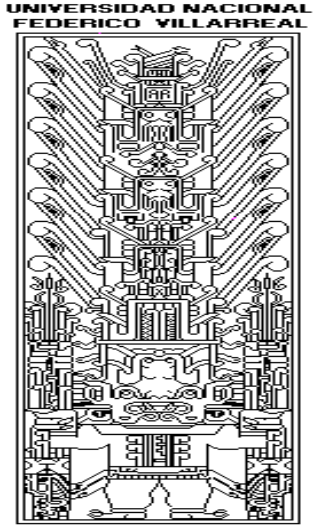
# UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

# ESCUELA UNIVERSITARIA DE POSGRADO




TESIS

**“MODELO SISTÉMICO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA GESTIÓN DE PROCESOS DE NEGOCIO PARA LA COMPETITIVIDAD FUNCIONAL DE LAS UNIVERSIDADES”.**

PRESENTADO POR:

RAYME SERRANO, RUBÉN ALEJANDRO

PARA OPTAR EL GRADO ACADEMICO DE:

DOCTOR EN INGENIERÍA DE SISTEMAS

LIMA – PERÚ

2018

## Dedicatoria

A mi madre y a mi padre que desde el cielo iluminan mi camino.
A mi esposa Patricia, por su compañía y su dedicación constante.
A mi hija Alexandra, por ser la alegría y la razón de mi vida.

## Agradecimientos

A mi asesor de tesis Dr. Ciro Rodríguez Rodríguez, por los conocimientos adquiridos, por su valioso apoyo y por su cooperación, que me permitieron concluir exitosamente la presente tesis doctoral.

A los Señores Doctores Javier Gamboa Cruzado, Jorge Mayhuasca Guerra y Elías Valverde Torres por haber dedicado su tiempo en la revisión del presente trabajo y sus valiosos aportes.

A todos mis colegas y amigos que han colaborado en la elaboración de la presente tesis doctoral.

Por último y de forma especial a mi esposa Patricia, por su comprensión y apoyo incondicional en los proyectos que realizo y en particular en este trabajo de tesis.

# ÍNDICE

**LISTA DE FIGURAS**

**LISTA DE TABLAS**

## RESUMEN

La seguridad de la información particularmente en las universidades es improvisada y son pocas las que se involucran con profundidad en el proceso investigativo de este nuevo horizonte. Pocas poseen un departamento o equipo formal que se encargue específicamente de la seguridad de la información, esto se refleja por la situación de bajo nivel de competitividad funcional.

Las universidades todavía adolecen de fallas para tratar adecuadamente asuntos de seguridad de la información, y se deben en gran medida a su incapacidad para definir seguridad y presentarla de manera que sea comprensible e importante para toda la comunidad universitaria.

Esta investigación propone la implementación de un modelo sistémico de seguridad de la información basado en la gestión de procesos de negocio. Para ello es necesario la automatización de los procesos a través de los sistemas BPM (Business Process Management) con el propósito de conseguir grupos de interés involucrados que sean proactivos y no reactivos, y con estos mecanismos en todo momento se pueda garantizar en las universidades la seguridad de la información. La aplicación también resulta válida para todo tipo de organización.

Se define el diseño de la investigación de tipo experimental y se realizan las pruebas de simulación tanto para el grupo de control como para el grupo experimental.

Finalmente se evalúan los resultados en base a los indicadores de gestión: tiempo medio de respuesta ante los incidentes de seguridad, porcentaje de acierto para resolver los incidentes de seguridad y grado de uso del recurso humano para resolver los incidentes de seguridad.



**Palabras clave**

Modelo sistémico, seguridad de la información, gestión de procesos de negocio, competitividad funcional, universidades, simulación, grupo de control, grupo experimental, indicadores.

## ABSTRACT

The information security particularly in universities is improvised and there are few which are deeply engaged in the research process of this new horizon. Few have a department or formal staff that is specifically responsible for the security of information, this is reflected, due to the situation of low level of functional competitiveness.

Universities still suffer from failure to adequately address issues of information security, and it is largely due to their inability to define security and present it in a way that is understandable and important to the entire university community.

This research proposes the implementation of a systemic model of information security based on business process management. This requires the automation of processes through (Business Process Management) BPM systems with the purpose of getting stakeholders involved to be proactive and not reactive, and these mechanisms at all times will ensure information security in universities. The application is also valid for all types of organization.

The research design is defined as experimental and the simulation tests are made for both the control group and the experimental ones.

Finally the results are evaluated based on management indicators: average response time to security incidents, success rate to solve security incidents and degree of human resources usage to solve security incidents.



**Keywords**

Systemic model, Information security, business process management, functional competitiveness, universities, simulation, control group, experimental group, indicators.

## RESUMO

A segurança da informação particularmente nas universidades é improvisada e são poucas que se involucram com profundidade no processo investigativo de isto novo horizonte, poucas possuem um apartamento ou equipe formal que se encargue especificamente da segurança da informação, isto se reflexa pela situação de baixo nível de competitividade funcional.

As universidades ainda estão doendo de erros para tentar adequadamente assuntos da segurança da informação, e se devem na grande medida a sua capacidade para definir segurança e apresentá-la de um jeito que seja compreensível e relevante para todas as partes interessadas.

O presente trabalho da investigação propõe a implementação de um modelo sistêmico de segurança da informação sustentado na gestão dos processos de negócio. Para isso é preciso a automatização dos processos a traves dos sistemas BPM (Business Process Management) com o propósito de conseguir grupos de interesse envolvidos que sejam proativos e não reativos, e com isto mecanismos em todo momento se possa garantir nas universidades a segurança da informação. O aplicativo também resulta válido para todo o tipo de organização.

Define-se o desenho da investigação de tipo experimental e realizam-se as provas de simulação tanto para o grupo de controle como para o grupo experimental.

Finalmente avaliam-se os resultados em base aos indicadores de gestão: tempo médio de resposta a incidentes de segurança, porcentagem de sucesso para resolver incidentes de segurança e grau de uso de recursos humanos para resolver incidentes de segurança.



**Palavras-chave**

Modelo sistêmico de segurança da informação, Segurança da informação, gestão de processos de negócio, competitividade funcional, universidades, simulação, grupo de controle, grupo experimental, indicadores.

# INTRODUCCIÓN

La complejidad de las organizaciones ha crecido mucho, debido en gran parte a la expansión a nuevos mercados y por consiguiente la aparición de nuevos marcos regulatorios que originan un aumento de la complejidad en el tratamiento y seguridad de la información.

Muchas organizaciones creen que tienen un sistema de seguridad de información que funciona con eficiencia y eficacia, y presumen de que poseen una enorme gama de controles para proteger la seguridad de la información, pero simplemente en el tiempo han ido diseñando controles, conforme han ido apareciendo los incidentes de seguridad. Esta complejidad creciente exige que deben adoptar estrategias integrales y eficaces que sean capaces de alcanzar y mantener niveles de competitividad funcional compatible con lo que exige el mercado global.

Las universidades todavía muestran poco interés acerca de la cultura de la seguridad de la información y no poseen un mayor nivel de aprendizaje organizacional con respecto a la seguridad de la información.

En las universidades a medida que los sistemas de información apoyan cada vez más los procesos críticos, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Por esta razón se tomó como objetivo de esta tesis, implementar un Modelo Sistémico de Seguridad de la Información basado en BPM que sea un avance hacia un mayor nivel de madurez en la gestión de la seguridad de la información de las universidades.

El desarrollo del presente trabajo, para su mejor comprensión se ha dividido en cinco capítulos los mismos que los describimos a continuación:

El primer capítulo se describe el problema, sus antecedentes, los objetivos, las hipótesis, la justificación, las hipótesis de la investigación, el tipo y diseño de la investigación, la población y muestra y los instrumentos de recolección de datos.

El segundo capítulo, está referido a un conjunto de temas y herramientas relacionadas con la temática abordada por el trabajo de investigación. Entre los puntos más relevantes de este aspecto se tienen la seguridad de la información, sistema de gestión de seguridad de la información, gestión de riesgos, gestión de incidentes de seguridad, procesos de negocio, el pensamiento sistémico y los aspectos generales de una universidad.

El tercer capítulo está referido al diseño e implementación del Modelo Sistémico de Seguridad de la Información para una universidad. Los procesos deben automatizarse para un mejor control la información y a través de reglas de negocio estén evaluando los valores de los mismos contra la métrica establecida en tiempo real. La implementación del Modelo Sistémico de Seguridad de la Información enfocado en procesos, toma como base fundamental la gestión de políticas de seguridad de la información, el proceso de inventario y clasificación de activos de información, gestión del riesgo y la gestión de incidentes de seguridad.

En el cuarto capítulo se presenta el análisis de resultados y contrastación de hipótesis.
En el procesamiento y análisis se ha tomado como proceso crítico la gestión de incidentes de seguridad de la información para lo cual se ha simulado el comportamiento de dicho proceso, tanto antes de la utilización del Modelo Sistémico de Seguridad de la Información como después, para este propósito se utiliza el simulador de una herramienta de BPM llamada bizagi. En la contrastación de hipótesis se tiene como objetivo demostrar que la realidad estudiada respalda a la hipótesis formulada.

En el último capítulo mostramos las conclusiones donde se extraen los principales hallazgos de la investigación realizada poniendo énfasis en los resultados tangibles de la prueba de hipótesis. En este caso particular, se concluye que la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM contribuye a mejorar la competitividad funcional de las universidades. Por último, las recomendaciones orientadas al aseguramiento del éxito en la aplicación de este modelo como una contribución a la competitividad funcional basada en la gestión de procesos de negocio, pero con un enfoque sistémico.

# CAPÍTULO I
# PLANTEAMIENTO METODOLÓGICO

## 1.1. ANTECEDENTES

Para el desarrollo de la presente investigación se consultó, con la siguiente bibliografía:
La tesis de Posgrado titulada: **"Metodología de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) en un grupo empresarial jerárquico"**, cuyo autor es Gustavo Pallas Mega (2009) por la Universidad de la República, Uruguay. Este trabajo de investigación se enfoca en la necesidad de gestionar la seguridad de una manera conveniente como es el sistema de gestión de seguridad de la información, para mejorar el uso eficaz y eficiente de los recursos tecnológicos como soporte de los procesos de negocios. Se analizan diferentes enfoques de estándares de gestión de seguridad de la información, con el objetivo de plantear un método de implementación y mejora de un SGSI en una empresa subordinada que forma parte de un grupo empresarial jerárquico. También resalta la importancia de promover un enfoque sistémico en favor de una metodología sustentable, buscando revalorizar los servicios, los activos y riesgos que tengan un impacto en la empresa.

También existe publicada la tesis doctoral cuyo título es: **"MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización)"**, cuyo autor es Elena Ruiz Larrocha (2010), perteneciente a la Universidad Nacional de Educación a Distancia, España. Este trabajo tiene como propósito fundamental presentar un nuevo método original para mejorar la usabilidad de la metodología ITIL, adoptar y mejorar la seguridad en sus procesos.
Se plantea enfocar el concepto de seguridad dentro de la "tecnología" ITIL, y a la vez se ahonda con detalle la relación de apoyo mutuo entre la seguridad y la gestión de los servicios, de tal manera que la gestión e implantación de estas dos disciplinas, refuerza la gestión de la seguridad de la información como uno de los servicios gestionados en este marco de trabajo, pues ITIL como tal no lo tiene.

La tesis doctoral titulada**: "Marco para el Gobierno de la Seguridad en Servicios de Cloud Computing"**, cuyo autor es Oscar Rebollo Martínez (2014), por la Universidad de Castilla-La Mancha, España, quien plantea un marco de gobierno de seguridad que tenga en consideración las particularidades de los servicios de Cloud Computing. Este marco está alineado con los actuales estándares de seguridad y mejores prácticas en la materia, ello quiere decir que sus actividades y tareas han sido diseñadas para ser consistentes con ellos y perseguir un objetivo común. La perspectiva de esta propuesta se encuentra orientada a procesos y ha sido modelada empleando la especificación SPEM 2.0 (Software & Systems Process Engineering Meta-Model), de forma que se pueda facilitar su implementación en cualquier organización. Esta tesis sugiere un conjunto de herramientas de apoyo, las cuales pueden emplearse para facilitar el desarrollo de los procesos de gobierno. Por último, para validar la utilidad práctica y mejorar su desarrollo, se proporcionan los resultados de la evaluación empírica que se ha llevado a cabo en una organización real.

La tesis de Posgrado titulada: **"Modelo de madurez para la gestión y administración de la seguridad informática en las universidades."**, cuyo autor es Marianella Villegas (2008), por la Universidad Simón Bolívar, Venezuela. El objetivo de esta investigación fue de construir un modelo de madurez organizacional para la gestión y administración y de la seguridad de la información en las universidades venezolanas de la Región Capital. Para ello se realizó un trabajo de campo para validar el modelo de madurez organizacional en que se encuentra la seguridad de la información en las universidades, y se elaboró un cuestionario de preguntas con entrevistas a personal experto, consultores de seguridad de la información y algunas autoridades con experticia en el área. Este trabajo de investigación permitirá comprender y estructurar el problema de inseguridad en las universidades, lo cual posibilitará en este proceso, plantear estrategias para mejorar el nivel de aprendizaje en el marco de seguridad de la información.

Por otro lado, hay un artículo científico denominado **"Modelo sistémico de la seguridad de la información en las Universidades",** cuyos autores son Orlando Viloria y Walter Blanco (2009), por la Universidad Central de Venezuela, Venezuela. Los autores proponen un modelo gerencial de la seguridad de la información en las Universidades, que es un marco referencial

que apoyará a los gerentes a elaborar planes estratégicos para abordar el problema de la inseguridad de la información en las Universidades.

El componente tecnología cambia por las tecnologías de la información (TI), la gente y la cultura, la estructura organizacional, así como los procesos y las tareas están descritos bajo un enfoque de la seguridad de la información. El modelo propuesto incorpora un quinto elemento, las disciplinas de las organizaciones inteligentes como factores críticos de éxito y elementos de orden en el caos generado por la adopción de las tecnologías de la información. La solución al problema de inseguridad de la información no es fácil de afrontar, requiere de mucha experticia técnica y gerencial. Las universidades no están exentas a este problema a pesar de la calidad de los profesionales que laboran en estas organizaciones, pues éstas son sistemas muy complejos con una diversidad de problemas que mantienen permanentemente un alto grado de entropía.

Por último, la tesis de Maestría titulada **"Gestión de Seguridad de la Información y los Servicios Críticos de las Universidades. Un estudio de tres casos en Lima Metropolitana"**, cuyo autor es Rubén Rayme Serrano (2007), por la Universidad Nacional Mayor de San Marcos, Perú. El autor realiza un análisis de tres universidades donde se obtiene información de los especialistas en seguridad de la información y se analizan aspectos críticos como: el uso de políticas de seguridad, la protección a los equipos de cómputo, las incidencias de seguridad, la capacitación o talleres de seguridad, el rediseño de las redes informáticas universitarias y los riesgos más frecuentes a los recursos de información. Luego se hace una propuesta de un plan de seguridad de la información para las universidades con un programa de implementación donde se establecen metas por las actividades que se van a realizar.
Como resultado de este análisis se formulan estrategias de seguridad para contribuir con la gestión de seguridad de la información en las instituciones educativas.

## 1.2. PLANTEAMIENTO DEL PROBLEMA

La descripción de la realidad problemática tiene dos elementos fundamentales sobre la cual gira el presente trabajo: por un lado, existen pocos modelos seguridad de la información que

permiten integrar en forma sistémica las relaciones complejas dentro de la organización, y por ende gestionar la seguridad más efectivamente. Por otro lado, vinculado con el primer elemento, se caracteriza el nivel de competitividad de las universidades de nuestro medio.

Muchos de los modelos de seguridad de seguridad de la información sólo toman en cuenta los controles y aspectos técnicos y no se basan en un enfoque por procesos, por ello es que muchas organizaciones llegan al alineamiento de la estrategia, pero en la fase de definición, gestión y control manual, lo cual lo hace mucho más complejo, costoso y menos fiable.

A medida que las empresas se apoyan cada vez más en las redes digitales para obtener ingresos y realizan operaciones, necesitan emprender pasos adicionales para asegurar que sus sistemas y aplicaciones estén siempre disponibles. El concepto de seguridad de la información siempre ha estado en las organizaciones desde hace mucho tiempo, sólo que disociado y especializado en los profesionales de tecnología y en otras áreas de negocio en el tema de los procesos organizacionales.

Existen modelos de seguridad de la información guiados desde un punto de vista meramente operativo con documentación voluminosa en sus políticas de seguridad, gran cantidad de formatos de información para la gestión de activos y gestión de riesgos, incluyendo sus metodologías particulares, pero al final estos modelos no protegen los activos de información de acuerdo a lo requerido por los procesos. Así, de nada sirve también que tengan estadísticas de incidentes de seguridad, si al final no se hace nada con esa información y no se implementan medidas para que estos incidentes no se vuelvan a presentar. Además, hay empresas que gastan grandes cantidades de dinero en campañas de capacitación y sensibilización de las personas, pero los resultados son negativos porque no cambian su comportamiento con respecto a la seguridad.

La situación de la seguridad de la información particularmente en las universidades es improvisada, son pocas las que se involucran con profundidad en el proceso investigativo de este nuevo horizonte y muy pocas son las que poseen un departamento o equipo formal que

se encargue específicamente de la seguridad de la información, esto se refleja por la situación de bajo nivel de competitividad funcional.

A continuación, se destacan los factores más importantes que contribuyen a crear un clima de inseguridad de la información en las universidades:

- Los planes de seguridad de la información no están alineados con las estrategias de negocio de la organización. Se evidencia en la falta de promoción y apoyo por la alta dirección. Las instituciones, a través de los departamentos de tecnología de la información (TI) y ante la necesidad, se enfocan erróneamente a buscar únicamente la protección de ataques externos o de reducir fugas internas de información, pero el problema de la inseguridad de la información es un problema de todos, no sólo de un departamento.

- Se hace difícil gestionar el riesgo en las universidades cuyos procesos dependen de la disponibilidad de las tecnologías de la información. Internet se ha convertido en una pieza fundamental de las operaciones de negocio aún más, cuando la seguridad de esos procesos es igualmente crítica para la funcionalidad del negocio y donde un fallo crítico puede suponer, en el mejor de los casos, una pérdida de la continuidad del negocio.

- Las universidades no aplican medidas de seguridad consistentes para almacenar y proteger la información, y esto se ve reflejado en las diferentes áreas académicas y oficinas administrativas. En las universidades los procesos manejan información crítica como la concerniente a matrícula de estudiantes, registro de calificaciones, planilla de personal y presupuestos entre otras, que es confidencial, pero está propensa a amenazas de alteración, divulgación no autorizada y sustracción de la información.
- Los intrusos lanzan ataques por denegación de servicios, ocasionan que en los sitios web de la universidad se altere el funcionamiento de los servicios académicos y administrativos. Estos ataques ocasionan costos muy grandes a la universidad porque

mientras el sitio web está fuera de línea, los estudiantes, docentes, egresados e investigadores no pueden realizar ninguna operación.

- La vulnerabilidad también se ha incrementado con el uso generalizado del correo electrónico, la mensajería instantánea y los programas de compartición de archivos. El correo electrónico podría contener archivos adjuntos que pueden contener software malicioso. Los empleados utilizan mensajes de correo electrónico para transmitir secretos comerciales valiosos, datos financieros o información confidencial de clientes a destinatarios no autorizados.

- Los ataques a la red no sólo provienen del exterior sino también del interior de la organización. Según Campbell y McCarthy (2002):

  > la mayoría de las estadísticas de seguridad computacional señalan que más del 80% de los ataques tecnológicos que fomentan la inseguridad de la información digital tienen su raíz en un proceder humano ya sea por error o en forma deliberada; éste a su vez se enmarca dentro de la gran crisis moral moderna de nuestra sociedad.

- La falta de entrenamiento al personal en temas de seguridad de la información en las universidades. Son muy pocas las universidades que apuestan por la educación y entrenamiento a los empleados sobre la conciencia de la seguridad de la información.

- El enfoque que se le da a la seguridad de la información es predominantemente técnico. Por ello, Ribagorda (2004) señala que la seguridad es un problema de gestión más que de tecnología, tal es el caso de que los administradores de las redes se encargan únicamente de realizar funciones propias de su área, sin ver lo que sucede dentro del contexto general de la organización pues mantienen una visión muy cerrada del problema de la seguridad y sus actitudes son reactivas.

Las causas mencionadas anteriormente, ocasionan un impacto en la funcionalidad de los procesos críticos de las universidades como son: imposibilidad que el personal académico y

administrativo pueda acceder a los sistemas de admisión, matrícula, historias clínicas, finanzas, presupuestos entre otros; por parte de los estudiantes no pueden acceder a las aplicaciones web para realizar servicios como matrícula en línea, consulta de calificaciones en el aula virtual, consulta de material bibliográfico, bolsa de trabajo entre otros. También traen como consecuencia el mal funcionamiento de los sistemas de información, la pérdida de información sensible, la divulgación de información confidencial por el personal, la modificación de calificaciones por parte de los mismos estudiantes entre otros.

De la realidad problemática, se ha identificado sus causas y sus efectos, de esta manera surge la necesidad de gestionar funcionalmente las universidades bajo una visión integral, apoyándose en las ventajas competitivas que puede proporcionar la seguridad de la información en el marco de un modelo que articule en forma coherente a todos los procesos.

Esta necesidad puede formularse mediante las siguientes interrogantes:

- ¿Existe relación de dependencia lógica entre la seguridad de la información y la gestión funcional de los procesos en las universidades?
- ¿La seguridad de la información puede mejorar la competitividad funcional de las universidades?
- ¿La seguridad de la información puede garantizar a los estudiantes la confianza para realizar sus transacciones académicas y administrativas en línea?
- ¿Cuál es el modelo que puede usar la seguridad de la información para que abarque los componentes como son: persona, procesos, tecnología y estructura organizacional?
- ¿El enfoque sistémico es apropiado o pertinente para mejorar la seguridad de la información en las universidades?
- ¿Esta mejora puede apoyarse con la existencia de metodologías con enfoque de modelamiento de procesos?
- ¿Es posible incorporar la gestión de procesos de negocio para disminuir la complejidad de la implementación del modelo de seguridad de la información?

En la figura 1.1 se presenta el flujograma del Proceso de Competitividad Funcional.

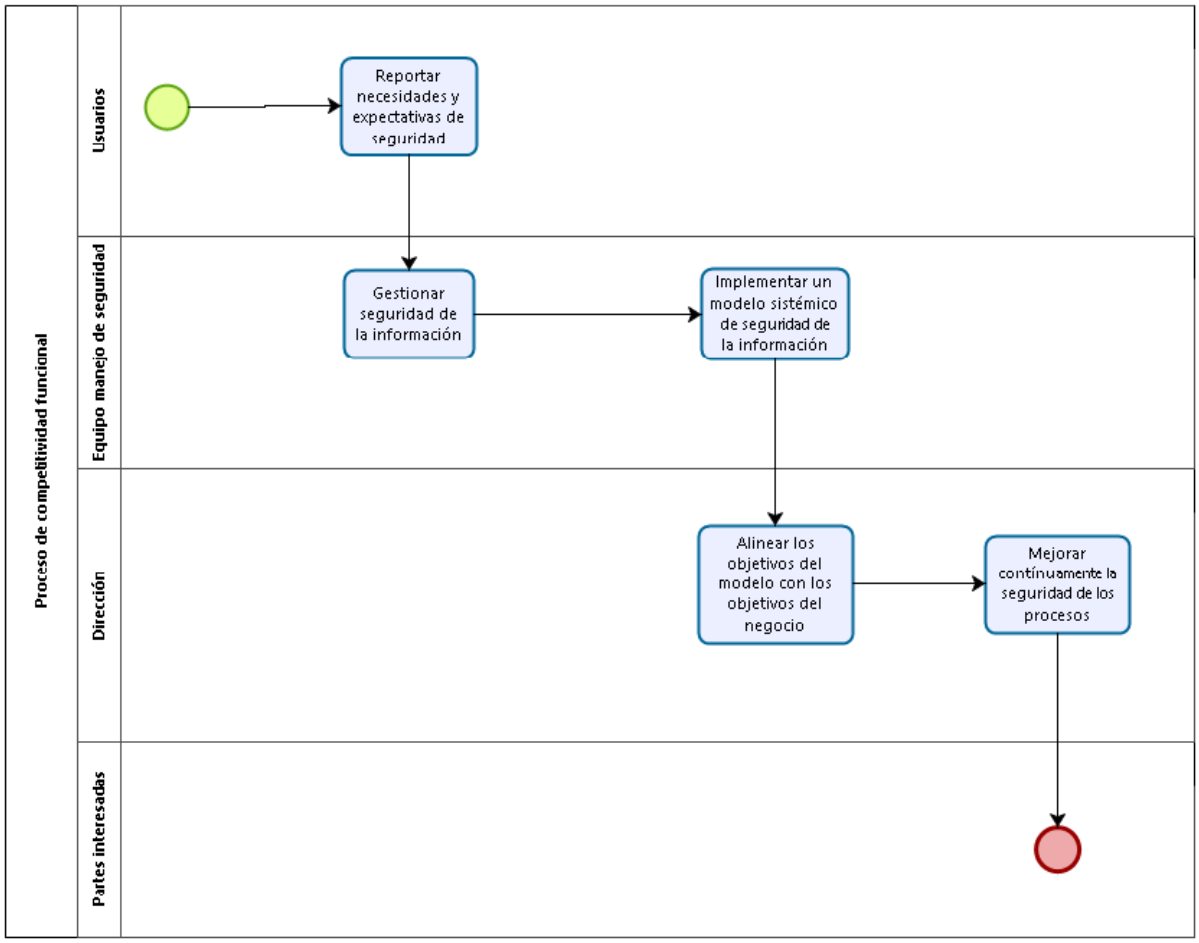



*Figura 1.1*: Proceso de Competitividad Funcional.

### 1.2.1. FORMULACIÓN DEL PROBLEMA

1. PROBLEMA PRINCIPAL

    - ¿De qué manera la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará la competitividad funcional de las universidades?

2. PROBLEMAS SECUNDARIOS

    - ¿De qué manera la puesta en práctica del Modelo Sistémico de Seguridad de la Información mejorará el tiempo medio de respuesta ante incidentes de seguridad de los procesos críticos de las universidades?

    - ¿De qué manera la puesta en práctica del Modelo Sistémico de Seguridad de la Información mejorará el porcentaje de acierto para resolver los incidentes de seguridad de los procesos críticos de las universidades?

    - ¿De qué manera la puesta en práctica del Modelo Sistémico de Seguridad de la Información mejorará el grado de uso del recurso humano para resolver los incidentes de seguridad de los procesos críticos de las universidades?

## 1.3. OBJETIVOS DE LA INVESTIGACIÓN

### 1.3.1. OBJETIVO GENERAL

Determinar el impacto que ejerce la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM en la competitividad funcional de las universidades.

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar el impacto que ejerce la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM en el tiempo medio de respuesta ante incidentes de seguridad de los procesos críticos de las universidades.

- Determinar el impacto que ejerce la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM en el porcentaje de acierto para resolver los incidentes de seguridad de los procesos críticos de las universidades.

