabajo pero la base de una correcta propuesta dependerá del análisis concienzudo de los resultados, cada dimensión tendrá sus resultados y luego se planteará una propuesta a medida de la institución. No serviría de nada tratar de realizar una propuesta de un sistema de gestión de seguridad si no se tiene una base sólida con respecto a la realidad encontrada.

En el quinto capítulo se plasma la propuesta del Sistema de Gestión de Seguridad de la Información, dicha propuesta está definida sobre la base de los resultados obtenidos en el presente trabajo de investigación.

Finalmente se precisan las conclusiones obtenidas luego de finalizada la presente investigación, y las recomendaciones que se han generado a partir de la misma, esto con el afán de contribuir con la gestión de seguridad de la información dentro de la Universidad Privada Antonio Guillermo Urrelo.

Es pues que partiendo de la idea de contribuir con un tema demasiado importante y que hoy en día es descuidado, se espera que este modesto trabajo sea un punto de inicio para este tipo de investigaciones y se empiece a dar la importancia requerida a la seguridad de la información, no solo de la universidad, sino también de otras

instituciones incluso de distintos sectores, ya que toda institución u organización tiene algo en común como son los procesos que justamente utilizan la información y de los que dependen en gran medida, y es esta dependencia la que obliga a dar mayor importancia a su seguridad, para garantizar la continuidad de las organizaciones.

El autor

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1. Desarrollo de la realidad problemática

Se conoce que desde tiempos antiguos, la seguridad se ha convertido en un aspecto primordial en el ser humano y además en la realización de cualquier actividad o situación diaria de su vida, como lo menciona Rosales (2002, p. 33), al establecer que "La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella". Según con lo afirmado, coincidimos que la seguridad se convierte en una necesidad básica, ya sea en nuestra vida cotidiana o dentro de alguna actividad científica o tecnológica y la que nos servirá para prevenir, mantener el funcionamiento y resguardar posesiones. En toda actividad humana siempre se necesita estabilidad y protección de bienes, siendo uno de ellos y quizá la más importante la información.

Al igual sucede en las organizaciones, donde existe el riesgo de perder la información, lo que podría causar que se detenga las operaciones, deteniendo los procesos de producción o procesos administrativos, en tal sentido es necesario poseer estrategias para mantener el funcionamiento de las organizaciones basadas también en preservar y asegurar su información; existen diferentes maneras o métodos de proteger la información y poder asegurar este activo tan importante.

La seguridad de la información se garantizará solo si se ordenan y reúnen todos los elementos y métodos que la hacen posible, ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables y riesgos, así lo da a entender, Hallberg (2003, p.97). "La seguridad informática

solo brinda áreas de oportunidad, en los sistemas informáticos y no brinda por si sola seguridad en la información de la organización, la seguridad informática, no puede por sí misma ser la que proporciona la protección para su información". La manera en que manejamos (Hallberg, 2003), la seguridad de la información ha evolucionado con el tiempo, a medida que nuestra sociedad y tecnología evolucionan, por ello es importante comprender esta evolución para entender como necesitamos enfocar la seguridad informática en la actualidad (Maiwald, 2005), puesto que, lo que en algún momento es seguro con el paso del tiempo ya no lo es. Hoy en día casi la totalidad de organizaciones han implementado tecnologías que le permiten mejorar sus procesos, en donde también es con el fin de que sus colaboradores puedan acceder rápidamente a toda la información empresarial, de aquí es que se ha confiado completamente la información a los sistemas computacionales.

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las organizaciones deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes, llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas (NTP ISO/IEC 17799). La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información (NTP ISO/IEC 17799); es decir, buscar protegerla tanto de ataques físicos, como robos o incendios, y de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información. En nuestro país, desde hace más de diez años, las políticas del

gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información. Posteriormente se mejora la norma y se publica en mayo del 2012, que corresponde al diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27001:2008 mediante la resolución ministerial N° 129-2012-PCM. Ambas normas técnicas peruanas están basadas en la familia de normas ISO 27000 correspondiente a seguridad de la información. La primera, es el estándar principal de esta familia y menciona cuáles son los requerimientos para desarrollar un sistema de gestión de seguridad de la información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check - Act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión (NTP ISO/IEC 27001).

En la Universidad Privada Antonio Guillermo Urrelo, no se ha implementado ninguna estrategia que tenga como fin el mitigar cualquier problema acerca de la seguridad de su información, se cuenta con unidades cuyas funciones tienen las tareas informáticas y el soporte informático, siendo esta última quien debería garantizar la seguridad en los ambientes informatizados y lo hace solo con la visión de la existencia de virus informáticos. Ante la gran importancia de la información que es manejada en esta organización, se debe ampliar obligatoriamente esta simple visión y considerar estrategias en todo nivel que permitan salvaguardar la información

que es el activo más importante, adicionalmente es importante señalar que existe información almacenada en forma física como documentos, así como también el conocimiento del personal de la organización, que deberían ser protegidos.

Además en la UPAGU, existen áreas unas más críticas que otras, en donde la información y su uso es más relevante, por la naturaleza de la organización que es una entidad educativa y la información académica es la más valiosa y se ha definido como la unidad más crítica al Departamento de Admisión y Registro Académico (DARA) y en donde se ha determinado que podía existir mayor riesgo en la seguridad de la información. A partir de esta preocupación y además de la carencia de estrategias que salvaguarden la información en todo nivel dentro de la UPAGU, se procedió a la elaboración de un trabajo de investigación que permita avizorar los problema concernientes a la seguridad de la información dentro del DARA, precisando como objeto de estudio la falta de políticas de seguridad y un sistema de gestión de seguridad de la información en dicho departamento de la Universidad Privada Antonio Guillermo Urrelo de Cajamarca.

1.2. Formulación del problema

¿Cuáles son las condiciones de seguridad de la información y qué propuesta se puede formular para el Departamento de Admisión y Registro Académico de la Universidad Privada Antonio Guillermo Urrelo - 2016?

1.3. Objetivo general

Diagnosticar las condiciones de seguridad de la información y formular una propuesta para el Departamento de Admisión y registro Académico de la Universidad Privada Antonio Guillermo Urrelo - 2016.

1.4. Objetivos específicos

a) Identificar los procesos core del Departamento de Admisión y Registro Académico (DARA) de la Universidad Privada Antonio Guillermo Urrelo.

b) Identificar y evaluar los activos de información ligados a los procesos core encontrados en el DARA.

c) Identificar los riesgos y valorar dichos riesgos a los que están expuestos los activos encontrados.

d) Proponer un Sistema de Gestión de Seguridad de la Información para el DARA.

1.5. Justificación de la investigación

En nuestra realidad actual donde la constante, son los cambios tecnológicos; la gestión de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda la importancia debida con un adecuado control y tratamiento apropiado. Una efectiva administración sobre este tema, se convierte en un aspecto estratégico de negocio y regulación no solo de tecnología. La gestión de la seguridad de la

información entonces debe lidiar con estos aspectos de una manera proactiva y oportuna, para así poder ser considerada como efectiva, y además estar siempre alineada a los objetivos y estrategias del negocio de la organización.

Tomando como base lo expuesto surge la necesidad que toda institución deba contar con un Sistema de Gestión de Seguridad de la Información, el cual le permita administrar toda su información, garantizando los principios de confidencialidad, integridad y disponibilidad que esta debe cumplir; no escapa a esta necesidad la UPAGU quien necesita garantizar la continuidad de su negocio, manteniendo una adecuada gestión en la seguridad de la información y en especial en su unidad más crítica, el Departamento de Admisión y Registro Académico, en donde se debe centrar el estudio, para analizar los riesgos y la manera de implementar una adecuada estructura de Políticas de Seguridad

1.6. Limitaciones del estudio

a) El estudio se limitó a la unidad del Departamento de Admisión y Registro Académico (DARA) de la Universidad Privada Antonio Guillermo Urrelo de la Ciudad de Cajamarca.

b) El estudio se medió en un momento específico, se consideró el periodo de enero a mayo del 2016.

c) La investigación no consideró la implementación del Sistema de Gestión de Seguridad de la información en la organización.

1.7. Viabilidad del estudio:

Para la viabilidad de este trabajo, se realizó la referencia en base a tres aspectos importantes, técnicos, económicos y legales.

a) Viabilidad económica: El presente trabajo fue viable económicamente pues el presupuesto fue asumido por el investigador y la UPAGU en los 6 meses que se llevó a cabo dicho trabajo de investigación así como la redacción del mismo, lo que no conlleva a costos elevados.

b) Viabilidad técnica: También este trabajo fue viable técnicamente pues el investigador posee el conocimiento y las herramientas tecnológicas para el desarrollo del mismo, a pesar de encontrar herramientas nuevas, estas no presentaron dificultad en su utilización.

c) Viabilidad legal: Finalmente en este aspecto el presente trabajo también fue viable legalmente pues no infringe ninguna normatividad legal actual del país, así como de la normatividad vigente de la UPAGU, además se da un compromiso ético por parte del investigador para la evaluación de la información que se encuentre durante el proceso de investigación.

Por lo expuesto anteriormente se precisa que este trabajo de investigación desde el momento de su formulación y hasta su conclusión fue viable acorde a los procedimientos y alcances establecidos.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Antecedentes de la realidad objeto de investigación

2.2.1. Internacionales

Pallas, en su propuesta de "*Metodología de Implantación de un SGSI en un grupo empresarial jerárquico",* En este trabajo, se analizan diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico. Se presentan además diferentes alternativas estratégicas y se discute sobre su conveniencia o no. Se analizan diferentes métodos conocidos de análisis y gestión de riesgos. Algunos de ellos promovidos por los gobiernos y/o industria de países de vanguardia y trayectoria reconocida en la seguridad de la información que han tenido gran aceptación. Concluye lo siguiente:

Un grupo empresarial, con una estructura de relación jerárquica o de subordinación, requiere de una metodología que permita gestionar la seguridad de la información atendiendo este aspecto estructural y jerárquico, con criterios alineados a la estrategia empresarial, y además de cooperación en todas las etapas del ciclo PHVA (PDCA), pero a su vez con la flexibilidad y agilidad operativa suficiente para alcanzar los niveles de seguridad (Pallas, 2009, pág. 149).

Buenaño y Granda, en su trabajo de tesis titulado "*Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001-27002*. Trabajo en el cual se realiza una evaluación a las políticas sobre seguridad de la información en la sede Guayaquil de la Universidad Politécnica Salesiana, a partir de estos resultados mejorar y reforzar las políticas, con la implementación de un Sistema de Gestión de la Seguridad de la Información. Concluyen que:

El adecuado manejo de una política documentada, ayudará en futuros procesos de auditoría, para conocer los orígenes de cada uno de los

cambios, como también identificar posibles omisiones a la seguridad que se han originado con el transcurso y avance de la tecnología.*"* (Buenaño & Granda, 2009, pág. 186)

2.2.2. Nacionales

Aguirre, en su trabajo "D*iseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A*.", decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo, todo el trabajo está basado en la normas derivadas de la familia de la norma ISO/IEC 17799:2007. En este trabajo de tesis se concluyó que:

Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas. (Aguirre, 2014, pág. 55)**.**

Ampuero, en su investigación *"Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros",* toma como referencia la circular G140 de la Superintendencia de Banca, Seguros y AFP del 2009, que estipula que todas las empresas peruanas que son reguladas por este organismo deben contar con un plan de seguridad de información. De ahí es que dicha tesis busca diseñar un sistema de gestión de seguridad de información para una compañía de seguros que cubra lo que pide la circular para evitar problemas

regulatorios con este organismo. Para esto, utiliza 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). En este trabajo, se concluye:

> Es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información de la compañía y, dado que se trata de una compañía de seguros peruana, poder cumplir con las regulaciones de la SBS cumpliendo con el contenido de la circular G-140 y evitar así que la compañía incumpla con las regulaciones de la superintendencia. (Ampuero, 2011, pág. 91).

2.2.3. Locales

Chávez, en su trabajo *"Implementación de un Sistema de Seguridad en la Municipalidad Distrital de Baños del Inca",* pretende implementar un sistema de controles para garantizar la seguridad de la información en la Municipalidad Distrital de Los Baños del Inca, tomando como base normas y estándares nacionales e internacionales. El trabajo solamente se enfocó en las áreas de contabilidad y logística, luego a partir de los resultados obtenidos se evaluó la implicancia de la implementación de este sistema de control en el comportamiento de los usuarios. Una de las conclusiones fue:

> Se ha determinado que casi la totalidad del personal de la Municipalidad de los Baños del Inca, no se encuentra preparada para un cambio en el sentido de preservar la seguridad informática, estos demuestran un rechazo a las nuevas políticas que se han propuesto y a los procesos que de ellos se desprenden, sin tener en cuenta la importancia que involucra para toda la organización. (Chávez, 2012, pág. 87)**.**

2.2. Bases teóricas

2.2.1. Bases teóricas sobre análisis de riesgos

Se ha tomado como referencia para describir el Análisis de riesgo, lo propuesto por Sotelo, Torres y Rivera (2012), en su guía:

2.2.1.1. Procesos del análisis de riesgos

La incorporación acelerada de las tecnologías de información en las entidades privadas y públicas ha dado paso a nuevos retos, siendo uno de los relevantes la gestión de la seguridad de sus activos de información, toda vez que son críticos para su competitividad o supervivencia. En una gestión por procesos, las organizaciones son representadas por un conjunto de procesos (estratégicos, tácticos y operativos), los cuales son asistidos por diversos activos de información, tales como los Servicios TI, constituidos por un conjunto de activos de TI.

En estos procesos, la información es uno de los recursos más importantes, por lo que su gestión eficiente constituye un factor crítico para el desempeño empresarial, debido a ello, requiere una adecuada protección. Una estrategia para darle esa protección es implantando un sistema de gestión de seguridad de información (SGSI), alineado al estándar ISO/IEC 27001; es decir, un proceso sistemático, documentado y conocido por toda la organización. Para el éxito de estos proyectos es fundamental la participación de la alta

dirección y el desarrollo de una cultura de seguridad de la información.

2.2.1.2. Actividades propuestas

En líneas generales, implantar un SGSI comprende los procesos o actividades, que pueden descomponerse en:

- Identificar los objetivos del negocio.
- Obtener el patrocinio de la alta dirección.
- Establecer el alcance (algunos procesos del negocio).
- Realizar un diagnóstico (Gap Analysis).
- Analizar los riesgos de activos de información.
- Elaborar y ejecutar un plan de tratamiento de riesgos.
- Establecer la normativa para controlar el riesgo.
- Monitorizar la implantación del SGSI.
- Prepararse para la auditoría de certificación.
- Llevar a cabo auditorías internas periódicas.

Siendo uno de los más relevantes el proceso de Análisis de Riesgos, que comprende la identificación, estimación y evaluación de riesgos. Para ello toma en consideración los elementos ilustrados en la Figura 1.

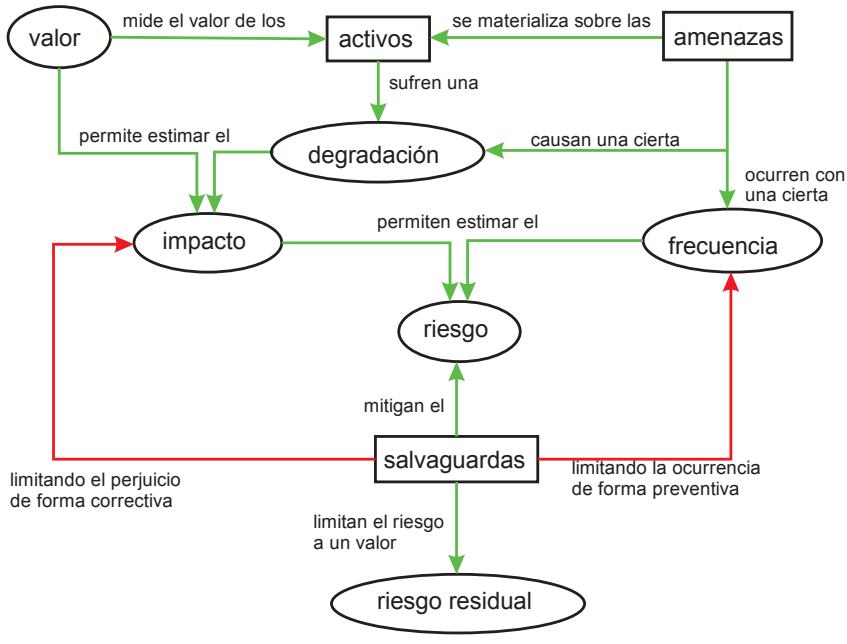

Figura 1. Elementos en el análisis de riesgos.

2.2.1.3. Los sub-procesos comprendidos son:

- Identificar los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Identificar las amenazas significativas sobre aquellos activos y valorarlos en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Identificar las salvaguardas existentes y valorar la eficacia de su implementación.
- Estimar el impacto y el riesgo al que están expuestos los activos del sistema.
- Interpretar el significado del impacto y el riesgo.

2.2.1.4. Acciones para satisfacer las necesidades encontradas

La gestión de riesgos consiste en la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis. Comprende las actividades:

- Elegir una estrategia para mitigar el impacto y riesgo.
- Determinar las salvaguardas oportunas para el objetivo anterior.
- Determinar la calidad necesaria para dichas salvaguardas.
- Diseñar un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Llevar a cabo el plan de seguridad.

2.2.1.5. Sub procesos de la norma NIST SP 800-30

El National Institute of Standards and Technology (NIST) ha dedicado una serie de publicaciones especiales a la seguridad de la información (SP 800). Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, NIST SP 800-30 [8], que comprende los siguientes subprocesos:

- Caracterización de Sistemas.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Análisis de controles.
- Determinación de probabilidades.

- Análisis de impacto.
- Determinación del riesgo.
- Recomendación de controles.
- Documentación de resultados.

2.2.1.6. Proceso propuesto para el análisis de riesgos

El proceso de análisis de riesgos de activos de información propuesto ha sido elaborado con base en su aplicación en una Institución del sector público, obteniéndose resultados satisfactorios, lo cual ha permitido su validación, haciendo a esta factible de aplicar a las demás organizaciones del sector.

El proceso se definió siguiendo los lineamientos de los estándares descritos en la sección anterior, especialmente MAGERIT, donde la diferencia principal radica en la forma de determinación del impacto, que en este caso se hace a través del "Business Impact Analysis, BIA".

El proceso comprende, la identificación, estimación y evaluación de riesgos. Este asume que el contexto está establecido, y se complementa con el tratamiento, monitorización y comunicación de riesgos, para completar la gestión de riesgos.