- Determinar el impacto que ejerce la implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM en el porcentaje de uso del recurso humano para resolver los incidentes de seguridad de los procesos críticos de las universidades.

## 1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Según Hernández (1997) y de acuerdo al enfoque de este trabajo, la justificación de la investigación se da por los siguientes puntos:
El trabajo de investigación con el Modelo Sistémico de Seguridad de la Información comprende metodologías estratégicas que va permitir a las organizaciones planificar bajo una perspectiva de seguridad de la información para garantizar la gestión funcional de los procesos en cuanto a la eficiencia, la eficacia y la productividad.

La seguridad de la información es cosa de todos, y la manera de entenderlo de forma práctica en la organización, es situarla en casi todos los procesos empresariales, difundiéndola en las personas, direccionando responsabilidades e integrándola en los flujos de trabajos internos y en los sistemas de información empresariales.

Para adoptar un enfoque basado en procesos para una organización es necesario saber cuáles son los procesos que deben aparecer en la estructura de procesos del sistema, después hay

que definirlos a fin de establecer las interrelaciones entre los mismos, para ello se construye el mapa de procesos.

La seguridad de la información va permitir a los estudiantes, realizar sus trámites universitarios sin interrupciones en los servicios, a los docentes, manejar sus herramientas tecnológicas como el aula virtual con mayor confiabilidad, al personal, manejar las aplicaciones, garantizando funcionalidad de los procesos y a los responsables de los procesos un mejor control y monitoreo de los mismos.

En el presente trabajo usaremos sistemas de BPM que permite la automatización de los procesos y a través de reglas de negocio estén evaluando los valores de los mismos contra la métrica establecida en tiempo real pudiendo desencadenar de manera automática nuevos procesos, procedimientos o alarmas y ganando en fiabilidad, control, costos, eficiencia y agilidad.

Este trabajo de investigación aporta al conocimiento porque se diseñará un modelo de seguridad de la información bajo un enfoque sistémico y el impacto que tendrá en la competitividad funcional de las universidades en la eficacia, eficiencia y productividad.

Por lo expuesto, resulta conveniente, necesaria, de relevancia social, de utilidad metodológica y práctica y de conocimiento; la justificación de este trabajo de investigación que permite contribuir a garantizar la gestión funcional de los procesos en las universidades.

## 1.5. ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN

### 1.5.1. ALCANCES DE LA INVESTIGACIÓN

En el trabajo de investigación se presentan los siguientes alcances:

- El trabajo a nivel de prototipo se desarrolló en una institución en particular como es la Universidad Privada San Juan Bautista en Lima, Perú, sin embargo, de acuerdo al método y validez científica, los resultados que se obtuvieron por inferencia inductiva se reflejará en todas las universidades. Se ha seleccionado esta universidad debido a que es una del sistema universitario que carece de una sólida estructura de la gestión de seguridad de la información, también debido a que el autor de la tesis es trabajador administrativo y docente ordinario de esta casa superior de estudios, hecho que le ha permitido identificar de cerca las deficiencias señaladas.
- En la universidad el trabajo de campo se realizó con los procesos de gestión de políticas de seguridad de la información, gestión de inventario y clasificación de activos de activos, gestión de riesgos y gestión de incidentes de seguridad.
- Para la validación de los resultados se procedió a aplicar los indicadores de rendimiento al proceso de gestión de incidentes de seguridad de la información, porque es uno de los procesos más críticos dentro de la universidad, y por los casos de incidentes que se registran como: alteración de calificaciones por los mismos estudiantes, divulgación de historias clínicas, manipulación de certificados de estudios entre otros.

### 1.5.2. LIMITACIONES DE LA INVESTIGACIÓN

En el trabajo de investigación se presentan las siguientes restricciones:

- La falta de herramientas de seguridad en la universidad para poder encontrar fallas en la administración interna de la red.
- La seguridad perimetral de la universidad está tercerizada, por lo que dependemos del proveedor de seguridad cada vez que solicitemos un informe sobre los comportamientos de los intrusos que se han detectado en la red.

## 1.6. HIPÓTESIS DE LA INVESTIGACIÓN

### 1.6.1. HIPÓTESIS GENERAL

- La implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará la competitividad funcional de las universidades

### 1.6.2. HIPÓTESIS ALTERNATIVAS

- La implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el tiempo medio de respuesta ante incidentes de seguridad de los procesos críticos de las universidades.

- La implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el porcentaje de acierto para resolver los incidentes de seguridad de los procesos críticos de las universidades.

- La implementación de un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el grado de uso del recurso humano para resolver los incidentes de seguridad de los procesos críticos de las universidades.

## 1.7. OPERACIONALIZACIÓN DE LA VARIABLE

### 1.7.1. VARIABLE INDEPENDIENTE

| Variable Independiente | Indicadores | Tipo de escala |
|---|---|---|
| Modelo sistémico de seguridad de la información | • Porcentaje de cumplimiento en el plan de tratamiento del riesgo | Ordinal |
| | • Número de empleados que han completado la capacitación de seguridad del total de empleados | Ordinal |

### 1.7.2. VARIABLE DEPENDIENTE

| Variable dependiente | Indicadores | Tipo de escala |
|---|---|---|
| La competitividad funcional de las Universidades | • Tiempo medio de respuesta ante los incidentes de seguridad | • Ordinal |
| | • Porcentaje de acierto para resolver los incidentes de seguridad | • Ordinal |
| | • Grado de uso del recurso humano para resolver los incidentes de seguridad | • Ordinal |

## 1.8. TIPO DE LA INVESTIGACIÓN

En la presente investigación, se aplica el método científico complementado con el enfoque sistémico, que ligado al desarrollo de la tecnología seguirá un método comprobado de recopilación, tabulación y análisis de los antecedentes que se obtienen y prueben su validez de la hipótesis directamente en el campo en el que se presenta el hecho materia de investigación.

A continuación, definimos el tipo y nivel de investigación:

1. **Tipo de investigación**

   En la presente investigación, se ha empleado tanto una investigación básica como una investigación aplicada.

   Se ha realizado una investigación básica para el planteamiento de un nuevo modelo de seguridad de la información, sistémico, óptimo y muy diferente a las existentes, basado en la gestión de procesos de negocios, para así conocer las necesidades y expectativas de seguridad de los estudiantes, docentes y empleados de una institución educativa.

   Se ha realizado una investigación aplicada porque el Modelo Sistémico de Seguridad de la Información con un enfoque en la gestión de procesos de negocio (basado en estándares de seguridad) cumpla con satisfacer los requisitos de seguridad de las partes interesadas y estos resultados contribuyen a mejorar la competitividad funcional de una institución.

2. **Nivel de investigación**

   Tomando como referencia a Hernández Sampieri (1997), este trabajo de investigación se inicia a nivel descriptivo y llega a ser explicativo porque hay una relación causal entre las variables, es decir que para medir si se mejora la competitividad funcional de las universidades (variable dependiente) es necesario proponer un Modelo Sistémico de Seguridad de la Información (variable independiente).

## 1.9. DISEÑO DE LA INVESTIGACIÓN

El trabajo de investigación presenta la clasificación de diseño experimental, de tipo "experimentos verdaderos ", que son aquellos que, para lograr el control interno y la validez, se necesita grupos de control equivalentes que tengan las mismas características para comparar los resultados.

En la figura 1.2, se muestra un diseño con pos prueba y grupos de control.
Este diseño comprende, además de la variable experimental, todos los elementos de la observación experimental. Concretamente, se conforma aleatoriamente (R) un grupo, constituido por procesos de negocio de la universidad donde ocurren incidentes de seguridad, este grupo de procesos se ha tomado como prototipo (G1) al que se le aplica un estímulo o tratamiento experimental, el Modelo Sistémico de Seguridad de la Información basado en BPM (X), aplicándosele una prueba posterior al tratamiento (O1). A un segundo grupo (G2), también conformado aleatoriamente, al que no se le suministra tal estímulo, el mismo que sirve únicamente como grupo de control, en forma simultánea se aplica una prueba (O2).

En ambos casos se asegura la representatividad estadística de los grupos, cumpliendo de este modo con el control de la validez interna.

| | | |
|---|---|---|
| RG1 | X | $O_1$ |
| RG2 | _ | $O_2$ |

*Figura 1.2*: Diseño de la Investigación

## 1.10. POBLACIÓN

En concordancia con el objetivo de la tesis, se ha identificado como unidad de análisis a los procesos de negocio de naturaleza académica y administrativa que se llevan a cabo en una institución educativa.

Si bien es cierto que los procesos, son eventos discretos, con frecuencia y volumen variables; ellos tienen lugar mientras el sistema de la organización universitaria tenga necesidad de utilizarlos, por tanto, la población considerada para este estudio es infinita, debido a que no es posible delimitarla con precisión.

## 1.11. MUESTRA

La muestra seleccionada es del tipo probabilística debido a que cualquier incidente de seguridad de la información que se suscite en los grupos de procesos de negocio, tiene la misma oportunidad de conformar el grupo de control y experimental.

## 1.12. TAMAÑO DE LA MUESTRA REPRESENTATIVA

La ficha técnica sobre la cual han sido probados los datos recolectados para la prueba de hipótesis corresponde a los siguientes parámetros:

Nivel de confianza: 95%
Margen de error: ± 1.67%

En consideración a las características de la población, a la muestra, nivel de confianza y margen de error elegidos, a los efectos que los resultados estén respaldados estadísticamente, es decir, que sean representativos. se ha seleccionado la siguiente expresión:

$$n = \frac{Z^2 \cdot \sigma^2}{e^2}$$

Para hallar la varianza $\sigma^2$ se puede recurrir a referencias bibliográficas (o estudios similares) o una muestra piloto. En este caso se ha elegido la muestra piloto de 10 elementos, como se presenta en la tabla 1.1

**Tabla 1.1**

*Muestra piloto*

| Grupo de Procesos | Número de incidentes |
|---|---|
| GP1 | 15 |
| GP2 | 17 |
| GP3 | 18 |
| GP4 | 22 |
| GP5 | 19 |
| GP6 | 24 |
| GP7 | 19 |
| GP8 | 23 |
| GP9 | 16 |
| GP10 | 21 |

Como se observa en la tabla cada elemento de la muestra es un grupo de procesos donde se dan un número de incidentes de seguridad de la información.

Haciendo el cálculo de la varianza se obtiene 8.24, de tal forma que reemplazando los siguientes valores en la fórmula:

Z = 1.96 (Para un nivel de confianza de 95%)

$\sigma^2$=8.24

e=1.67 (Margen de error)

Se obtiene una muestra de n=30.

## 1.13. TÉCNICAS DE INVESTIGACIÓN

### 1.13.1. TÉCNICAS

La técnica de recolección de información es a través de la simulación y por observaciones directas a los procesos críticos de las universidades.

### 1.13.2. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Se utilizará como instrumento de recolección de información, el software de modelamiento de procesos llamado Bizagi, esta herramienta aplica la metodología de BPM para medir la confiabilidad de la información; además contiene un simulador, apropiado para simular procesos de negocio.

También se usará las herramientas Microsoft Excel e IBM SPSS Statistics para la recolección y análisis de los datos.

# CAPÍTULO II
# MARCO TEÓRICO

## 2.1. SEGURIDAD DE LA INFORMACIÓN

La seguridad se puede definir como el grado de protección frente a actividades, daños, peligros y/o pérdida criminal. Asimismo," seguridad de la información se refiere a todos los procesos y políticas diseñadas para proteger la información de una organización y los sistemas de información de acceso, uso, revelación, interrupción, modificación o destrucción no autorizados" (Rainer,2013).

Según el estándar NTP-ISO/IEC 17799:2007: "La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser política, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware".

## 2.2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un sistema de gestión de seguridad de información consta de las políticas, procedimientos, directrices y recursos asociados y actividades, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos empresariales. (ISO/IEC 27000:2016)

Para Alberts y Dorofree (2003), "SGSI es el establecimiento de un sistema que determine qué requiere ser protegido, y por qué, de qué debe ser protegido y cómo protegerlo".

Según Peltier (2011), "SGSI es la preservación de la confidencialidad, integridad y disponibilidad de la información".

Para gestionar la seguridad de la información es necesario contemplar toda una serie de tareas y procedimientos que permitan garantizar los niveles de seguridad en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar.

Para Gómez (2011), al momento de implantar un sistema de gestión seguridad de la información, una organización debe contemplar los siguientes aspectos:

- Formalizar la gestión de la seguridad de la información
- Analizar y gestionar los riesgos
- Establecer los procesos de gestión de la seguridad siguiendo la metodología PHVA, como se muestra en la figura 2.1.


*Figura 2.1*: Metodología PHVA en la gestión de seguridad.

- ✓ "Plan": selección y definición de medidas y procedimientos.
- ✓ "Hacer": implantación de medidas y procedimientos de mejora.
- ✓ "Verificar": comprobación y verificación de las medidas implantadas

- ✓ “Actuar”: actuación para corregir todas las deficiencias detectadas en el sistema.

- Certificación de gestión de la seguridad

Podemos distinguir varias etapas o niveles de madurez en la Gestión de la Seguridad de la Información en una organización:

1. **Implantación de medidas básicas de seguridad por “sentido común”.**
   En una primera etapa la organización se preocuparía de la implantación de las medidas básicas de seguridad aplicadas por “sentido común”: realización de copias de seguridad, control de acceso a los recursos informáticos, etc. Podemos considerar que muchas de las empresas se encuentran todavía en esta primera etapa, aplicando unas mínimas medidas de seguridad que pueden resultar insuficientes para garantizar una gestión adecuada de los riesgos.

2. **Adaptación a los requisitos del marco legal y de las exigencias de los clientes.**
   En esta segunda etapa la organización toma conciencia de la necesidad de cumplir con las exigencias de la legislación vigente o de otras derivadas de sus relaciones y compromisos con terceros (clientes, proveedores u otras instituciones), protección de los datos de carácter personal, delitos informáticos, protección de la propiedad intelectual entre otros.

3. **Gestión integral de la Seguridad de la Información.**
   En la tercera etapa la organización ya se preocupa de gestionar con un planteamiento global e integrado la seguridad de la información, mediante la definición de una serie de políticas de seguridad de la información, la implantación de los planes y procedimientos de seguridad, el análisis y gestión de riesgos, y la definición de un plan de respuesta a incidentes y de continuidad del negocio.

4. **Certificación de la Gestión de la Seguridad de la Información.**

   Por último, en la cuarta etapa se pretende llevar a cabo una certificación de la gestión de la seguridad de la información para obtener el reconocimiento de las buenas prácticas implantadas para la organización y poder acreditarlo ante terceros: clientes, administraciones públicas y otras instituciones. Para ello, se recurre un proceso de certificación basado en estándares como la ISO 27001.

## 2.3. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

### 2.3.1. INFORMACIÓN

La información es uno de los activos más valiosos de la organización, por ello requiere una protección adecuada (NTP-ISO/IEC 17799 2007).

### 2.3.2. ACTIVO

Para Alexander (2007): "Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones".

Se clasifican los activos de información (NTP-ISO/IEC 17799 2007) en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.).
- Documentos de papel (contratos)
- Activos de software (aplicación, software de sistemas, etc.)
- Activos físicos (computadoras, medios magnéticos, etc.)
- Personal (clientes, personal)
- Imagen de la empresa y reputación
- Servicios (comunicaciones, etc.)

### 2.3.3. AMENAZA

**“**Una amenaza es la indicación de un potencial evento no deseado” (Alberts y Dorofee, 2003). En esta definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural.

Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza, para así facilitar su ubicación. Las amenazas también difieren los métodos para estimar su posibilidad de ocurrencia:

1. Amenazas naturales (inundaciones, terremotos, maremoto, incendios, entre otros).
2. Amenazas a instalaciones (caída de energía, explosión, fallas mecánicas, entre otros).
3. Amenazas humanas (huelgas, pérdida de clave personal, epidemias, entre otros).
4. Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas en la red, fallas, entre otros).
5. Amenazas operacionales (crisis financieras, fallas en equipos, entre otros).
6. Amenazas sociales (sabotaje, motines, bombas, protestas, entre otros).

### 2.3.4. VULNERABILIDAD

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Para Peltier, vulnerabilidad “es una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema” (Peltier, 2001).

“Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas” (Alberts y Dorofee, 2003).

Las vulnerabilidades se pueden clasificar en:

1. Seguridad de los recursos humanos (falta de mecanismos de monitoreo, falta de políticas para el uso de las telecomunicaciones, carencia de conciencia en seguridad, falta de entrenamiento en seguridad, entre otros).
2. Control de acceso (falta de políticas se seguridad respecto a las pantallas, falta de protección de los equipos, passwords sin modificaciones frecuentes, falta de políticas de control de acceso, entre otros).
3. Seguridad física y ambiental (control de acceso físico inadecuado a oficinas y edificios, condiciones físicas no adecuadas, falta de equipos de protección de variación de voltaje, entre otros).
4. Gestión de operaciones y comunicaciones (interfaces de usuarios complicada, inadecuado control de cambio, inadecuada gestión de red, entre otros).
5. Mantenimiento, desarrollo y adquisición de sistemas de información (falta de protección de llaves criptográficas, carencia de políticas para el uso de criptografías, falta o carencia de políticas de validación de datos, entre otros).

Cuando son identificadas las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza. Se debe entender que las vulnerabilidades y amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de relación de causalidad y probabilidad de ocurrencia.

En la figura 2.2, se muestra la relación causa-efecto entre activos, riesgo, vulnerabilidades y amenaza.

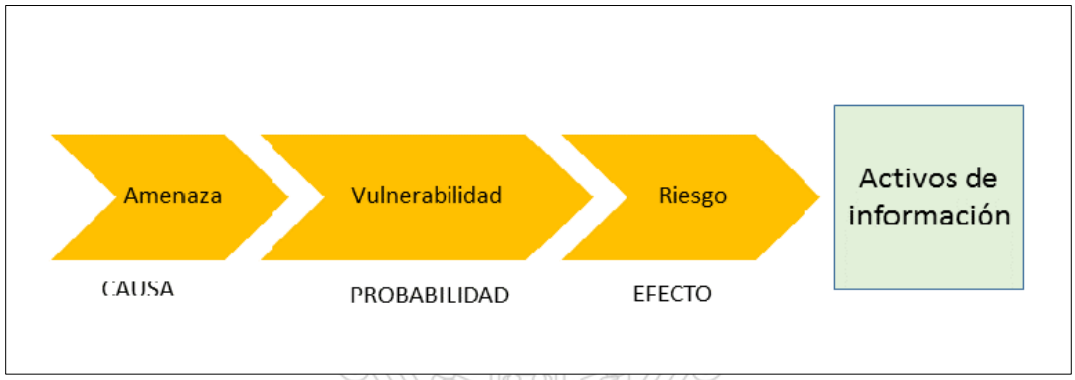



*Figura 2.2*: Relación causa-efecto entre elementos del análisis de riesgo.

Esos elementos del análisis de riesgo no pueden verse de manera aislada. Existe una interdependencia de ellos bajo una relación de causa-efecto. Como se puede apreciar, la variable que la empresa puede manipular y fortalecer, para minimizar que se ponga de manifiesto el riesgo y proteger los activos de información de una penetración de la amenaza, son las vulnerabilidades.

### 2.3.5. RIESGO

El riesgo se puede definir como "la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular" (Peltier, 2001).

"El riesgo se caracteriza a menudo por la referencia a eventos y consecuencias potenciales, o una combinación de éstos" (ISO/IEC Guide 73:2002).

Las organizaciones están expuestos a una gran cantidad de amenazas que aprovechan, cualquiera de las vulnerabilidades presentes y pueden someter a activos de información a una variedad de fraude, espionaje o sabotaje.

En la figura 2.3 se aprecia el riesgo de seguridad de la información.


*Figura 2.3*: Riesgo de seguridad de la información.

### 2.3.6. GESTIÓN DEL RIESGO

La gestión del riesgo puede utilizar distintos enfoques gerenciales y métodos de cálculo que satisfagan las necesidades de la organización. La organización decidirá que método de cálculo del riesgo se escoge. No importa el método que decida la organización, pero debe cerciorarse de que el enfoque es adecuado y apropiado para atender los requerimientos organizacionales, legales o regulatorios.

La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información**.** La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001**.**

Las empresas gastan una gran cantidad de tiempo y recursos físicos y económicos en proteger sus recursos de información. Antes de realizar esas inversiones se han de realizar el análisis y gestión de riesgos.

Existen numerosas metodologías que realizan el análisis y gestión de riesgos. En España, la metodología oficial del Ministerio de Administraciones Públicas, Magerit (2012), estudia en profundidad la puesta en marcha de estas estrategias.

El análisis del riesgo contempla:

- Identificación de activos de información.
- Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
- Cálculo de la posibilidad que las amenazas y vulnerabilidades ocurran.

La evaluación del riesgo incluye:

- Cálculo del riesgo.
- Identificación del significado de los riesgos. Esto se hace definiendo criterios y evaluando los riesgos contra una escala predeterminada.

## 2.4. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Por incidente de seguridad de la información se define "una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocio" (ISO/IEC 27000:2016).

Según Gómez (2011), la gestión de incidentes de seguridad de la información plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad:

- Constitución de un equipo de respuesta a incidentes de Seguridad
- Detección de un incidente de seguridad
- Análisis de un incidente de seguridad
- Contención, erradicación y recuperación

- Documentación del incidente de seguridad
- Actividades Post-incidente

Seguidamente se desarrollan cada una de las actividades:

### 2.4.1. EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, Computer Security Incident Response Team) está constituido por las personas que cuenta con la experiencia y la formación necesaria para poder actuar ante las incidencias y desastres que pudieran afectar a la seguridad de la información de una organización.

En la mayoría de las organizaciones que no cuentan con un Equipo de Respuesta formalmente constituido, será necesario identificar quiénes son las personas responsables de acometer cada una de las tareas, definiendo claramente responsabilidades, funciones y obligaciones de cada persona implicada en el Plan de Respuesta de Incidentes.

La organización deberá mantener actualizada la lista de direcciones y teléfonos de contacto para emergencias, para poder localizar rápidamente a las personas clave.
Conviene prestar especial atención a la formación continua de los miembros del equipo, contemplando tanto los aspectos técnicos como los aspectos legales. Estas personas deben contar con la dotación de medio técnicos y materiales necesarios para poder cumplir con eficacia, su misión.

### 2.4.2. DETECCIÓN DE UN INCIDENTE DE SEGURIDAD

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido. Se presentan una relación de los principales indicadores de posibles incidentes de seguridad:

- Alarmas ocasionadas en los Sistemas de Detección de Intrusiones (IDS), en los cortafuegos o en las herramientas antivirus.

- Registro de actividad extraña en los “logs” de servidores y dispositivos de red.
- Caída o mal funcionamiento de los servidores.
- Notable caída en el rendimiento de la red o de algún servidor, debido a un incremento inusual del tráfico de datos.
- Existencia de herramientas no autorizadas en el sistema.
- Reportes de usuarios del sistema alertando de alguna situación extraña o de su imposibilidad de acceder a ciertos servicios.
- Notificación de un intento de ataque lanzado contra terceros desde equipos pertenecientes a la propia organización.
- Otros funcionamientos fuera de lo normal del sistema.

### 2.4.3. ANÁLISIS DE UN INCIDENTE DE SEGURIDAD

Se podría utilizar una “Matriz de Diagnóstico” como se muestra en la tabla 2.1 para facilitar la actuación del equipo en momentos de máximo estrés, evitando que se puedan tomar decisiones precipitadas que conduzcan a errores, constituyendo además un valioso apoyo para el personal con menos experiencia en la actuación frente a incidentes de seguridad.

**Tabla 2.1**

*Ejemplo de Matriz de Diagnóstico*

| **Síntomas** | **Código malicioso** | **Denegación de Servicio (DoS)** | **Acceso no autorizado** |
|---|---|---|---|
| Escaneo de puertos | Bajo | Alto | Medio |
| Caída de un servidor | Alto | Alto | Medio |
| Modificación de ficheros de un equipo | Alto | Bajo | Alto |
| Tráfico inusual en la red | Medio | Alto | Medio |
| Ralentización de los equipos o red | Medio | Alto | Bajo |
| Envío de mensajes de correo sospechoso | Alto | Bajo | Medio |

Luego, conviene realizar una valoración inicial de los daños y de sus posibles consecuencias, para a continuación establecer un orden de prioridades en las actividades

que debería llevar a cabo el equipo de respuesta, teniendo para ello en consideración aspectos como el posible impacto del incidente en los recursos y servicios de la organización y en el desarrollo de su negocio o actividad principal.

Con el fin de permitir una atención adecuada a los incidentes de seguridad, se propone en la tabla 2.2. la priorización de las actividades a realizar por parte de un equipo de respuesta a incidentes:

**Tabla 2.2**

*Priorización de actividades*

| Niveles de prioridad | Actividad |
|---|---|
| Prioridad uno | Proteger la vida humana y la seguridad de las personas |
| Prioridad dos | Proteger datos e información sensible de la organización |
| Prioridad tres | Proteger otros datos e información de la organización |
| Prioridad cuatro | Prevenir daños en los sistemas de información como la pérdida o modificación de ficheros básicos para las aplicaciones y servidores. |
| Prioridad cinco | Minimizar la interrupción de los servicios ofrecidos a los distintos usuarios |

### 2.4.4. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de Tecnología de la Información y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

1. **Contención:**

   Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de tecnología de la información. Una primera opción sería llevar a cabo una rápida actuación para evitar que el incidente pueda tener mayores consecuencias para la organización: apagar todos los equipos afectados, desconexión de estos equipos de la red informática, desactivación de ciertos servicios entre otros.

Una segunda opción sería retrasar la contención para poder estudiar con más detalle el tipo de incidente. Esta estrategia se puede implementar siempre y cuando sea posible monitorizar y controlar la actuación de los atacantes, para de este modo reunir las evidencias necesaria y tomar acciones legales contra los responsables del incidente. No obstante, se corre el riesgo de que el incidente pueda tener peores consecuencias por no haber actuado a tiempo.

2. **Erradicación:**

Es la etapa donde se llevan a cabo todas las actividades necesarias para eliminar los agentes causantes del incidente y de sus secuelas, entre los que podríamos citar posibles "puertas traseras" instaladas en los equipos afectados u otros códigos malignos (virus, gusanos), contenidos y material inadecuado que se haya introducido en los servidores, cuentas de usuarios creadas por los intrusos o nuevos servicios activados en el incidente. También será conveniente llevar a cabo una revisión de otros incidentes que se pudieran ver comprometidos a través de las relaciones de confianza con el sistema afectado.

3. **Recuperación:**

Es la etapa en la que se trata de restaurar los sistemas para que puedan volver a su normal funcionamiento. Para ello, será necesario contemplar las tareas como la reinstalación del sistema operativo y de las aplicaciones partiendo de una copia segura, la configuración adecuada de los servicios e instalación de los últimos parches y actualizaciones de seguridad, el cambio de contraseñas que puedan haber sido comprometidas, la desactivación de las cuentas que hayan sido utilizadas y la prueba del sistema para comprobar su correcto funcionamiento.

### 2.4.5. DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD

La documentación de un incidente de seguridad es importante y se debe reflejar en forma clara y precisa los siguientes aspectos:

- Descripción del tipo de incidente

- Hechos registrados (eventos en los “logs” de los equipos).
- Daños producidos en el sistema
- Decisiones y actuaciones del equipo de respuesta.
- Comunicaciones que se han realizado con terceros y con los medios.
- Lista de evidencias obtenidas durante el análisis y la investigación.
- Comentarios e impresiones del personal involucrado.
- Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en el futuro.

### 2.4.6. ACTIVIDADES POST-INCIDENTE

Se tiene que realizar un análisis y revisión a posteriori de cada incidente de seguridad, a fin de determinar las lecciones aprendidas que la organización tiene que tomar en cuenta.
Es necesario emitir un reporte final sobre el incidente, en el que se pueda desarrollar los siguientes aspectos:

- Investigación sobre las causas y las consecuencias del incidente.
- Revisión de las decisiones y actuaciones del equipo de respuesta a incidentes.
- Análisis de los procedimientos y de los medios técnicos empleados en la respuesta al incidente.
- Revisión de las políticas de seguridad de la organización.

## 2.5. POLÍTICAS DE SEGURIDAD

Una vez que identifique los principales riesgos para sus sistemas, se tendrá que desarrollar una política de seguridad para proteger sus activos. “Una política de seguridad consiste de enunciados que clasifican los riesgos de la información, identifican los objetivos de seguridad aceptables y también mecanismos para lograr estos objetivos” (Laudon y Laudon, 2012).

La política de seguridad controla las políticas que determinan el uso aceptable de los recursos de información de la organización y qué miembros tienen acceso a sus activos de información. Una política de uso aceptable define los usos admisibles de los recursos de

información y el equipo de cómputo de la organización, que incluye las computadoras, laptop y de escritorio, los dispositivos inalámbricos e Internet. La política debe clarificar la política de la empresa con respecto a la privacidad, la responsabilidad de los usuarios y el uso personal tanto del equipo como de las redes de la empresa.

Según Shinder (2003), "Política de seguridad hace referencia a un documento escrito que define el enfoque de seguridad de una empresa o un área de seguridad específica y que establece una serie de normas que deben seguirse al aplicar la filosofía de seguridad de la empresa".

Podemos definir una Política de Seguridad como una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Las empresas pueden establecer tanto normas escritas como no escritas relacionadas con los problemas de seguridad, además de emitir varios tipos diferentes de documentos relacionados con estos temas. Un procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implementar las políticas de seguridad que han sido aprobadas por la organización.

## 2.6. ESTÁNDARES RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN

Diferentes organizaciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente. A continuación, se detallan los de mayor utilización a nivel mundial:

### 2.6.1. ISO SERIE 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación sobre realización de auditorías de SGSI, así como una orientación sobre competencia de auditores de SGSI (ISO 27007), una guía para la aplicación de controles de seguridad de la información en las organizaciones de telecomunicaciones (ISO 27011), una guía de apoyo para la preparación de las tecnologías de información y comunicaciones para la continuidad de negocio (ISO 27031), un marco de orientación para mejorar el estado de la ciberseguridad (ISO 27032), orientación detallada sobre la aplicación de controles de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), una guía de incidentes de seguridad en la información (ISO 27035), una guía de seguridad relacionada con proveedores (ISO 27036): visión general y conceptos, requisitos comunes, seguridad de la cadena de suministro TI y seguridad en entornos de servicios cloud, una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales localizadas en dispositivos móviles, cámaras digitales y de video y otros dispositivos (ISO 27037), una guía de especificación para seguridad en la redacción digital (ISO 27038) y una guía de seguridad de la información en el sector sanitario (ISO 27799).

En la figura 2.4 se muestra gráficamente la Familia ISO 27000.

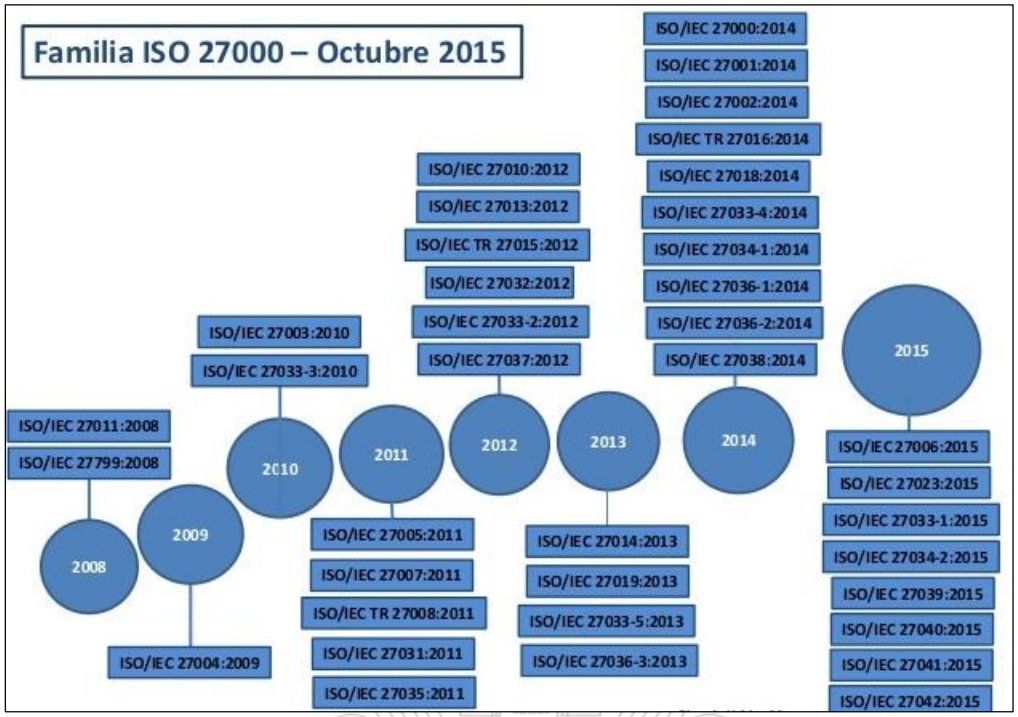



*Figura 2.4*: Familia ISO 27000.

### 2.6.2. NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014

La Norma Técnica Peruana NTP-ISO/IEC 27001:2014. TECNOLOGíA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2da. Edición fue oficializada el 1ro de diciembre de 2014.

Esta norma ha sido preparada por el Comité Técnico de Normalización e intercambio electrónico de datos utilizando como antecedente a la norma ISO/IEC 27001:2013 y la ISO/IEC 27001:2013/COR 1 2013.

Fue aprobada el uso obligatorio de esta norma en todas las entidades integrantes del Sistema Nacional de Informática, con Resolución Ministerial N° 004-2016-PCM (Presidencia de Consejo de Ministros PCM, 2016).

Esta Norma Técnica Peruana proporciona los requerimientos para mejorar un SGSI dentro del contexto de la organización. La norma también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

### 2.6.3. ISO 17799

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Es una guía que proporciona recomendaciones para desarrollar normas de seguridad de la información dentro de las organizaciones y ser una práctica efectiva de la gestión de la seguridad.

### 2.6.4. COBIT

Acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TI. La organización desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante.

Como se puede apreciar en la figura 2.5, los principios de COBIT 5 en la nueva guía son:

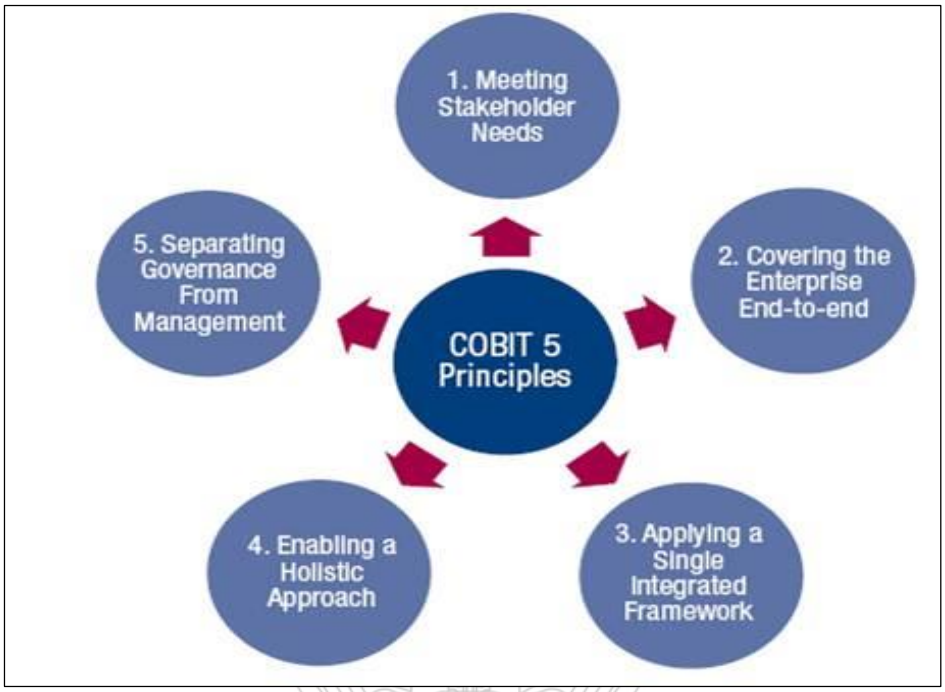



*Figura 2.5*: Los principios de COBIT 5

1. **Satisfacer las necesidades de los colaboradores.** Es crítico definir y vincular los objetivos empresariales y los objetivos relacionados con TI.
2. **Cubrir la empresa de extremo a extremo**. Las empresas deben cambiar de visión, con el objetivo de considerar el área de TI como un activo y no un costo. Los directivos deben tomar la responsabilidad de gobernar y gestionar los activos relacionados con TI dentro de sus propias funciones.
3. **Aplicar un solo marco integrado**. Usar un solo marco de gobierno integrado puede ayudar a las organizaciones brindar valor óptimo de sus activos y recursos de TI.
4. **Habilitar un enfoque holístico.** El gobierno de TI empresarial requiere de un enfoque holístico que tome en cuenta muchos componentes, también conocidos como habilitadores. Los habilitadores influyen en si algo va funcionar o no. Cobit 5 incluye 5 habilitadores como son los principios, las políticas y marcos, los procesos, la cultura, la información y la gente.

5. **Separar al gobierno de la administración**. Los procesos de gobierno aseguran que los objetivos se alcancen mediante la evaluación de las necesidades de los interesados, el establecimiento de la dirección a través de la priorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento y el progreso. De acuerdo con los resultados de las actividades de gobierno, la administración de la empresa y de TI entonces debe planear, crear, realizar y monitorear las actividades para asegurar el alineamiento con la dirección que se estableció.

### 2.6.5. ITIL

Acrónimo de "Information Technology Infrastructure Library", ITIL es una norma de mejores prácticas para la administración de servicios de Tecnología de Información, desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es la Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL describe la manera de gestionar TI como un negocio, desde la creación de una estrategia de servicios hasta el diseño de los servicios de negocio; al implementar ITIL consigue que TI se convierta en un activo estratégico y una ventaja competitiva para cualquier organización.

ITL agrupa elementos principales en 5 volúmenes, que se presentan con los siguientes títulos: Service Strategy, Service Designe, Service Operation, Continual Service Improvement y Service Transition.

En la figura 2.6 el ciclo de vida ITIL.

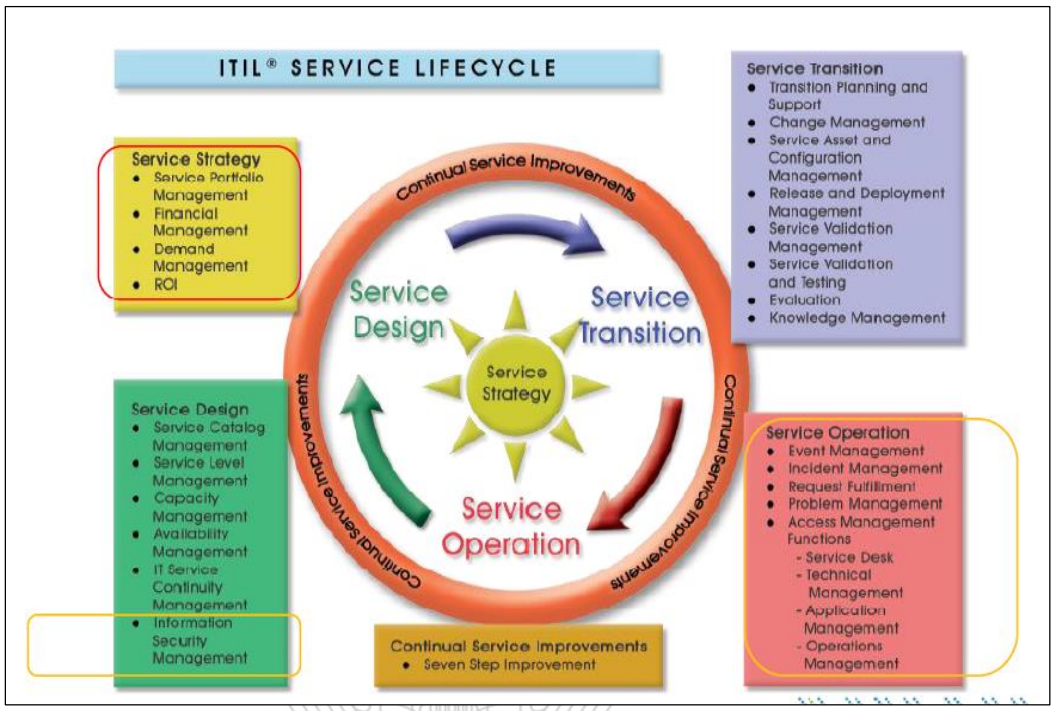



*Figura 2.6*: Ciclo de vida de ITIL.

1. **Service Strategy (SE) - Estrategia de Servicios.**

   Diseña el plan de acción que permitirá desarrollar una estrategia en la Organización en cuanto a las Tecnologías de la Información. Desarrolla varias áreas; entre ellas se incluyen las siguientes: Estrategia general, competitividad y posicionamiento de mercado, tipos de proveedores de servicio, gestión del servicio como un factor estratégico, diseño organizacional y estratégico, procesos y actividades clave, gestión financiera, dossier de servicios, gestión de la demanda, y responsabilidades y responsabilidades clave en la estrategia de servicios.

2. **Service Designe (SD)- Diseño de Servicios.**

   Se desarrollan los conceptos relativos al diseño de Servicios TI, como diseño de arquitecturas, procesos, políticas, documentación. Se adentra además en la Gestión de niveles de servicio, diseño para gestión de capacidad, continuidad en los servicios TI, gestión de proveedores, y responsabilidades clave en diseño de servicios.

3. **Service Operation (SO) – Operaciones de Servicios**

   En el libro de operaciones, se exponen las mejores prácticas a poner en marcha para conseguir ofrecer un nivel de servicio de la Organización acorde a los requisitos y necesidades de los Clientes (establecimiento del SLA – Service Level Agreement o Acuerdo de Nivel de Servicio). Los temas incluyen objetivos de productividad/beneficios, gestión de eventos, gestión de incidentes, caso de cumplimiento, gestión de activos, servicios de helpdesk, técnica y de gestión de las aplicaciones, así como las principales funciones y responsabilidades para el personal de servicios que llevan a cabo los procesos operativos.

4. **Continual Service Improvement (CSI) – Mejora Continua de Servicios**

   En este volumen se explica la necesidad de la mejora continua como fuente de desarrollo y crecimiento en el Nivel de Servicio de TI, tanto interno como con respecto al cliente.

   De acuerdo con este concepto, las entidades han de estar en constante análisis de sus procesos de negocio, y poner en marcha actuaciones una vez detectadas las necesidades con respecto a las TI de manera que estas sean capaces de responder a los objetivos, la estrategia, la competitividad y la gestión de la estructura y organización de las organizaciones que dispongan de infraestructura TI. De esta manera se trata de estar al tanto de los cambios que se producen en el mercado y de las nuevas necesidades de este también en cuanto a las TI.

5. **Service Transition (ST) – Transición de Servicios.**

   En el último libro se definen los temas relacionados a la transición de servicios, es decir, los cambios que se han de producir en la prestación de servicios comunes (del trabajo diario) en las empresas.

   Aspectos tales como la gestión de la configuración y servicio de activos, la planificación de la transición y de apoyo, gestión y despliegue de los Servicios TI, Gestión del Cambio, Gestión del Conocimiento, y por último las responsabilidades y las funciones de las personas que participen en el Cambio o Transición de Servicios.

### 2.6.6. LEY SOX

La Ley Sarbanes-Oxley (SOX), de EE.UU., nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la Securities and Exchange Comission a llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como Enron y Worldcom, durante el año 2002, en los cuales se comprobó que información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que transan sus valores en la bolsa de EE.UU.

### 2.6.7. COSO

La normativa COSO, acrónimo de The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma. Junto a esto son muchas otras las normas que están directa o indirectamente relacionadas con ésta como por ejemplo COBIT. En síntesis, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un sistema de Control Interno, con alcances al área informática.

### 2.6.8. ISO 31000

ISO 31000 es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa en forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades (ISO 31000:2009).

ISO 31000 muestra en la figura 2.7 el proceso de gestión de riesgos, el cual tiene 3 etapas: establecimiento de contexto, valuación de riesgos y tratamiento de los mismos.

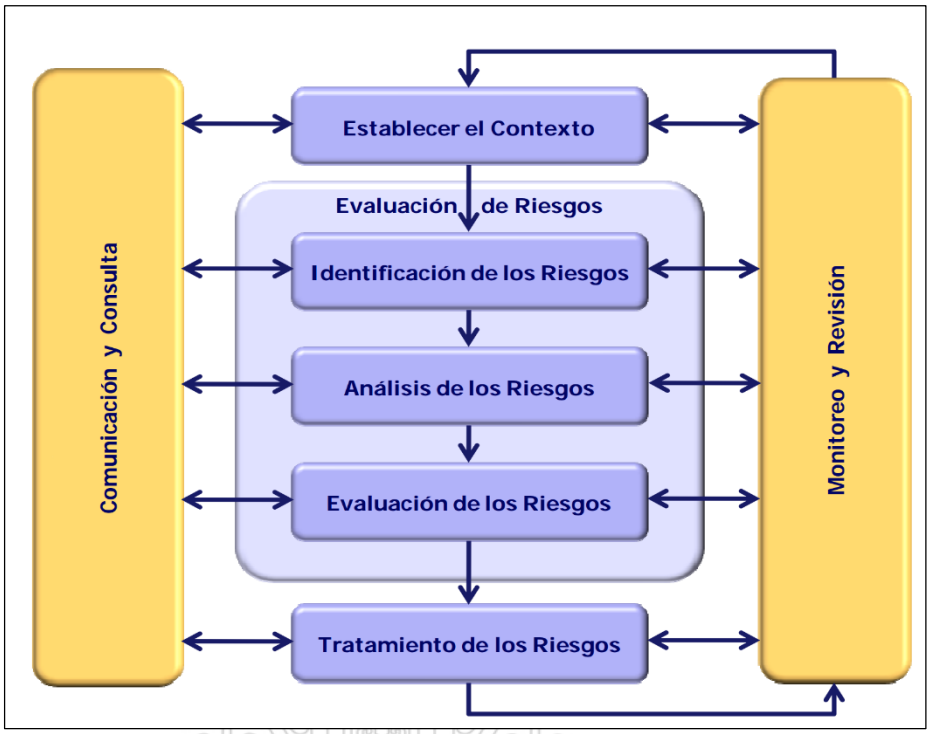



*Figura 2.7*: Proceso de gestión de riesgos.

## 2.7. ENFOQUE BASADO EN PROCESOS

Hoy en día, las empresas se enfrentan a un entorno cambiante y altamente competitivo a nivel global. Para poder afrontar con éxito los cambios continuos que se producen, las empresas han de ser ágiles, flexibles y gestionar adecuadamente sus procesos de negocio.

Una definición de proceso muy utilizada en las escuelas de negocio más prestigiosas es la siguiente: Un proceso es un conjunto de actividades o tareas que transforman unos insumos (materiales, clientes, información) en resultados (productos y/o servicios), éstos últimos dirigidos a agregar valor (satisfacer una necesidad) a un cliente (interno o externo).

Existen infinidad de procesos y muchos de ellos son transversales y afectan a diferentes áreas funcionales o departamentos. Por ejemplo, el desarrollo de un producto implica

investigación, diseño, ingeniería, producción, mercadotecnia, y afecta a varios departamentos; otros procesos sólo afectan a un departamento, como la contratación de un empleado suele depender del departamento de Recursos Humanos con independencia de que este departamento realice consultas a otros departamentos y a la dirección.

Un proceso, según la norma de ISO 9000:2005 puede definirse como un "conjunto de actividades interrelacionadas o que interactúan, las cuales transforman elementos de entrada en resultados".

Estas actividades requieren la asignación de recursos como personal y material. La figura 2.8 muestra un proceso genérico:

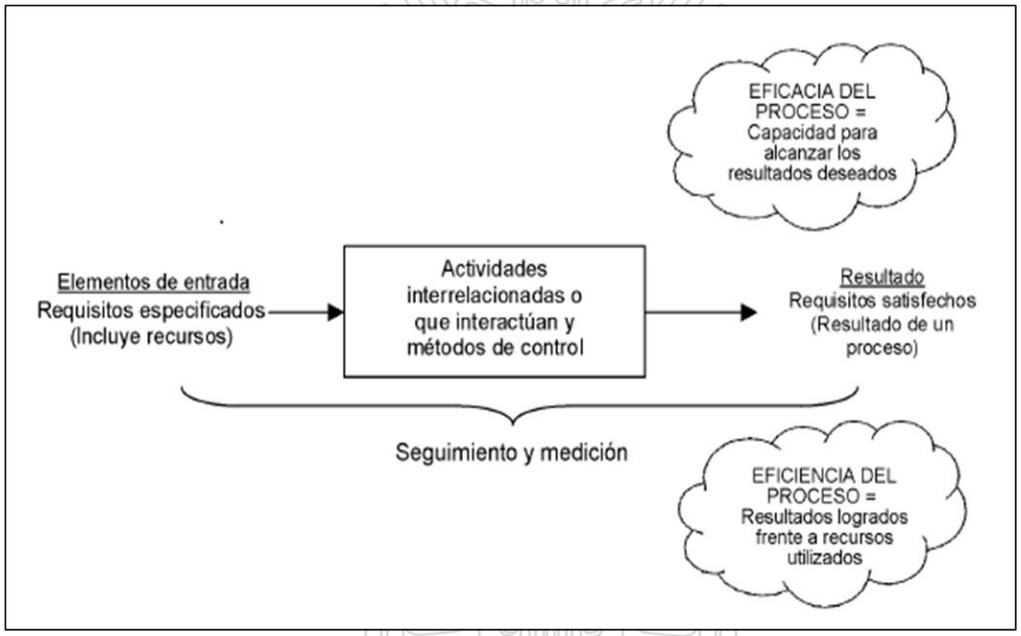



*Figura 2.8*: Proceso genérico.

Cada proceso tiene clientes y otras partes interesadas (quienes pueden ser internos o externos a la organización) que son afectados por el proceso y quienes definen los resultados requeridos de acuerdo a sus necesidades y expectativas. Debería utilizarse un sistema para recopilar datos, los cuales pueden analizarse para proveer información sobre el desempeño del proceso, y determinar las acciones correctivas o de mejora.

Todos los procesos, deberían estar alineados con los objetivos, el alcance y la complejidad de la organización, y deberían estar diseñados para aportar valor. La eficacia y la eficiencia del proceso pueden evaluarse a través de procesos de revisión internos o externos.

Las organizaciones desde hace tiempo han optado por el enfoque basado en procesos, y la norma ISO 9001:2008 lo define como: “La aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacción de estos procesos, así como la gestión para producir el resultado deseado”.

Las organizaciones habitualmente se gestionan verticalmente, con la responsabilidad por los resultados obtenidos dividida entre unidades funcionales. El cliente final u otra parte interesada no siempre ven todo lo que está involucrado. En consecuencia, a menudo se da menos prioridad a los problemas que ocurren en los límites de las interfaces que a las metas a corto plazo de las unidades. Esto conlleva a la escasa o nula mejora para las partes interesadas, ya que las acciones están frecuentemente enfocadas en las funciones más que en el beneficio global de la organización.

El enfoque basado en procesos introduce la gestión horizontal, cruzando las barreras entre las distintas unidades funcionales y unificando sus enfoques hacia las metas principales de la organización. Además, es una excelente vía para organizar y gestionar la forma en que las actividades de trabajo crean valor para el cliente y otras partes interesadas. El desempeño de una organización puede mejorarse a través del uso del enfoque basado en procesos. Los procesos se gestionan como un sistema, mediante la creación y entendimiento de una red de procesos y sus interacciones.

Para Alexander (2007), el enfoque basado en proceso para la gestión de seguridad de la información enfatiza la importancia de:

- La comprensión de los requisitos de seguridad de la información de una organización y la necesidad de establecer la política y objetivos para la seguridad de la información;
- Implementar y operar controles para dirigir los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
- Realizar seguimiento y revisar el desempeño y la eficacia del SGSI;
- La mejora continua con base en mediciones objetivas.

### 2.7.1. MAPA DE PROCESOS

El primer paso para adoptar un enfoque basado en procesos en una organización es identificar cuáles son los procesos que deben aparecer en la estructura de procesos del sistema y en qué nivel de detalle. Luego de la identificación y selección de los procesos, surge la necesidad de definir y reflejar esta estructura de forma que facilite la determinación e interpretación de las interrelaciones existentes entre los mismos. La manera más representativa de reflejar los procesos identificados es a través de un mapa de procesos, que viene a ser la representación gráfica de la estructura de procesos que conforman el sistema de gestión.

Para la elaboración de un mapa de procesos, es necesario reflexionar previamente en las posibles agrupaciones en las que pueden encajar los procesos identificados. La agrupación de los procesos dentro del mapa permite establecer analogías entre procesos, al tiempo que facilita la interrelación y la interpretación del mapa en su conjunto.

Los procesos de una organización se pueden agrupar en tres tipos, según la figura 2.9:

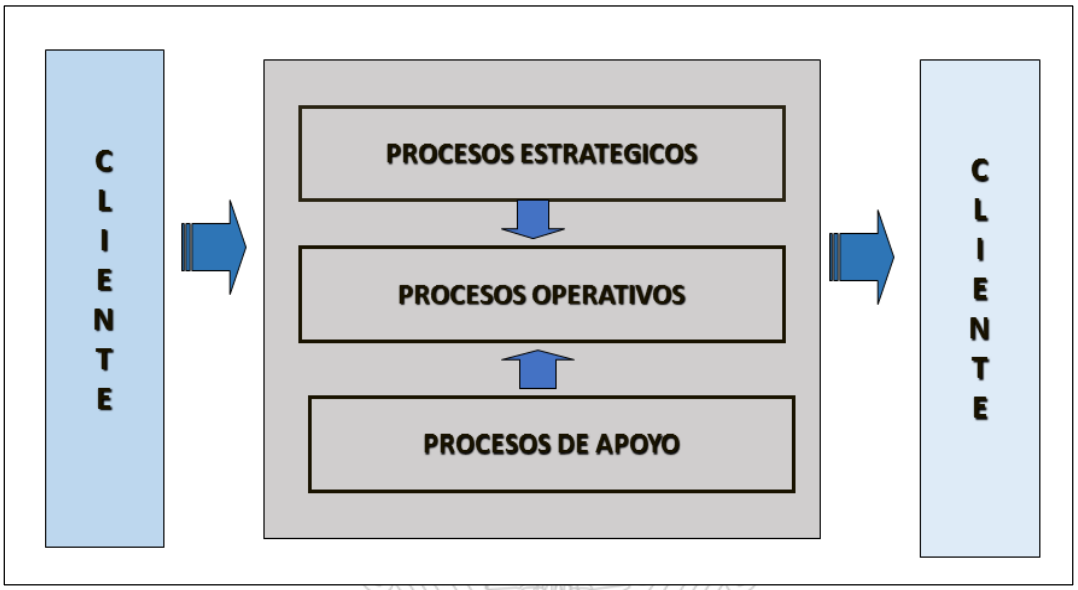



*Figura 2.9*: Mapa de procesos.