2.2.1.7. Establecimiento del contexto

El análisis de riesgos se realiza en el marco de la gestión integral del riesgo institucional. En el ámbito del SGSI el alcance del análisis de riesgos es el del SGSI; es decir, un conjunto de activos de información (Ai), que asisten a los procesos institucionales (Pk), que constituyen el alcance del SGSI.

En este proceso, el riesgo se determina en forma cualitativa, a partir de la Probabilidad, de que se materialice una amenaza por el Impacto, que ocasione en la institución, a través de los procesos que asiste. La valoración de los dos factores se realiza con base en escalas de 5 valores, como se muestran consignados en la Tabla 1 y Tabla 2.

Tabla 1. Valoración de la probabilidad.

Probabilidad		
Valor	**Grado**	**Descripción**
1	Raro	Puede ocurrir una vez cada 2 años
2	Muy baja	Al año
3	Baja	En 6 meses
4	Media	Al mes
5	Alta	A la semana

Fuente: Elaboración del investigador sobre la base teórica de Sotelo, Torres y Rivera (2012)

Tabla 2. Valoración del impacto.

Impacto		
Valor	Grado	Descripción
1	Insignificante	Impacta levemente en la operatividad del proceso
2	Menor	Impacta en la operatividad del proceso
3	Moderado	Impacta en la operatividad del macro proceso
5	Mayor	Impacta en la operatividad de los procesos
8	Desastroso	Impacta fuertemente en la operatividad de los procesos

Fuente: Elaboración del investigador sobre la base teórica de Sotelo, Torres y Rivera (2012)

El riesgo resultante se clasifica en 4 niveles: aceptable, tolerable, intolerable y extremo

Nivel de aceptación o tolerancia al riesgo con base en el resultado del análisis de riesgos y lo consignado en la Tabla 3, los activos con riesgo extremo e intolerable deben ser llevados por lo menos al nivel tolerable, y aquellos activos críticos con nivel de riesgo tolerable deben ser llevados al nivel aceptable.

Tabla 3. Valoración del nivel de aceptación/tolerancia.

Aceptación / Tolerancia		
Valor	Nivel	Descripción
1	Aceptable	Retenido
2	Tolerable	Para activos no críticos, pero intolerable para críticos
3	Intolerable	Atención inmediata y monitoreo permanente
4	Extremo	Tratado como intolerable, pero a nivel de Gerencia General

Fuente: Elaboración del investigador sobre la base teórica de Sotelo, Torres y Rivera (2012)

2.2.1.8. Identificación de riesgos

Comprende la identificación de los riesgos de los activos de información, por lo que demanda del inventario de estos activos, incluyendo su valor, determinado a partir de sus tres dimensiones de seguridad (Disponibilidad, Integridad y Confidencialidad) como mínimo. Para este proceso, los activos son agrupados en las distintas categorías de acuerdo a como se muestran consignadas en la Tabla 4.

Tabla 4. Clasificación de activos de información

Categorías de Activos de Información		
Identificador	Categoría	Ejemplos
STI	Servicios TI	Aplicaciones + infraestructura TI de soporte
SW	Software / Aplicaciones	Aplicaciones, sistemas operativos, herramientas de desarrollo y utilitarios
HW	Hardware / Equipos	Servidores (S.O.), PCs, routers, hubs, firewalls, medio magnético, gabinetes, cajas Fuertes, salas, mobiliario, sistemas de alarma, etc
SI	Soportes de Información	SAN, discos, cintas, USB, CD, DVD
COM	Redes de comunicación	Medios de transporte que llevan datos de un sitio a otro.
DAT	Datos / Información	BD, archivos de datos, contratos y acuerdos, documentación del sistema, información de investigación, manuales de usuario, material de entrenamiento, de operación, procedimientos de soporte, planes de continuidad y contingencia, acuerdos, documentación.
AUX	Equipamiento Auxiliar	Equipamiento de soporte a los sistemas de información (UPS, Generadores, aire acondicionado, cableado, etc.)
INS	Locales / Instalaciones	Lugares donde se hospedan los sistemas de información, registros vitales y comunicaciones.
PER	Personal / RRHH	Personas, calificaciones, experiencia y capacidades (usuarios, proveedores, personal de TI)
SRV	Servicios Generales	Vigilancia, servicios de impresión, computación, telecomunicaciones, eléctrica, agua, etc

Fuente: Elaboración del investigador sobre la base teórica de Sotelo, Torres y Rivera (2012)

2.2.2. Bases teóricas sobre Sistema de Gestión de la Seguridad de la Información

Para poder seguir con una adecuada metodología, es conveniente basarse en estándares que han sido utilizados con buenos resultados en distintos sectores a nivel global. Se referencia la norma ISO/IEC 27001:2008 y la metodología descrita en los módulos de la Academia Latinoamericana de Seguridad Informática.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y

disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

¿Para qué sirve un SGSI?

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Figura 2. Riesgos - SGSI

Fuente: (ISO27000.ES, 2012)

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema

como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Figura 3. Documentación del Sistema de Seguridad

Fuente: (ISO27000.ES, 2012)

- **Documentos de nivel 1**

  Manual de seguridad: Documentación que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

- **Documentos de nivel 2**

  Procedimientos: Documentación en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- **Documentos de nivel 3**

  Instrucciones, checklists y formularios: Documentación que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- **Documentos de nivel 4**

  Registros: Documentación que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- ***Alcance del SGSI:*** Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- ***Política y objetivos de seguridad:*** Documento de contenido genérico que establece el compromiso de la dirección y el

enfoque de la organización en la gestión de la seguridad de la información.

- ***Procedimientos y mecanismos de control que soportan al SGSI:*** Aquellos procedimientos que regulan el propio funcionamiento del SGSI.

- ***Enfoque de evaluación de riesgos:*** Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

- ***Informe de evaluación de riesgos:*** Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- ***Plan de tratamiento de riesgos:*** Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- ***Procedimientos documentados:*** Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

- ***Registros:*** Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

- ***Declaración de aplicabilidad:*** (SOA -*Statement of Applicability*-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

¿Qué aspectos de seguridad cubre un SGSI?

Son diez aspectos relevantes que son evaluados y cubiertos por un sistema de gestión de la seguridad de la información. Se indican en la siguiente figura:

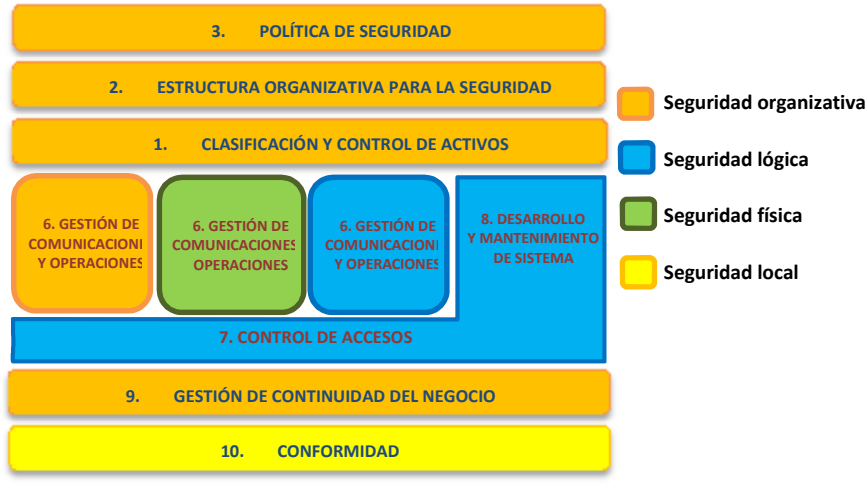

Figura 4: Aspectos que cubre el SGSI

Fuente: (ISO27000.ES, 2012)

Niveles de seguridad:

- Lógica: Confidencialidad, integridad y disponibilidad del software y datos de un SGI.
- Organizativa: Relativa a la prevención, detección y corrección de riesgos.
- Física: Protección de elementos físicos de las instalaciones: servidores, PCs, etc.
- Legal: Cumplimiento de la legislación vigente.

¿Cómo se implementa un SGSI?

Se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

Figura 5. Modelo de Desarrollo del SGSI
Fuente: (ISO27000.ES, 2012)

Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.

- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de: negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.

- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

2.2.3. Análisis y evaluación del riesgo

Es un conjunto de pasos metodológicos que debe desarrollar la empresa, que abarca desde que se identifican los activos de información hasta que se establece la importancia de las amenazas por su impacto en el riesgo de los activos. En esencia el análisis del riesgo busca estimar la magnitud del riesgo que afecta a los activos de información. A continuación mostramos la secuencia de pasos metodológicos que sigue el "análisis del riesgo".

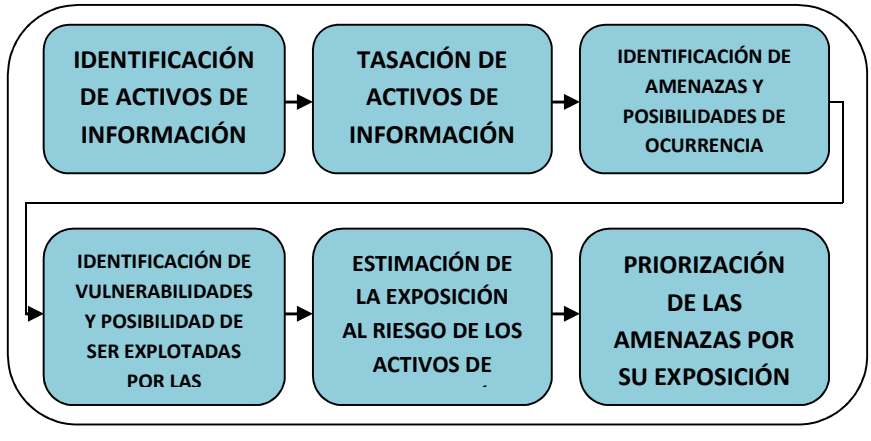

Figura 6: Pasos para la Metodología De Análisis de Riesgos

Fuente: (ISO27000.ES, 2012)

2.2.3.1. Tratamiento del riesgo y la toma de decisiones gerenciales

Una vez que el riesgo ha sido evaluado y la empresa ha determinado cuáles son aquellos activos de información sujetos a riesgo con significado para la firma, debe tomar la decisión de elegir la estrategia adecuada para tratar al riesgo.

Los riesgos pueden ser gestionados a través de una serie de combinaciones de prevención y controles de detección, tácticas de aceptación o realizando la transferencia a otra empresa.

La gerencia para tomar la decisión sobre cómo tratar el riesgo, siempre estará influenciada por dos factores, los cuales deben ser siempre bien analizados:

- ✓ El posible impacto si el riesgo se cristalizara.
- ✓ La posibilidad de su ocurrencia.

Al margen de considerar el impacto financiero del riesgo en la empresa, la firma debe considerar el costo de actuar sobre alguna de las opciones del tratamiento del riesgo. La organización debe asegurarse que existe un buen balance entre poder alcanzar seguridad y los beneficios de protección, sin perjudicar la rentabilidad ni la competitividad de la empresa.

2.2.3.2. Opciones para el tratamiento del riesgo

Para el tratamiento del riesgo existen cuatro estrategias, que son las más difundidas a nivel internacional. A continuación se hará una breve descripción de cada una de ellas:

a) Reducción del riesgo

Para los riegos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa. Los controles deben obtenerse del anexo "A" del ISO 270001:2005. Al identificar el nivel de los controles es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como la vulnerabilidad y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando y recuperándose de ellos.

Cualquiera de estas maneras que la empresa escoja para controlar los riesgos, es una decisión que dependerá de

una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.

b) Aceptación del riesgo

En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

Cuando la situación se presenta donde es muy costoso para la empresa mitigar el riesgo a través de los controles o las consecuencias del riesgo son devastadoras para la organización, se deben visualizar las opciones de "transferencia de riesgo" o la de "evitar el riesgo".

c) Transferencia del riesgo

La transferencia del riesgo es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente viable, transferir el riesgo a una aseguradora.

Se debe estar pendiente al escoger esta opción de tratamiento de riesgo, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicaran dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuando el riesgo actual está siendo transferido.

Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. Claro está, en la medida que exista la preparación para dicho efecto, por parte de la empresa que ofrece los servicios de tercerización. Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual no se delega, es responsabilidad de la empresa.

d) Evitar el riesgo

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras tradicionales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

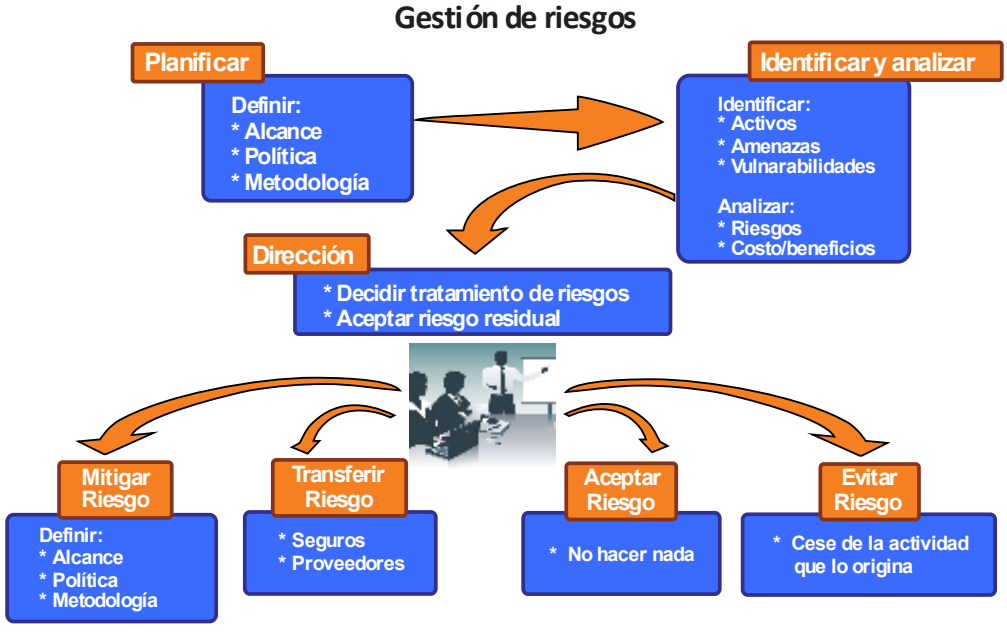

Figura 7: Gestión de Riesgos
Fuente: (ISO27000.ES, 2012)

2.3. Familia de normas ISO/IEC 27000. (Ormella Meyer, 2014) La Organización Internacional para la Estandarización – ISO por sus siglas en inglés – se encarga de publicar estándares sobre diferentes temas que tienen

una gran importancia en diferentes aspectos relacionados con el comercio, fabricación, etc. Siguiendo el constante crecimiento que ha tenido el desarrollo del campo de las Tecnologías de Información, dicho ente ha emitido varios estándares que regulan el ciclo de vida del software, estándares de calidad, sistemas de información y seguridad de la información. Correspondiente a este último grupo, se realizó la publicación de la familia de normas de la serie 27000, enfocadas directamente a la estandarización de los aspectos relacionados con la gestión de la seguridad de la información en las empresas y organizaciones que requieran contar con sistemas de gestión para este fin. A continuación se detallan las principales normas pertenecientes a esta serie:

- ISO 27001:2013, Information security management systems - Requirements Especifica los requisitos a cumplir para poder establecer el Sistema de Gestión de Seguridad de la Información.

- ISO 27002:2013, Code of practice for information security controls Presenta una guía de recomendaciones y buenas prácticas a seguir en la gestión de seguridad de la información.

- ISO 27003:2010, Information security management system implementation guidance Establece una guía de implementación para las normas de la serie. - ISO 27005:2009, Information security risk management Centrada en presentar una metodología para el análisis de riesgos.

2.4. Norma técnica peruana NTP ISO/IEC 27001 (Talavera, 2015) Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos. La norma utiliza la metodología Plan-Do-Check-Act – también llamado ciclo de Deming – para definir las fases de vida y mejora continua del SGSI a través de un seguimiento del mismo que asegura el mantenimiento de los controles y los cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema.

Recientemente, mediante la Resolución Ministerial N° 129-2012/PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012), fue aprobado el uso obligatorio de esta norma para todas las entidades que pertenezcan al Sistema Nacional de Informática

2.5. Ley de protección de datos personales la Ley N° 29733 de protección de datos personales (Talavera, 2015) publicada en julio del 2011 y siendo aprobada su aplicación en marzo del 2013, nace como respuesta a la necesidad de tener un documento que regule la manera en la que se hace uso

de la información personal en los procesos de negocio de todas las organizaciones que realicen operaciones en Perú. Anteriormente se crearon diferentes normas que hablaban acerca de las limitaciones que se debería tener en cuenta para el manejo de la información personal de los clientes o interesados. Sin embargo, la falta de especificación en los casos, así como el carácter un tanto abierto de las sanciones que dichos documentos especificaban requirieron que se cree una norma más específica que sirva como ente reglamentario sobre la información personal. Según detalla la ley, se considera dato personal a cualquier dato que pueda ser utilizado para identificar a una persona natural, de esta forma se puede considerar como datos personales el nombre de una persona, su dirección, su sexo, etc. Profundizando más en este concepto, se define además como dato sensible a aquellos que comprendan los datos biométricos, origen racial, religión, etc. Si bien es cierto que dichos datos casi siempre son necesarios para poder acceder a algún servicio – ya sea financiero, educativo o de salud – la ley detalla que el titular de dichos datos tiene los siguientes derechos respecto de esta información:

- Solicitar información sobre el uso que se dará a la información que facilite.
- Solicitar acceso a la información que la organización posee sobre él.
- Solicitar la actualización, rectificación, adición o supresión de datos.
- Solicitar que su información personal no sea suministrada a terceros.

A pesar de constituir una medida de protección para la información de las personas naturales, cabe destacar que ejercer muchos de estos derechos conlleva a un pago para poder hacerlos cumplirse. Como objetivo respecto al reglamento que establece esta ley, se menciona a los dueños y encargados de los bancos de datos personales – también denominados sujetos pasivos, tanto de la administración pública como privada – los cuales deberán modificar sus procedimientos para poder cumplir los requerimientos de esta norma. Se señala además que aquellos bancos de datos que sean de uso privado, así como los que se utilicen para las operaciones de la administración pública – incluidas las que soportan los procedimientos de defensa nacional, seguridad pública e investigación penal – se encuentran exceptuadas de la aplicación de la norma. El principal objetivo de la norma es que las personas naturales puedan tener conocimiento de quién tiene acceso a su información personal, además de conocer el tipo de uso que se le dará. De esta forma establece como garantía principal que el uso de datos personales debe estar sujeto al conocimiento – previo, informado, expreso e inequívoco – por parte del titular de dicha información. Sin embargo dicha garantía puede quedar invalidada en el caso que el ejercicio de este derecho afecte, por ejemplo, intereses de terceros o investigaciones judiciales. Dado su carácter de ley, todas las instituciones públicas o privadas que se encuentren en operación, deben garantizar el cumplimiento del reglamento especificado por la misma. (CONGRESO DE LA REPÚBLICA, 1997).