1. **Procesos estratégicos.**

   Son los procesos responsables de analizar las necesidades y condicionantes de la sociedad, del mercado y de los accionistas, para asegurar la respuesta a las mencionadas necesidades y condicionantes estratégicos.

2. **Procesos operativos**

   Son los procesos que tiene una relación directa con el cliente. Por ejemplo, los procesos operativos necesarios para la realización del producto/servicio, a partir de los cuales, el cliente percibirá y valorará la calidad.

3. **Procesos de soporte.**

   Son los procesos responsables de proveer a la organización de todos los recursos necesarios en cuanto a personas, maquinaria y materia prima, para poder generar el valor añadido deseado por los clientes (contabilidad, compras, nóminas, sistemas de información, etc.).

## 2.8. BUSINESS PROCESS MANAGEMENT (BPM)

BPM, es un sistema de gestión enfocado a perseguir la mejora continua del funcionamiento de las actividades empresariales mediante la identificación y selección de procesos y la descripción, documentación y mejora de los mismos, partiendo del despliegue de la estrategia de la organización, asegurando la misión empresarial y alineada a la visión de la empresa.

### 2.8.1. EVOLUCIÓN DE LA BPM

Al principio, la mejora de los procesos de negocio tenía un tratamiento fundamentalmente teórico, en el que la metodología estaba basada en identificar los procesos, determinar los procesos estratégicos, documentarlos, crear un mapa de procesos de toda la entidad, etc. que permitiera "entender la empresa" bajo este nuevo punto de vista que es BPM. Como ayuda a estos trabajos comenzaron a utilizarse herramientas que por evolución natural fueron cada vez más y mejores. Así, hasta la llegada de la BPMS (Business Process Management Suites), que es el software que soporta BPM. BPMS tiene un enfoque eminentemente práctico ya que en su implantación lo que se hace es introducir en el sistema: la modelización de los procesos y las reglas de negocio, para que el propio sistema se encargue de automatizarlos, controlar su cumplimiento y proporcionar los análisis necesarios para la mejora continua. En la figura 2.10 se puede apreciar la evolución de la BPM.

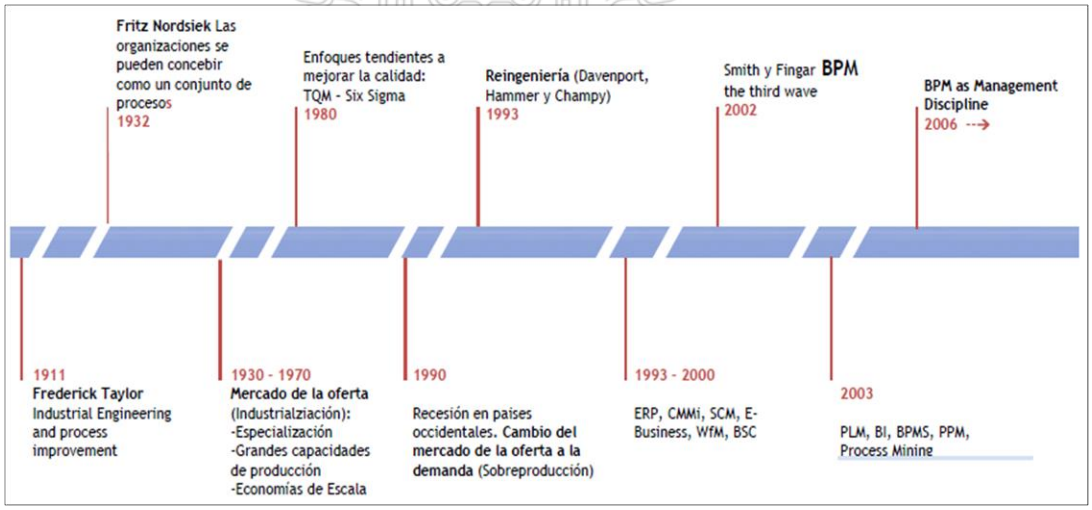



*Figura 2.10*: Evolución de la BPM.

### 2.8.2. ETAPAS DE LA BPM

Las organizaciones recurren a la BPM, que provee de una variedad de herramientas y metodologías para analizar los procesos existentes, diseñar nuevos procesos y optimizarlos. En la figura 2.11 se muestra el ciclo de vida, porque la BPM nunca finaliza debido a que la mejora de los procesos requiere de un cambio continuo.

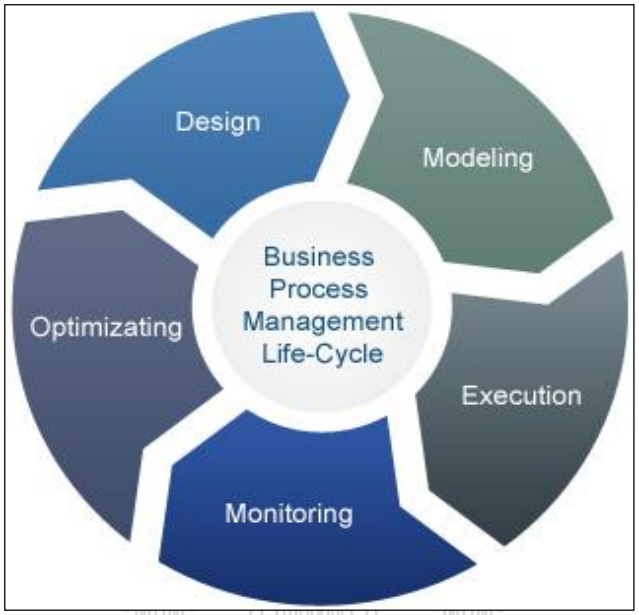



*Figura 2.11*: Ciclo de vida de la BPM.

Para Laudon y Laudon (2012), las empresas que practican la administración del proceso de negocios pasan por las siguientes etapas:

1. **Identificar los procesos a cambiar:** una de las decisiones estratégicas más importantes que debe tomar una firma no es la de decidir cómo usar las computadoras para mejorar los procesos de negocios, sino comprender qué procesos necesitan mejorar. Cuando los sistemas se utilizan para fortalecer el modelo de negocios o los procesos de negocios incorrectos, la empresa puede volverse más eficiente en cuanto a hacer lo que no debería. Como resultado, la firma se vuelve vulnerable a los competidores que tal vez hayan descubierto el modelo de negocios correcto. Además, es posible que se invierta una cantidad considerable de tiempo y costo para mejorar los procesos de negocios que tengan poco impacto sobre el desempeño y los ingresos de la firma en general. Los

gerentes necesitan determinar qué procesos de negocios son los más importantes y cómo es que la mejora de éstos ayudará al desempeño de la empresa.

2. **Analizar los procesos existentes:** es necesario modelar y documentar los procesos de negocios existentes, además de anotar las entradas, las salidas, los recursos y la secuencia de actividades. El equipo de diseño de procesos identifica los pasos redundantes, las tareas que requieren de mucha papelería, los cuellos de botella y demás ineficiencias.

3. **Diseñar el nuevo proceso:** una vez que se planea el proceso existente y se mide en términos de tiempo y costo, el equipo de diseño del proceso diseñará uno nuevo para tratar de mejorarlo. Se documentará y modelará un nuevo proceso "para ser" optimizado con el fin de compararlo con el proceso anterior.

4. **Implementar el nuevo proceso:** una vez que se ha modelado y analizado el nuevo proceso en forma detallada, hay que traducirlo en un nuevo conjunto de procedimientos y reglas de trabajo. Tal vez haya que implementar nuevos sistemas de información o mejoras a los sistemas existentes para dar soporte al proceso rediseñado. El nuevo proceso y los sistemas de soporte se despliegan en la organización de negocios. A medida que la empresa empieza a utilizar este proceso, se descubren los problemas y se tratan de solucionar. Los empleados que trabajan con el proceso pueden recomendar mejoras.

5. **Medición continua:** una vez que se implementa y optimiza el proceso, hay que medirlo de manera continua. ¿Por qué? Los procesos se pueden deteriorar con el tiempo a medida que los empleados recurren al uso de métodos antiguos, o tal vez pierdan su efectividad si la empresa experimenta otros cambios.

La BPM impone desafíos. Los ejecutivos informan que la barrera individual más grande para el cambio exitoso del proceso de negocios es la cultura organizacional. A los empleados no les gustan las rutinas que no son familiares y a menudo tratan de

resistirse al cambio. Esto es muy cierto para los proyectos en donde los cambios organizacionales son muy ambiciosos y de largo alcance.

### 2.8.3. FACTORES CLAVES DE ÉXITO DE LA BPM

Definimos los factores claves de éxito de la BPM:

- Alineamiento de la estrategia de negocio, cadena de valor y procesos de negocio.
- Establecimiento de metas de las unidades de negocio y de la organización.
- Desarrollo de planes de acción y tácticas de negocio buscando lograr el éxito de las metas organizacionales.
- Patrocinio ejecutivo y gobernanza.
- Designación clara de la propiedad del proceso.
- Establecimiento de métricas, medición y monitoreo de procesos.
- Institucionalización de prácticas, tales como investigaciones de mejora continua, gestión de cambios, controles de cambios.
- Automatización de procesos de negocio y metodologías relacionadas en toda la organización.

## 2.9. EL PENSAMIENTO SISTÉMICO

El pensamiento sistémico es la actividad realizada por la mente con el fin de comprender el funcionamiento de un sistema y resolver el problema que presenten sus propiedades emergentes. Es un modo de pensamiento holístico que contempla el todo y sus partes, así como las conexiones entre éstas.

El pensamiento sistémico integra el pensamiento creativo, el estratégico y el control para lograr que los proyectos se lleven a la práctica. El pensamiento sistémico va más allá de lo que se muestra como un incidente aislado, para llegar a comprensiones más profundas de los sucesos. Es un medio de reconocer las relaciones que existen entre los sucesos y las partes que los protagonizan, permitiéndonos mayor conciencia para comprenderlos, y capacidad para poder influir o interactuar con ellos.

La evolución de la Teoría de Sistemas aplicada a la empresa tiene un claro exponente actual en Peter Senge, quien manifiesta: “La empresa de mayor éxito será algo llamado organización inteligente, la capacidad de aprender con mayor rapidez que los competidores quizá sea la única ventaja competitiva sostenible" (Senge,1992).

El pensamiento sistémico está basado en la dinámica de sistemas y es altamente conceptual. Provee de modos de entender los asuntos empresariales mirando los sistemas en términos de tipos particulares de ciclos o arquetipos e incluyendo modelos sistémicos explícitos (muchas veces simulados por ordenador) de los asuntos complejos. Es un marco conceptual cuya esencia pretende producir una "Metanoia", un "cambio de enfoque" y que nos ayuda de dos formas:

1.- A ver interrelaciones entre las partes más que cadenas lineales de causas y efectos.

2.- A ver los procesos de cambio más que fotografías estáticas.

Su práctica comienza con el concepto de "retroalimentación" (feedback), un concepto que nos muestra cómo las acciones pueden tanto reforzarse como contrarrestarse (o balancear) entre ellas. Ayuda a aprender a reconocer tipos de "estructuras" que se repiten una y otra vez.

> Por último, el pensamiento sistémico permite comprender el aspecto más sutil de la organización inteligente, la nueva percepción de sí mismo y del mundo. En el corazón de una organización inteligente hay un cambio de perspectiva: en vez de considerarnos separados del mundo, nos consideramos conectados con el mundo; en vez de considerar que un factor “externo” causa nuestros problemas, vemos que nuestros actos crean los problemas que experimentamos. Una organización inteligente es un ámbito donde la gente descubre continuamente cómo crea su realidad. (Senge, 1992)

## 2.10. EL MODELO DE LEAVITT

La introducción en la empresa de cambios en su sistema de información fracasa con demasiada frecuencia. Esto es debido casi siempre a que no se han tenido en cuenta los problemas de carácter social o los cambios necesarios en las tareas y en la estructura

organizativa de la empresa. El plan de sistemas ha de ser formulado correctamente, pero tan importante como planificar el cambio es saber implantarlo en forma adecuada. Para tal fin, se han desarrollado modelos de cambios útiles para ser seguidos por las empresas (la implantación de un nuevo plan de sistemas de información no deja de ser un proceso de cambio). De entre éstos, destaca el modelo de Leavitt, que es muy utilizado en procesos de cambio que tenga relación con el sistema de información.

Leavitt (1965) propone un modelo que permite caracterizar a las organizaciones en general, y a los sistemas de información en particular, como un sistema formado por cuatro elementos en interacción: tareas, personas, tecnología y estructura. El modelo de Leavitt se representa en la figura 2.12.

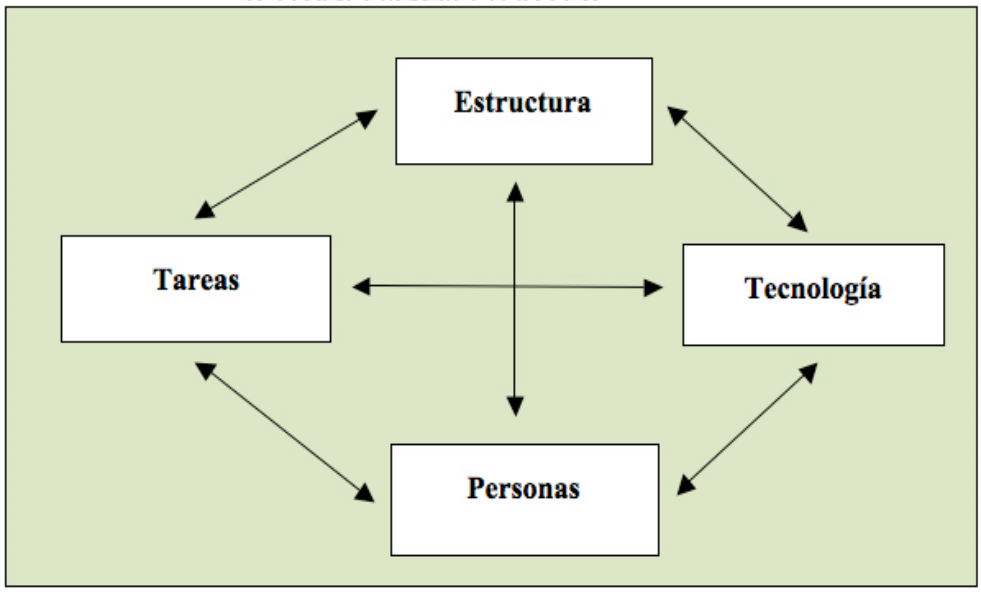



*Figura 2.12*: El diamante de Leavitt.

Las tareas son las razones que justifican la existencia del sistema de información: las personas con las encargadas de realizar las tareas; la tecnología está formada por el conjunto de herramientas que facilitan que las personas puedan realizar las tareas; y la estructura es el marco (síntesis de comunicación, autoridad y flujo de trabajo e información) dentro del cual se realizan las tareas.

> Estos cuatro elementos se encuentran en equilibrio inestable, de tal manera que cuando se altera cualquiera de ellos se inducen cambios, planificados o no, en los restantes. Así, la introducción de las tecnologías de información puede originar cambios en la estructura (en el diseño de puestos, de las unidades organizativas, de los mecanismos de coordinación o del sistema decisor), en las personas (habilidades o actitudes requeridas) y en la definición de las tareas (pueden aparecer nuevas tareas, modificarse las actuales, o incluso, desaparecer tareas actuales). (Arjonilla y Medina,2010)

El Diamante de Leavitt como también se le llama, contribuye a la disminución de la complejidad de la gestión del proceso de implantación de una tecnología. Facilita la identificación sistémica de los componentes afectados por la decisión estratégica de adoptar la nueva tecnología, en consecuencia, contribuye a la formulación de estrategias o lazos retro alimentadores negativos necesarios para bajar la entropía en sus componentes.

## 2.11. LA ESTRUCTURA DE LA UNIVERSIDAD COMO ORGANIZACIÓN

Según Gonzáles y Codagnone (2004), la universidad como organización tiene tres fines fundamentales: El desarrollo de la enseñanza, la investigación y la extensión y por ende en ella se realizan actividades acordes a esos fines. Si tomamos aisladamente cada una de esas actividades para alguna disciplina, podríamos considerar que ellas son posibles de realizar en forma independiente sin requerir ninguna estructura que la contenga. Cuando las especialidades que se desarrollan en una universidad comienzan a crecer en cantidad y en sus propios conocimientos, comienza a surgir la necesidad de darle a la actividad una cierta organización. La historia de las universidades ha tenido como una de sus características el permanente crecimiento de las distintas disciplinas que en ella se desarrollan lo que trajo aparejado una necesaria coexistencia y vinculación entre las tres actividades como así también entre las propias disciplinas, lo que ha traído aparejado una permanente adecuación de los mecanismos que ordenan esa coexistencia y vinculación.

Es por ello que este permanente desarrollo hizo cada vez más compleja esa interrelación entre actividades y disciplinas que llevó a la universidad como organización a requerir una división del trabajo en tareas definidas y la coordinación entre ellas, lo cual originó una nueva actividad que es intrínseca a la organización, la gestión. Esto llevó a la universidad a tener su propia estructura.

## 2.12. PARTES CONSTITUTIVAS DE UNA UNIVERSIDAD

La ubicación de la estructura universitaria, distribuida en núcleos, para las cinco partes fundamentales de una organización definidas por Mintzberg, se simboliza en la figura 2.13:


*Figura 2.13*: Núcleos constitutivos de una organización.

En el ***núcleo de las operaciones*** se agrupan las siguientes unidades:

- Áreas / Cátedras
- Institutos / Centros / Grupos de investigación y/o extensión

De la observación puede inferirse que aquí se concentran el ***núcleo de operaciones*** que constituyen la razón de la existencia de la universidad en sus tres actividades básicas: enseñanza, investigación y extensión.

Al ser esta la parte de la organización que con más notoriedad refleja la eficiencia de ella, es donde se aplica la mayor de las normalizaciones utilizadas en la organización universitaria.

Dada las fuertes transformaciones que las universidades vienen sufriendo, estos núcleos deberán adaptarse a una mayor flexibilidad de sus tareas. Es posible la conformación transitoria de grupos para dar solución a problemas puntuales con una forma de adaptación mutua.

En la ***línea intermedia*** se ubican en un orden de importancia

- Departamentos de facultades
- Escuelas secundarias
- Institutos dependientes de Rectorado
- Escuelas superiores
- Facultades

Todas ellas con sus correspondientes estructuras de gobierno, las cuales por si solas se pueden estudiar como una organización con sus propios núcleos de ***ápice estratégico***, ***línea intermedia*** *y* ***núcleo de operaciones.***

En el ***ápice estratégico*** se ubican:

- Rector
- Consejo Superior
- Asamblea Universitaria

En la generación de estrategias, confluyen la participación de los cuerpos colegiados y unipersonales, siendo clave la capacidad de interpretar cuales son los fines de la organización de modo que esta mantenga su pertinencia para la sociedad que la contiene. Esta parte de la estructura deberá definir temas tan trascendentales tales como cuáles serán sus estudiantes de grado y posgrado en los próximos años, cuáles serán las tendencias económicas y su relación con los tipos y perfiles de los graduados, como deberá ser el

desarrollo de los conocimientos mediante la investigación y como ellos puedan rápidamente transferirlos al medio.

En la gestión, con el contexto que rodea a la organización también resultan clave las capacidades de los cargos unipersonales, pues resulta ser la "cara visible" de la organización.

En el ***Staff de Apoyo***, se encuentra ubicada la estructura administrativa no docente, casi en su totalidad, con sus diversos departamentos, divisiones, etc.

En la ***Tecnoestructura***, se ubican personas o grupos de personas que asesoran en forma permanente o temporaria a las unidades de ápice estratégico. Las personas involucradas en este núcleo pueden pertenecer a la estructura no docente o poseer contratos específicos.

## 2.13. LAS UNIVERSIDADES: ORGANIZACIONES COMPLEJAS

Wissema (2009), analiza a las universidades de los países desarrollados y encuentra seis factores que impulsan el cambio de los modelos de universidad:

1. Competencia: las mejores universidades que quieren continuar llevando a cabo la investigación científica de vanguardia, está buscando alternativas de financiamiento a las que los gobiernos brindaban. Esto las lleva a acercarse a empresas de base tecnológica.
2. Globalización: esta ha generado una gran competencia por contar con los mejores alumnos, los mejores docentes y las empresas interesadas en invertir en investigación y desarrollo en las universidades. Esta competencia ya no es regional, sino mundial.
3. Impulso a la creación de empresas: los gobiernos ya no se interesan en que las universidades se dediquen tan solo a la formación y a la investigación. También esperan que las universidades faciliten la incubación de nuevas empresas o de nuevos emprendimientos de empresas ya existentes.
4. Interdisciplinariedad: tradicionalmente la investigación era mono disciplinaria. En la actualidad, se observa que los científicos trabajan con equipos interdisciplinarios que se centran en áreas específicas de la investigación. Los cursos de posgrado a menudo se conectan a estos equipos de investigación. En este nuevo escenario, el

sistema de facultades puede ser un obstáculo para las actividades interdisciplinarias.

5. La masificación: desde la década de los sesenta, la enseñanza universitaria se ha masificado, lo que ha generado el aumento del gasto por parte de los gobiernos y, en consecuencia, su interés por un mayor control sobre las universidades. Esto ha dado pie a la incorporación de los sistemas de gestión de la calidad y de acreditación de las universidades.
6. El desafío de nuevas instituciones y centros de investigación no universitarios. Se observa que, como ocurrió en el pasado, el desarrollo científico y tecnológico nuevamente evoluciona con mayor rapidez fuera de los ambientes universitarios. Frente a ello, el desarrollo de los emprendimientos en tecnologías de información ofrece oportunidades muy interesantes para que las universidades puedan cerrar esta brecha.

Wissema (2009) plantea que se está en medio de una nueva transición en la forma de ser y actuar de las universidades y propone que están apareciendo lo que él denomina: "universidades de tercera generación". Las de primera generación fueron universidades medievales, orientadas fundamentales a la instrucción y formación; las universidades de segunda generación fueron aquellas que surgieron en el siglo XIX y en particular sustentadas por el modelo alemán, que fomentaba tanto la formación como la investigación. Bajo este esquema, las universidades de tercera generación son aquellas que realizan actividades de formación, investigación e innovación.

## 2.14. SISTEMA UNIVERSITARIO PERUANO

El Congreso de la República aprobó la Ley N° 30220, Ley Universitaria el 03/07/2014, fue promulgada el 08/07/2014 y publicada en el diario Oficial El Peruano el 09/07/2014, entrando en vigencia al día siguiente de su publicación.

El dispositivo legal tiene por objeto normar la creación, funcionamiento, supervisión y cierre de las universidades, sean públicas o privadas, nacionales o extranjeras, que funcionen en el territorio nacional, promoviendo el mejoramiento permanente de la calidad educativa.

La presente Ley se estructura en 16 Capítulos, 133 artículos, 13 Disposiciones complementarias transitorias, 2 Disposiciones complementarias modificatorias, 10 Disposiciones complementarias finales y 1 Disposición complementaria derogatoria.

Los aspectos más resaltantes son los siguientes:

- Se designa al Ministerio de Educación como el ente rector de la política de aseguramiento de la calidad de la educación superior universitaria. Permite a las universidades que conformen redes interregionales; pero deja en claro los principios, fines y funciones de la universidad y el respeto y garantías a la autonomía universitaria; así como a la transparencia que debe tener toda universidad al publicar información (Arts. 1 al 11).

- Se crea la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), como un Organismo Público Técnico Especializado adscrito al Ministerio de Educación, entre sus funciones es el encargado de supervisar la calidad del servicio educativo universitario a nivel nacional y otorgar el licenciamiento a las universidades, el cual será temporal, renovable y con una vigencia de 6 años. Este organismo es competente en el ámbito nacional, público y privado, con la facultad para sancionar a las universidades que realicen infracciones, las cuales serán establecidas en el respectivo Reglamento de Infracciones y Sanciones; además al ser la autoridad central de la supervisión de la calidad establece mecanismos de coordinación y articulación con entidades del Poder Ejecutivo, gobiernos regionales y locales, y finalmente queda fijado su régimen económico y laboral (Arts. 12 al 25).

- Sobre la creación y licenciamiento de universidades, señala la forma de creación de las universidades, y los requisitos básicos que se deben contemplar en los instrumentos de planeamiento para la creación de una institución universitaria como las condiciones básicas para que obtengan su licenciamiento (Arts. 26 al 29).

## 2.15. LAS UNIVERSIDADES EN EL PERÚ

Según Ísmodes (2014), si se revisan los estatutos de las universidades en cualquier parte del mundo, como ya se ha visto para el caso del Perú, es recurrente encontrar tres grandes objetivos. En primer lugar, las universidades se reconocen, en su gran mayoría, como instituciones que forman egresados con una elevada calidad académica. En segundo lugar, identifican a la investigación como un tema inherente a la organización universitaria. Finalmente, consideran como muy importante la labor de proyección social y extensión universitaria.

Es importe analizar que el objetivo principal que se debe buscar en un país, no solo es el crecimiento del PBI, sino el desarrollo humano de sus ciudadanos, para ello se deben formar líderes, emprendedores, innovadores, investigadores, así como invertir de manera eficiente en la generación de conocimiento y en su aprovechamiento, es decir, en actividades de investigación, desarrollo e innovación.

Las universidades son organizaciones, en las que potencialmente, deberían desarrollarse importantes actividades relacionadas con las innovaciones y el desarrollo, y así contribuir al progreso de las industrias y de las empresas; sin embargo, en el Perú, las universidades no destacan por hacer aquello que más necesita el país. Los indicadores, las cifras, los rankings en los que se compara las universidades del Perú con sus pares en el resto del mundo no son alentadores. Por ello es necesario innovar dentro de la universidad, oxigenar el sistema, romper con la endogamia intelectual y para ello es bueno conocer qué han hecho otros, conocer que se ha hecho en el propio país, y tratar de crear un nuevo modelo que permita pasar a una etapa útil y beneficiosa para el país y para la propia comunidad universitaria.