2.6. Definición de términos básicos

Para la definición de los términos básicos tomaremos como referencia a: (ISO27000.ES, 2012) (Microsoft; Tec de Monterrey; Information Security Inc.; Módulo Security, 2005) (Sotelo, Torres, & Rivera, 2012)

a. **Activo**: Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor.

   Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

b. **Amenaza**: Las amenazas son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando a sus negocios. Se pueden dividir en:

   - **Amenazas naturales** – condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos,

   - **Intencionales** – son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.

- **Involuntarias** - son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

c. **Información**: Es un activo, el cual, como cualquier otro activo de negocios, tiene valor para una organización y consecuentemente necesita ser protegido adecuadamente.

d. **Objetivos de control:** Declaraciones de resultados deseados o propósitos a lograr. Proveen los lineamientos necesarios para delinear las políticas de manera clara y los controles necesarios.

e. **Seguridad de información:** Está caracterizada por la preservación de los siguientes aspectos:

   i. **Confidencialidad**: Asegurando que la información sea accesible solo por aquellos que están autorizados.

   ii. **Integridad**: Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada.

   iii. **Disponibilidad**: Asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea requerido.

f. **Sistema de gestión:** Es un sistema para establecer políticas y objetivos de tal manera que se puedan cumplir estos últimos. Son

usados por las organizaciones para diseñar sus políticas y para poner estas en funcionamiento a través de objetivos. Para ello se basa en:

i. Estructuras organizacionales.

ii. Procesos sistemáticos y recursos asociados

iii. Metodologías de evaluación y medida.

iv. Revisión de procesos para asegurar que los problemas sean corregidos y las oportunidades para mejorarlos sean reconocidas e implementadas cuando sea necesario.

g. **Sistema de gestión de seguridad de información (SGSI):** Es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la Seguridad de la Información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad.

h. **Tipos de información:** La información puede ser clasificada de diversas maneras, según la forma de comunicarse:

i. Impresa o escrita en papel

ii. Almacenada electrónicamente

iii. Transmitida por correo convencional o electrónicamente.

iv. Exhibida en videos corporativos

v. Hablada en reuniones No importando la forma que tome la información, esta deberá ser siempre protegida.

i. **Vulnerabilidades:** Los puntos débiles o vulnerabilidades son los elementos que, al ser explotados por amenazas afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información.

   Al ser identificadas las vulnerabilidades, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

j. **Riesgo:** Es la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio; es decir, afectando: la confidencialidad, la integridad y la disponibilidad de la información.

k. **Mejor práctica**: Es la aplicación de controles o costumbres que han sido comunes o analizados e implementados en otras empresas de la misma naturaleza a la nuestra.

l. **Ciclo de Deming**: Es conocido como el ciclo de mejora continua, es decir cada vez que el ciclo es completado, este vuelve a iniciar; con el objetivo de aprender y mejorar sobre las actividades que ejecutamos al final.

m. **Valoración de activos**: Es la estimación cuantitativa o cualitativa de la importancia de un activo en un SGSI.

2.7. Formulación de la hipótesis de investigación

La información, las personas que hacen uso de ella y los equipos e infraestructura que la soportan son elementos que se encuentran con riesgos de seguridad y que deben necesitar de la formulación de un Sistema de Seguridad de la Información para el Departamento de Admisión y Registro Académico de la UPAGU.

CAPÍTULO 3

PROCEDIMIENTO METODOLÓGICO

3.1. Unidad de análisis

Para el desarrollo del presente trabajo de investigación, se consideró como unidad de análisis a una unidad académica la misma en donde se lleva a cabo todos los procedimientos académicos de alumnos y docentes. Esta unidad es el Departamento de Admisión y Registro Académico de la Universidad Privada Antonio Guillermo Urrelo de Cajamarca.

3.2. Tipo y descripción de la investigación

La investigación que se llevó a cabo en este estudio es de tipo ***descriptivo – de carácter propositivo***, debido a que se analizó cómo se encuentra actualmente lo relacionado con la seguridad de la información, en donde como investigador me involucré con el entorno a investigar.

La investigación es meramente aplicada, pues pretende a partir de un diagnóstico solucionar un problema.

Es microsociológica pues se analizó solo en el entorno de la organización y es transversal. Se dio en el periodo 2015-2016.

3.3. Diseño de la investigación

El diseño que se utilizó para el presente trabajo es una investigación no experimental, dado que no se manipuló ninguna variable y se observó el fenómeno tal y como se da en su natural contexto para posteriormente después del análisis, realizar una propuesta de mejora.

3.4. Métodos y procedimientos

Se ha definido como metodología, con el objetivo de desarrollar el presente trabajo de investigación, la propuesta que da la norma ISO/IEC 27002 o el equivalente dentro de la legislación peruana NTP-ISO/IEC 17799:2007, que nos brindó las pautas y procedimientos que encauzó el trabajo. Es una norma referida a las Tecnología de la Información y código de buenas prácticas para la Gestión de la Seguridad de la Información.

El procedimiento general, está definida en las siguientes etapas:

a) Identificar los procesos "core" de negocio, con los que opera normalmente la universidad, así poder estratificar los datos que vayamos encontrando y poder procesarlos de manera eficiente.

b) Realizar un análisis de impacto del negocio, a los procesos identificados, para definir el alcance de las políticas de seguridad y definir sobre qué procesos trabajar. Se deberá seleccionar solo los procesos académicos de la UPAGU y dentro de éstos se seleccionan los más importantes los cuales serán los que afectan directamente el desarrollo de los procesos del Departamento de Admisión y Registro Académico de la UPAGU. A continuación se identificaran los activos importantes de información propios de estos procesos, teniendo en cuenta las dimensiones propuestas.

c) Realizar un análisis de riesgo en cada uno de los procesos identificados. Este análisis de riesgo estará enfocado en analizar las vulnerabilidades y las amenazas que existen para la información del DARA, orientadas a los activos los cuales son clasificados de acuerdo a las dimensiones definidas: la información, las personas que utilizan esta información y a los equipos e infraestructura que la soportan, entendiendo que la infraestructura que soportan la información, referencian a la infraestructura física y digital.

d) Definir los controles que se ajusten a los procesos identificados, una vez identificadas las amenazas y vulnerabilidades, se actuará en las tres dimensiones establecidas: información, personas que utilizan la información y equipos e infraestructura que soportan la información.

e) Definir una política de seguridad, apoyada en normas, estándares y procedimientos, que den un sustento a los controles seleccionados para cubrir la problemática. De estas políticas se desprenderá un sistema para gestionarlas, el mismo que se convertirá en la propuesta del Sistema de Gestión de Seguridad de la Información

3.5. Matriz definición operacional de variables

VARIABLES	DIMENSIONES	INDICADORES	SUB INDICADORES	TÉCNICA DE RECOJO DE INFORMACIÓN
Análisis de riesgo	Información Personas que usan la Información Equipos que soportan la Información	Para todas las dimensiones: Amenazas Vulnerabilidades	Naturales Intencionales Involuntarias Físicas Naturales De hardware De software De medios de almacenaje De comunicación Humanas	Encuestas Observación Revisión y Análisis Documental
Propuesta de un Sistema de Seguridad de Información	Información Personas que usan la Información Equipos que soportan la Información	Políticas de uso y manejo de la información. Políticas de seguridad del personal. Políticas de seguridad física y ambiental, de seguridad y administración de operaciones de cómputo y de controles de acceso lógico y uso de software.		Revisión y Análisis Documental

3.6. Población de estudio

La población de estudio estará conformada por usuarios internos que utilizan y mantienen la información en la parte administrativa y académica de la Universidad Privada Antonio Guillermo Urrelo de Cajamarca, durante los años 2015-2016.

Se detalla a continuación a la población elegida para el presente estudio:

- Estudiantes: Fueron 24 estudiantes, dos por cada carrera profesional, en donde el criterio de elección fue de incluir a alumnos que se encuentren ocupando los primeros puestos que será uno de cada carrera profesional y alumnos que tengan la condición de irregularidad, además hayan tenido en algún momento la condición de extemporáneos también se consideró a un alumno por cada Carrera profesional. Estos criterios con el fin de tener todos los escenarios en los que actúan los alumnos cuando utilizan los sistemas que manejan su información académica.

- Docentes: Se consideró a un docente por carrera profesional (12 en total), que por fines de acceso a ellos se trabajó con los coordinadores de cada carrera profesional pues, además de tener trabajo administrativo se les considera dentro de la carga horaria, para el dictado de asignaturas en sus respectivas Carreras Profesionales.

- Administrativos: Se consideró a los tres integrantes del Departamento de Admisión y Registro Académico, puesto que son los actores principales dentro de esta unidad académica.

- Personal de seguridad y mantenimiento, se consideró al 100% de los integrantes, pues en número son solo 10 personas, quienes tienen que ver directamente con la seguridad control y manipulación directa de los activos de la universidad.

- Directivos: Son 4 personas, quienes tienen a su cargo la Gerencia General, Rectorado, Vicerrectorado Académico y Dirección de la Escuela de Posgrado y son los que de una u otra forma determinan los procedimientos académicos y administrativos de la institución.

En cuanto a considerar una muestra pequeña de la población, obedece al hecho de que lo que se está evaluando es una percepción de estas personas y al ser su interacción con el DARA de manera semejante entre todos los miembros es que consideramos solo algunas características para su elección. Además se debe tener en cuenta que se han tomado algunos criterios de exclusión de personal dentro de la UPAGU, el mismo que se refiere a las personas o unidades que no hacen uso o interactúan con la información que es procesada en el Departamento de Admisión y Registro Académico. Además también están excluidos los egresados de esta casa superior de estudios, pues ellos no realizan proceso alguno que tenga que ver con alguna transacción con la información académica.

3.7. Técnicas e instrumentos de recojo de información

a) Observación

Es un procedimiento de recolección de datos e información que consiste en utilizar los sentidos para observar hechos y realidades sociales presentes y a la gente donde desarrolla normalmente sus actividades.

Para la presente investigación se enfocará en la perspectiva de los problemas que existen en las áreas a trabajar, dicha observación se realizará en todas las unidades organizacionales de la UPAGU, administrativas así como académicas, para esto se utilizará: ***Guías y fichas de observación***, donde se irán describiendo los problemas de seguridad en los tres activos definidos; es decir, en el uso y manipulación de la **información**, además de las actividades cotidianas que realizan los trabajadores considerándolas como las **personas que utilizan la información** y finalmente todos los aspectos que se refieren al activo, **de equipos que soportan a la información**, que están referidos a los equipos de cómputo con el software y hardware respectivo; además, de la infraestructura de comunicaciones y los ambientes físicos de cada unidad organizacional de la UPAGU. Las fichas de observación deberán estar codificadas de acuerdo a las respectivas áreas, anotando las fechas en que son utilizadas.

La Observación estará orientada a investigar a la variable Análisis de Riesgos.

b) Encuestas

Técnica de adquisición de información de interés sociológico, a través del cual se puede conocer la opinión o valoración del sujeto seleccionado en una muestra sobre un asunto dado, mediante un cuestionario previamente elaborado.

Permitirá conocer las expectativas que tienen los usuarios respecto a la información, la protección de esta y bajo su propia percepción y con el conocimiento de los procesos que ellos realizan, puedan darnos nociones de cómo se presenta el nivel de seguridad de la información en sus respectivas áreas, tratando de encontrar las posibles vulnerabilidades y la aparición de amenazas que pueden ocurrir teniendo en cuenta también los tres activos definidos para este estudio. Los instrumentos a utilizar serán cuestionarios de preguntas abiertas y cerradas y Checklist.

Las encuestas se irán aplicando en la mayoría de los casos paralelamente a la observación que se esté realizando en el área correspondiente, de esta manera podremos asegurarnos que los datos que vayan a brindar los trabajadores sean lo más sinceros posibles y más cercanos a la realidad. Las Encuestas también estarán orientadas a investigar a la variable Análisis de Riesgos.

c) Análisis documental y de información

Es una técnica de investigación, cuyo objetivo es la captación, evaluación, selección y síntesis de los mensajes subyacentes en el contenido de los documentos y en la información, a partir del análisis de sus significados, a la luz de un problema determinado.

Con esta técnica se pretende analizar la documentación e información en cada una de las áreas de la UPAGU. El análisis documental centrará su atención en la producción documental que se genera diariamente, así como su organización e importancia. El análisis de información, por su parte, colocará su atención en la información que contienen los documentos, en su significado; así como en las fuentes y en su autoridad. Se orientará también a los documentos e información que son producidos o son utilizados por los sistemas informatizados.

Hay que considerar como importante, que quizá el uso de esta técnica sea de carácter restringido en algunas unidades por la confidencialidad de los documentos y la información, pero se tiene el acceso total al Departamento de Admisión y Registro Académico, lo que permitirá hacer un adecuado levantamiento de la información requerida.

3.8. Aspectos éticos de la investigación

Para el presente trabajo de investigación, así como en cualquier trabajo de esta índole, el investigador asume una posición de ética y moral en el desarrollo de la misma con el fin de obtener un trabajo fidedigno. En tal sentido no asumiré comportamientos incorrectos como la **falsificación** de datos o resultados. Pues, no se trata de alcanzar indebidamente información que no sea la verdadera, tampoco es la intención acopiar información inventada, que tal vez vaya a ser usada de buena fe por otros. El interés que persigo es de realizar una investigación lo más objetiva posible ya que como se persigue el brindar una propuesta, esta solo será correcta en la medida en que la información sea la verdadera.

Hay que resaltar también que la información que se obtendrá de esta investigación es bastante delicada y de carácter privado para la institución por lo que se mantendrá en total reserva hacia entes externos a la universidad.

CAPÍTULO 4

PRESENTACIÓN DE RESULTADOS Y DISCUSIÓN

4.1. Presentación de los resultados

En esta sección se presentará los resultados que fueron obtenidos a través de los distintos instrumentos, se clasificaran los resultados en base a las tres dimensiones trabajadas: información, equipos e infraestructura y personas, además indicando los procesos "core" que se realizan dentro del DARA.

4.1.1. Identificación de los procesos core del DARA:

Los procesos relevantes que se encontraron fueron en base a la aplicación de entrevistas al personal que labora en el DARA:

- **Proceso de admisión**: Es el proceso que permite a la Universidad seleccionar a los estudiantes que postulan a ella, evaluando sus capacidades y aptitudes para seguir una carrera académico profesional y desarrollarse adecuadamente en la vida universitaria. Dichos procesos ocurren tres a más veces en cada año.

  Dentro de este proceso, las tareas son: diseñar, planificar y determinar las características de los procesos de admisión; así como de la ejecución y operativización del mismo. Además para estos procesos de admisión, se tienen que actualizar el banco de preguntas, que es utilizado para los exámenes ordinarios de admisión.

- **Proceso de matrícula**: La matrícula es el acto formal y voluntario que confiere la condición de estudiante de la Universidad, conlleva el compromiso de cumplir con la Ley Universitaria, el Estatuto y demás

normatividad universitaria.

La matrícula de alumnos es el procedimiento por el cual los alumnos son inscritos en las asignaturas, de acuerdo al Plan de Estudios del Currículo vigente y en concordancia con lo normado en la normatividad vigente. La planificación, organización, ejecución y control del proceso de matrícula lo realiza el DARA, con la coordinación del Vicerrectorado Académico, Gerencia General y la Gerencia de Informática. Además para este proceso se requieren tareas que corresponden a otras unidades académicas de la universidad, como:

a. Generación y firma de Actas del periodo anterior, por parte de los docentes y el DARA

b. Elaboración y publicación de carga horaria y horarios al sistema de registro académico, por parte de los coordinadores de carrera de cada facultad, la gerencia de Planificación deberá también coordinar los ambientes de las aulas para tal fin.

c. Revisión del módulo de matrícula e información, por parte de la Gerencia de Informática.

Dentro de este proceso, también se considera a la Regularización de Matrícula, qué sucede cuando un alumno luego de finalizada su matrícula, por distintas razones desea realizar cambios, ya sea en las asignaturas, turnos, docentes, etc., este procedimiento se realiza de manera virtual en el sistema y también en el DARA.

- **Proceso de generación de actas de evaluación:** Los docentes una vez finalizado un periodo académico deben consolidar las evaluaciones en el documento llamado Acta de Evaluación. Este documento es generado por el sistema de manera automática de acuerdo a los criterios de evaluación que existen en cada carrera profesional. Al generar el acta se da por finalizada la evaluación y las notas son almacenadas en el sistema correspondiente, a continuación cada docente deberá acercarse al DARA, donde se imprime las actas generadas y ellos firmaran, dando la conformidad a estos documentos, que son centralizados y archivados en el DARA.
- **Proceso de emisión de documentos académicos:** Este proceso es muy importante, pues es la emisión de los reportes académicos a un alumno de la universidad, los mismos que acreditan una condición al alumno, el avance que ellos llevan del plan de estudios correspondientes o la finalización de sus estudios. La información provista en estos documentos deben guardar los principios básicos de la información, en su generación, proceso y salida.
- Además existen otros procesos, que son parte del quehacer de este departamento, pero que no son tan relevantes para nuestra investigación.

Estos procesos luego nos servirán para clasificar los controles de seguridad que se vayan a propones una vez identificadas las amenazas y vulnerabilidades.

4.1.2. Identificación de los activos de información

A continuación se presentaran los resultados obtenidos de la evaluación teniendo en cuenta las dimensiones establecidas previamente para esta investigación. Estos activos fueron identificados en base a la observación en el DARA y la aplicación de las entrevistas al personal que labora en esta área:

a. Dimensión información:

Información física, este punto se ha trabajado en base a una entrevista al personal del DARA y también con la observación directa. Hay bastante información que se encuentra almacenada en el ambiente físico del DARA, donde encontramos: Resoluciones Oficiales de Directorio, Rectorado y Facultades; Reglamentos y Directivas; Actas de Evaluación; Fichas de Matrícula; Carpetas de Postulantes y todo tipo de documentos de comunicación interna. Son documentos antiguos y actuales, de acuerdo a los integrantes del DARA estos documentos son importantes pues son la base de la información de la UPAGU. Los documentos se encuentran clasificados y ordenados por fecha de emisión, pero se tiene una dificultad en cuanto al espacio para almacenarlos. La mayoría de documentos son fáciles de ubicar y así como también su accesibilidad. En general la información es confidencial, íntegra y es disponible solo para los fines que los procesos de la universidad los requiera.

Información digital, para este caso lo vamos a diferenciar en distintos criterios:

- **I**nformación documental, que se encuentran almacenados en los dispositivos de almacenamiento de los equipos del DARA, correspondencia oficial, formatos de documentos emitidos, etc.

- Software y Aplicaciones de escritorio**. S**e ha encontrado que la universidad en su conjunto cuenta con software original, aquí están incluidos los equipos del DARA, por lo que tienen un valor con respecto a la seguridad de los equipos por tener el soporte de los fabricantes, en este caso es el sistema operativo Windows 7 y Office 2013, otras aplicaciones de escritorio son descargadas a través de internet. El punto desfavorable se da con respecto a los antivirus, que en su totalidad o son copias de evaluación, copias piratas o versiones básicas y que es más, por políticas implementadas en el servidor de firewall, no se pueden actualizar.

- Información corporativa centralizada, esta información es la que se encuentra en la base de dato corporativa de la UPAGU, la misma que está almacenada en servidores externos a la universidad, el servicio es tercerizado, lo que garantiza la integridad, confiabilidad y disponibilidad, esto de acuerdo a los documentos de contrato del servicio. Para acceder a esta información, se lo hace a través de aplicaciones web, las

aplicaciones también se han desplegado dentro del paquete de alojamiento contratado.

b. Dimensión equipos e infraestructura que soportan a la información:

Para esta dimensión se evaluará desde los elementos de nivel más bajo, hasta lo más general. La identificación de los activos pertenecientes a esta dimensión, también se realizó en base a la observación directa en el DARA, así como con la aplicación de las entrevistas al mismo personal:

- Equipos de cómputo y comunicaciones. A continuación se listarán los equipos encontrados y algunas deficiencias que se han encontrado: Computadora portátil, unido a la red vía cable UTP y a través del wireless, el equipo es utilizado por el responsable del área; dos equipos de escritorio utilizados por la secretaria y asistente del DARA, están unidos a la red vía cable UTP; dos impresoras láser con scanner que están unidas también a la red a través del cableado dentro del ambiente del DARA; un switch D'link básico para la conexión de los equipos del DARA y otras áreas a la red de la UPAGU y el cableado de comunicación y eléctrico dentro del departamento.

- Infraestructura física del DARA. El ambiente donde se ubica el DARA, se encuentra en la parte posterior del local central, en el primer piso, el ambiente no es compartido con otras áreas, hay

una división que define 3 sub ambientes, una para el jefe del departamento, otra para la secretaría y el asistente y la tercera es una área pequeña donde se ubicarían los usuarios. La división es de madera a una altura de 2 metros, quedando al descubierto una altura de 1.3 metros. El edificio donde se encuentra el DARA es una construcción relativamente nueva que cuenta con una adecuada estructura.

Dentro de esta dimensión también se considera al personal de seguridad y mantenimiento de la universidad, quienes brindan el servicio de vigilancia y el de mantener de manera correcta la infraestructura respectivamente.

c. Dimensión personas que utilizan la información:

En esta dimensión se evaluará a las personas que están involucradas con la información del DARA, al personal que utiliza la información y la procesa, son 3 personas el jefe del área, la secretaria y el asistente del DARA. Además se considera a los alumnos, docentes, administrativos, autoridades y entidades externas que son grupos grandes de personas o entidades pero que para nuestro estudio se las deberá considerar tan solo como usuarios que brindan y consumen la información que administra el DARA.

A continuación se muestra la relación de activos encontrados en el DARA, de acuerdo a las dimensiones propuestas (Tabla 5)

Tabla 5. Identificación de los activos de información

N°	Activo identificado	¿Tangible?	Tipo de Activo	Dimensión
1	Computadoras de escritorio	Si	Tecnología	Equipos - Infraestructura
2	Computadora portátil	Si	Tecnología	Equipos - Infraestructura
3	Sistema Operativo (Windows 7)	No	Aplicación	Equipos - Infraestructura
4	Microsoft Office 2013	No	Aplicación	Equipos - Infraestructura
5	Página web de la Universidad	No	Aplicación	Equipos - Infraestructura
6	Intranet de la UPAGU	No	Aplicación	Equipos - Infraestructura
7	Correo Electrónico	No	Aplicación	Equipos - Infraestructura
8	Software de aplicaciones de escritorio	No	Aplicación	Equipos - Infraestructura
9	Intercomunicadores	Si	Tecnología	Equipos - Infraestructura
10	Impresoras / fotocopiadoras / scanner	Si	Tecnología	Equipos - Infraestructura
11	Cableado Ethernet	Si	Tecnología	Equipos - Infraestructura
12	Wireless	No	Tecnología	Equipos - Infraestructura
13	Switch	SI	Tecnología	Equipos - Infraestructura
14	Sistema de Información Académico	SI	Aplicación	Equipos - Infraestructura
15	Vitrinas informativas	Si	Instalación	Equipos - Infraestructura
16	Anaqueles	SI	Instalación	Equipos - Infraestructura
17	Instalaciones eléctricas	SI	Instalación	Equipos - Infraestructura
18	Archivadores para los documentos	Si	Equipamiento Auxiliar	Equipos - Infraestructura
19	Gabinetes y armarios	Si	Equipamiento Auxiliar	Equipos - Infraestructura
20	Llaves de ingreso	Si	Equipamiento Auxiliar	Equipos - Infraestructura
21	Jefe del DARA	Si	Personal	Personas
22	Secretaria del DARA	Si	Personal	Personas
23	Asistente del DARA	Si	Personal	Personas
24	Alumnos	Si	Personal	Personas
25	Egresados	Si	Personal	Personas
26	Padres de familia y/o tutores de los alumnos	Si	Personal	Personas
27	Docentes	Si	Personal	Personas
28	Autoridades y demás trabajadores de la UPAGU	Si	Personal	Personas
29	Entidades externas	Si	Instituciones	Personas

30	Resoluciones (en físico y digital)	SI	Dato	Información
31	Documentación interna de la UPAGU	SI	Dato	Información
32	Reglamentos Académicos de estudios	Si	Dato	Información
33	Plan de estudios	Si	Dato	Información
34	Plan Estratégico de la UPAGU	Si	Dato	Información
35	Estatuto de la UPAGU	Si	Dato	Información
36	Plan operativo anual del DARA	Si	Dato	Información
37	Cronogramas Académicos	Si	Dato	Información
38	Reporte de alumnos	Si	Dato	Información
39	Información académica de alumnos	Si	Dato	Información
40	Carga horaria semestral de docentes	Si	Dato	Información
41	Información de postulantes	Si	Dato	Información
42	Reportes de ingresantes	Si	Dato	Información
43	Guías de Postulantes	Si	Dato	Información
44	Reglamento de admisión	Si	Dato	Información
45	Carpeta de postulantes	Si	Dato	Información
46	Ficha de Admisión	Si	Dato	Información
47	TUPA actualizado de la UPAGU	Si	Dato	Información
48	Consolidados de vacantes, postulantes e ingresantes	Si	Dato	Información
49	Exámenes de admisión / Banco de preguntas	Si	Dato	Información
50	Registro de las matriculas	Si	Dato	Información
51	Reportes de categorización	Si	Dato	Información
52	Reporte de distribución de aulas	Si	Dato	Información
53	Horarios	Si	Dato	Información
54	Fotografías de los alumnos (físico y digital)	Si	Dato	Información
55	Acta de evaluación de alumnos	Si	Dato	Información
56	Reportes de evaluaciones	No	Dato	Información
57	Reportes de asistencias	No	Dato	Información

Fuente: Elaboración del investigador de acuerdo a la aplicación de los instrumentos

De acuerdo a los procedimientos establecidos por las normas que guían la presente investigación, se tendría que valorar a los activos encontrados, pero teniendo en cuenta la información obtenida se aprecia que el número de activos es relativamente bajo, por otro lado considerando la criticidad del DARA, se consideró necesario tomar en consideración todos los activos identificados para la evaluación de los riesgos.

4.1.3. Identificación de los riesgos

Para el desarrollo de identificación de riesgos se realizó una valorización detallada de riesgos, y de acuerdo a su definición para identificar dichos riesgos, se consideró la identificación de las vulnerabilidades y amenazas que puedan afectar a los activos que se encontraron anteriormente

Para la efectiva valorización de los riesgos, el estándar ISO 27000 propone varios métodos. Para el presente trabajo se optó por utilizar una matriz de calor, la cual tiene como criterios la probabilidad que ciertas amenazas exploten ciertas vulnerabilidades, las mismas que tendrán un impacto en los procesos operativos y la continuidad de las actividades del DARA

A continuación se presenta la matriz de calor con los criterios que se han definido, donde se cruzaron la probabilidad de afectación (que una amenaza explote una vulnerabilidad) frente al impacto que este riesgo afecte a la unidad evaluada, en este caso al DARA:

Tabla 6. Matriz de calor

Impacto en el Negocio	Probabilidad de Afectación				
	Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Muy Alto	Medio	Medio	Alto	**Crítico**	**Crítico**
Alto	Bajo	Medio	Alto	Alto	**Crítico**
Medio	Bajo	Medio	Medio	Alto	**Alto**
Bajo	Tolerable	Bajo	Medio	Medio	Medio
Muy Bajo	Tolerable	Tolerable	Bajo	Bajo	Medio

Fuente: Elaboración del investigador de acuerdo a la recomendación de la norma.

Estos criterios se tomaron teniendo en cuenta los siguientes significados de los valores de la Probabilidad de Afectación y del Impacto en el Negocio:

Probabilidad de Afectación, se interpreta de la siguiente manera:

- Muy Alta: Es seguro que la amenaza explotará la vulnerabilidad.
- Alta: Es muy probable que la amenaza explote la vulnerabilidad.
- Media: Es posible que la amenaza explote la vulnerabilidad.
- Baja: Es poco probable que la amenaza explote la vulnerabilidad.
- Muy Baja: Es impensable que la amenaza explote la vulnerabilidad.

Impacto en el Negocio, se interpreta de la siguiente manera:

- Muy Alto: Afecta por más de una semana las operaciones.
- Alto: Afecta hasta en 72 horas las operaciones.
- Medio: Afecta hasta en 24 horas las operaciones.
- Bajo: Afecta hasta en 6 horas las operaciones
- Muy Bajo: Tiene un efecto nulo o muy pequeño en las operaciones.

Una vez que se definieron los controles de valorización de los riesgos, se procedió a identificar las amenazas a las que se encuentran expuestos los activos y sus vulnerabilidades, para ellos se procedió a una evaluación de los resultados de los instrumentos aplicados, encuestas, entrevistas y observación. Además estos resultados fueron comparados con las amenazas y vulnerabilidades que propone la norma ISO/IEC 27000, de esta manera se pudo conseguir con más certeza todos los elementos necesarios para la evaluación. La presentación de estos resultados se da a continuación:

- La computadora portátil está unida a la red UPAGU vía cable UTP y a través del wireless, el equipo es utilizado por el responsable del área, incluso es llevado a otro lugar cuando tiene que realizar o completar alguna tarea fuera del horario de trabajo. En su disco duro se guardan los documentos que se emiten de manera oficial a otras áreas, así como las respuestas a solicitudes de información, el equipo guarda un valor elevado para esa unidad y por ende para la universidad.

- Los equipos de escritorio, utilizados por la secretaria y asistente del DARA están unidos a la red vía cable UTP, solo el personal mencionado tiene acceso a ellos, aunque en algunas oportunidades son utilizados por docentes, pero con la supervisión y vigilancia respectiva por parte del personal. Estos equipos aunque tienen instalados antivirus, pero no pueden ser actualizados. Están unidos al dominio corporativo de la universidad, pero son también utilizados con cuentas locales, debido al excesivo control por parte del administrador.

- Dos impresoras láser con scanner que están unidas también a la red a través del cableado dentro del ambiente del DARA.

- Un switch D'link básico para la conexión de los equipos del DARA y otras áreas a la red de la UPAGU.

- Los puntos negativos encontrados es que los equipos pueden ser accedidos por otra persona que también esté conectada dentro de la red, sea por medio de cables o la red inalámbrica. Los antivirus no son actualizados y al tener acceso a internet y realizar trabajos con dispositivos de almacenamiento móvil los equipos se convierten en vulnerables a un ataque sea de virus o un hacker. Los equipos almacenan información delicada sin cifrar y si son sustraídos se pone en riesgo la información. Las comunicaciones dentro de la red de la universidad tampoco están cifradas pudiendo ser interceptadas dentro y fuera de la universidad.

- Infraestructura física del DARA, el ambiente donde se ubica el DARA, se encuentra en la parte posterior del local central, en el primer piso, el ambiente no es compartido con otras áreas, hay una división que define 3 sub ambientes, una para el jefe del departamento, otra para la secretaría y el asistente y la tercera es un área pequeña donde se ubicarían los usuarios. La división es de madera a una altura de 2 metros, quedando al descubierto una altura de 1.3 metros. A favor se tiene que las llaves del departamento solo lo tienen los integrantes de este departamento, al igual que la oficina de tesorería, pues después de

estos dos ambientes las llaves son centralizadas en vigilancia y a solicitud podrían ser abiertos en cualquier momento. Puntos desfavorables son, que el ambiente es demasiado reducido para la cantidad de información en físico con que se cuenta, lo cual genera un desorden general. Otro punto negativos es que la división interna es fácilmente vulnerable, si alguien sin consentimiento quisiera ingresar, lo podría hacer sin dificultad por la parte de arriba de la división. También se puede mencionar que como ambiente que contiene una cantidad excesiva de papel, y este es material altamente inflamable; por ende, este ambiente es altamente vulnerable a un incendio. También las instalaciones eléctricas han sido modificando inadecuadamente, que combinado con el punto anterior se duplica el peligro de contar con un incendio. También el hecho de estar en el primer piso y estar junto con una alcantarilla, que en épocas de lluvia, el agua se rebalsa llegando a inundar parcialmente a la oficina, pudiendo provocar cortos circuitos e inclusive deteriorar o desaparecer la documentos. Adicionalmente, se suma el hecho de no contar con extintores dentro o cerca de la oficina.

- El edificio donde se encuentra el DARA es una construcción relativamente nueva, cuenta con una adecuada estructura que podría asegurar en el supuesto de la ocurrencia de sismos.

- También en el tema de infraestructura se consideró al personal de seguridad y mantenimiento de la universidad, con respecto a los primeros no cuentan con un manual formal y aprobado de manejo de

incidencias por lo que su actuar corresponde al criterio que puedan tomar ellos o su supervisor en un determinado momento. Este personal solo está capacitado teóricamente para actuar en caso de algún desastre, además para algunos de ellos no es tan sencillo identificar a las personas que ingresan a la universidad, pues fácilmente pueden ser considerados alumnos y las intenciones podrían ser de realizar algunos actos indebidos como la sustracción de equipos o de la misma información. Para el personal de mantenimiento al igual que los primeros no cuentan con manuales de manejo de incidencias por lo que su trabajo lo realizan a solicitudes de tal o cual área o cuando su supervisor cree conveniente.

- Personal de seguridad capacitado, el total del personal de seguridad solo cuenta con el conocimiento teóricos de los que se debe hacer cuando se encuentra una incidencia que vaya a poner en riesgo a los activos de la universidad, además no se cuenta con un manual de trabajo en el tema de seguridad, que haya sido formalmente aprobado y difundido.

- Con respecto al personal de seguridad, se ha obtenido la siguiente información, de acuerdo a las encuestas aplicadas, además se contrasto con la observación y entrevista a otro grupo de trabajadores, con el fin de tener una visión más certera con respecto a las respuestas que ofrecieron:

Tabla 7. Respuestas a los ítems de la encuesta por parte del personal de seguridad

Ítem	SI	NO

Existencia de Manual de Incidencias	100%	0%
Conocimiento de ubicación de extintores	100%	0%
Manejo adecuado de un extintor	100%	0%
Identificación de personas que ingresan a la universidad	75%	25%
Percibe que el DARA es seguro	75%	25%
Participación en simulacros de sismos	100%	0%
Inspección de equipos en el ingreso y la salida	75%	25%

Fuente: Elaboración del investigador de acuerdo a los resultados de la aplicación de encuestas.

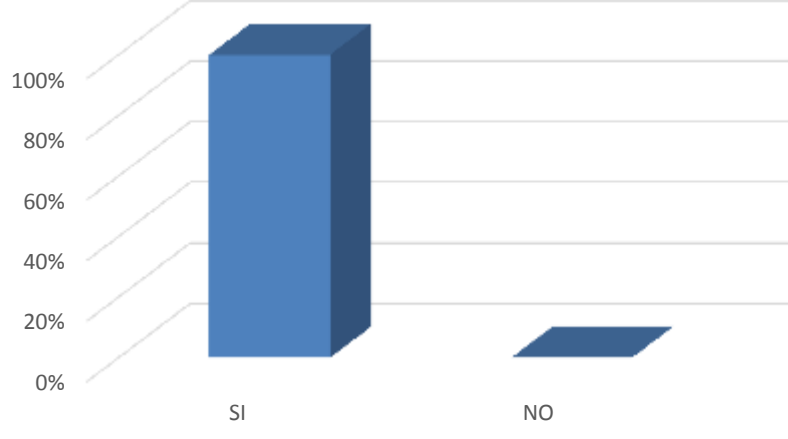

Figura 8. Existencia de Manual de Incidencias

Fuente: Elaboración del investigador

- Aunque el total del personal de seguridad indican en su totalidad que existe un manual de incidencias, según la figura 6, tal documento no se encuentra aprobado ni socializado en la institución, además que no es de conocimiento del resto de personal, ni de directivos, por el que no se conoce las acciones que se tomarán al momento de la ocurrencia de un

incidente.

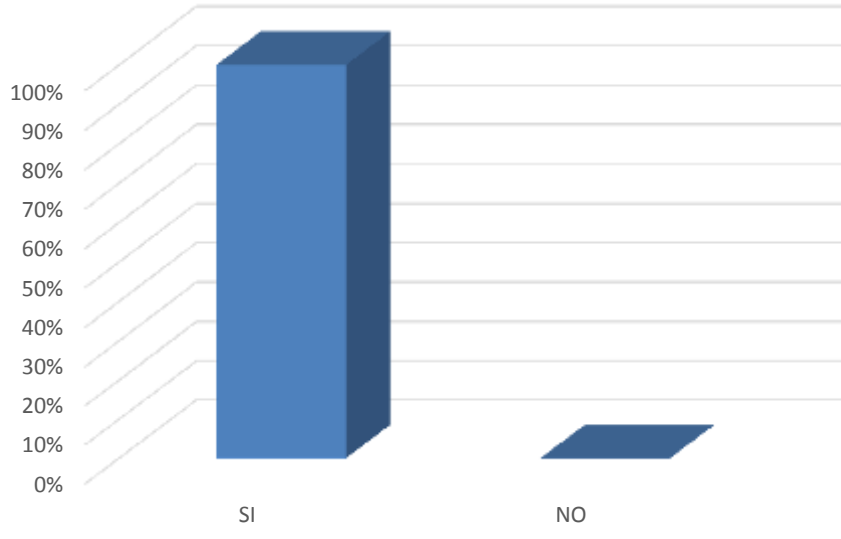

Figura 9. Participación en simulacros de sismos
Fuente: Elaboración del investigador

- De la figura anterior, se puede mencionar que el total del personal de seguridad ha participado en simulacros de desastres, aunque se podría dar por un factor positivo. Hay que tener en cuenta que este tipo de simulacros solo se ha realizado para estar preparados en desastres sísmicos mas no en desastres naturales y humanos, aún más sin la capacitación correspondiente.