## 2.16. LA COMPETITIVIDAD

Porter (1991) en su libro Ventaja Competitiva de las Naciones explica lo siguiente:
Mi teoría empieza a partir de competidores y sectores individuales y va aumentando hasta la economía como un todo. El sector en particular ... es donde se gana o se pierde la ventaja competitiva. La nación donde radican (dichas ventajas) influye en la capacidad de sus

empresas para triunfar en determinados sectores. El resultado de miles de luchas en sectores individuales determina el estado de la economía de una nación y su capacidad para progresar.

El principal objetivo económico de una nación consiste en crear para sus ciudadanos un nivel de vida elevado y en ascenso. La capacidad para lograrlo no depende de la competitividad, sino de la productividad con que se utilizan los recursos de un país (el capital y el trabajo). La productividad es la eficiencia en el uso de la mano de obra o de capital. Para producir y está relacionada con la calidad y las características de los productos que determinan los precios que se pueden cobrar.

Porter plantea cuatro conceptos, que relacionados entre sí, fomentan el desarrollo de ventajas competitivas para las empresas de algunos sectores. Así se tiene:

- Condiciones de los factores productivos necesarios para la empresa.
- Condiciones de la demanda interna de los productos del sector.
- Existencia se sectores proveedores o conexos de la empresa que sean internacionalmente competitivos, y
- Las condiciones en que se crean, organizan y gestionan las empresas, así como la naturaleza de la rivalidad entre ellas o "estrategia, estructura y rivalidad de la empresa".

Otros dos elementos también influyen en el sistema, pero su influencia se canalizaría a través de algunos de los cuatro elementos presentados: el papel de acontecimientos causales y la política del Gobierno.

## 2.17. LA COMPETITIVIDAD DE LAS UNIVERSIDADES

Las universidades han iniciado un camino, con el desarrollo de políticas activas, que las lleve a ser más eficientes y efectivas, a satisfacer mejor las demandas y expectativas de los ciudadanos con una alta calidad en programas y servicios, a potenciar la mejora continua en la actividad docente, investigadora y de gestión, al tiempo que se asume siempre su

responsabilidad de servicio a la sociedad, fomentando la transparencia, la comparación, la cooperación, la movilidad y la competitividad.

Las universidades buscan la mejora de la eficacia, la eficiencia y la competitividad, compartiendo principalmente tres objetivos: la satisfacción de las expectativas y necesidades de los usuarios y de la sociedad en la que se insertan; orientar la cultura de la organización o institución hacia la mejora continua, la calidad total y la excelencia; y motivar a todo el personal, para que sea capaces de contribuir a la consecución de productos o servicios de alta calidad.

Lane y Owens (2012) mencionan adecuadamente que los pilares de la competitividad se han transformado en forma notable; la discusión en torno al rol que cumplían las universidades en el incremento de la competitividad era mínima. Porter centró su análisis, casi en forma exclusiva, en el papel desempeñado por las firmas en términos de la creación de factores que conducían la economía y que con ello orientaban el quehacer de las universidades, las cuales a su vez buscaban satisfacer las necesidades de la industria. En la actualidad, la universidad norteamericana de investigación ha sido considerada como uno de los factores primarios que dirigen la competitividad económica de la nación.

Las universidades se manifiestan dentro del aumento de la competitividad de los países a través de: 1) brindar conocimiento al gobierno, a empresas grandes privadas y públicas, y en generala todo de tipo de organizaciones; 2) contribuir al soporte de empresas medianas y pequeñas de carácter regional; 3) la revitalización de la comunidad como empleadora de fuerza de trabajo, y con ello, la retención de estudiantes, profesores y personal calificado en general, y 4) producir fuerza de trabajo calificada para la industria local (Trani y Holsworth, 2010).

A medida que la globalización del mundo se extiende y las tecnologías de la información progresan (López, 2016), también se generaliza el uso de rankings y de sistemas de comparación. Entre los sistemas de clasificación más difundidos, aparte del Ranking de Shanghái, se encuentran el QS World University Rankings (publicado por el grupo

Quacquarelli Symonds) y el Ranking Webometrics (publicado por el Laboratorio de internet del Centro de Información y Documentación Científica, CINDOC). En todos estos sistemas de comparación, la información que se utiliza tienen relación con las capacidades de generación y gestión del conocimiento y de la información.

# CAPÍTULO III
# DISEÑO E IMPLEMENTACIÓN DEL MODELO SISTÉMICO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN PROCESOS

## 3.1. DISEÑO DEL MODELO SISTÉMICO DE SEGURIDAD DE LA INFORMACIÓN

El presente trabajo propone un modelo con un enfoque sistémico y dinámico para abordar relaciones complejas dentro de las universidades y, entender el problema de la inseguridad de la información, lograr la sinergia deseada y gestionar la seguridad más efectivamente.

El pensamiento sistémico es actualmente un término ampliamente reconocido que se refiere a examinar cómo interactúan los sistemas, cómo funcionan los más complejos y porqué "el todo es más que la suma de sus partes".

Es importante destacar los resultados positivos que el enfoque sistémico ha logrado en otros campos y es una buena señal de las ventajas que puede contribuir a la seguridad de la información. Las casi siempre significativas fallas de las instituciones para tratar adecuadamente asuntos de seguridad en años recientes se deben, en gran medida, a su incapacidad para formular estrategias de seguridad y presentarla de un modo que sea comprensible y relevante para todas las partes interesadas.

Para ISACA (2009), el uso del enfoque sistémico para la gestión de seguridad de la información ayudará a los gerentes de este campo a tratar ambientes complejos y dinámicos, y generará un efecto beneficioso sobre la colaboración dentro de la empresa, adaptación al cambio operativo, navegación de incertidumbre estratégica y tolerancia del impacto causado por factores externos.

En la figura 3.1 se muestra el Modelo Sistémico de Seguridad de la Información conformada por los siguientes elementos: Diseño y estrategia de la organización, persona, proceso y tecnología. El modelo se describe bajo un enfoque de una organización aprendiente y tiene como base el modelo dinámico organizacional de Leavitt. Todos los elementos del modelo interactúan entre sí. Si una de las partes del modelo es modificada, no es considerada o no es gestionada adecuadamente, es posible que el equilibrio del modelo esté en riesgo.

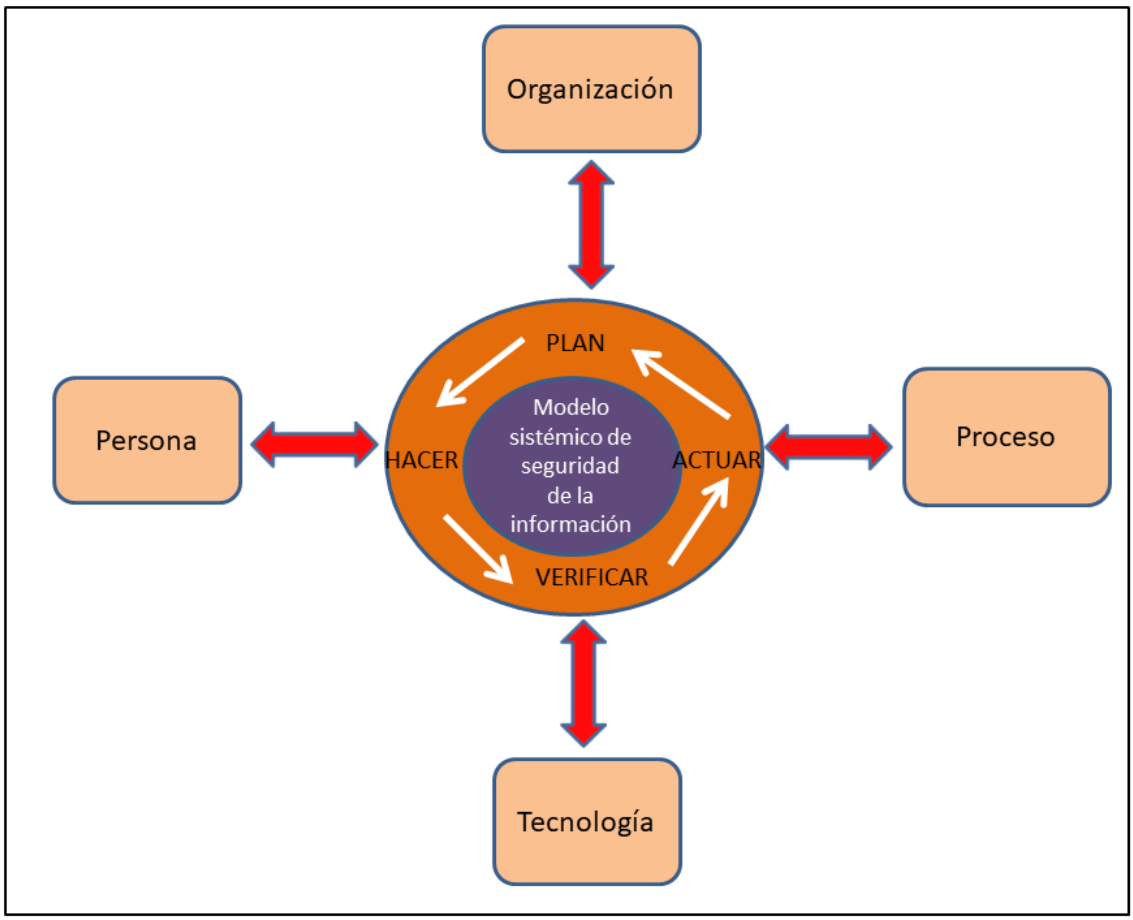



*Figura 3.1*: Modelo Sistémico de Seguridad de la Información.

Este trabajo de investigación presenta una descripción de los elementos que integran el modelo sistémico, las relaciones sistémicas entre ellas, la sinergia, las barreras de aprendizaje que son necesarias para lograr el diseño e instrumentación de cualquier plan de seguridad de la información.

Para que la implementación del Modelo Sistémico de Seguridad de la Información tenga éxito se adopta el ciclo de Deming: "Planear, hacer, verificar, actuar" (PHVA). El ciclo PHVA representa una mejor forma de organizar los cambios o las acciones de mejora en las organizaciones.

### 3.1.1. ELEMENTOS DE MODELO

#### 3.1.1.1. DISEÑO Y ESTRATEGIA DE LA ORGANIZACIÓN

Una organización es una red de personas, activos y procesos que interactúan entre sí con roles definidos y trabajan para alcanzar un propósito común.

Los recursos como personas, equipos, conocimientos, técnicos entre otros, constituyen el principal elemento para diseñar la estrategia. El diseño define la manera en que la organización implementa su estrategia. Los procesos, la cultura de la organización y la arquitectura de información son importantes para determinar el diseño.

Entre los objetivos de la organización están: el establecer un vínculo definido entre las medidas de seguridad tradicionales y la empresa; ofrecer una visión de negocios sobre los riesgos intrínsecos y culturales de cualquier diseño de la organización y si estos riesgos afectan la visión del impacto en la seguridad. Por ejemplo, parte de la visión puede ser: lograr que la universidad sea una de las más seguras del país, pero bajo un enfoque de la seguridad de los activos de información.

Es responsabilidad de la Dirección los siguientes aspectos:

- Determinar políticas de seguridad de la información.
- Establecer roles y responsabilidades para la seguridad de la información.
- Proporcionar los recursos suficientes para desarrollar, implementar, operar y mantener la gestión de seguridad de la información.
- Verificar que los recursos de la organización se utilicen con responsabilidad.
- Decidir el criterio para la aceptación del riesgo, los criterios de aceptación deben estar claramente definidos y documentados.

- Asegurar que todo el personal relevante esté consciente de la importancia de sus actividades de seguridad de la información, para ello la Dirección debe realizar programas de capacitación, conocimiento y capacidad del personal.

### 3.1.1.2. PERSONAS

Define quién implementa cada parte de la estrategia. Las personas dentro de una organización tienen sus propias creencias, valores, comportamientos y tendencias que surgen de sus personalidades y experiencias.

Para entender cómo afecta la seguridad de la información, y se ve afectada por las personas, es necesario que deben aprender a trabajar en conjunto alineado al pensamiento sistémico para ocasionar la interacción de las personas con el resto de los elementos del modelo. Las personas tienen que poseer las destrezas cognoscitivas y las actitudes proactivas y reactivas para resolver los problemas de seguridad, además el diálogo y la discusión deben estar permanentemente presentes, así todos estos atributos determinan un perfil que genera sinergia.

La cultura de la seguridad de la información puede definirse como una subcultura de la cultura organizacional, conformada por valores éticos y actitudes, las tradiciones, creencias, hábitos, las normas, los procedimientos, y todo lo que permita identificar la madurez de la institución en la gestión de la seguridad de la información.

Las políticas de seguridad de la información y los valores éticos son elementos básicos para crear la cultura de la seguridad de la información en las universidades, son las condiciones iniciales que ayudan a la protección de los activos de información de una universidad.

Es fundamental asegurar que los empleados entienden sus responsabilidades y si son convenientes para los roles para los que se les considera:

- Estrategias de reclutamiento (acceso, verificación de antecedentes, entrevistas, acuerdos contractuales, roles y responsabilidades).
- Aspectos relacionados con el empleo (ubicación de la oficina, acceso a herramientas y datos, capacitación y concienciación, proceso disciplinario).
- Término de relaciones laborales (razones de la desvinculación, momento de salida, roles y responsabilidades, acceso a los sistemas, acceso a otros empleados).

Por otra parte, los estudiantes, docentes, investigadores y proveedores, y las partes interesadas, entre otros, pueden tener una fuerte influencia sobre la universidad y se deben considerar dentro de la postura de seguridad.

### 3.1.1.3. PROCESOS

Para ISACA (2009), los procesos incluyen mecanismos formales e informales (grandes y pequeños, simples y complejos) para realizar las tareas y proporcionar un vínculo vital con todos los elementos del modelo. Los procesos identifican, miden, gestionan y controlan el riesgo, la disponibilidad, la integridad y la confidencialidad, además de asegurar la responsabilidad. Son resultado de la estrategia e implementan la parte operacional del elemento organización.

Es importante resaltar que los procesos tienen que estar documentados y ser comunicados de forma adecuada a los recursos humanos apropiados y ser revisados periódicamente, una vez establecidos, para asegurar su eficiencia y eficacia en la organización.

Las organizaciones actuales están orientadas a los procesos de negocio, y así una organización ejecutará unos determinados procesos para poder sobrevivir. Si alguno de estos procesos falla de forma considerable, durante el día a día, se debilita la seguridad global, y la organización también se somete a un riesgo determinado, también global. Cada proceso para ser ejecutado en forma correcta, completa y continua, necesita una gestión determinada para que las personas de la organización puedan ejecutarlo satisfactoriamente con una técnica o tecnología concreta y bajo unas condiciones de entorno establecidas.

En las universidades, los procesos manejan información crítica como la concerniente a estudiantes, como son: registro de calificaciones, proceso de matrícula, aula virtual entre otros, que puede ser confidencial y estar propensa a amenazas de alteración, divulgación no autorizada y sustracción.

Para Viloria y Blanco (2009), el riesgo de materializarse un ataque que provenga de la Internet o desde el interior de la misma institución aumenta si no se aplican los correctivos a tiempo, hace que participen los procedimientos de seguridad, que es la instrumentación de las políticas de seguridad de la información, asociados a las características de la universidad, a las tecnologías de la información y, en consecuencia, a los procesos. Por último, los procedimientos que ejecutan los miembros de la comunidad universitaria son para proteger los recursos informáticos, activos de la organización, y son diseñados en función de la tecnología de la información y de los sistemas existentes, ya que los procesos están sumergidos en las relaciones entre los tres componentes de un modelo básico de seguridad: procedimientos, personas y la tecnología.

#### 3.1.1.4. TECNOLOGÍA

Conformada por todas las herramientas, aplicaciones y la infraestructura que incrementan la eficiencia de los procesos. La tecnología incluye todas las aplicaciones técnicas del conocimiento utilizado en la organización y es un factor crítico para alcanzar su misión.

La implementación de un sistema de información en la red, o la adopción de aplicaciones intranet o extranet, altera el equilibrio aparente de una organización, por ello es necesario implementar una serie de estrategias en cada elemento de este modelo, así el sistema se auto organiza y evoluciona a otra estructura más compleja. En el caso de las universidades, son víctimas de ataques desde la intranet o extranet, y acarrean los mismos problemas de la Internet como es la inseguridad de la información. Cuando el impacto ha tenido éxito, y comprometa la seguridad de un activo crítico, entonces se desencadena a la vez un ataque a una serie de recursos asociados al árbol de activos de este bien informático. Es así, que

el modelo sistémico contempla las metodologías estratégicas bajo una perspectiva de la seguridad de la información que integren el análisis y gestión de riesgos entre sus procesos.

Los mecanismos de seguridad como: el cifrado, la firma digital certificada, el intercambio de autenticación entre otros; en el modelo sistémico se utilizan para garantizar los servicios de seguridad como la integridad, la autenticación, la disponibilidad, el no repudio, el control de acceso y la confidencialidad. Cabe resaltar que la seguridad de la información no termina con la implementación las herramientas de seguridad, sino hay un monitoreo permanente con los cambios que ocurren en el entorno interno y externo, como, por ejemplo, las nuevas modalidades de ataque o las diversas variaciones de la ingeniería social.

La tecnología suele ser considerada por la Dirección como un instrumento para resolver las amenazas y los riesgos de seguridad. Aunque los controles técnicos son útiles para mitigar ciertos tipos de riesgos, la tecnología no debe ser vista como una solución de seguridad de la información.

Los usuarios y la cultura de la organización tienen un alto grado de influencia sobre la tecnología. Por su naturaleza, las personas aún desconfían de ella o se han resistido a los cambios organizacionales, sea cual fuere la razón los encargados de seguridad de la información deben estar prevenidos de que muchas personas intentarán burlar los controles técnicos.

### 3.1.2. MODELO SISTÉMICO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN PROCESOS PARA UNA UNIVERSIDAD

Una organización a partir de la definición de su misión y visión, debe establecer estrategias de negocio coherentes que la lleven alcanzar sus objetivos, y como parte de esta estrategia definir el sistema que garantice la protección de la información de la información usada en cualquiera de los procesos de negocios y a través de cualquiera de los mecanismos tecnológicos o humanos que la traten.

El modelo sistémico de seguridad de la información cumple con los requisitos básicos de seguridad de la información como son la preservación de la confidencialidad, integridad y disponibilidad de la información dentro de una organización como se puede apreciar en la figura 3.2.

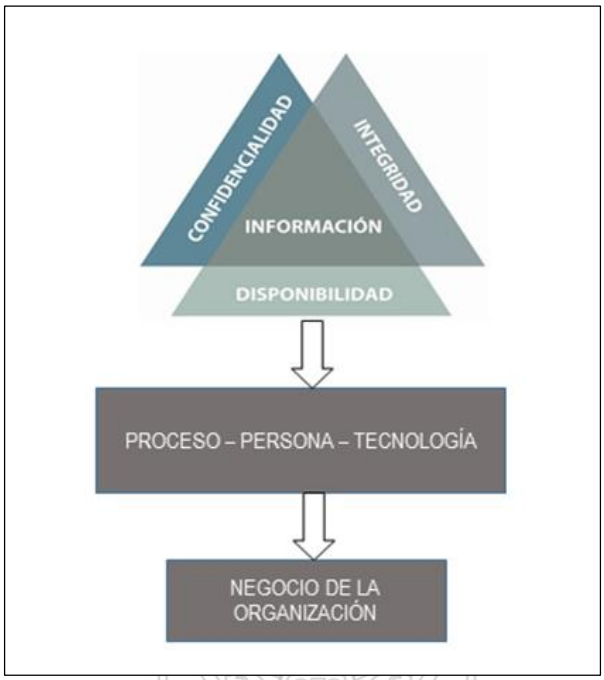



*Figura 3.2*: Requisitos básicos de seguridad de la información.

Estos principios de seguridad son muy importantes para aplicar y administrar el riesgo operacional a los procesos, a las personas y a la tecnología de acuerdo a las necesidades del negocio, y así lograr el cumplimiento del objetivo de la organización.

La forma que las organizaciones tienen que gestionar el grado de cumplimiento de la estrategia es a través de la definición de controles viables para ser implementados por la organización y embebidos como parte de los procesos.

Por otro lado, la seguridad de la información compromete a todos, y la manera de entenderlo de manera práctica en la organización, es situarla en casi todos los procesos empresariales, difundiéndola en las personas, direccionando responsabilidades e integrándola en los flujos de trabajos internos y en los sistemas de información empresariales.

Una organización necesita identificar y gestionar muchas actividades a fin de funcionar eficazmente. Cualquier actividad que utiliza recursos, y que se gestiona para permitir que los elementos de entrada se transformen en resultados, se puede considerar como un proceso. El Modelo Sistémico de Seguridad de la Información adopta un enfoque basado en procesos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información de una organización.

La Figura 3.3 muestra como el modelo sistémico está concebido para que tome como entrada los requisitos y expectativas de seguridad de la información provenientes de las partes interesadas como son: estudiantes, docentes, investigadores, empleados y otros, y a través de las acciones y procesos necesarios, produce los resultados de seguridad de la información que cumplen esos requisitos y expectativas y ofreciendo de esta manera "calidad" en la seguridad de la información.

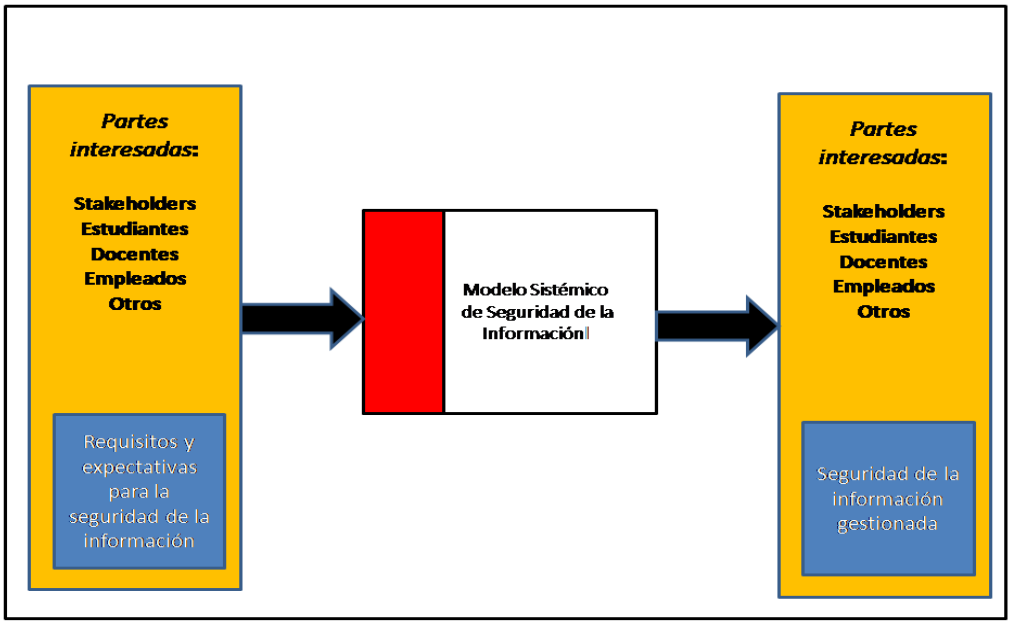



*Figura 3.3: Modelo Sistémico de Seguridad de la Información basado en procesos.*

Para conseguir que las partes interesadas sean proactivos y no reactivos y que las organizaciones reaccionen de manera eficiente y rápida, y se garantice en todo momento la seguridad de la información, es automatizar los procesos como son los sistemas BPM, esto se puede implementar para que realicen los controles automáticamente y a través de reglas

de negocio estén evaluando los valores de los mismos contra la métrica establecida en tiempo real, ganando en fiabilidad, control, costos, eficiencia y agilidad.

Ante las necesidades cambiantes del entorno y las amenazas del manejo de la información en la universidad, el modelo sistémico de seguridad de la información tiene como alcance identificar los activos de información, hacerles un análisis y evaluación de riesgos, asegurar la continuidad de los procesos de negocio, prevenir y responder ante cualquier incidente de seguridad y brindar servicios seguros y de calidad a la comunidad universitaria.

### 3.1.3. MAPA DE PROCESOS DE UNA UNIVERSIDAD

Para adoptar un enfoque basado en procesos en una organización es necesario saber cuáles son los procesos que deben aparecer en la estructura de procesos del sistema, después hay que definirlos a fin de establecer las interrelaciones entre los mismos, para ello se construye el mapa de procesos.

La Universidad Privada San Juan Bautista (UPSJB) es una institución de educación superior universitaria, de carácter privado, que plantea el uso de orientaciones pedagógicas para favorecer un cambio cualitativo de la sociedad a través del impacto de sus egresados en el desarrollo de la misma.

La mejora de la gestión institucional se orienta a satisfacer las necesidades de los clientes (estudiantes, docentes, investigadores, egresados y empleados), es por ello que la UPSJB ha implementado la gestión por procesos, que es un elemento central de un sistema de calidad, catalizador de la demanda ciudadana. Además, la gestión por procesos constituye una efectiva estrategia de gestión, porque fortalece la capacidad para lograr resultados que contribuyan a mejorar la competitividad funcional de las instituciones educativas.

En la figura 3.4, se presenta el mapa de procesos de UPSJB.

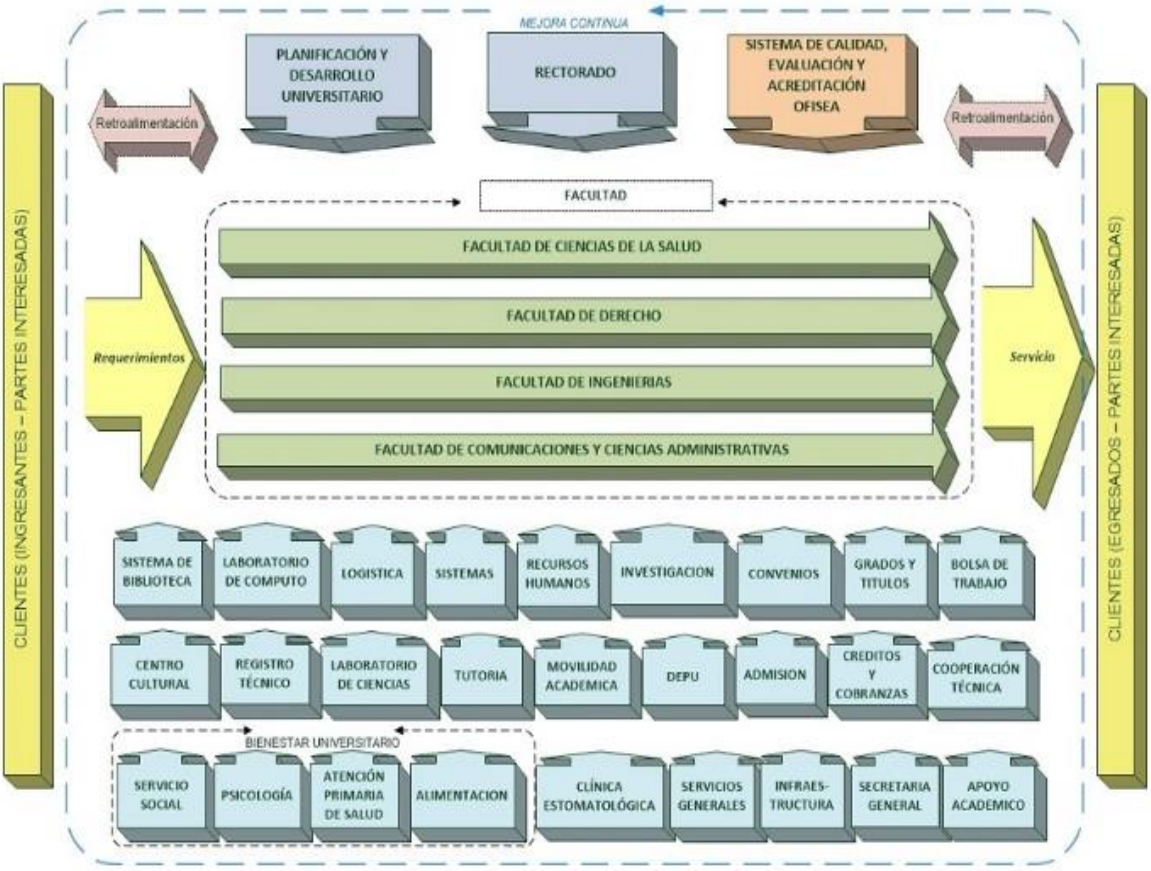



*Figura 3.4*: Mapa de procesos de la UPSJB.