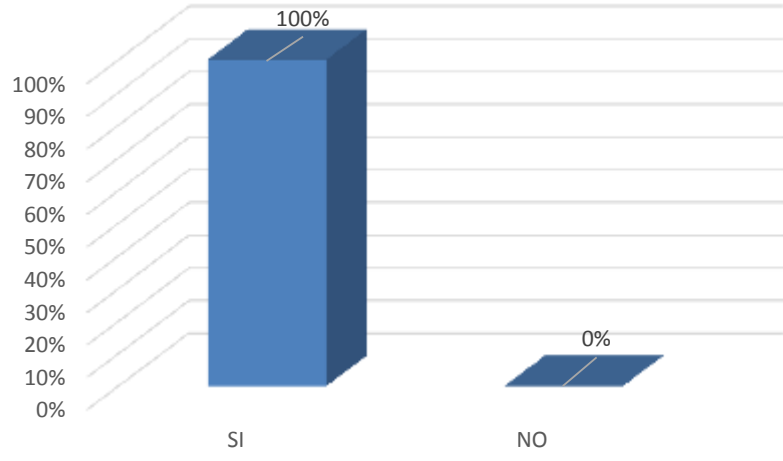

Figura 10. Conocimiento de ubicación de extintores

Fuente: Elaboración del investigador

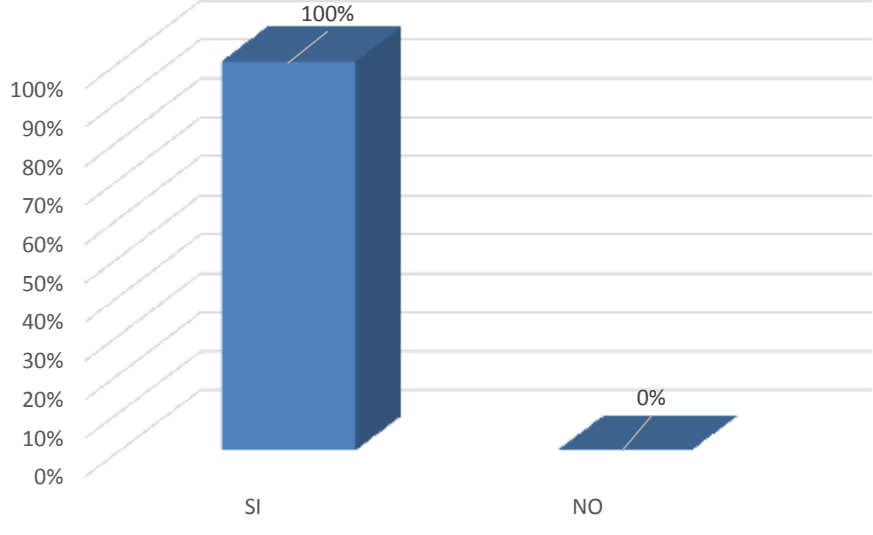

Figura 11. Manejo adecuado de un extintor

Fuente: Elaboración del investigador

- Con respecto a la seguridad, estos puntos son muy importantes, ya que el DARA, al contener una gran cantidad de material inflamable, en su mayoría papel, es susceptible a un incendio, y el actuar inmediatamente, será de gran ayuda. En las figuras 7 y 8 nos refleja de que el personal

de seguridad conocen la ubicación de los extintores y así como el uso correcto de ellos, el inconveniente se da en que dentro del DARA no se cuenta con ningún extintor, lo que dificultaría combatir por ejemplo un incendio.

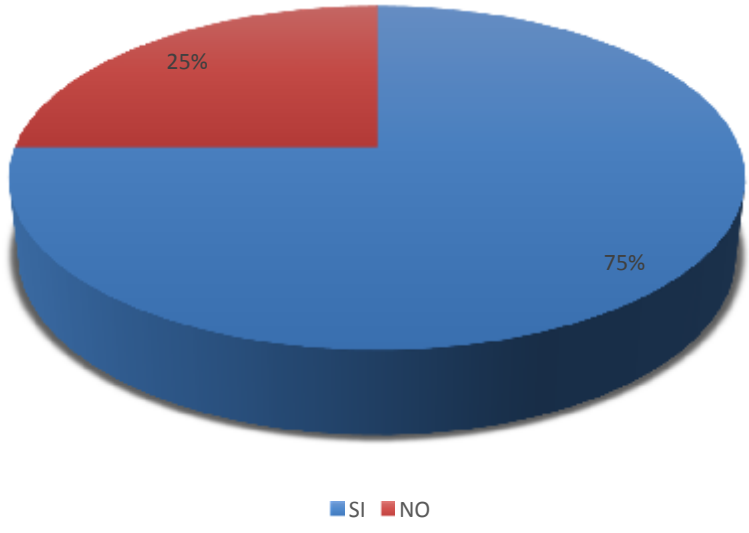

Figura 12. Identificación de personas que ingresan a la UPAGU
Fuente: Elaboración del investigador

- Este punto también es importante pues hace ver que la universidad así como el DARA, se encuentran vulnerables frente al ingreso de personas que podrían ingresar y cometer actos dolosos, lo que pondría expuesta a los activos de la información a una serie de incidentes, pues al no existir un control de que personas ingresarían y las intenciones de éstas, se pone en peligro los activos mencionados.

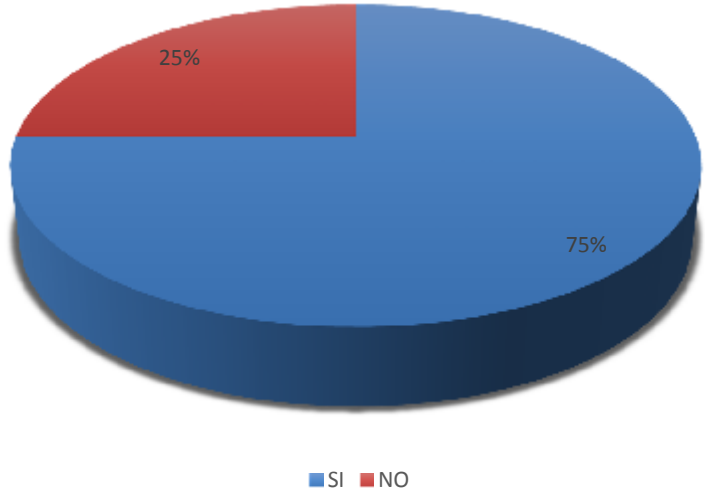

Figura 13. Inspección de equipos en el ingreso y salida
Fuente: Elaboración del investigador

- En la figura 11, que corresponde a la inspección de equipos al ingreso y a la salida de la universidad, solo el 75% realiza esta acción, problema que también deja vulnerable a cualquier área o unidad de la universidad por el hecho de que fácilmente pueden ser extraídos equipos de cómputo, de comunicación o incluso de almacenamiento, quedando también en peligro además de los activos físicos, la información que está almacenados en dicho equipos, o se podría perder la continuidad de las actividades del DARA, si es sustraído un equipo de cómputo.

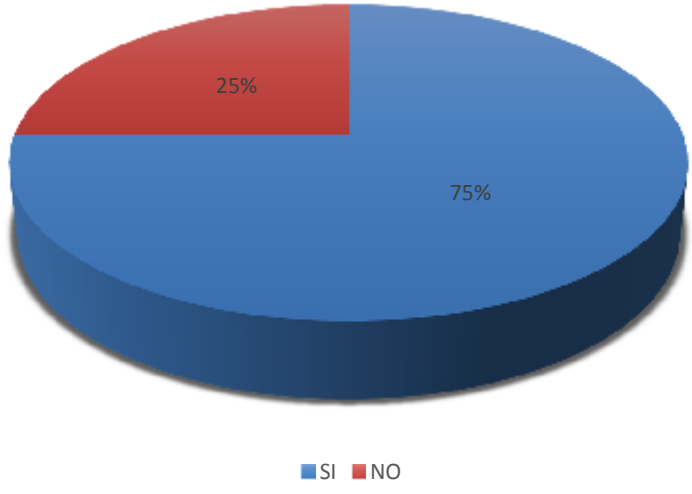

Figura 14. Percepción de seguridad del DARA
Fuente: Elaboración del investigador

- De acuerdo a la figura anterior, en cuanto a la percepción de la seguridad en su conjunto del DARA, el 75% del personal de seguridad nos indica que el ambiente es seguro, lo que a través de la observación directa y la entrevista al personal, queda demostrado que esta percepción es errónea, pues las instalaciones de este departamento no lo son, por el contrario son una amenaza por el hecho de que esta percepción al considerarla segura, deja vulnerable a este departamento, pues se asume que no podrían ocurrir algún tipo de peligro, o que es segura y no se encuentra expuesta a ciertos incidentes también peligrosos.

- Los problemas de seguridad encontrados con respecto al software de aplicación que es descargado en los equipos, además de los antivirus que nos son actualizados, dejando una vulnerabilidad grande. Referente

a la información física y digital se puede indicar que guarda los componentes para aceptar que cumplen con los criterios de confiabilidad, integridad y disponibilidad.

- Con respecto a las tecnologías de comunicación, se ha obtenido como datos que, las comunicaciones no se encuentran seguras, no se ha dado el cifrado respectivo a las transmisiones de la información a través de la red, por ende cualquier persona una vez que tiene acceso a la red y tenga conocimiento de transmisión de datos podría tomar el control de dichas comunicaciones.

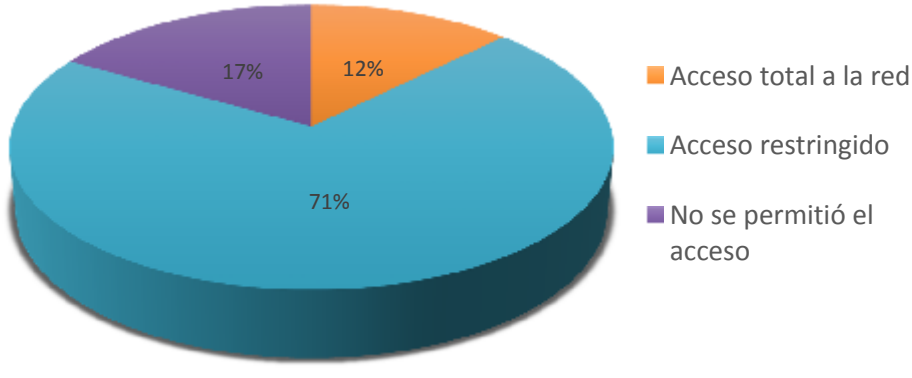

Figura 15. Acceso a la red de la UPAGU
Fuente: Elaboración del investigador

- Otro punto importante es el acceso a la red de la UPAGU, ya sea vía cable o a través del wireless, de acuerdo al gráfico 13, se aprecia que del total de personas entre docentes, alumnos y administrativos que intentan acceder a la red, el mayor porcentaje tiene un acceso restringido y a un 12% de personas no se le permitió el acceso, pero el

12% que en realidad es un porcentaje peligroso que logro el acceso total a la red, lo convierte en punto muy vulnerable puesto que aquí podrían explotarse una serie de amenazas.

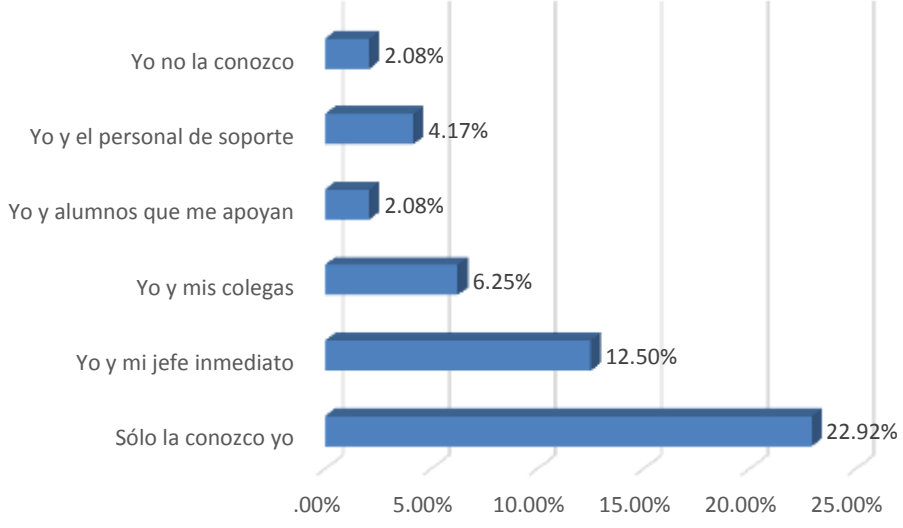

Figura 16. Conocimiento de las contraseñas de la UPAGU
Fuente: Elaboración del investigador

- En este punto que corresponde a las contraseñas utilizadas para acceder a un servicio informático de la UPAGU, como puede ser el correo electrónico, acceso a la intranet, incluso el acceso al mismo equipo, según la información detallada en la figura 13, la mayoría del personal docente y administrativo señala que solo ellos conocen sus contraseñas, se puede apreciar que existen personas que han entregado sus contraseñas a otras personas, lo que resulta en un problema de seguridad, puesto que si ocurriera un incidente en la seguridad, a pesar de identificar al usuario, quizá se trató de otra persona utilizando las credenciales de dicho usuario y sería complicado encontrar al responsable.

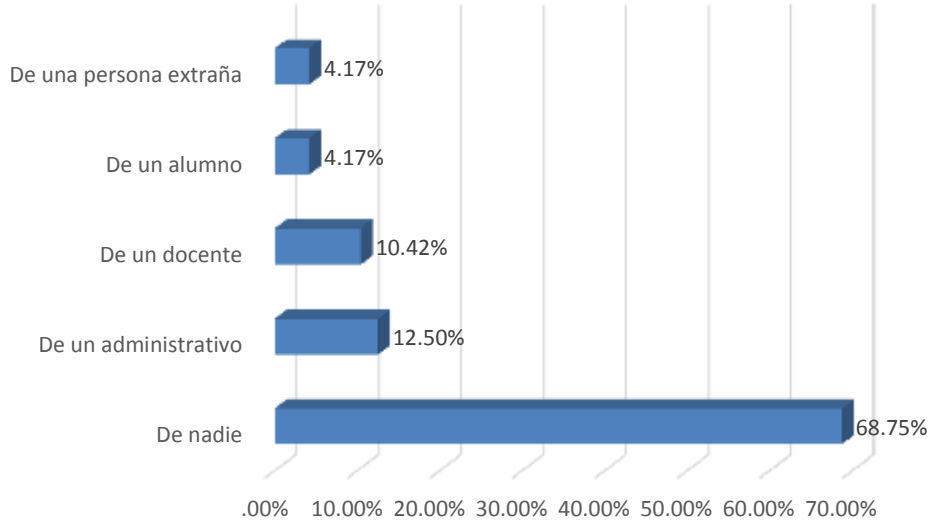

Figura 17. Apoyo las tareas informáticas

Fuente: Elaboración del investigador

- En lo que se refiere al apoyo que pueda solicitar un usuario sea docente o administrativo, dentro de la UPAGU, de acuerdo a los señalado en la figura 15, el mayor porcentaje del personal no necesita ayuda, pero se puede apreciar de que existen personas que en algún momento determinado han solicitado el apoyo en la realización de tareas informáticas a otras personas, que fueron alumnos e incluso personas extrañas, de aquí también se originan una serie de amenazas, ya que la información quedaría vulnerable ante una persona no autorizada.

- Con respecto a la seguridad de la información y que corresponde a las personas, los integrantes del DARA son claves para brindar a la información la seguridad que le corresponde, como punto favorable. Las personas que laboran en el DARA se sienten identificadas con la institución y existe un ambiente de alta confianza, además de conocer

de manera adecuada los procesos que se dan en esta unidad. El ambiente laboral es adecuado lo que permite conocer sus estados de ánimo y es más sus necesidades, y deja una baja probabilidad de que se pueda cometer algún acto doloso o de manipulación inapropiada de la información.

- En personas también tenemos a los alumnos que no solo son consumidores de información a través de reportes académicos, sino también alimentan las bases de datos con su información personal. Los alumnos en oportunidades han cometido adulteraciones con los reportes académicos para beneficio personal, pero lo hacen de manera externa a la universidad, por ejemplo una falsificación de un record de notas cuando se encuentra desaprobado. Se detectaron también casos de alumnos que han podido ingresar a los módulos del sistema que es utilizado por los docentes y han realizado modificaciones en los calificativos, hechos que son generados por descuido de los docentes y acciones de protección en las aplicaciones con que cuenta la universidad.

- En cuanto al personal docente, se cuenta con profesionales calificados y que son evaluados constantemente, pero hay hechos que son generados por la no identificación de los docentes, pues a veces el incumplimiento de algunas actividades en los procesos académicos hace que la información no esté disponible o en todo caso incompleta. Por parte de existir alguna manipulación, o hecho doloso, no se han

registrado hasta el momento ninguna incidencia, solo lo expresado anteriormente que corresponde al incumplimiento de tareas.

- Luego de una evaluación de las amenazas y vulnerabilidades, debemos tener en cuenta las percepciones y lo que en este momento existe con respecto a la normativa que podría apoyar la implementación del sistema de gestión de la seguridad de la información (SGSI). La Regulación de la seguridad de la información en la UPAGU, de acuerdo a la entrevista con personal de informática y de algunas autoridades, se ha encontrado que, la institución no cuenta con un sistema de gestión de seguridad de la información, ni de manuales o políticas de seguridad de la información y que tampoco existen planes para en un corto o mediano plazo se pueda realizar algún proyecto de este tipo.

- Conocimiento acerca de la seguridad de la información, este punto es muy importante para determinar cómo los integrantes de la institución conocen y pueden determinar la importancia de una gestión de la seguridad de la información, el 87% respondió que no conoce lo que es un SGSI, de aquí se puede considerar que al no conocer estos conceptos, tampoco pueden dar la importancia que corresponde y tampoco sentirse involucrados en el tema.

- Los procedimientos se encuentran claramente establecidos a través de reglamentos y directivas dentro del DARA, esto permite tener en claro lo que se debe y no hacer durante la ejecución de un proceso que corresponde al área, pero no se tiene establecido una normatividad para

gestionar la información y brindarle los criterios básicos como es la integridad, confiabilidad y disponibilidad. Adicionalmente las actividades se encuentran definidas en el DARA, pero no están definidos de manera formal, no se cuenta con un reglamento o manual de funciones del departamento, por lo que sólo se cumplen las actividades de los procesos establecidos y luego, en algunas ocasiones, se realizan actividades que no son de competencia de este departamento. De acuerdo a la observación directa y la entrevista a los integrantes se pudo apreciar que esta dependencia apoya en una serie de actividades que son solicitadas por otras áreas.

De acuerdo a este análisis se puede determinar que existen una serie de activos de información que se encuentran en riesgo en su seguridad, que existen amenazas y estas pueden vulnerar sus puntos débiles y provocar una serie de problemas que podrían ocasionar incluso la interrupción de los procesos. Se presenta a continuación el mapeo de activos detallados encontrados y los riesgos que se han podido determinar, en la matriz de riesgos

Tabla 8. Matriz de riesgos

ID de Riesgo	Activo	Vulnerabilidad	Amenaza	Posibilidad que la amenaza explote la vulnerabilidad	Impacto estimado en la institución	Nivel de Riesgo

R1	Computadora de escritorio	No se bloquea al momento de salir de la estación de trabajo	Manipulación de información	Alto	Alto	Alto
R2	Computadora de escritorio	Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	Medio	Muy Alto	Alto
R3	Computadora de escritorio	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	Alto	Muy Alto	Crítico
R4	Computadora de escritorio	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Bajo	Muy Alto	Medio
R5	Computadora de escritorio	Falta de backups de información	Robo de información o del mismo equipo	Muy Alto	Muy Alto	Crítico
R6	Computadora de escritorio	Mala seguridad de contraseñas	Espionaje remoto	Alto	Muy Alto	Crítico
R7	Computadora portátil	No se bloquea al momento de salir de la estación de trabajo	Manipulación de información	Alto	Alto	Alto
R8	Computadora portátil	Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	Medio	Muy Alto	Alto
R9	Computadora portátil	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	Alto	Muy Alto	Crítico
R10	Computadora portátil	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Bajo	Muy Alto	Medio
R11	Computadora portátil	Falta de backups de información	Robo de información o del mismo equipo	Muy Alto	Muy Alto	Crítico
R12	Computadora portátil	Mala seguridad de contraseñas	Espionaje remoto	Alto	Muy Alto	Crítico
R13	Computadora portátil	Traslado fuera de la universidad	Robo de información o del mismo equipo	Muy Alto	Muy Alto	Crítico
R14	Computadora portátil	Todos los dispositivos están unidos	Deterioro de un dispositivo que afecta a todo el equipo	Alto	Muy Alto	Crítico
R15	Sistema Operativo (Windows 7)	Falta de mecanismos de autenticación e identificación de usuarios	Abuso o forzado de derechos	Bajo	Muy Alto	Medio
R16	Sistema Operativo (Windows 7)	Mala gestión de contraseñas	Abuso o forzado de derechos	Bajo	Muy Alto	Medio
R17	Sistema Operativo (Windows 7)	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy Alto	Crítico
R18	Microsoft Office 2007	Mala gestión de contraseñas	Abuso o forzado de derechos	Bajo	Alto	Medio
R19	Microsoft Office 2008	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Alto	Alto

R20	Página web de La universidad	Falta de pruebas del software	Abuso de derechos	Medio	Medio	Medio
R21	Página web de La universidad	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Medio	Alto
R22	Página web de La universidad	Interfaz de usuario complicada	Error en el uso del software	Alto	Medio	Alto
R23	Página web de La universidad	Falta de documentación	Error en el uso del software	Medio	Medio	Medio
R24	Página web de La universidad	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Medio	Alto
R25	Intranet de la UPAGU	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R26	Intranet de la UPAGU	Pocos o nulos controles de acceso	Abuso de derechos	Alto	Alto	Alto
R27	Intranet de la UPAGU	Interfaz de usuario complicada	Error en el uso del software	Alto	Alto	Alto
R28	Intranet de la UPAGU	Fechas incorrectas	Error en el accionar	Bajo	Alto	Medio
R29	Intranet de la UPAGU	Mala gestión de contraseñas	Abuso de derechos	Medio	Alto	Alto
R30	Intranet de la UPAGU	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Alto	Alto
R31	Correo Electrónico	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R32	Correo Electrónico	Falta de un log de pistas de auditoria	Abuso de derechos	Medio	Alto	Alto
R33	Correo Electrónico	Fechas incorrectas	Error en el accionar	Muy Bajo	Alto	Bajo
R34	Correo Electrónico	Falta de mecanismos de autenticación e identificación de usuarios	Abuso de derechos	Medio	Alto	Alto
R35	Correo Electrónico	Falta de backups de información	Manipulación de información	Medio	Alto	Alto
R36	Software de aplicaciones de escritorio	Mala gestión de contraseñas	Abuso o forzado de derechos	Bajo	Alto	Medio
R37	Software de aplicaciones de escritorio	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Alto	Alto
R38	Software de aplicaciones de escritorio	Programas troyanos	Manipulación de información	Medio	Alto	Alto
R39	Cableado Ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	Medio	Alto	Alto
R40	Cableado Ethernet	Cableado desprotegido	Falla en los equipos de comunicaciones	Alto	Alto	Alto
R41	Cableado Ethernet	Arquitectura de red insegura	Espionaje remoto	Bajo	Alto	Medio

R42	Cableado Ethernet	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R43	Wireless	Trafico de información desprotegido	Escuchar información ilegalmente	Medio	Alto	Alto
R44	Wireless	Contraseñas inadecuadas en los access point	Espionaje remoto	Alto	Alto	Alto
R45	Wireless	Arquitectura de red insegura	Espionaje remoto	Bajo	Alto	Medio
R46	Wireless	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R47	Switch	Contraseñas inadecuadas	Espionaje remoto	Alto	Alto	Alto
R48	Switch	Gestión inadecuada de la red	Escuchar información ilegalmente	Alto	Alto	Alto
R49	Sistema de Información Académico	Defectos en el funcionamiento del software	Abuso de derechos	Medio	Muy Alto	Alto
R50	Sistema de Información Académico	Falta de cierre de sesión al momento de salir de la estación de trabajo	Manipulación de información	Alto	Muy Alto	Crítico
R51	Sistema de Información Académico	Falta de un log de pistas de auditoria	Abuso de derechos	Medio	Muy Alto	Alto
R52	Sistema de Información Académico	Pocos o nulos controles de acceso	Abuso de derechos	Alto	Muy Alto	Crítico
R53	Sistema de Información Académico	Interfaz de usuario complicada	Error en el uso del software	Alto	Muy Alto	Crítico
R54	Sistema de Información Académico	Falta de documentación	Error en el uso del software	Medio	Muy Alto	Alto
R55	Sistema de Información Académico	Fechas incorrectas	Error en el accionar	Muy Bajo	Muy Alto	Medio
R56	Sistema de Información Académico	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy Alto	Crítico
R57	Sistema de Información Académico	Software nuevo o con fallas	Mal funcionamiento del software	Muy Alto	Muy Alto	Crítico
R58	Sistema de Información Académico	Falta de backups de información	Manipulación de información con software	Medio	Muy Alto	Alto
R59	Sistema de Información Académico	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Muy Alto	Crítico
R60	Anaqueles	Deterioro de los anaqueles	Destrucción de documentos impresos	Bajo	Muy Alto	Medio
R61	Instalaciones eléctricas	Instalaciones en mal estado	corto circuitos	Medio	Muy Alto	Alto

R62	Archivadores para los documentos	En mal estado	Perdida de documentos impresos	Muy Bajo	Muy Alto	Medio
R63	Llaves de ingreso	Uso inadecuado o sin cuidado de accesos a instalaciones o habitaciones	Destrucción o robo de equipos o medios de comunicación	Alto	Muy Alto	Crítico
R64	Personal del DARA	Disponibilidad total de la información	Cometa actos dolosos con la información	Medio	Muy Alto	Alto
R65	Alumnos	Disponibilidad parcial de la información	Cometa actos dolosos con la información	Muy Bajo	Muy Alto	Medio
R66	Personal docente y administrativo	Disponibilidad parcial de la información	Cometa actos dolosos con la información	Bajo	Muy Alto	Medio
R67	Resoluciones (en físico y digital)	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R68	Resoluciones (en físico y digital)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R69	Resoluciones (en físico y digital)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R70	Documentación interna de la UPAGU	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R71	Documentación interna de la UPAGU	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R72	Documentación interna de la UPAGU	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R73	Reglamentos Académicos de estudios	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R74	Reglamentos Académicos de estudios	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R75	Reglamentos Académicos de estudios	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R76	Plan de estudios	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R77	Plan de estudios	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R78	Plan de estudios	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R79	Plan Estratégico de la UPAGU	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R80	Plan Estratégico de la UPAGU	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto

R81	Plan Estratégico de la UPAGU	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R82	Estatuto de la UPAGU	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R83	Estatuto de la UPAGU	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R84	Estatuto de la UPAGU	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R85	Plan operativo anual del DARA	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R86	Plan operativo anual del DARA	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R87	Plan operativo anual del DARA	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R88	Cronogramas Académicos	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R89	Cronogramas Académicos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R90	Cronogramas Académicos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R91	Reporte de alumnos	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R92	Reporte de alumnos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R93	Reporte de alumnos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R94	Información académica de alumnos	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R95	Información académica de alumnos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R96	Información académica de alumnos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R97	Carga horaria semestral de docentes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R98	Carga horaria semestral de docentes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R99	Carga horaria semestral de docentes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico

R100	Información de postulantes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R101	Información de postulantes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R102	Información de postulantes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R103	Reportes de ingresantes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R104	Reportes de ingresantes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R105	Reportes de ingresantes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R106	Guías de Postulantes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R107	Guías de Postulantes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R108	Guías de Postulantes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R109	Reglamento de admisión	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R110	Reglamento de admisión	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R111	Reglamento de admisión	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R112	Carpeta de postulantes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R113	Carpeta de postulantes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R114	Carpeta de postulantes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R115	Ficha de Admisión	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R116	Ficha de Admisión	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R117	Ficha de Admisión	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R118	TUPA actualizado de la UPAGU	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio

R119	TUPA actualizado de la UPAGU	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R120	TUPA actualizado de la UPAGU	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R121	Consolidados de vacantes, postulantes e ingresantes	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R122	Consolidados de vacantes, postulantes e ingresantes	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R123	Consolidados de vacantes, postulantes e ingresantes	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R124	Exámenes de admisión / Banco de preguntas	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R125	Exámenes de admisión / Banco de preguntas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R126	Exámenes de admisión / Banco de preguntas	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R127	Registro de las matriculas	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R128	Registro de las matriculas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R129	Registro de las matriculas	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R130	Reportes de categorización	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R131	Reportes de categorización	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R132	Reportes de categorización	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R133	Reporte de distribución de aulas	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R134	Reporte de distribución de aulas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R135	Reporte de distribución de aulas	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R136	Horarios	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio

R137	Horarios	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R138	Horarios	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R139	Fotografías de los alumnos (físico y digital)	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R140	Fotografías de los alumnos (físico y digital)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R141	Fotografías de los alumnos (físico y digital)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R142	Acta de evaluación de alumnos	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R143	Acta de evaluación de alumnos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R144	Acta de evaluación de alumnos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R145	Reportes de evaluaciones	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R146	Reportes de evaluaciones	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R147	Reportes de evaluaciones	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico
R148	Reportes de asistencias	Falta de mecanismos de backup	Robo o pérdida de documentos	Bajo	Muy Alto	Medio
R149	Reportes de asistencias	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Medio	Muy Alto	Alto
R150	Reportes de asistencias	Pocos o nulos controles de acceso	Robo o manipulación del activo	Alto	Muy Alto	Crítico

Fuente: Elaboración del investigador de acuerdo a los resultados hallados.

4.1.4. Evaluación y aceptación de riesgos

Una vez identificados y valorizados los riesgos, de acuerdo a las vulnerabilidades de cada activo y las amenazas que puedan afectar los principios de integridad, confidencialidad o disponibilidad; se definió la aceptación del riesgo, en donde se establece la aceptación o no del riesgo, y si es no aceptado, se deberá proponer un plan de tratamiento, para posteriormente proponer las políticas necesarias.

A continuación se presenta la tabla que define el tratamiento de los riesgos:

Tabla 9. Tratamiento de riesgos

Nivel de Riesgo	Política para la toma de Acciones
Crítico	Riesgo no aceptable
Alto	Riesgo no deseable
Relevante	Riesgo aceptable
Moderado	Riesgo aceptable
Bajo	Riesgo aceptable

Fuente: Elaboración del investigador de acuerdo a la recomendación de la norma.

De acuerdo a la norma, el tratamiento de los riesgos, se evalúa en base a las incidencias y se propone el tratamiento adecuado en el caso del DARA. Además, se consideró que para los niveles Crítico y Alto, se deberá tomar medidas para el tratamiento de los riesgos, con la finalidad de mitigar o desaparecer dichos riesgos, en los demás casos no se requerirá de tratamiento pues se considera que la incidencia en el DARA es baja y se puede convivir con dichos riesgos.

4.2. Discusión

Según el presente estudio se determina que la UPAGU, no cuenta con planes de protección de la seguridad de su información, al igual que una gran cantidad de organizaciones a nivel local, nacional e incluso internacional, pero la tendencia en tomar una serie de medidas de protección a la información empieza a crecer. Será importante para la universidad evaluar este trabajo de investigación, pues es muy necesaria y al igual que en el DARA se asume que otras unidades críticas necesitan de la implementación de estas medidas, en este caso la implementación de un SGSI, que por la acelerado crecimiento de amenazas debería convertirse en un proyecto corporativo en donde se cuente con el apoyo de las distintas direcciones y áreas.

Según (EY PERU, 2015) en el resumen de la Encuesta Global de Seguridad de Información 2015, nos indica: La evolución de las tecnologías de cómputo y comunicaciones plantean un reto para la seguridad de la información frente al surgimiento de un nuevo tipo de amenaza, la delincuencia cibernética. “El estar preparados es la única manera de estar delante de los delincuentes cibernéticos”. Ese es el mensaje de EY a las empresas en todo el mundo como resultado de las respuestas de 1,825 organizaciones que respondieron la “17va. Encuesta Global de Seguridad de Información 2014”, que este año se centra en explorar qué tan bien gestionan las organizaciones las amenazas cibernéticas y qué están haciendo para mitigar los riesgos de hoy. Por consiguiente, al concluir el presente trabajo, la UPAGU debería estar preparada para afrontar las incidencias que se puedan presentar, pues se ha llegado a determinar una serie de vulnerabilidades y amenazas en el DARA, que se podrían ir acrecentando cuando se realice un proyecto global.

La importancia de seguir una metodología estándar y que es utilizada de manera creciente por las empresas, nos da una posibilidad de poder realizar un trabajo que podría darnos mejores resultados, en el caso de las instituciones educativas sobre todo las universidades. A partir del 2007, cuando Rubén Alejandro Rayme Serrano, cuando realiza su trabajo de investigación: "Gestión de seguridad de la información y los servicios críticos de las universidades" determina que aún las universidades en la mayoría de los casos aún no toman planes formales para la seguridad de su información, y al trabajar con los especialista de algunas universidades crean los ambientes que dan una base para el establecimiento de políticas de seguridad, incluso de implementación de SGSI's; de aquí es que los resultados que se han encontrado en el presente trabajo, al obedecer a una norma basada en estándares, brinda la posibilidad de alcanzar una eficiente propuesta.

El factor humano en este tipo de trabajos es fundamental. Desde la planificación se tiene que involucrar a todos, quienes sean los actores de la organización. En el caso de este trabajo se está considerando un área específica, pero de igual manera se debe comprometer a todo el personal y más aún a la alta dirección, justamente también (Talavera, 2015) nos indica que "Es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Dirección General de modo que se facilite el acceso a la información de todas las áreas pertinentes".

Los activos y su evaluación conjuntamente con sus riesgos inherentes, juegan el punto más importante que se debe tener en cuenta al momento de la

implementación de un SGSI, para el caso del DARA, el análisis de riesgos jugó un papel determinante para que se pueda formular un adecuado SGSI, de estos resultados dependerá si la propuesta es coherente y cumple con las condiciones necesarias para la protección de los activos principales. Lo mencionado es también comprobado por (De La Cruz Guerrero & Vásquez Montenegro, 2008) en su trabajo de investigación, donde concluyen que "El SGSI se encuentra estrechamente relacionado con la gestión de riesgos de una institución y tal como se puede evidenciar en el presente documento, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera".

4.3. Contrastación de la hipótesis

Para la presente investigación se formuló como hipótesis: "La información, las personas que hacen uso de ella y los equipos e infraestructura que la soportan son elementos que se encuentran con riesgos de seguridad y que deben necesitar de la formulación de un Sistema de Seguridad de la Información para el Departamento de Admisión y Registro Académico de la UPAGU", para contrastar dicha hipótesis con la realización de esta investigación, se utiliza el siguiente flujograma:

Del flujograma, se puede señalar lo siguiente, se realizó la identificación de los procesos core del DARA, estos procesos para su efectivo desarrollo necesita valerse de activos, activos de información que se han clasificado en tres grupos que para la presente investigación se ha hecho coincidir con las dimensiones. Se encontraron un total de 57 activos, luego una vez identificados los activos se realizó una evaluación de los riesgos en base a las amenazas y vulnerabilidades de cada uno de los activos, se identificaron y valoraron dichos riesgos, analizando las probabilidades de ocurrencias, además de las incidencias ocurrentes a la fecha en este departamento. De acuerdo a este último paso se ha determinado que existen una serie de riesgos que son catalogados como críticos y con una probabilidad alta de ocurrencia, en definitiva hay riesgos con los que se tiene que lidiar para proteger la continuidad de las operaciones del DARA, en tal sentido la hipótesis propuesta ha sido contrastada pues es necesario tomar medidas con el fin de proteger la

seguridad de la información y esta medida resulta como la propuesta de un SGSI, pues ya con los datos trabajados hasta la valoración de los riesgos, tan solo se debe completar con las políticas necesarias para preservar dicha información.