En el presente trabajo de investigación, se hace énfasis al proceso: Registro Técnico porque es un proceso crítico que brinda múltiples servicios académicos y administrativos a los estudiantes, y como tal está propenso a riesgos de seguridad de la información.

### 3.1.4. PROCESO: REGISTRO TÉCNICO

El proceso Registro Técnico tiene como objetivo brindar servicios de apoyo a las áreas académicas y administrativas en el registro y actualización de la información con un servicio de calidad, que beneficie a la comunidad universitaria. En la figura 3.5 se muestra el diagrama del proceso. Los subprocesos que lo conforman son: Planificación y Administración Académica, Matrícula, Registro y Control de Situación Académica y Registro y Control de Documentos.

Dentro de las actividades que cumple Registro Técnico se tienen las siguientes:

- Apertura del semestre académico.
- Registro de las asignaturas según programación académica.
- Codificación de planes curriculares.
- Registro de matrícula de ingresantes.
- Emisión y entrega de constancia de ingreso.
- Mantener actualizado los historiales académicos y base de datos de los estudiantes.
- Verificar y controlar la actualización de datos de los sistemas de información como la matrícula en línea, las calificaciones del estudiante por la plataforma virtual.

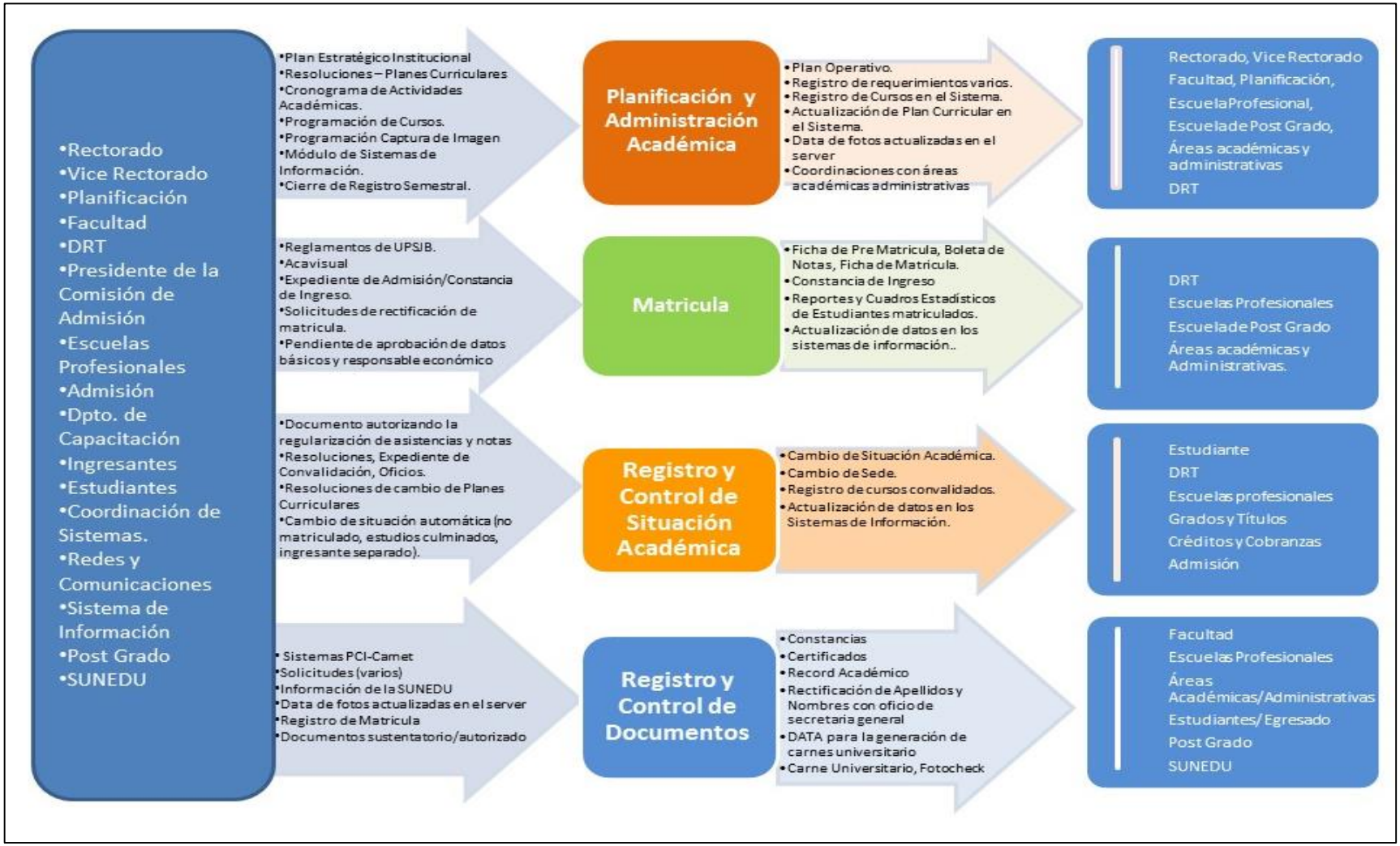



*Figura 3.5*: Diagrama de proceso de Registro Técnico

### 3.1.4.1. GESTION DE CALIFICACIONES DEL ESTUDIANTE

La gestión de calificaciones del estudiante, realizada por las unidades académicas de la universidad, está propenso a los incidentes de seguridad como puede ser la manipulación de calificaciones por los mismos estudiantes. Este incidente se presenta por la falta de control y por las vulnerabilidades presentadas en los sistemas de información. Por tanto, se ha visto en la necesidad de proteger el activo: **calificaciones del estudiante** de las amenazas a la seguridad de la información.

La gestión de calificaciones del estudiante involucra la participación de los siguientes actores del negocio: las escuelas profesionales, los docentes, Registro Técnico y los estudiantes.

A continuación, se desarrolla el procedimiento de gestión de calificaciones del estudiante:

1. **ROLES Y RESPONSABILIDADES**

   Involucra a los actores de negocio que intervienen en la gestión de calificaciones del estudiante con sus funciones y responsabilidades.

**Tabla 3.1**
*Roles y Responsabilidades. Gestión de calificaciones del estudiante*

| Roles | Responsabilidades |
|---|---|
| Escuela Profesional | Registra la programación de los horarios de las asignaturas y la programación de los horarios de los docentes. |
| Docente | Registra las calificaciones de los estudiantes de su asignatura en la plataforma virtual. |
| Registro Técnico | Se encarga de brindar servicios académicos y administrativos a los estudiantes, entre ellos la gestión de sus calificaciones. |
| Estudiante | Consulta su calificaciones en la plataforma virtual y también solicita documentos académicos y administrativos. |

2. **FLUJO DE ACTIVIDADES Y TAREAS**

   a. Flujo de actividades

   Se representa en la figura 3.6.

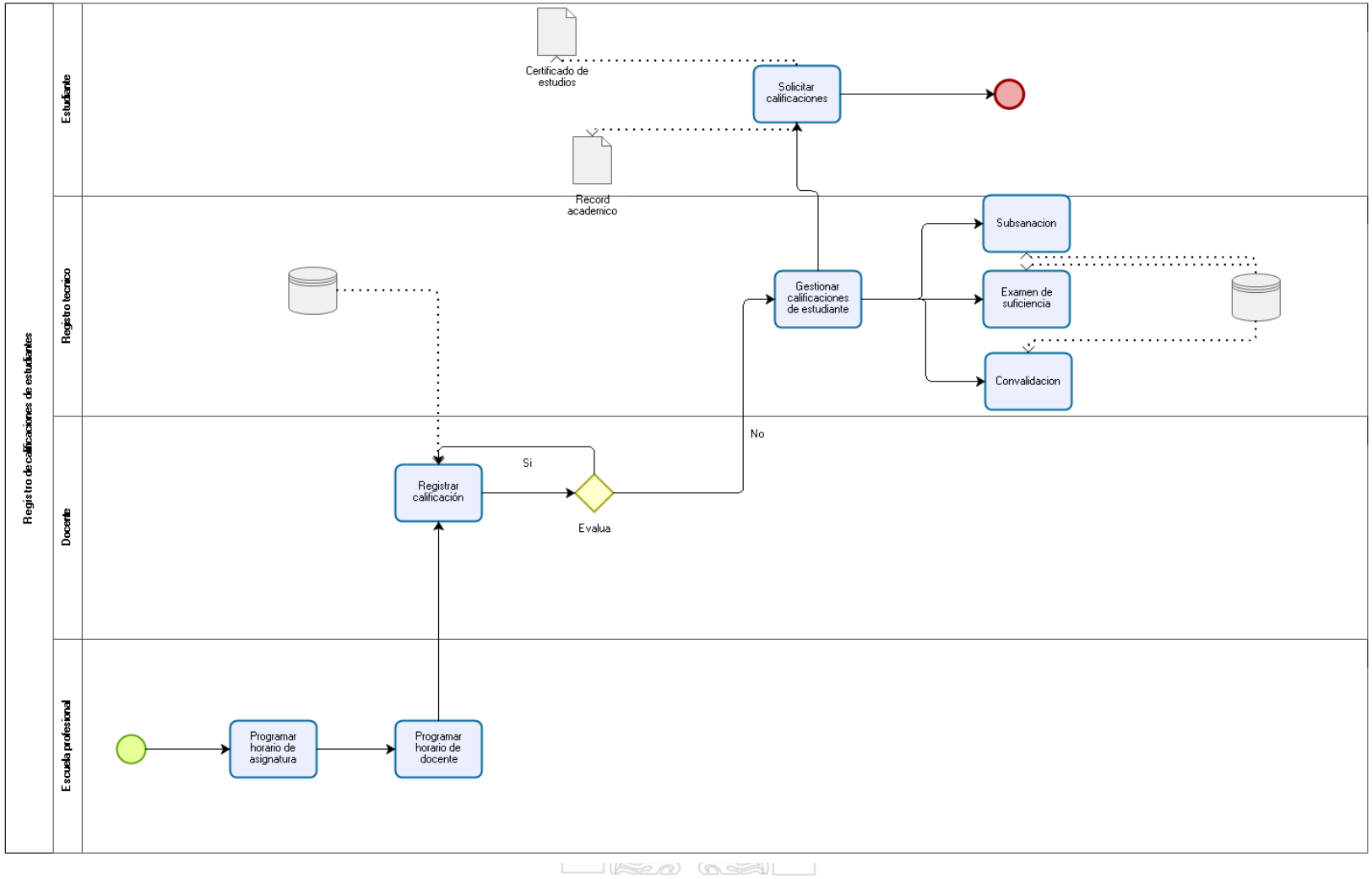



*Figura 3.6*: Registro de calificaciones del estudiante.

b. Descripción de las tareas

En la tabla 3.2 se desarrollan las tareas donde intervienen los actores del negocio.

**Tabla 3.2**
*Tareas. Gestión de calificaciones del estudiante*

| Actividades | Tareas |
|---|---|
| Programar horario de asignatura | Una vez registrada la programación académica de un semestre, las escuelas profesionales se encargan de programar los horarios de sus asignaturas un mes antes del inicio del semestre académico |
| Programar horario de docente | Luego programan los horarios de sus docentes en las asignaturas respectivas. |
| Registrar calificación | El docente tiene un código y contraseña para ingresar a la plataforma virtual. Las calificaciones de su asignatura que registra son almacenadas en la base de datos académica. |
| Gestionar calificaciones del estudiante | El departamento de registro de técnico se encarga de gestionar las calificaciones a través de las actas finales de las asignaturas que los docentes han cerrado al término del semestre académico. También se encargan de registrar calificaciones de procesos de convalidación, subsanación y exámenes de suficiencia. |
| Subsanación | Registro de calificación de estudiante por el examen de subsanación. |
| Examen de suficiencia | Registro de calificación Examen de suficiencia para que el estudiante pueda culminar sus estudios. |
| Convalidación | Registro de calificación de asignaturas convalidadas. |
| Solicitar calificaciones | El estudiante solicita record académico de sus asignaturas, boleta de calificaciones, certificados de estudios y otros documentos relacionados con las calificaciones de estudiantes. |

## 3.2. IMPLEMENTACIÓN DEL MODELO SISTÉMICO DE SEGURIDAD DE LA INFORMACIÓN

En el modelo sistémico de seguridad de la información, los procesos deben reflejar cómo se implementa lo que fue definido en la estrategia de la organización, por lo tanto, deben reflejar de qué forma interviene el recurso humano, la información y la tecnología, y establecer sobre ellos los controles a realizar.

En el modelo se plantea los siguientes procesos:

- Gestión de políticas de seguridad de la información
- Proceso de gestión de inventario y clasificación de activos de información
- Proceso de gestión del riesgo
- Proceso de gestión de incidentes

### 3.2.1. GESTIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad tienen como objetivo proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.

Las políticas de seguridad de la información de la universidad es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Los sistemas de información deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.

Las Políticas de Seguridad de la Información de la universidad se basan en las normas de seguridad NTP-ISO/IEC 17799 2007 y también se ha tomado como referencia las políticas de seguridad de la información de otras universidades.

### 3.2.1.1. POLÍTICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

**1. Organización Interna**

- La alta dirección debe definir, aprobar, publicar y comunicar políticas de seguridad de la información a los empleados y terceros, asignar roles y responsabilidades y controlar la implementación de la seguridad de la información.

**2. Relación con terceras partes**

- Cuando la universidad requiere los servicios de terceros debe estar respaldada con los requisitos legales como las obligaciones contractuales relevantes a proveedores de servicios y con la aprobación del departamento de Asesoría Legal de la universidad.
- Cuando es necesario permitir el acceso que terceros tendrán a la información y el procesamiento de información desde los procesos de negocio, se debe identificar los riesgos como la conexión a la base de datos o acceso a los sistemas de información.

### 3.2.1.2. POLÍTICAS DE ADMINISTRACION DE ACTIVOS DE INFORMACIÓN

**1. Propiedad de la información**

- La Dirección de Sistemas debe proteger los activos de información y asegurar un adecuado manejo de los sistemas de información de la universidad.
- Todos los recursos de procesamiento de la información de las diferentes áreas académicas y administrativas están sujetos a revisiones periódicas por parte de Auditoría Interna.

**2. Administración y protección de la Información**

- Deben asignarse responsabilidades a los usuarios que usan los activos de la universidad respaldado con una documentación.
- Los usuarios tienen prohibido de compartir carpetas en sus estaciones de trabajo y dentro de la red.
- Los usuarios al momento de retirarse de sus oficinas, así sea por 5 minutos deben bloquear sus equipos de cómputo.
- Está prohibido divulgar información confidencial de la universidad y copiar programas de software a terceros sin autorización, estas faltas pueden motivar sanciones administrativas y hasta acciones legales.
- La Dirección de Sistemas debe establecer herramientas de control y monitoreo para proteger la información que se encuentra en los recursos informáticos (portátiles y estaciones de trabajo) y sistemas de información que están bajo su custodia.

**3. Uso adecuado de los activos de información.**

- Todos los equipos y demás recursos informáticos son asignados a un usuario responsable, quién debe hacer un uso aceptable de los mismos y no para uso personal o ajenas a la universidad.
- En caso de presentarse una falla o problema al recurso informático, el usuario no debe tomar acciones por sí mismo, sino debe llamar al Soporte Técnico de la Dirección de Sistemas.
- La Gerencia de Logística se encarga de recepcionar estaciones de trabajo, impresoras y servidores del proveedor, controla las cantidades recibidas y verifica las especificaciones técnicas del fabricante. También se encarga de despachar estos equipos a la Dirección de Sistemas.
- La Dirección de Sistemas es la única área autorizada para el ingreso o salida de los recursos informáticos, de tal manera que tiene que ser comunicada con anticipación cuando hay un traslado de equipos a otros locales y el área de

Seguridad debe hacer un seguimiento y control adecuado de éstos.

- Se debe clasificar y establecer procedimientos de marcado a los recursos de información de acuerdo a la necesidad y grado de protección.
- Se debe tener actualizado el inventario de los equipos informáticos y éstos deben tener una etiqueta física.

### 3.2.1.3. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

**1. Antes del empleo**

- Todos los empleados de la universidad antes de ingresar o reingresar a la institución deben firmar la "Declaración Jurada de Confidencialidad" (Anexo 1) según estable el Reglamento Interno de Trabajo
- La Gerencia de Recursos Humanos es la encargada de asegurar que todos los empleados de la universidad conozcan los acuerdos contractuales y sus responsabilidades en el uso de los recursos de información de la universidad.
- La universidad debe asegurarse que los empleados y terceros acepten los términos y condiciones referentes a la seguridad de la información y el grado de acceso a los sistemas y recursos de información.

**2. Durante el empleo**

- Todos los empleados de la universidad, y cuando fuera relevante, los terceros deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la universidad.
- Debe haber un proceso disciplinario correcto y justo contra los empleados que hayan cometido infracción grave a la seguridad de la información.

**3. Terminación o cambio de empleo**

- A los empleados se les debe comunicar sobre las responsabilidades y deberes de la seguridad de la información luego de la terminación o cambio de empleo.
- Los empleados y terceros deben retornar software, documentos, manuales y equipos informáticos de la universidad cuando termine su empleo o contrato.
- Para evitar cualquier acceso desautorizado dentro de la universidad, el personal de Seguridad debe acompañar al empleado del retiro de ésta.

### 3.2.1.4. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

**1. Condiciones eléctricas y ambientales**

- Se debe vigilar permanentemente las condiciones ambientales que pueden tener un impacto negativo a los equipos de procesamiento de información.
- Sólo personal especializado debe realizar la reparación de equipos eléctricos, redes eléctricas, cableado de datos para asegurar su continua disponibilidad e integridad.
- En cuanto a los extinguidores, deben contar con la capacidad adecuada, fácil acceso y peso; y se deberá recargar periódicamente según el tiempo estimado por el proveedor.
- Se recomienda instalar un sistema de alimentación ininterrumpida, en inglés uninterruptible power suply (UPS) y se debe revisar regularmente de acuerdo a las recomendaciones del fabricante.

**2. Control de acceso a los Centro de Datos**

- Los Centro de Datos deben contar con un sistema de control de acceso basado en la utilización de tarjetas inteligentes y con la instalación de cámaras de video vigilancia.

- Las áreas y el entorno donde se encuentran los Centros de Datos, deben ser áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad, controles de entrada y acceso apropiados para prevenir la exposición a riesgos.
- Se debe contar con controles de acceso para el ingreso de personal al Centro de Datos. Los tipos de accesos son:

  **Acceso directo** que se otorga a los administradores de servidores y al personal de Redes y Comunicaciones.

  **Acceso autorizado** que se otorga al personal que requiere ingresar eventualmente, pero debe figurar en la lista autorizada.

  **Acceso especial** que se otorga excepcionalmente a personal diverso y por lo tanto requiere autorización expresa del responsable de Centro de Datos.

**3. Seguridad de oficinas e instalaciones de la universidad**

- Todo personal debe tener puesto en un lugar visible un fotocheck o carné que los identifique como empleados de la universidad.
- Las visitas que ingresen a la universidad, deben ser identificados y se debe registrar la fecha, hora de entrada y salida. Deben llevar puesta de alguna forma un carné que los identifique.
- Las áreas académicas y administrativas con atención a la comunidad universitaria y público en general, deben permanecer cerradas.
- Las oficinas e instalaciones donde se maneje información confidencial deben estar cerradas y se debe monitorear durante las 24 horas del día.

### 3.2.1.5. POLÍTICAS DE GESTIÓN DE LAS OPERACIONES Y COMUNICACIONES

**1. Seguridad de las operaciones**

- Se debe elaborar guías e instructivos para una mejor administración del sistema como: prendido y apagado de la computadora, copia de seguridad, reparación de equipos, manejo de correos entre otros.

- Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.
- Se debe monitorear y revisar los servicios de proveedores de seguridad.
- El empleado debe tener conocimiento sobre la protección del software antivirus, por ello no está autorizado a cambiar o eliminar la configuración del software en su equipo.

**2. Protección frente a software malicioso**

- Si detecta alguna infección de virus informático y no se logra erradicarlo, notificar al área de Redes y Comunicaciones.
- Los empleados de la universidad, están prohibidos de instalar y ejecutar software en equipos de la universidad que no hayan sido autorizados por la Dirección de Sistemas.
- Si los empleados requieran algún programa del tipo gratuito, la Dirección de Sistemas debe evaluar los riesgos y verificar la existencia de virus antes de usarlos.
- Antes de descargar un archivo adjunto de un correo electrónico debe comprobar que no contiene virus.
- Se debe instalar y actualizar frecuentemente los softwares de detección y reparación de virus. Periódicamente se tiene que hacer un control preventivo a los equipos informáticos.

**3. Gestión de almacenamiento y respaldo de la información**

- La extensión y frecuencia de los respaldos de información debe reflejar las necesidades de la universidad como es la criticidad de la información.

- Los respaldos de información deben estar almacenados en una locación remota de tal forma que se obtenga un plan de contingencia cuando hay un desastre en la sede principal.
- Se prohíbe el almacenamiento y compartición a través de la red, de archivos de música y video, cuando estos no sean utilizados en sus actividades laborales y funciones asignadas.

**4. Gestión del uso de las comunicaciones electrónicas (correo electrónico)**

- Queda terminantemente prohibido la descarga de archivos (software gratuito) de tipo ejecutable, comprimidos, de música y videos en todo su formato pues pueden contener virus, spyware y malware en general.
- Se debe contar con una solución de Filtro de Contenido Web para restringir la navegación de páginas web prohibidas y para reducir la infección por descarga de archivos y software de internet.
- Cuando se detecte una infección o ataque en progreso, el usuario será responsable por los daños del software y/o hardware causados por dicha infección.
- Se debe utilizar el correo institucional para fines de trabajo, los empleados bajo ningún motivo lo pueden usar para fines personales que puedan comprometer la imagen de la universidad.

**5. Seguridad en los servicios de internet**

- El acceso al programa de FTP (Protocolo para la transferencia de archivos) no está autorizado para los usuarios.
- El acceso remoto a las estaciones de trabajo dentro de la red está permitido sólo al personal de la Dirección de Sistemas de Información, el resto de los usuarios de la red tienen esta funcionalidad deshabilitada.

- El acceso a los servicios restringidos de la red (Youtube, Facebook, etc.) deberá ser solicitado por el gerente, director del área usuaria, al que pertenece el usuario.
- El intercambio de software incluyendo descargas de archivos y ejecución de programas desde el Internet, debe estar restringida a las actividades necesarias para la operación del negocio de la universidad.

**6. Uso de periféricos**

- Está prohibido que el usuario pueda instalar o conectar cámaras web, cámaras digitales, grabadoras de sonido, impresoras, scanner entre otros. Si se presenta un requerimiento extra, tendrá que solicitarlo a Soporte Técnico.
- Los medios removibles como CD, DVD, USB, CINTAS, etc. que almacenen información sensible y cuando han dejado de ser necesaria, se destruirán de forma segura ya sea incinerándolas, triturándolas o borrando sus datos.

### 3.2.1.6. POLÍTICAS DE CONTROL DE ACCESO

**1. Gestión de accesos de cuentas de usuario y contraseñas**

- La creación de una cuenta de acceso al dominio interno de la universidad es factible para todo el personal al momento de adquirir vínculo laboral con la misma.
- Para acceder al sistema operativo se tiene controladores de Dominio que autentican a los equipos cuando éstos inician una sesión e ingresan a la red de la universidad.
- La conexión será validada sólo si el usuario ha ingresado todos los datos solicitados: usuario y contraseña, y se registra en el visor de eventos de los Controladores de Dominio su intento de ingreso.

- La desactivación de una cuenta de acceso a los recursos de la red de la UPSJB, se realizará de manera automática cuando al usuario se ha dado de baja en el Sistema de Recursos Humanos. Para los casos en que un usuario haga uso de su período de descanso físico (vacaciones), esté de licencia (por salud, maternidad, etc.), o se ausente de la universidad por un período de tiempo, se procederá de manera automática con la suspensión temporal de su cuenta de dominio y del servicio de correo electrónico durante el período de su ausencia.
- El usuario será el único responsable de la administración de su cuenta y su contraseña. Queda terminantemente prohibido dar a conocer a terceras personas la cuenta de usuario y contraseña por ser de carácter personal e intransferible.
- Para garantizar la confidencialidad de la información, el formato y sintaxis de cada contraseña es la siguiente: No puede tener menos de 8 caracteres, combinación mínima obligatoria de letras mayúsculas, letras minúsculas y números.
- Las contraseñas no deben ser palabras comunes o simples variaciones del nombre del usuario, servidor o compañía.
- Los empleados, estudiantes, docentes y egresados pueden reestablecer sus contraseñas en cualquier momento.
- Es una mala práctica, pegar post-it con las contraseñas en el monitor o debajo del teclado.

**2. Control y mantenimiento de los derechos de acceso**

- Cuando a un usuario se le otorga una cuenta para garantizar el acceso a los sistemas y servicios de información debe responsabilizarse de sus acciones con la consistencia de la política de seguridad de la universidad.
- Se permite el acceso remoto a los servicios de la red vía el sistema VPN (Virtual Private Network), en la cual los datos y la información viajan sobre canales de acceso cifrados. Se autoriza el acceso remoto por VPN en horarios definidos y exclusivamente para labores de administración de sistemas, aplicaciones y

servicios críticos de la universidad, únicamente a usuarios autorizados por la Dirección de Sistemas.

- Se debe establecer horarios de conexión y el tipo de información a la cual es posible acceder remotamente.
- Se permite el uso de laptops o aparatos para conectarse a la red de la universidad con los controles necesarios.
- Se debe revisar periódicamente los accesos de los recursos y servicios de red a los usuarios externos para los cuales han sido autorizados y por la vigencia de tiempo establecida.
- Se deben aplicar medidas de protección a los dispositivos de la red para la protección y acceso de los mismos y para evitar que usuarios no autorizados puedan modificar las configuraciones establecidas.
- Los accesos autorizados para administración de servidores, dispositivos de red, bases de datos y sistemas de información sólo deben otorgarse a aquellas personas que son directamente responsables a la administración de los recursos informáticos y sistemas de información.
- La universidad debe establecer redes de datos segmentadas tanto en el área académica como administrativa.
- El Administrador de las Bases de Datos es la persona autorizada para que pueda tener acceso a los datos sin hacer uso de las aplicaciones o programas.
- Se debe contar con controles apropiados como una fuerte autenticación y métodos criptográficos cuando la comunidad en general hace uso de los servicios inalámbricos.