CAPÍTULO 5

PROPUESTA DEL SGSI

5.1. Presentación de la propuesta

La propuesta está basada en la presentación de un SGSI, fundada en la norma ISO/IEC 27000, el sistema se basa en una serie de tablas donde se describen los controles desde la identificación de los procesos importantes de la unidad evaluada, hasta la Declaración de la Aplicabilidad. En la presentación de resultados en el capítulo anterior se han mostrado algunas de estas tablas que para efectos de contrastar la hipótesis de la investigación, fueron utilizadas para presentar los resultados, a continuación se mencionaran dichas tablas y se complementará el sistema con las demás tablas que son requeridas, incluso como los entregables del SGSI:

a) Identificación de los procesos core del DARA, donde se identificaron los varios procesos, de los cuales son cuatro los más importantes dentro de este departamento:

- Proceso de Admisión:
- Proceso de Matrícula
- Proceso de Generación de Actas de Evaluación
- Proceso de Emisión de Documentos Académicos

b) La identificación de Activos (Tabla 5), estuvo basada en las dimensiones establecidas para la investigación la misma información, los equipos e infraestructura que soporta la información y las personas que usan la información, tales activos se desprenden de los procesos encontrados anteriormente.

c) Valoración de activos (estas tablas se obviaron puesto que la cantidad de activos era relativamente pequeña y la unidad observada era crítica para la organización a la que pertenece, en este caso a la UPAGU, por lo que se llegó a considerar a todos los activos para la posterior identificación y valorización de los riesgos.

d) Matriz de calor, Tabla 6, en donde se da una propuesta para la valoración de los riesgos en base a como una amenaza podría tomar una vulnerabilidad encontrada en los activos. En esta matriz se define los niveles de probabilidad de ocurrencia y el impacto que ejercerá el riesgo a la unidad objeto de la investigación.

e) Matriz de riesgos, Tabla 8, en donde a partir de las amenazas y vulnerabilidades encontradas, se los valora en base a la matriz de calor, aquí se asigna un nivel a cada riesgo encontrado.

f) Tratamiento de riesgos, Tabla 9, esta tabla ofrece los niveles que son propuestos para el tratamiento de los riesgos, una vez que estos han sido valorados, en donde se consideran a los riesgos con valores críticos y altos, a los que se les aplicará las políticas.

g) Controles para el tratamiento de riesgos, de acuerdo a lo indicado en la norma (ISO/IEC 27002:2005), se presenta la siguiente tabla con los Dominios, Objetivos de control y Controles, para el establecimiento de las políticas:

Tabla 10. Políticas a través de controles de la norma

Dominio	Categoría de Seguridad	Nombre Control	Descripción
Política de seguridad	Política de seguridad de información	Documentar política de seguridad de información	La alta gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
		Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
	Organización interna	Coordinación de la seguridad de información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
		Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
		Proceso de autorización para los medios de procesamiento de información	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información.
		Acuerdos de confidencialidad	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
	Entidades externas	Tratamiento de la seguridad cuando se trabaja con clientes	Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
Gestión de activos	Responsabilidad por los activos	Inventarios de activos	Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
		Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
	Clasificación de la información	Lineamientos de clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
		Etiquetado y manejo de la información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.
Gestión de las comunicaciones y operaciones	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
Control de acceso	Gestión del acceso del usuario	Revisión de los derechos de acceso del usuario	La alta gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Seguridad en los procesos de desarrollo y soporte	Desarrollo de outsource software	El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.

Gestión de incidentes en la seguridad de la información	Reporte de eventos y debilidades en la seguridad de la información	Reporte de eventos en la seguridad de la información	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
		Reporte de debilidades en la seguridad	Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
	Gestión de incidentes y mejoras en la seguridad de la información	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
		Aprendizaje de los incidentes en la seguridad de la información	Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
		Recolección de evidencia	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
		Protección de data y privacidad de información personal	Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
		Prevención de mal uso de medios de procesamiento de información	Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
Conformidad	Cumplimiento con requerimientos legales	Protección los registros organizacionales	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

Fuente: Elaboración del investigador de acuerdo a la recomendación de la norma.

h) Declaración de la aplicabilidad, una vez definidas las políticas de seguridad que se deben adoptar, se procede a listar los controles para el tratamiento de los diversos riesgos identificados; especificando el control, su descripción según la norma ISO 27002, los riesgos que mitigará, la adaptación de dicho control con la realidad evaluada y la justificación de la implementación.

Tabla 11. Declaración de la aplicabilidad

Nombre Control	Riesgos a Controlar	¿Aplica?	Descripción adecuada de la norma a la UPAGU	Justificación
Controles de entrada físicos	R63	Si	Se deberán proteger las áreas críticas en especial al DARA, mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	A la fecha no se cuenta con políticas de acceso a los lugares que deberían ser restringidos, incluye al DARA
Seguridad de oficinas, habitaciones y medios	R60, R62, R63	Si	Se deberán diseñar y aplicar controles de seguridad físicos en las oficinas, habitaciones y medios.	Con el fin del aseguramiento de los ambientes físicos, se deben tomar en cuenta controles, brindados por instituciones como Defensa Civil, Cia. De Bomberos, entre otros
Ubicación y protección del equipo	R2, R8, R61	Si	Los equipos electrónicos críticos deberán estar ubicados de tal manera que ayudarán a reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	No se cuentan con políticas que apoyen a reducir los riesgos en cuanto a las amenazas ambientales, ni los accesos no autorizados
Servicios públicos	R2, R3, R9, R61	Si	Los equipos electrónicos críticos deberán ser protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios eléctricos o de telecomunicaciones	Tampoco se cuenta con algún control contra las fallas de energía, a pesar que estas vulnerabilidades están presentes
Seguridad en el cableado	R3, R9, R39, R40, R42, R43, R61	Si	El cableado eléctrico y de las telecomunicaciones que llevan data o sostienen los servicios de información de dentro y fuera del DARA, deberán ser protegidos mediante tubos u otros controles	No se cuentan con políticas ni tampoco se realizan las instalaciones teniendo en cuenta las normas básicas.
Mantenimiento de equipo	R2, R3, R14, R39, R40, R42	Si	Los equipos deberán pasar por mantenimiento 1 vez mensual para asegurar la continuidad de los sistemas y demás aplicativos que dan soporte a los procesos críticos	Ya que el mantenimiento no es preventivo, sino correctivo, se necesitan políticas para poder mejorar la continuidad de los equipos.
Aceptación del sistema	R21, R22, R24, R25, R27, R30, R31, R37	Si	El responsable del DARA, deberá asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deberán pasar a producción luego de obtener la aceptación formal.	Es importante la participación del responsable del DARA, cuando se realice adquisiciones de sistemas nuevos, y es en las políticas donde se definirán estos procedimientos.

Controles contra software malicioso	R28, R32, R33, R38, R55	Si	La protección contra códigos maliciosos se deberá basar en la detección de códigos maliciosos dentro de los sistemas del DARA y la reparación del software, conciencia de seguridad, y los apropiados controles de acceso a los sistemas.	Es necesario implementar controles para la detección y prevención de ataques maliciosos a los sistemas, ya que este tipo de amenaza puede afectar la continuidad de las operaciones del DARA.
Back-up o respaldo de la información	R11, R35, R58, R59, R65, R66, R67, R70, R73, R76, R79, R82, R85, R88, R91, R94, R97, R100, R103, R106, R109, R112, R115, R118, R121, R124, R127, R130, R133, R136, R139, R142, R145, R148	Si	El DARA deberá proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y crítica se pueda recuperar después de algún desastre o falla de medios.	La única política en cuanto a los resguardos de la información, se da en la gerencia de informática y es sólo orientado a la base de datos corporativa
Controles de red	R39, R40, R42, R46, R48	Si	La Gerencia de Informática de la UPAGU, deberá implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.	El personal de soporte de informática debe ser quien proponga las mejores políticas con respecto al aseguramiento de las redes, pues hasta el momento no existen
Procedimientos de manejo de la información	R68, R71, R74, R77, R80, R83, R86, R89, R92, R95, R98, R101, R104, R107, R110, R113, R116, R119, R122, R125, R128, R131, R134, R137, R140, R143, R146, R149	Si	Se deberán establecer procedimientos para la manipulación, procesamiento, almacenamiento y comunicación de la información consistente con su clasificación	Este control se relaciona directamente a las políticas de seguridad de información que la institución implementará.
Procedimientos y políticas de información y software	R68, R71, R74, R77, R80, R83, R86, R89, R92, R95, R98, R101, R104, R107, R110, R113, R116, R119, R122, R125, R128, R131, R134, R137, R140, R143, R146, R149	Si	Se deberán establecer políticas, procedimientos y controles para proteger el intercambio de información que se da en el interior de la UPAGU, a través de todos los tipos de medios de comunicación que se maneje (teléfonos, correo electrónico, etc.).	Este control se relaciona directamente a las políticas de seguridad de información que se vayan a implementar

Mensajes electrónicos	R31, R34, R69, R72, R75, R78, R81, R84, R87, R90, R93, R96, R99, R102, R105, R108, R111, R114, R117, R120, R123, R126, R129, R132, R135, R138, R141, R144, R147, R150	Si	Los responsables de la seguridad, deberá manejar distintas políticas y controles que le permitan manejar de manera segura el intercambio de información vía Email.	Sólo se mantiene las reglas de correo electrónico del mismo proveedor, que en la caso de la UPAGU es Gmail
Registro de auditoria	R32, R51	Si	Los encargados de la seguridad, deberán producir logs de auditoría, excepciones y eventos de seguridad de información. Estos registros se deben mantener durante un período determinado para ayudar en investigaciones futuras y monitorear los sistemas y aplicativos que se necesiten	Se requiere mecanismos de monitoreo y registro de acciones para auditorias, así como de incidencias que son necesarias si se quiere llegar al nivel de seguridad deseado
Uso del sistema de monitoreo	R32, R51	Si	Los encargados de la seguridad, deberán determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo. Asimismo, deberá cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo.	Este control se lo podría implementar al utilizar un software que este alineado a la norma ISO/IEC 27000, para monitorear la seguridad
Inscripción del usuario	R17, R19, R17, R19, R23, R27, R34, R41, R45, R64, R67, R70, R73, R75, R78, R81, R88, R91, R94, R101, R108, R111, R116, R119, R122, R125	Si	Los encargados de la seguridad, deberán manejar un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a los usuarios de todos los sistemas y servicios de información que posea.	No existen controles adecuados para añadir o eliminar accesos a los usuarios, el proceso se realiza por demanda.
Gestión de privilegios	R15, R26, R17, R19, R24, R30, R37, R56	Si	Los sistemas multi-usuario del DARA que requieran protección contra el acceso no autorizado deberán controlar la asignación de privilegios a través de un proceso de autorización formal.	La Gerencia de Informática maneja procedimientos para la asignación de accesos y privilegios dentro de los sistemas de información, pero no se realizan de una manera formal o teniendo criterios definidos y aprobados
Gestión de la clave del usuario	R18, R29, R36	Si	La Gerencia de Informática, deberá proporcionar directrices para la gestión para las contraseñas de los distintos sistemas de información que se implementen en el DARA. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.	No existe una política formal para la gestión de las contraseñas dentro de los sistemas de información

Sistema de gestión de claves	R6, R12, R16	Si	La Gerencia de Informática, deberá proporcionar políticas para las contraseñas de sesiones de Windows de los colaboradores con acceso a una PC. Estas políticas pueden abarcar la generación, cambio y entrega de la contraseña.	Se manejan procedimientos para la gestión de contraseñas para que los usuarios que tienen acceso a una PC y a Windows, pero tales procedimientos no son establecidos de manera formal
Uso de clave	R18, R29, R36	Si	La Gerencia de Informática, deberá proporcionar políticas para las contraseñas de los distintos sistemas de información que sean implementados en el DARA. Estas políticas deberán seguir buenas prácticas de seguridad en la selección y uso de claves.	Se manejan procedimientos para la gestión de contraseñas para que los usuarios que tienen acceso a una PC y a Windows, pero tales procedimientos no son establecidos de manera formal
Equipo de usuario desatendido	R1,R7, R5, R13, R50	Si	Todos los usuarios de la UPAGU, en especial del DARA, deberán estar al tanto de los requerimientos de seguridad y los procedimientos para proteger su respectivo equipo desatendido, así como sus responsabilidades para implementar dicha protección	Dentro de las políticas de seguridad que se implantarán, esta es una de las más importantes ya que es un factor básico el implantar una concientización en seguridad por parte de los usuarios.
Política de pantalla y escritorio limpio	R1,R7, R5	Si	La políticas de escritorio limpio que los responsables de la seguridad proporcione deberá tomar en cuenta las clasificaciones de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización	Es importante porque así cada usuario estará alineado a la información y a los equipos que deberá utilizar
Política sobre el uso de servicios en red	R41, R45	Si	Se deberá formular una política relacionada con el uso de las redes y los servicios de la red, de tal manera que los usuarios de la UPAGU sólo deberán tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.	La red y los servicios que se dan a través de la red no tienen políticas que garantizan la seguridad de la información
Identificación y autenticación del usuario	R52, R6, R12	Si	Todos los usuarios de los sistemas implementadas por la Gerencia de Informática deberán tener un identificador singular (ID de usuario) para su uso personal y exclusivo (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos) para poder verificar la identidad de la persona que acceda a la PC.	Con esta política se pretende llevar un control en el uso de la información y de los equipos por parte de los usuarios, la autenticación garantizará que se asigne los accesos a quien corresponda
Uso de utilidades del sistema	R17, R19, R24, R30, R37, R56	Si	Se restringirá y controlará estrictamente el uso de los programas de utilidad que podrían ser capaces de superar los controles de Windows y de las aplicaciones a las cuales el usuario tiene acceso.	El uso sin control de cualquier tipo de software podría conllevar a la instalación de código malicioso, por eso la importancia de este control

Sesión inactiva	R1, R7, R15	Si	Las sesiones inactivas de los usuarios de Windows deberán cerrarse después de un período de inactividad definido por el área de Sistemas.	Esto con el fin de proteger los equipos cuando el responsable no se encuentra en su lugar de trabajo
Aislamiento del sistema sensible	R2, R3, R4, R8, R9, R10, R42, R44, R46, R47, R48, R61, R54, R55	Si	Los sistemas críticos para el DARA, deberán tener un ambiente de cómputo dedicado (aislado) respecto a los demás sistemas que se manejen. Esta área seguirá otro lineamiento de seguridad (por su nivel de criticidad).	Es necesario el resguardar a los equipos que contengas la información o las aplicaciones que procesan tal información
Análisis y especificación de los requerimientos de seguridad	R20, R22, R49, R53, R54, R57	Si	Los requerimientos de seguridad deberán ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.	Con este control se busca obtener mayor seguridad en los sistemas cuando son adquiridos o desarrollados

Fuente: Elaboración del investigador de acuerdo a la recomendación de la norma y los resultados de la investigación

CONCLUSIONES

A la finalización del presente trabajo se puede concluir lo siguiente:

1. La información es el activo más importante que posee el DARA, y esta se halla desprotegida. Se encontraron una serie de riesgos ~~a~~ los que es necesario prestarles la importancia debida; a partir de esto es que se presenta la propuesta de un SGSI, con el fin de resguardar a dicha información, en donde se incluyen efectivas políticas orientadas a la seguridad, con el fin de preservar la continuidad de los procesos y por ende el cumplimiento de los objetivos organizacionales.

2. Los procesos más importantes que se dan en el DARA, son los que sirvieron de base para identificar los activos de información, bases para el presente trabajo. Estos procesos que son parte de un área crítica son también muy importantes dentro de la organización.

3. La identificación de los activos de información, se ha podido realizar de una manera ordenada, al cumplir los lineamentos de las normas base que fueron empleados en el presente trabajo, como lo son la familia de normas derivadas del ISO 27000, que al mismo tiempo fueron el soporte para la formulación de la propuesta del Sistema de Gestión de Seguridad de la Información

4. Se ha determinado que existen una serie de riesgos que ponen en peligro a la información, estos riesgos se han determinado a través de encontrar las vulnerabilidades que podrían explotar las amenazas existentes, es así que la propuesta del SGSI, propone mitigar o eliminar estos riesgos y así permitir

la continuidad de las operaciones en el DARA y por ende en la UPAGU en su conjunto.

5. Como universidad, disponer que este SGSI se convierta en un marco común de gestión de la seguridad, con el fin de asegurar la integridad, disponibilidad y la confidencialidad de los datos pertenecientes a la institución, por tal motivo este proceso debería pasar a formar parte de los objetivos estratégicos de la organización.

SUGERENCIAS

Se presentan algunas sugerencias, luego de planteadas las conclusiones:

1. Se recomienda a la directiva de la UPAGU, involucrarse e involucrar a todo su personal en el tema de la seguridad de información, así mismo brindar la respectiva capacitación de tal manera que todos los empleados en los diversos niveles jerárquicos existentes en la UPAGU, conozcan la importancia y las consecuencias de no seguir los lineamientos de seguridad en el día a día.

2. El responsable del DARA, debería aprobar la implementación inmediata del SGSI que se está proponiendo en este trabajo, pues se ha definido que realmente los activos de información del DARA se encuentran en constante peligro debido a los riesgos existentes. Una vez implementado el SGSI, se debería, tal como lo recomienda la norma, realizar los seguimientos continuos para obtener los mejores resultados.

3. Los especialistas en información e informática de la UPAGU, tomando como punto de partida los resultados de esta investigación, deberían extender la propuesta a las distintas áreas de la UPAGU, para contar con un SGSI corporativo y que ayude con la continuidad de las operaciones de manera segura de toda la organización, además de lograr la certificación de tal sistema.

4. El personal de informática y el responsable del DARA, una vez lograda la implementación del SGSI, deberían emplear software especializado que

permita llevar de manera adecuada el control efectivo del tal sistema. Existen distintas herramientas para este fin, como las aplicaciones de paga, pero, así mismo hay aplicaciones gratuitas que cumplen con lo requerido, es más están alineadas a la norma vigente como lo es “Securia-SGSI”.

5. Como universidad, disponer que este SGSI se convierta en un marco común de gestión de la seguridad, con el fin de asegurar la integridad, disponibilidad y la confidencialidad de los datos pertenecientes a la institución, por tal motivo este proceso debería pasar a formar parte de los objetivos estratégicos de la organización.

REFERENCIAS

Aguirre, D. A. (Octubre de 2014). Diseño de us Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. Lima, Perú.

Ampuero, C. E. (Abril de 2011). Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía De Seguros. Lima, Perú.

Bernal, C. A. (2010). *Metodología de la Investigación* (Tercera ed.). Bogota, Colombia: Prentice Hall.

Buenaño, J. L., & Granda, M. A. (Diciembre de 2009). Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 - 27002. Guayaquil, Ecuador.