### 3.2.1.7. POLÍTICAS DE ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

**1. Requisitos de seguridad de los sistemas**

- Los requerimientos para la adquisición o desarrollo de sistemas de información o software, deberán comprender requisitos de seguridad de la información

como controles de autenticación de usuarios en base a contraseñas, configuración de permisos a los usuarios, herramientas para control de versiones, plataforma del sistema operativo, navegadores web, un sistema de gestión de base de datos, librería de componentes que usan los sistemas entre otros.

- Se deben usar metodologías para el análisis y diseño de los sistemas, pues son las buenas prácticas de seguridad para la construcción de software.
- La información sobre servicios de aplicaciones que fluye sobre redes públicas debe ser protegida de actividad fraudulenta o divulgación no autorizada.

**2. Seguridad de las aplicaciones del sistema**

- Los usuarios que usan sistemas de información son responsables del ingreso de los datos.
- Se deben establecer validaciones a los datos que son ingresados a los sistemas de información, que garanticen la calidad de la información.
- La universidad debe establecer y proteger ambientes de desarrollo seguros para la integración de los sistemas que cubre todo el ciclo de vida de desarrollo del sistema.
- El proceso de migración de datos cuando hay cambios de sistemas de información debe ser revisada y aceptada por los usuarios que lo usan.
- Las pruebas de funcionalidad de la seguridad deben ser llevada a cabo durante el desarrollo.
- La Dirección de Sistemas debe establecer herramientas para la gestión de calidad de software para los sistemas de información, las actualizaciones y nuevas versiones.
- Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados por la Dirección de Sistemas.

**3. Uso de controles criptográficos**

- La información sensitiva de la universidad debe ser almacenada y/o transmitida bajo técnicas de cifrado con el propósito de salvaguardar su confidencialidad y para proteger la integridad de los mensajes.
- Se debe identificar el nivel requerido de protección y, de acuerdo con ello, elegir el tipo de algoritmo de cifrado.
- Se debe usar técnicas criptográficas para proteger las claves secretas y evitar que se distribuyan sin autorización. Estas técnicas deben tener en cuenta las regulaciones y restricciones de su uso tanto a nivel nacional como si aplica en otros países del mundo.

**4. Seguridad en los procesos de desarrollo y soporte**

- El acceso a los programas de códigos fuente por parte de los programadores deben ser controlados y autorizados por el Jefe de Desarrollo de Sistemas.
- Al introducir nuevos sistemas de información y cambios mayores al sistema existente debe seguir un proceso formal de documentación, especificación, prueba e implementación. Este proceso debe asegurar que no se comprometa los procedimientos de control y que se debe tener una aprobación para cualquier cambio.
- Los sistemas de información o software no pasan a producción sino es aprobado por Control de Calidad y con la aceptación del usuario.
- Los parches de software deben ser aplicados para reducir las vulnerabilidades de los sistemas de información, asegurando que no haya impacto adverso en las operaciones o en la seguridad de la universidad.
- Los procedimientos de control de cambios deben estar respaldado por el mantenimiento de un control de versiones de toda la actualización de software.
- Las modificaciones a los paquetes de software deben ser limitadas a los cambios necesarios y deben pasar por un control estricto.

**5. Gestión de vulnerabilidades**

- Se debe tener con anticipación un inventario de los sistemas de información utilizados con la identificación de sus vulnerabilidades técnicas.
- La Dirección de Sistemas debe tomar en cuenta las principales funciones para la administración de vulnerabilidades como son: el test a la programación, el monitoreo en la configuración de los sistemas de información, el seguimiento de activos, el monitoreo de los servicios de los equipos de los fabricantes y cualquier otra responsabilidad coordinada.
- Se debe realizar un análisis de vulnerabilidades y pruebas de penetración para prevenir los riesgos asociados a los sistemas de información.

### 3.2.1.8. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

**1. Reportes de eventos y debilidades de la seguridad de la información**

- Es responsabilidad de todos los empleados de la universidad y terceros que usan los sistemas de información, advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a la seguridad de la información de los sistemas o servicios.
- Los eventos de seguridad deben ser reportados tan rápido como sea posible, a través de Mesa de Ayuda, quien lo canalizará con el área de Desarrollo de Sistema o con el proveedor de software.
- Los incidentes de seguridad de la información que impliquen una acción legal, deben ser reportadas a las autoridades correspondientes.

**2. Gestión de las mejoras e incidentes en la seguridad de información**

- Cuando ocurra el incidente de seguridad, Mesa de Ayuda, debe comunicarse con los afectados o implicados sobre los planes a seguir.
- Todos los incidentes de seguridad deben ser evaluados de acuerdo a su

criticidad. Si es necesario, una vez evaluado el incidente se deben aplicar sanciones disciplinarias contra la persona que cometió la falta.

- La evaluación de los incidentes en la seguridad de la información debe permitir la implementación de controles adicionales y reducir la probabilidad o impacto de incidentes futuros.

### 3.2.2. PROCESO DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Para el proceso de inventario de activos se requiere activar, valorar y clasificar los activos de información más importantes de la universidad, y así darles el tratamiento adecuado.

Se realizó un trabajo documental que estuvo apoyado por trabajos previos, y procedimientos en forma manual y electrónica. El trabajo de campo estuvo conformado por el personal que labora en la Dirección de Sistemas de Información (DSI), quiénes realizaron visitas guiadas a las instalaciones de la universidad para el levantamiento de la información.

#### 3.2.2.1. ALCANCE

El alcance de esta investigación son los activos de información con que cuenta la universidad. Muchos de estos activos están bajo la custodia de la Dirección de Sistemas de Información, la cual para el logro de sus objetivos cuenta con 3 departamentos: Desarrollo de Sistemas, Redes y Comunicaciones, Soporte Técnico, quiénes se encargan de brindar servicios de tecnología y comunicaciones.

#### 3.2.2.2. IDENTIFICACIÓN DE ACTIVOS

Una vez definido el alcance, según Magerit (2012), se procedió a identificar los activos con que cuenta la universidad:

1. DATOS/INFORMACION

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

a. Ficheros propios de la universidad.
   - Registro de calificaciones, registro de asistencias, títulos y grados académicos, estado de cuenta e historia clínica de los estudiantes, ficha personal de los docentes, registro de pagos de matrículas y pensiones de estudiantes, nómina de empleados y docentes, entre otros.

b. Copias de respaldo
   - Backup de las bases de datos, código fuente y código ejecutable.

c. Credenciales (contraseñas)
   - Registradas en el Active Directory del controlador de dominio

d. Registro de actividad
   - El registro y control de los logs de todos los servidores.

e. Código fuente
   - Código fuente de desarrollo propio y subcontratado a medida.

f. Código ejecutable
   - Código ejecutable de desarrollo propio y de terceros.

g. Datos de prueba
   - El test con datos de prueba se realiza en el servidor de Desarrollo.

2. CLAVES CRIPTOGRAFICAS

La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

a. Certificados de clave pública

- Certificado digital de los sitios web de Intranet, correo electrónico y documentos digitales (boletas de pagos).

3. SERVICIOS

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

a. Al público en general

- Estudios de pregrado, posgrado y educación a distancia.
- Admisión, Centro Pre-universitario, Extensión Profesional, Idiomas.
- Residentado médico, consultorio jurídico gratuito, servicio de atención de especialidades médicas

b. Interno (a usuarios de la propia organización)

- Intranet académica y administrativa.
- Servicio de laboratorio de cómputo y Ciencias
- Bienestar social
- Servicio de biblioteca

c. World Wide Web
d. Acceso remoto a cuenta local
e. Correo electrónico
f. Almacenamiento de datos
g. Transferencia de archivos

4. SOFTWARE - APLICACIONES INFORMÁTICAS

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

**Tabla 3.3**
*Software-aplicaciones informáticas*

| Tipo | Descripción |
|---|---|
| a. Desarrollo propio (in house) | • Página del portal institucional, intranet académica y administrativa, aula virtual de estudiantes, docentes y coordinadores académicos, aplicación móvil de estudiantes, sistema de admisión, sistema de Biblioteca, sistema integrado y administrativo (SIA). |
| b. Subcontratado | • Sistemas de Planillas y Gestión de Recurso Humanos, Contabilidad, Almacén, Compras, Activo Fijo, Caja y Bancos y Cuentas por Pagar. |
| c. Navegador web | • Internet explorer de Microsoft<br>• Google Chrome de Google<br>• Mozila Firefox |
| d. Software para servidor de aplicaciones | • Visual Studio 2008<br>• Foxpro 2.6 para Dos<br>• Telerik Portion Of Ultimate Collection. |
| e. Software para servidor de correo electrónico | • Microsoft Exchange Server 2010 |
| f. Sistema de gestión de base de datos | • Microsoft SQLServer Enterprise Server 2012<br>• MySQL |
| g. Ofimática | • Office Profesional de Microsoft<br>• Adobe Creative Cloud Educativo y Comercial<br>• CorelDraw Graphics Suites |
| h. Antivirus | • ESET NOD 32 Antivirus End point |
| i. Sistema Operativo | • Windows Server 2012 y 2008 para servidores y Windows 8, 7 y Xp para pcs.<br>• Windows phone, Android, iOS para dispositivos móviles |
| j. Sistema de backup | • Data Protector Manager, System Center |

## 5. HARDWARE - EQUIPAMIENTO INFORMATICOS

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

**Tabla 3.4**
*Hardware-equipamientos informáticos*

| Tipo | Descripción |
|---|---|
| a. Controlador de dominio | • HP DL-360G5, Xeon Core 2Duo 3.0 Ghz, 8.0 GB |
| b. Servidores de correos | • HP DL-380e G8, Xeon Quad Core 2.20 Ghz, 16.0 GB |
| c. Servidores de aplicaciones | • HP DL-380 G5, Xeon Core 2.67 Ghz, 16.0 GB |
| d. Servidores web/Intranet | • HP DL-360p G8, Xeon 6 Core 2.3 Ghz, 16.0 GB |
| e. Servidores de base de datos | • Virtual HP (2x4) Core, 32GB |
| f. Servidor Sistema de backup | • Virtual HP Xeon 2.6 Ghz (2x2) Core, 8 GB |
| g. Servidor antivirus | • Virtual HP (2x2) Core, 4 GB |
| h. Terminal server | • Virtual HP (2x2) Core, 8 GB |
| i. Computadoras personales | • Computadoras HP y compatibles |
| j. Equipo virtual | • Servidor Blade HP BL-460c G8.Sist. Oper. Vmware Esxi 5.5.50 |
| k. Periféricos (Medios de impresión, escáneres) | • Impresoras HP |
| l. Soporte de la red (cortafuegos) | • SWITCH, Cisco |
| m. Centralita telefónica | |

## 6. REDES DE COMUNICACIONES

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

a. Red telefónica
b. Red de datos
c. Red inalámbrica (Servicio Wifi)
d. Red local
e. Internet

7. SOPORTES DE INFORMACIÓN

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

a. Discos
b. Almacenamiento en red
c. Memorias USB
d. DVD
e. Tarjeta de memoria
f. Material impreso

8. EQUIPAMIENTO AUXILIAR

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

a. Sistemas de alimentación ininterrumpida (ups)
   - Ups EATON 15 KVA
b. Generadores eléctricos
   - Grupo electrógeno PERKINS 27KW
c. Equipos de climatización
   - Split ducto CARRIER 60,000 BTU/Hr.

9. INSTALACIONES

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

a. Edificio
   - Av. José Antonio Lavalle s/n (Ex Hacienda Villa), Chorrillos
   - Av. San Luis 1923 – 1925, San Borja
   - Av. Carlos Izaguirre 216 - 230 – Independencia

- Av. Carretera Panamericana Sur Ex km. 300, La Angostura, Subtanjalla. Ica
- Calle Albilla s/n Urbanización Las Viñas, (Ex Toche). Chincha.

b. Vehículos

- Automóvil Sedan, Mazda año 2010, color azul.
- Camioneta rural, Mitsubishi año 2010, color beige metálico.
- Microbus, King Long color blanco.
- Omnibus Iveco año 2010, color blanco.
- Camión Baw año 2010, color blanco.
- Camioneta Pick Up, Nissan año 1991, color gis acero metálico.
- Ambulancia clase CMTApanel, Peugeot, año 2005, color blanco.

10. PERSONAL

En este epígrafe aparecen las personas relacionadas con los sistemas de información.

a. Usuarios externos
b. Usuarios internos: estudiantes, docentes, investigadores y personal administrativo
c. Director de Sistemas de Información
d. Jefe de Desarrollo de Sistemas
e. Jefe de Redes y Comunicaciones
f. Jefe de Soporte Técnico
g. Administrador de base de datos
h. Analistas programadores
i. Personal de Mesa de Ayuda
j. Proveedores

### 3.2.3. PROCESO DE GESTIÓN DEL RIESGO

Es necesario evaluar los riesgos a los cuales pueden estar sometidos los activos de información de tal forma que permita descubrir y planificar las medidas oportunas para mantener los riesgos bajo control en la universidad.

Este análisis y evaluación de riesgos es importante porque permitirá mantener la continuidad de los procesos críticos que soportan los activos a resguardar. También contribuirá a mejorar la calidad y confiabilidad de los programas de software.

Comprende las actividades de: análisis de riesgos, evaluación y tratamiento del riesgo.

#### 3.2.3.1. ANÁLISIS DE RIESGOS

**1. Tasación de activos**

Es necesario tasar su valor para proteger apropiadamente los activos en términos de importancia a la gestión académica y administrativa de la universidad.

En la tabla 3.5 se muestra los activos más importantes sujetos a una protección apropiada. La tasación de los activos se procedió en términos de su impacto con relación a su confidencialidad, integridad y disponibilidad. Cada activo se tasó, utilizando una escala de Likert. El valor 1 significa “muy poco”, 2 “poco”, 3 “medio”, 4 “alto” y 5 “muy alto”.

**2. Identificación de amenazas**

Una amenaza para poder causar daño a un activo debe estar asociada a una vulnerabilidad en el sistema, aplicación o servicio.

Según Magerit (2012), “Una amenaza es la indicación de un potencial evento no deseado”.

En la universidad, se realizaron reuniones con las personas encargadas de estos activos con la finalidad de explorar las principales amenazas por cada activo de información.

**Tabla 3.5**
*Tasación de activos de información*

| Activos | Confidencialidad | Integridad | Disponibilidad | Total |
|---|---|---|---|---|
| Títulos y grados académicos | 3 | 5 | 5 | 4 |
| Certificados de clave pública | 3 | 3 | 4 | 3 |
| Servidor Sistema de backup | 5 | 5 | 3 | 4 |
| Servidor Web/Intranet | 3 | 3 | 3 | 3 |
| Calificaciones del estudiante | 5 | 5 | 5 | 5 |
| Servidor de correos | 4 | 5 | 5 | 5 |
| Cableado (cable eléctrico, fibra óptica) | 2 | 2 | 5 | 3 |
| Red Inalámbrica | 4 | 5 | 5 | 5 |
| Desarrollo propio | 4 | 5 | 5 | 5 |
| Estado de cuenta de estudiantes | 4 | 5 | 4 | 4 |

## 3. Identificación de vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

En la tabla 3.6, se muestra los activos de información con sus amenazas y vulnerabilidades.

**Tabla 3.6**
*Activos de información. Amenazas y vulnerabilidades*

| Activos | Amenazas | Vulnerabilidad | Propietario | Proceso | Tipo |
|---|---|---|---|---|---|
| Títulos y grados académicos | Inundaciones, sismos. | Falta de seguridad física, ubicación propensa a inundaciones. | Jefe de oficina | Grados y Títulos | Físico |
| Certificados de clave pública | Phishing. | Todas las páginas no cuenta con certificados de seguridad | Administrador de redes | Sistemas | Digital |
| Servidor Sistema de backup | Fallas en los medios de almacenamiento. Inundaciones, sismos. | Carencia de control de copiado, no existen equipos apropiados para el copiado | Administrador de redes | Sistemas | Digital |
| Servidor Web/Intranet | Intrusos, virus y/o programas maliciosos | Falta de herramientas para detectar vulnerabilidades. | Administrador de redes | Sistemas | Digital |
| Calificaciones del estudiante | Estudiantes manipulan calificaciones usando ingeniería social y software key logger | Protección de seguridad débil, política de seguridad inadecuada | Jefe de Oficina | Registro Técnico | Digital |
| Servidor de Correos | Intrusos, virus y/o programas maliciosos | Software desactualizado mal configurado | Administrador de redes | Sistemas | Digital |
| Red inalámbrica | Intrusos | Bajo nivel de encriptación de la señal wi-fi. Pérdida de conectividad | Administrador de redes | Sistemas | Digital |
| Desarrollo propio | SQL inyector, intrusiones, hacking | Carencia de pruebas de software adecuada | Jefe de Desarrollo de Sistemas | Sistemas | Digital |
| Cableado (cable eléctrico, fibra óptica) | Caída de energía, fallas en las líneas de red | Gestión de red inadecuada | Administrador de redes | Sistemas | Digital |
| Estado de cuenta de estudiantes | Acceso a los estados de cuentas de estudiantes usando ingeniería social y software key logger | Protección de seguridad débil, política de seguridad inadecuada | Gerente de Finanzas | Finanzas | Digital |

Para realizar la evaluación, se recomienda preparar una escala que permita medir los niveles de riesgo. Los criterios que usualmente se recomiendan para determinar los niveles de riesgo son:

- Impacto económico del riesgo
- Posible explotación de la vulnerabilidad
- Probabilidad de ocurrencia del riesgo

En la tabla 3.7 se puede observar el vaciado del análisis y evaluación del riesgo realizado. La valoración del riesgo del activo se obtiene de la suma del impacto económico del riesgo, la posible explotación de la vulnerabilidad y la probabilidad de ocurrencia del riesgo dividido entre 3.

Siguiendo la metodología, se aprecia que la mayoría de los activos que se encuentran en la DSI son activos de información considerados de alto riesgo, con los cuales habría que identificar sus respectivos controles.

**Tabla 3.7**
*Análisis y Evaluación de riesgo*

| Activos | Amenazas | Vulnerabilidad | Posible explotación vulnerabilidad | Impacto económico Valor activo | Posible ocurrencia | Total riesgo |
|---|---|---|---|---|---|---|
| Títulos y grados académicos | Inundaciones, sismos. | Falta de seguridad física, ubicación propensa a inundaciones. | **4** | **4** | **3** | **4** |
| Certificados de clave pública | Phishing. | Todas las páginas no cuenta con certificados de seguridad. | **4** | **3** | **4** | **4** |
| Servidor Sistema de backup | Fallas en los medios de almacenamiento. Inundaciones, sismos. | Carencia de control de copiado, no existen equipos apropiados para el copiado | **4** | **4** | **3** | **4** |
| Servidor Web/Intranet | Intrusos, virus y/o programas maliciosos. | Falta de herramientas para detectar vulnerabilidades | **5** | **5** | **4** | **5** |
| Calificaciones del estudiante | Estudiantes manipulan calificaciones usando ingeniería social y software key logger. | Protección de seguridad débil, política de seguridad inadecuada. | **5** | **4** | **5** | **5** |
| Servidor de Correos | Intrusos, virus y/o programas maliciosos | Software desactualizado mal configurado | **4** | **3** | **3** | **3** |
| Red inalámbrica | Intrusos | Bajo nivel de encriptación de la señal wi-fi. Pérdida de conectividad | **4** | **5** | **4** | **4** |
| Desarrollo propio | SQL inyector, intrusiones, hacking | Carencia de pruebas de software adecuada | **4** | **5** | **5** | **5** |
| Cableado (cable eléctrico, fibra óptica) | Caída de energía, fallas en las líneas de red | Gestión de red inadecuada | **4** | **3** | **3** | **3** |
| Estado de cuenta de estudiantes | Acceso a los estados de cuentas de estudiantes usando ingeniería social y software key logger | Protección de seguridad débil, política de seguridad inadecuada | **5** | **4** | **3** | **4** |

### 3.2.3.2. TRATAMIENTO DEL RIESGO

En el caso de los activos pertenecientes a la universidad, una vez efectuado el análisis y evaluación, se propuso mitigar los riesgos encontrados en los activos de información de acuerdo a los siguientes criterios:

- MUY ALTO RIESGO: *Calificaciones del estudiante* tiene que ser íntegra porque refleja su desempeño y record académico, *Servidor web/Intranet* por tratarse de los servicios que se brinda a la comunidad universitaria a través de aplicaciones web y el *Desarrollo Propio* porque las aplicaciones tienen que tener la seguridad de ser usados por la comunidad universitaria y el público en general.

- ALTO RIESGO*: Títulos y grados académicos, certificado de clave pública, servidor sistema de backup, red inalámbrica y estado de cuenta de estudiantes*. Es muy importante la aplicación de controles apropiados para estos activos.

- MEDIANO RIESGO: *Servidor de correos y cableado*. Se le consideró un riesgo aceptable, por ser evaluado como un riesgo medio y visualizarlo compatibles con las políticas de la organización.

**Enunciado de aplicabilidad:** Es un documento donde se incluye los objetivos de control para mitigar los riesgos identificados. En la Tabla 3.8 se muestra a nivel de ilustración un enunciado de aplicabilidad como producto del análisis y evaluación de riesgo efectuados a los activos de la universidad.

**Tabla 3.8**
*Enunciado de aplicabilidad*

| *Activos* | *Plan de acción* |
|---|---|
| Títulos y grados académicos | Tener ambientes físicos más seguros, sin humedad ni demasiada luz para preservar la documentación.<br>Reubicar el ambiente en una zona donde no esté propensa a desastres naturales como inundaciones, terremotos entre otros |
| Certificados de clave pública | Implementar certificados digitales de seguridad. Evitar el acceso no autorizado. Minimizar los incidentes de seguridad |
| Servidor Sistema de backup | Implementar un sistema de copias de respaldo que garantice la reversión de información. Implantar planes para la recuperación de operaciones |
| Servidor Web/Intranet | Evitar la interrupción de servicios y la contaminación de software malicioso. Controlar el acceso a la información |
| Calificaciones del estudiante | Políticas sobre la gestión de los usuarios, tanto para los docentes como estudiantes. Sensibilización sobre el manejo de información. Implementar herramientas que detecten software malicioso como los keylogger. |
| Servidor de Correos | Programas de mantenimiento preventivo y correctivo adecuados. Actualización y configuración permanente. Evitar el acceso físico no autorizado |
| Red inalámbrica | Implementar técnicas de cifrado seguro. Limitar la cobertura de señal de red de Wi-Fi |
| Desarrollo propio | Implementar estándares y metodologías en el desarrollo de software. Implementar mejores prácticas de seguridad. |
| Cableado (cable eléctrico, fibra óptica) | Implementar estándares de seguridad. Minimizar pérdida de conectividad. Seguridad, confiabilidad e integridad de los datos |
| Estado de cuenta de estudiantes | Políticas sobre la gestión de los usuarios, tanto para los empleados como para los estudiantes. Sensibilización sobre el manejo de información. |

### 3.2.4. PROCESO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El objetivo principal de este proceso es definir acciones que permitan manejar adecuadamente los incidentes a través de un esquema que involucra actividades de manera cíclica: preparación, detección y análisis, contención y actividades post incidentes para evitar la ocurrencia nuevamente del incidente. Este proceso es fundamental para la medición de la efectividad de los controles implementados siempre y cuando los incidentes sean relacionados con los controles que debieron impedir su ocurrencia.

Se ha tomado como documento aplicable del proceso: el procedimiento de atención de incidentes de seguridad.

#### 3.2.4.1. PROCEDIMIENTO DE ATENCIÓN DE INCIDENTES DE SEGURIDAD

**a) Propósito y alcance**

**i. Propósito**

El presente procedimiento tiene como propósito asegurar que los eventos e incidentes de seguridad de la información sean comunicados para permitir tomar acciones correctivas a tiempo y brindar una gestión efectiva de los incidentes de seguridad de la información.

**ii. Alcance**

A todas las unidades académicas y administrativas de la universidad.

## b) Roles y Responsabilidades

**Tabla 3.9**
*Roles y Responsabilidades. Gestión de incidentes de seguridad*

| Roles | Responsabilidades |
|---|---|
| Usuarios | Informan a Mesa de Ayuda cada vez que sospeche o tenga certeza de un incidente de seguridad de la información. Comprende el personal administrativo y académico |
| Mesa de Ayuda | Recibe reporte, resuelve el incidente si está dentro de su alcance. Clasifica, contiene e informa del incidente de seguridad de la información |
| Equipo de Manejo de Incidentes | Monitorean infraestructura, revisan logs, contienen y resuelven los incidentes de seguridad; Está conformado por los responsables de monitoreo y operación de sistemas |
| Proveedor | Especialista en incidentes de seguridad de la información. Se solicita sus servicios cuando no puede ser resuelto internamente |

## c) Descripción de tareas

En la tabla 3.10 se definen las actividades y tareas del procedimiento de atención de incidentes de seguridad.

**Tabla 3.10**
*Tareas. Gestión de incidentes de seguridad*

| Actividades | Tareas |
|---|---|
| Reporta incidente de seguridad | El reporte de un incidente de seguridad se puede dar por 2 fuentes: por los usuarios de las áreas académicas y administrativas y por la misma Dirección de Sistemas. |
| Revisar el incidente – Nivel 1 | Mesa de ayuda registra el incidente: fecha y hora del incidente, propietario del activo, información de contacto, descripción del incidente, sistemas y unidades afectadas. Resuelve el incidente, de lo contrario reporta al equipo de manejo de incidentes |
| Revisar el incidente – Nivel 2 | El equipo de manejo de incidentes determina el tipo de incidente para ello se presenta en el Anexo 2 una "Guía para la clasificación de incidentes de seguridad" y se toma en cuenta la criticidad del incidente. Accede a los log y registros de información disponible para construir una línea de tiempo y determinar la traza de las acciones sucedidas. El equipo de manejo de incidentes resuelve el incidente, de lo contrario lo escala a un proveedor, especialista en seguridad. |
| Documenta la base de conocimiento | Si Mesa de ayuda o el equipo de manejo de incidente resuelve el incidente es necesario documentar la base de conocimiento para tener en cuenta las lecciones aprendidas y la forma en que se resolvió el incidente. |
| Escala-Nivel3 | El proveedor especialista en seguridad de la información analiza y resuelve el incidente de seguridad. |
| Revisar el informe | Si el proveedor no resolviera el incidente, el equipo de manejo de incidentes revisa el informe del proveedor. |
| Cerrar el incidente | Con el informe técnico, Mesa de Ayuda se encarga de cerrar el incidente de seguridad. |

# CAPÍTULO IV
# ANÁLISIS DE RESULTADOS Y CONTRASTACIÓN DE HIPÓTESIS

## 4.1. ANÁLISIS DE RESULTADOS

Lo que se va mostrar es el rendimiento del proceso de gestión de incidentes de seguridad de la información, que es un proceso clave en los reportes de incidentes de seguridad que se presentan en la gestión académica y administrativa con los usuarios que manejan activos de información en la universidad.