Chávez, D. H. (09 de 2012). Implementación de un Sistema de Seguridad en la Municipalidad Distrital de Baños del Inca. Cajamarca, Perú.

De La Cruz Guerrero, C. W., & Vásquez Montenegro, J. C. (Junio de 2008). Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT. Chiclayo, Perú.

De los Santos, S. (Octubre de 2009). Una al día, once años de seguridad informática. España: Hispasec Sistemas.

Ernst & Young. (2011). Seguridad de la Información en un Mundo sin Fronteras. Londres, Inglaterra.

Estándar Internacional ISO/IEC 27002, Primera Edición. (15 de 06 de 2005).

EY PERU. (2015). Encuesta Global de Seguridad de Información. Lima, Perú.

Gomez, A. (2011). Enciclopedia de la Seguridad Informática. Madrid, España: Ra-Ma.

Hallberg, B. A. (2003). *Fundamentos de Redes* (Primera ed.). Mexico DF., Mexico: McGraw-Hill.

INDECOPI. (22 de 01 de 2007). Norma Técnica Peruana ISO/IEC 17799:2005. Lima, Perú.

International Standard ISO/IEC 27000, Second Edition. (01 de 12 de 2012).

ISO/IEC 27002:2005. (s.f.). *Dominios, Objetivos de control y Controles*. Obtenido de ISO/IEC 27000 Web Site: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

ISO27000.ES. (2012). *El portal de ISO 27001 en Español*. Recuperado el 02 de 10 de 2015, de http://www.iso27000.es/

Maiwald, E. (2005). *Fundamentos de seguridad en redes* (Primera ed.). Mexico DF.: McGraw-Hill.

Microsoft; Tec de Monterrey; Information Security Inc.; Módulo Security. (2005). Módulos del 1 al 8. *Academia Latinoamericana de Seguridad Informática*.

Ministerio de Hacienda y Administraciones Públicas. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid, España. Recuperado el 17 de 09 de 2015, de

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ormella Meyer, C. (Marzo de 2014). *Normas ISO de Seguridad de la Información*. Obtenido de http://www.criptored.upm.es/guiateoria/gt_m327a.htm

Pallas, G. (Diciembre de 2009). Metodología de Implantación de un SGSI. Montevideo, Uruguay.

Portantier, F. (2012). Seguridad Informática. *Primera*. Buenos Aires, Argentina: Fox Andina.

Rosales, G. (2002). *Estrategias para la seguridad de la información* (Primera ed.). La Paz, Bolivia: Yanapti.

Sotelo, M., Torres, J., & Rivera, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. *COMTEL 2012 - IV Congreso Internacional de Computación y Telecomunicaciones*. Lima, Perú.

Talavera, V. R. (Mayo de 2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. Lima, Perú.

APÉNDICES

INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

ENCUESTA APLICADA A LOS DOCENTES Y/O ADMINISTRATIVOS DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO SOBRE SEGURIDAD DE LA INFORMACIÓN

Objetivos:

- Evaluar la existencia de vulnerabilidades en el tratamiento y soporte de la información del Departamento de Admisión y Registro Académico (DARA) de la UPAGU
- Conocer las medidas con que cuentan los docentes y/o administrativos para el resguardo de la Información.
- Conocer si docentes y/o administrativos utilizan de manera correcta las TIC's y de qué manera ayudarían a salvaguardar la información.

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.

Tenga en cuenta que la información que brinde usted servirá para evaluar la seguridad de la información y proponer estrategias para mejorarla.

---

1. Sexo: Masculino ( ) Femenino ( )
2. Cargo dentro de la UPAGU:

   .....
3. Unidad de la UPAGU a la que pertenece:

   .....

   .....
4. ¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la UPAGU?

   SI ( ) NO ( )
5. ¿Si en el transcurso del uso de su equipo informático, se detecta 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 ( )

6. ¿Hace usted uso de los antivirus en los equipos informáticos de la UPAGU cuando ingresa o saca información en algún dispositivo de almacenamiento?

   Si ( ) A veces ( ) Nunca ( )

7. ¿Usted ha detectado que el antivirus de la UPAGU funciona adecuadamente y que se encuentra actualizado?

   SI ( ) NO ( )

8. ¿Qué hace cuando detecta un virus en la computadora de la UPAGU?
   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 qué no sé) ( )
   f. Comunica al personal de soporte de informática ( )
   g. Otros, Especificar**……** ( )
9. En alguna ocasión recibió ayuda de algún alumno o de algún asignado de ocupación temporal (bolsa de trabajo u otro), en alguna de las siguientes actividades dentro de la universidad:
   a. Llenando o elaborando algún documento de la universidad ( )
   b. Pasando información en Word, Excel, Power Point, etc. ( )
   c. Ingresando al correo de la UPAGU y enviando mensajes a través de él ( )
   d. Clasificando documentos de la universidad ( )
   e. Otros, especificar**……** ( )
   f. Ninguno. ( )
10. ¿Puede identificar a las personas que no trabajan y no estudian en la UPAGU?

    SI ( ) NO ( )

    Si tu respuesta es **Si,** fue por medio de:
    a. Identificación personal del individuo ( )
    b. Indumentaria ( )
    c. Fotocheck de visitante (entregado por la UPAGU) ( )
    d. Otros, Especificar…… ( )
    e. Ninguno ( )
11. ¿Ha observado que algún alumno o compañero de trabajo de la UPAGU ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en la computadora?

    SI ( ) NO ( )

12. Cuándo usted se ausenta temporalmente de su área de trabajo, ¿qué acciones realiza con respecto a su equipo?
    a. Apaga el equipo ( )
    b. Bloquea el equipo ( )
    c. Ha configurado bloqueo del equipo luego del protector de pantalla ( )
    d. Apaga el monitor ( )
    e. Otros, especificar…… ( )
    f. Ninguno ( )
13. ¿Percibe seguridad en los ambientes donde se encuentran los equipos informáticos dentro de la universidad frente a cualquier desastre natural o humano?
    SI ( ) NO ( )
14. ¿Ha observado algún extinguidor cerca de los equipos informáticos?
    SI ( ) NO ( )
15. ¿Sabe utilizar de forma adecuada un extintor?
    SI ( ) NO ( )

    Si la respuesta es **Si;** 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 ( )
16. ¿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:

    ……

    ……
17. ¿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 ( )
18. ¿Ha percibido, si el cable de red de su computador es de fácil de acceso para desconectarlo y utilizarlo en otros equipos?
    SI ( ) NO ( )

19. ¿Tu clave de acceso es la misma para todos los servicios que te brinda la Intranet de la UPAGU?

    SI ( ) NO ( )

20. Normalmente tu clave hace referencia a:

    a. Su nombre y apellido ( )
    b. Su fecha de nacimiento ( )
    c. Teléfono (de casa o móvil) ( )
    d. Nombre de su esposo(a) o hijo(a) ( )
    e. No comparte con nadie su clave ( )

21. Y si nunca cambio su clave, ¿porque motivo no lo hizo?

    ……

22. La Clave con la cual ingresa a la Intranet de la UPAGU es conocida también por:

    a. Un compañero de trabajo ( )
    b. Mi esposo(a) o hijo(a) ( )
    c. Algún alumno ( )
    d. Otros, Especifica**……** ( )

23. ¿Cada que tiempo cambia su clave de la Intranet de la UPAGU?

    Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

24. ¿Usted recibió alguna capacitación acerca de Seguridad de la Información en la UPAGU?

    SI ( ) NO ( )

25. ¿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 de la Intranet de la UPAGU ( )
    d. Como parte de algún curso en tu carrera ( )
    e. Otros, Especifique: **……** ( )

26. ¿Ha sufrido algún problema que tenga que ver con la alteración de su información en la Intranet de la UPAGU

    SI ( ) NO ( )

27. Usted ha realizado alguna de las siguientes actividades en su computador personal (PC):
    a. Instalando algún software que necesitaba ( )
    b. Haciendo limpieza de su PC (teclado, mouse, cpu, etc.) ( )
    c. Desarmando el CPU por algún sonido o falla ( )
    d. Otros, Especifique.....( )
    e. Ninguna ( )

28. ¿Qué hace usted cuando uno de sus componentes o aplicativos no funcionan correctamente en su PC?
    a. Intenta arreglarlo ( )
    b. Lo arregla mi compañero de trabajo más cercano ( )
    c. Llamo a un técnico del área de soporte de informática ( )
    d. No sé qué hacer en ese momento ( )

29. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

    A veces ( ) Casi Siempre ( ) Nunca ( )

30. Cada vez que sufre algún inconveniente con la PC o aplicación la cual desea trabajar, porque medio informa o reporta el inconveniente:
    a. Teléfono (anexo) ( )
    b. Correo electrónico al área de cómputo ( )
    c. Voy físicamente a buscar algún encargado de cómputo ( )
    d. Espero que pasen por mi área de trabajo ( )
    e. Otros, Especifique..... ( )
    f. Ninguna ( )

Gracias por su colaboración

ENCUESTA APLICADA A LOS ALUMNOS DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO SOBRE SEGURIDAD DE LA INFORMACIÓN

Objetivos:

- Evaluar la existencia de vulnerabilidades en el tratamiento y soporte de la información del Departamento de Admisión y Registro Académico (DARA) de la UPAGU
- Conocer las medidas con que cuentan los alumnos para el resguardo de la Información.
- Conocer si alumnos utilizan de manera correcta las TIC's y de qué manera ayudarían a salvaguardar la información.

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.

Tenga en cuenta que la información que brinde usted servirá para evaluar la seguridad de la información y proponer estrategias para mejorarla.

---

1. Sexo: Masculino ( ) Femenino ( )
2. Carrera Profesional:

   .....
3. ¿Hace usted uso de los antivirus en sus equipos de cómputo, cuando ingresa o saca información en algún dispositivo de almacenamiento?

   Si ( ) A veces ( ) Nunca ( )
4. Ha colaborado o conoce de algún alumno que colabora con algún docente o administrativo, en alguna de las siguientes actividades dentro de la universidad:
   a. Llenando o elaborando algún documento de la universidad ( )
   b. Pasando información en Word, Excel, Power Point, etc. ( )
   c. Ingresando al correo de la UPAGU ( )
   d. Clasificando documentos de la universidad ( )
   e. Otros, especificar..... ( )
   f. Ninguno. ( )
5. ¿Es sencillo para usted como alumno acceder a algún equipo de cómputo de la UPAGU?

   SI ( ) NO ( )

6. ¿Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU de algún equipo de la UPAGU?

   SI ( ) NO ( )

7. ¿Ha percibido, si el cable de red de cualquier computador de la UPAGU es de fácil de acceso para desconectarlo y utilizarlo en otros equipos?

   SI ( ) NO ( )

8. ¿Tu clave de acceso es la misma para todos los servicios que te brinda la Intranet de la UPAGU?

   SI ( ) NO ( )

9. Normalmente tu clave hace referencia a:

   a. Su nombre y apellido ( )
   b. Su fecha de nacimiento ( )
   c. Teléfono (de casa o móvil) ( )
   d. Nombre de su esposo(a) o hijo(a) ( )
   e. No comparte con nadie su clave ( )

10. Y si nunca cambio su clave, ¿porque motivo no lo hizo?

    ……

11. La Clave con la cual ingresa a la Intranet de la UPAGU es conocida también por:

    e. Un compañero de la UPAGU ( )
    f. Algún familiar ( )
    g. Algún trabajador de la UPAGU ( )
    h. Otros, Especifica**……** ( )

12. ¿Cada que tiempo cambia su clave de la Intranet de la UPAGU?

    Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

13. ¿Qué tan veloz es el acceso a la Intranet dentro o fuera de la UPAGU?

    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 ( )

14. ¿Utiliza el servicio de correo electrónico que se le asigna en la UPAGU?

    SI ( ) NO ( )

Si su respuesta es **Si**; ¿Con qué frecuencia recibe correos no deseados o spam?

a. De 1 a 10 correos al día ( )
b. De 10 a 20 correos al día ( )
c. De 20 a más correos al día ( )

15. ¿Usted recibió alguna capacitación acerca de Seguridad de la Información en la UPAGU?

    SI ( ) NO ( )

16. ¿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 de la Intranet de la UPAGU ( )
i. Como parte de algún curso en tu carrera ( )
j. Otros, Especifique: **……** ( )

17. ¿Ha sufrido algún problema que tenga que ver con la alteración de su información en la Intranet de la UPAGU

    SI ( ) NO ( )

18. ¿Conoce de algún caso en que la información personal o académica de un alumno ha sido utilizada sin su consentimiento?

    SI ( ) NO ( )

19. ¿Conoce de algún caso en que algún alumno o alumnos hayan accedido a través de la Intranet a la información de otros alumnos sin su consentimiento?

    SI ( ) NO ( )

Gracias por su colaboración

ENTREVISTA AL PERSONAL DE SEGURIDAD Y LOGÍSTICA DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO SOBRE SEGURIDAD DE LA INFORMACIÓN

Objetivos:

- Evaluar la existencia de vulnerabilidades en el tratamiento y soporte de la información del Departamento de Admisión y Registro Académico (DARA) de la UPAGU
- Conocer las medidas con que cuentan el personal de seguridad y logística para el resguardo de la Información.

---

1. Sexo: Masculino ( ) Femenino ( )
2. Cargo dentro de la UPAGU:

   .....
3. Unidad de la UPAGU a la que pertenece:

   .....
4. Cantidad de personal de seguridad dentro de la Institución: .....
5. Cantidad de personal de mantenimiento dentro de la Institución: .....
6. ¿Existe un manual de manejo de incidencias que es adoptada por todo el personal?

   Si ( ) NO ( )

   Si es NO, que acciones realiza cuando detecta alguna incidencia de un problema:

   a. Comunica al jefe inmediato para que le dé indicaciones ( )
   b. Realiza acciones que a su parecer son las indicadas. ( )
   c. Con sus compañeros toman una decisión conjunta. ( )
   d. Espera que le indiquen que hacer. ( )

7. ¿Sabe si existen extintores en los ambientes de la Universidad, conoce la ubicación exacta de éstos?

   SI ( ) NO ( )
8. ¿Sabe utilizar de forma adecuada un extintor?

   SI ( ) NO ( )
9. ¿Existen cámaras de vigilancia?

   SI ( ) NO ( )

10. ¿El responsable comunica inmediatamente cuando detecta un problema con las cámaras?

SI ( ) NO ( )

11. ¿Las llaves de los ambientes de la UPAGU, son centralizadas en alguna unidad?

SI ( ) NO ( )

Si respondió SI, cree que el lugar donde se ubican cuenta con medidas de seguridad para proteger estas llaves

SI ( ) NO ( )

12. ¿Puede identificar a las personas que no trabajan y no estudian en la UPAGU?

SI ( ) NO ( )

Si tu respuesta es **Si,** fue por medio de:

a. Identificación personal del individuo ( )
b. Indumentaria ( )
c. Fotocheck de visitante (entregado por la UPAGU) ( )
d. Otros, Especificar..... ( )
e. Ninguno ( )

13. ¿Percibe seguridad en los ambientes donde se encuentran los equipos informáticos y el Departamento de Admisión y Registro Académico frente a cualquier desastre natural o humano?

SI ( ) NO ( )

14. ¿Ha participado de algún simulacro frente a cualquier desastre natural o humano?

SI ( ) NO ( )

Si tu respuesta es **No;** Como nos sugieres que se realice y cada que tiempo:

.....

.....

15. ¿Se realiza algún tipo de inspección con el ingreso y salida de equipos de cómputo por parte de personal, alumnado o personas extrañas a la institución?

SI ( ) NO ( )

16. ¿Se realiza alguna medida cuando observa que alguna persona extraña ingresa a algún ambiente de la UPAGU, cuando no se encuentra el personal responsable?
    a. Comunica a su supervisor ( )
    b. No permite el ingreso de la persona ( )
    c. No realiza ninguna medida ( )
    d. Observa y luego comunica si detecta alguna actividad sospechosa ( )

17. ¿Se realiza alguna medida cuando observa que alguna persona extraña se encuentra manipulando los equipos de cómputo de alguna oficina, así sea que se encuentre el personal responsable?
    a. Comunica a su supervisor ( )
    b. No permite el ingreso de la persona ( )
    c. No realiza ninguna medida ( )
    d. Observa y luego comunica si detecta alguna actividad sospechosa ( )

18. ¿Cuál cree Ud., que es la unidad donde se encuentra la información más importante de la Universidad? ……

19. Según su parecer ¿cuál cree Ud., que es el activo más importante que se debe proteger en nuestra institución? ……

20. ¿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 de la Intranet de la UPAGU ( )
    d. Como parte de algún curso en tu carrera ( )
    e. Otros, Especifique: **……** ( )

Gracias por su colaboración

ANEXOS

Tabla Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	TÉCNICA DE RECOJO DE INFORMACIÓN
¿Cuáles son las condiciones de seguridad de la información y qué propuesta se puede formular para el Departamento de Admisión y Registro Académico de la Universidad Privada Antonio Guillermo Urrelo - 2016?	**Objetivo General** Diagnosticar las condiciones de seguridad de la información y formular una propuesta para el Departamento de Admisión y Registro Académico de la Universidad Privada Antonio Guillermo Urrelo. **Objetivos específicos** a) Identificar los procesos core del Departamento de Admisión y Registro Académico de la UPAGU. b) Identificar y evaluar los activos de información ligados a los procesos encontrados. c) Identificar los riesgos y valorarlos. d) Proponer un Sistema de Gestión de Seguridad de la Información para el DARA.	La información, las personas que hacen uso de ella y los equipos e infraestructura que la soportan son elementos que se encuentran con riesgos de seguridad y que deben necesitar de la formulación de un Sistema de Seguridad de la Información para el Departamento de Admisión y Registro Académico de la UPAGU	– Análisis de riesgo – Propuesta de un Sistema de Seguridad de Información	– Amenazas – Vulnerabilidades – Políticas de uso y manejo de la información. – Políticas de seguridad del personal. – Políticas de seguridad física y ambiental, de seguridad y administración de operaciones de cómputo y de controles de acceso lógico y uso de software.	Unidad de análisis: Es el Departamento de Admisión y Registro Académico de la UPAGU. La investigación de tipo descriptivo – de carácter propositivo, Es aplicada, microsociológica y transversal Diseño de la Investigación: investigación no experimental La metodología se centra en la norma ISO/IEC 27000. El procedimiento: – Identificar los procesos “core” de negocio, – Realizar la identificación de los activos de información del DARA. – Realizar un análisis de riesgo de los activos encontrados – Definir los controles, valorando los riesgos – Definir las políticas de seguridad La población elegida para el presente estudio: Estudiantes, Docentes, Administrativos, Personal de seguridad y mantenimiento y Directivos