En los procesos de negocio donde se suscitan los incidentes de seguridad, éstos tienen la misma oportunidad de conformar el grupo de control y el grupo experimental. En primer lugar, para el grupo de control, se ha procedido a los indicadores de rendimiento tomando en cuenta la situación actual de cómo se responde ante los incidentes de seguridad de la información. En segundo lugar, para evaluar los resultados del grupo experimental se ha diseñado un Modelo Sistémico de Seguridad de la Información basado en BPM con el que se logrará reducir y responder en menos tiempo los incidentes de seguridad.

Para los dos grupos se ha diseñado el modelamiento del proceso de gestión de incidentes de seguridad de la información usando la herramienta llamada Bizagi, y luego se ha simulado el comportamiento del proceso.

### 4.1.1. GRUPO DE CONTROL

Aplicando la herramienta Bizagi, se ha calculado el tiempo de espera de cada una de las actividades que conforman tal proceso. Se ha calculado el tiempo promedio de duración en responder a los incidentes de seguridad y se han eliminado tiempos improductivos e innecesarios.

En la figura 4.1 se muestra el diagrama del procedimiento de Atención de Incidentes de Seguridad de la Información, conformado por los actores del negocio: los usuarios de los procesos, el personal de sistemas, el equipo de mesa de ayuda y el proveedor (especialista en seguridad de la información); y las tareas donde intervienen.

Como se aprecia en el diagrama cuando se origina un incidente de seguridad, el usuario académico o administrativo reporta el incidente de seguridad a mesa de ayuda, quiénes se encargan de documentar y reportar el incidente de seguridad al equipo de sistemas. Ellos verifican que, si el incidente ya está registrado, informan el estado del incidente al usuario, y si no está registrado, entonces tienen que analizar el incidente; una vez resuelto informan a mesa de ayuda y se cierra el incidente, de lo contrario proceden a escalar a un proveedor. Cabe resaltar que el equipo de Sistemas no cuenta con personal especializado en seguridad de la información, pero igual, se toma al personal idóneo para resolver el incidente de seguridad. Si el proveedor no lo resuelve, el equipo de sistemas revisa su informe técnico, y finalmente mesa de ayuda se encarga de cerrar el incidente e informar al usuario.

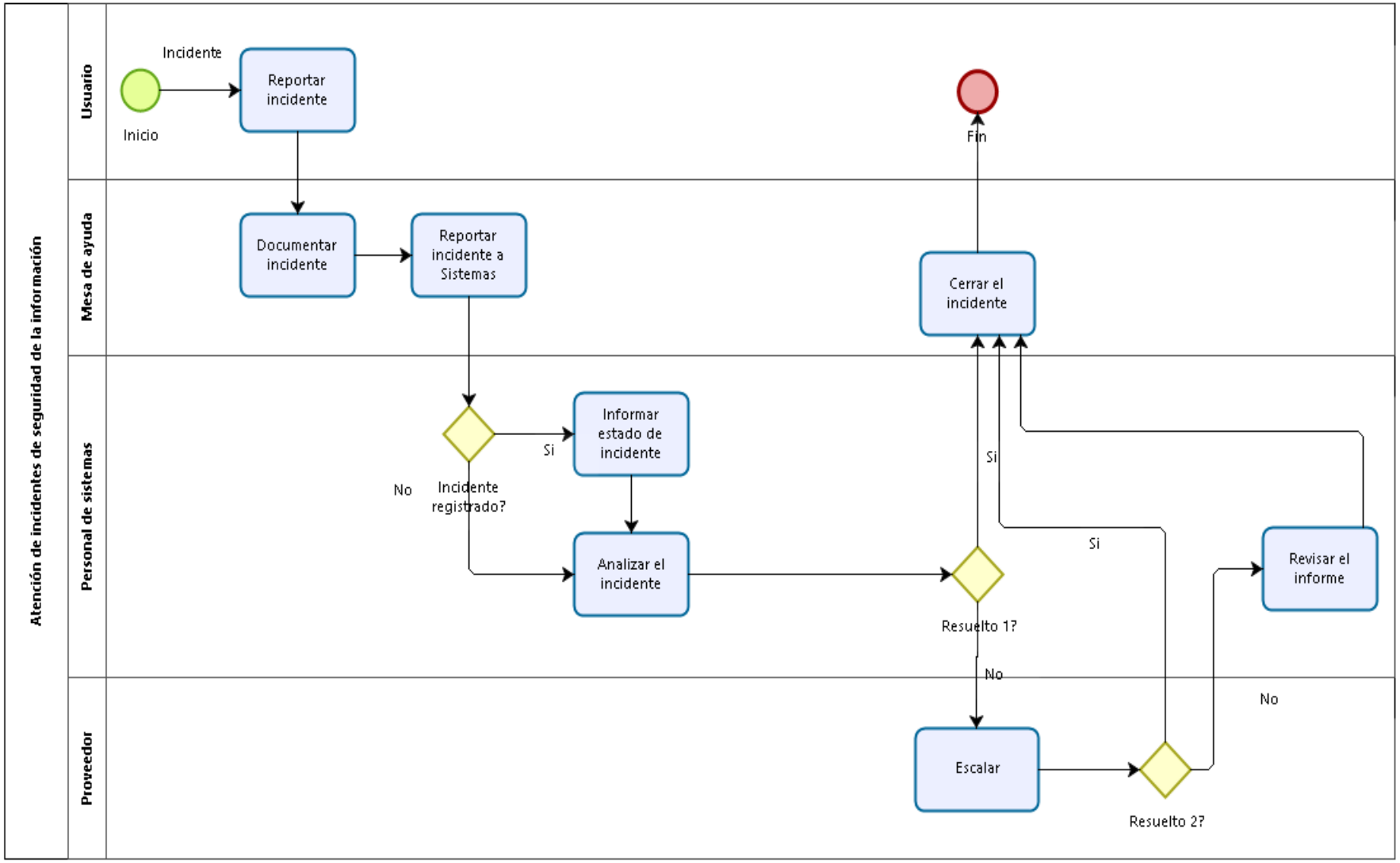



*Figura 4.1*: Atención de Incidentes de Seguridad para el Grupo de Control.

En la figura 4.2 presentamos la vista de simulación de la herramienta Bizagi, con el modelo de proceso: Atención de incidentes de seguridad de la información. Para un completo análisis de simulación es importante seguir los cuatro niveles:

- Validación de proceso
- Análisis de tiempo
- Análisis de recursos
- Análisis de calendarios

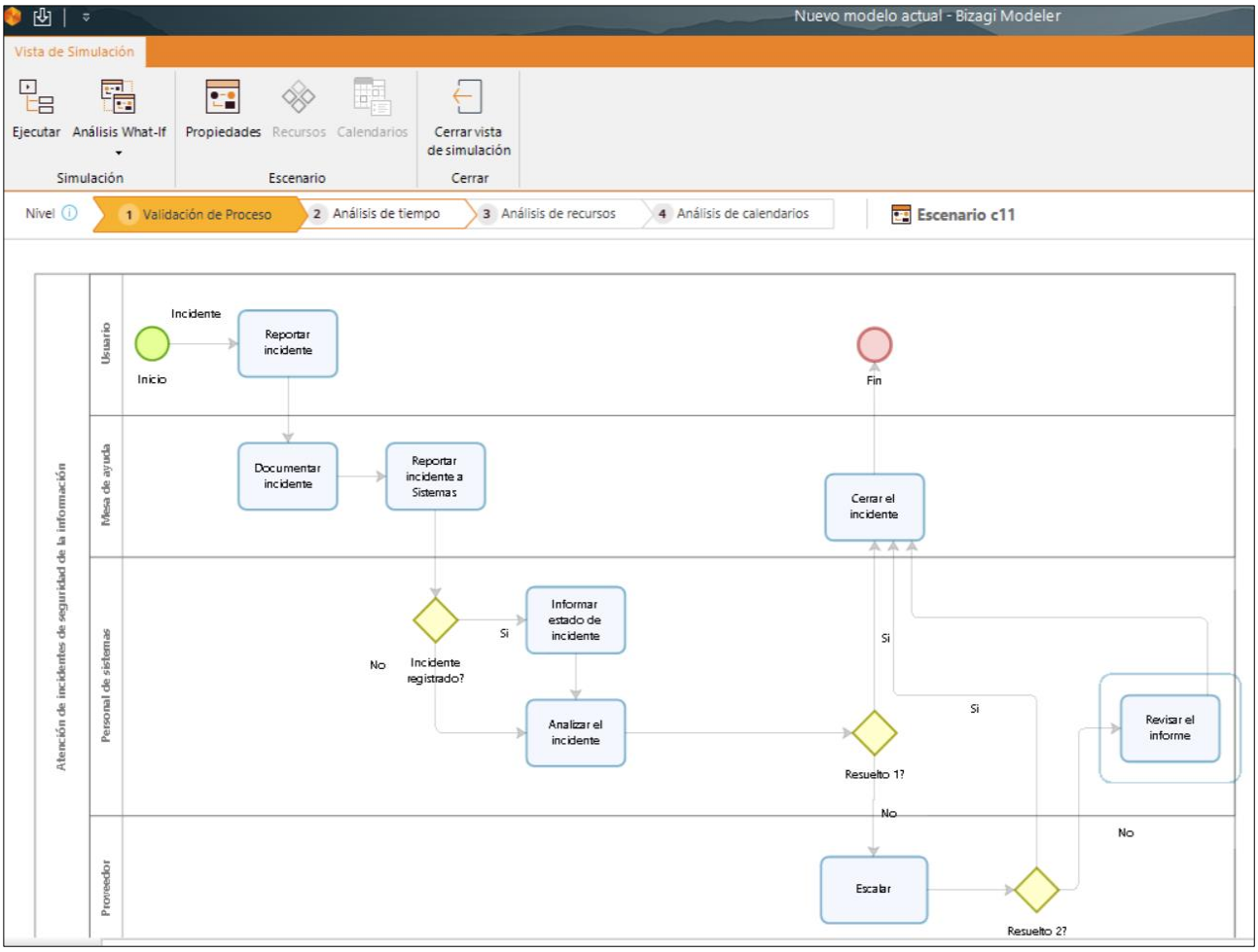



*Figura 4.2*: Vista de Simulación de Bizagi.

Se procede a la presentación y análisis de resultados de los indicadores: tiempo medio de respuesta ante un incidente de seguridad, grado de acierto en resolver incidentes de seguridad y uso de recursos para resolver incidentes de seguridad en el grupo de control.

#### 4.1.1.1. PARA EL INDICADOR: TIEMPO MEDIO DE RESPUESTA ANTE LOS INCIDENTES DE SEGURIDAD

### 1. RESULTADOS

Para evaluar el comportamiento del indicador, se toma la duración en minutos equivalentes de respuesta ante los incidentes de seguridad de la información que se dan en los procesos de negocio de la universidad.

Usando el simulador de Bizagi se pueden obtener el tiempo promedio del proceso, para ello ejecutamos el nivel: **Análisis de tiempo** como se muestra en la figura 4.3.

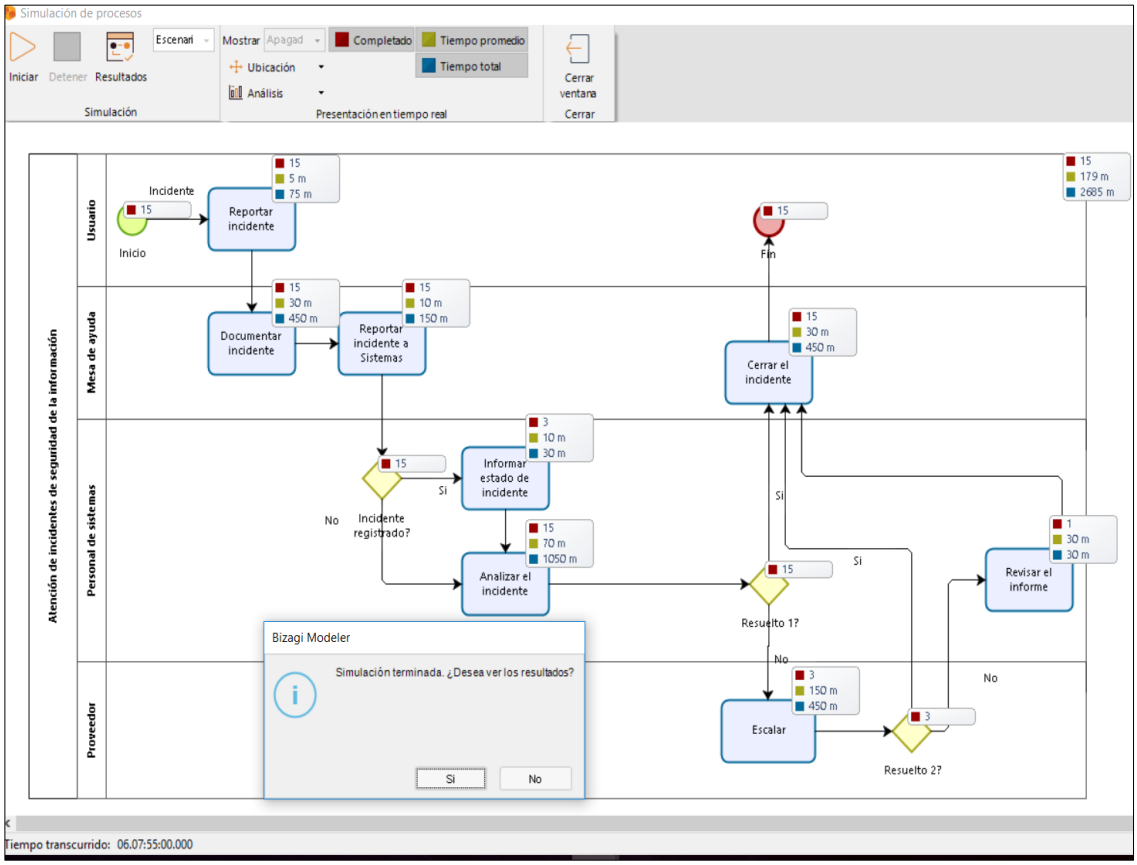



*Figura 4.3*: Análisis de Tiempo del Grupo de Control

Para un mejor análisis en el simulador de Bizagi se va a utilizar dos escenarios con el fin de evaluar y predecir los efectos de las decisiones en las medidas de desempeño. En la figura 4.4 se muestran los resultados: en el escenario No. 1 se obtiene un tiempo promedio 4h y 1m (241 minutos) y en el escenario No. 2, el tiempo promedio es 3h 26m (206 minutos). Estos resultados se muestran en la tabla 4.1 en la ejecución No. 1, de igual forma para las demás ejecuciones seleccionadas (conformadas por grupo de procesos) en la muestra se ha seguido el mismo método de trabajo.

| Nombre | Escenario | Tipo | Instancias completadas | Instancias iniciadas | Tiempo mínimo | Tiempo máximo | Tiempo promedio |
|---|---|---|---|---|---|---|---|
| Atención de incidentes de seguridad de la información | Escenario 1 | Proceso | 15 | 15 | 3h | 6h 10m | 4h 1m 20s |
| Atención de incidentes de seguridad de la información | Escenario 2 | Proceso | 15 | 15 | 2h 25m | 5h 35m | 3h 26m 20s |
| Inicio | Escenario 1 | Evento de inicio | 15 | | | | |
| Inicio | Escenario 2 | Evento de inicio | 15 | | | | |
| Resuelto 1? | Escenario 1 | Compuerta | 15 | 15 | | | |
| Resuelto 1? | Escenario 2 | Compuerta | 15 | 15 | | | |
| Incidente registrado? | Escenario 1 | Compuerta | 15 | 15 | | | |
| Incidente registrado? | Escenario 2 | Compuerta | 15 | 15 | | | |
| Resuelto 2? | Escenario 1 | Compuerta | 5 | 5 | | | |
| Resuelto 2? | Escenario 2 | Compuerta | 5 | 5 | | | |
| Revisar el informe | Escenario 1 | Tarea | 4 | 4 | 30m | 30m | 30m |
| Revisar el informe | Escenario 2 | Tarea | 4 | 4 | 30m | 30m | 30m |
| Reportar incidente | Escenario 1 | Tarea | 15 | 15 | 5m | 5m | 5m |
| Reportar incidente | Escenario 2 | Tarea | 15 | 15 | 5m | 5m | 5m |
| Documentar incidente | Escenario 1 | Tarea | 15 | 15 | 30m | 30m | 30m |
| Documentar incidente | Escenario 2 | Tarea | 15 | 15 | 30m | 30m | 30m |

*Figura 4.4*: Resultado de escenarios en el Análisis de tiempo del Grupo de Control.

Como se aprecia en la tabla 4.1, el grupo de control lo constituyen 30 ejecuciones seleccionadas aleatoriamente. Cada ejecución representa a un grupo de procesos, en los cuales se suscitan una cantidad de incidentes de seguridad de la información. Se han contemplado 2 escenarios y a cada uno de ellos se les ha medido la duración en

responder los incidentes de seguridad para las condiciones actuales esto es, sin la aplicación del modelo sistémico de seguridad de la información. De la relación entre estas dos duraciones, se ha calculado el porcentaje del tiempo medio de respuesta ante los incidentes de seguridad por cada ejecución.

**Tabla 4.1**
*Tiempo medio de respuesta ante los incidentes de seguridad del Grupo de Control*

| No. de Ejecuciones | No. de incidentes | Duración (Minutos) | | Porcentaje de tiempo medio de respuesta ante incidentes de seguridad |
|---|---|---|---|---|
| | | Escenario No. 1 | Escenario No. 2 | |
| 1 | 15 | 241 | 206 | 85.48 |
| 2 | 18 | 231 | 208 | 90.04 |
| 3 | 21 | 230 | 200 | 86.96 |
| 4 | 17 | 228 | 193 | 84.65 |
| 5 | 23 | 220 | 195 | 88.64 |
| 6 | 19 | 228 | 207 | 90.79 |
| 7 | 16 | 237 | 213 | 89.87 |
| 8 | 24 | 218 | 191 | 87.61 |
| 9 | 20 | 226 | 206 | 91.15 |
| 10 | 23 | 220 | 190 | 86.36 |
| 11 | 25 | 216 | 181 | 83.80 |
| 12 | 22 | 221 | 196 | 88.69 |
| 13 | 23 | 220 | 197 | 89.55 |
| 14 | 19 | 228 | 205 | 89.91 |
| 15 | 25 | 216 | 199 | 92.13 |
| 16 | 28 | 213 | 190 | 89.20 |
| 17 | 26 | 215 | 194 | 90.23 |
| 18 | 27 | 214 | 189 | 88.32 |
| 19 | 16 | 237 | 210 | 88.61 |
| 20 | 23 | 220 | 196 | 89.09 |
| 21 | 29 | 212 | 185 | 87.26 |
| 22 | 18 | 231 | 202 | 87.45 |
| 23 | 15 | 241 | 211 | 87.55 |
| 24 | 27 | 214 | 188 | 87.85 |
| 25 | 22 | 221 | 197 | 89.14 |
| 26 | 28 | 213 | 185 | 86.85 |
| 27 | 18 | 231 | 201 | 87.01 |
| 28 | 24 | 218 | 188 | 86.24 |
| 29 | 17 | 234 | 201 | 85.90 |
| 30 | 25 | 216 | 185 | 85.65 |
| | | | **Promedio** | 88.06 |
| | | | **Desv. Standard** | 1.98 |

## 2. ANÁLISIS

De los resultados obtenidos podemos analizar que cuando se tiene que responder un incidente de seguridad, los tiempos de duración en el escenario No.2 son menores que en el escenario No.1. Esto se ha logrado porque en el escenario No.2 se ha eliminado tiempos improductivos e innecesarios en sus tareas, y por ello el personal de Sistemas ha mejorado y reducido el tiempo en resolver los incidentes de seguridad.

Sin embargo, al calcular la relación entre estas dos duraciones da lugar a un promedio de 88.06 % que para temas de seguridad de la información se plantea la necesidad de un mejoramiento del sistema.

### 4.1.1.2. PARA EL INDICADOR: PORCENTAJE DE ACIERTO PARA RESOLVER LOS INCIDENTES DE SEGURIDAD

## 1. RESULTADOS

Para evaluar el comportamiento del indicador, se toma el número de incidentes de seguridad solucionados sobre el total de incidentes de seguridad de la información, reportados por los usuarios de los procesos de negocio de la universidad.

.

Para conocer sobre el número de incidentes de seguridad que han sido resueltos, ejecutamos el nivel: **Validación del proceso** en el simulador de Bizagi, como se muestra en la figura 4.5.

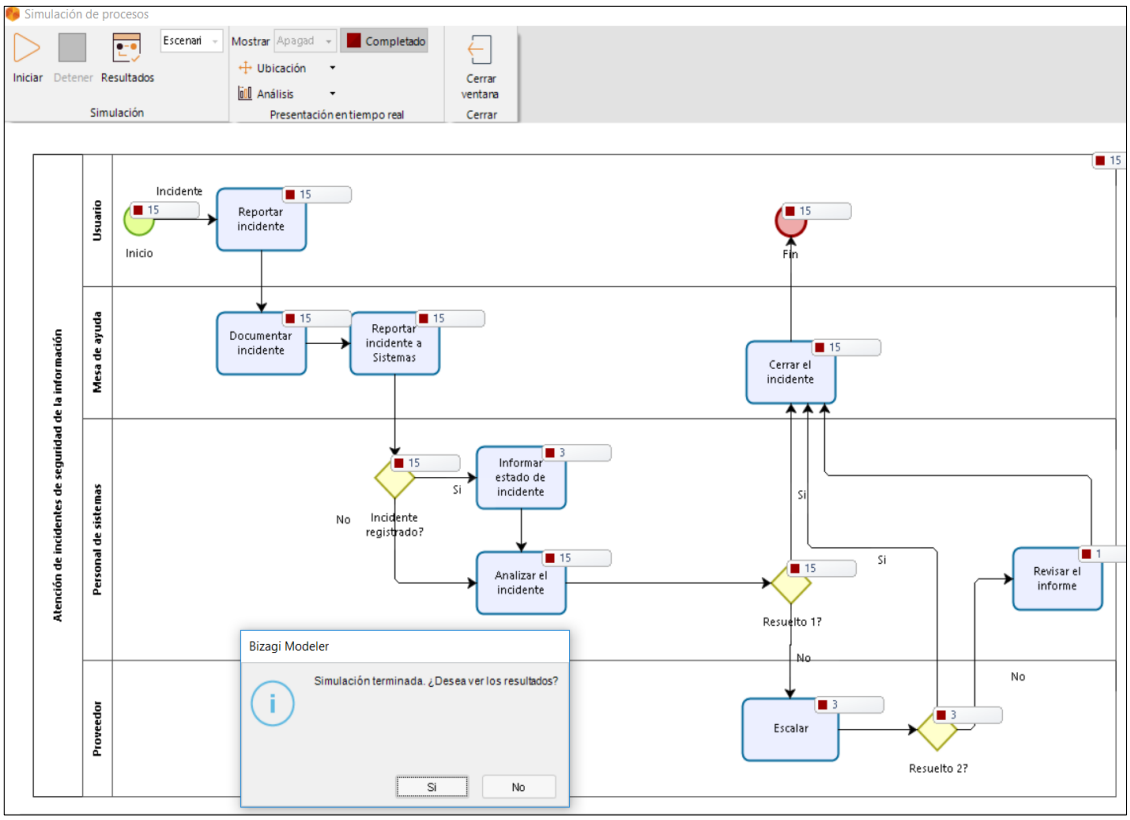
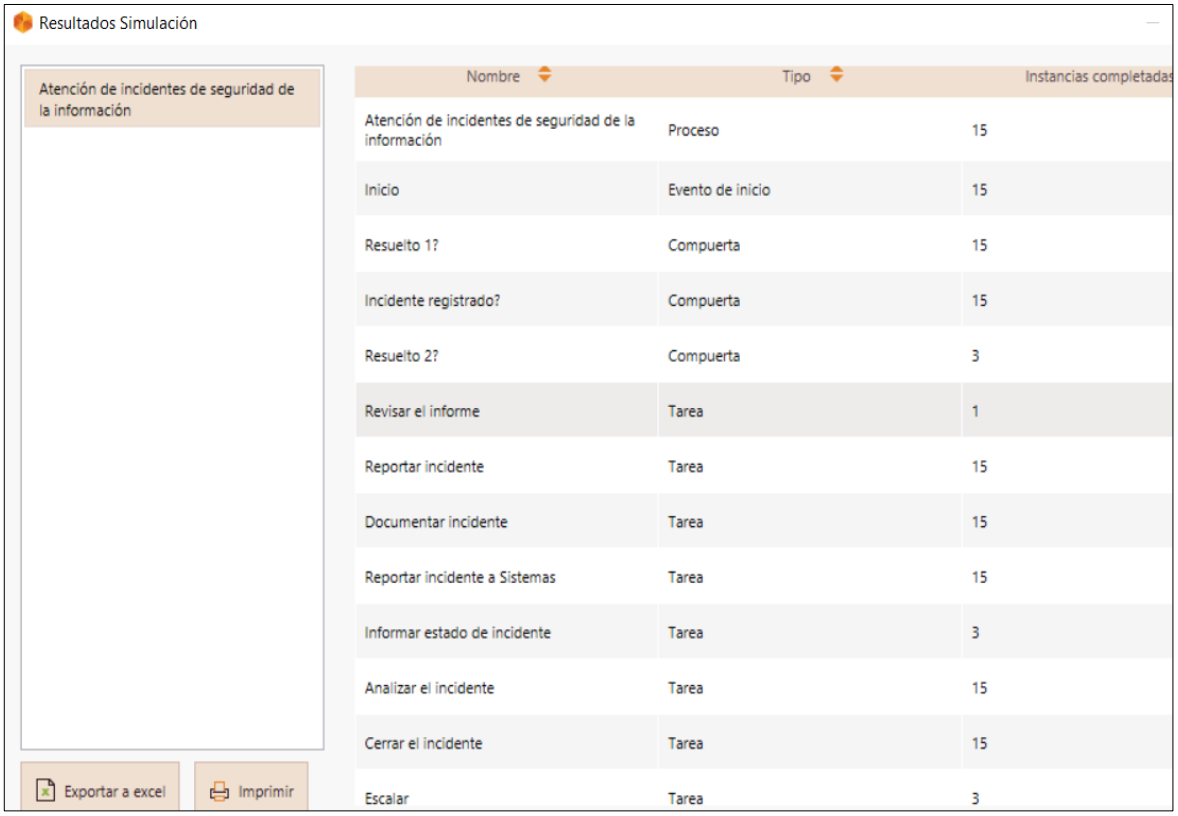



*Figura 4.5*: Validación del proceso del Grupo de Control.

Se muestra las instancias completadas cuando se ejecutan el total de incidentes de seguridad reportados. Se puede apreciar que la tarea: “Revisar informe” tiene una instancia completada que es el incidente de seguridad que no fue resuelto, donde si bien tres incidentes de seguridad fueron escalados, uno de ellos no fue resuelto.

En la figura 4.6. se puede apreciar los resultados de la simulación.




| Nombre | Tipo | Instancias completadas |
|---|---|---|
| Atención de incidentes de seguridad de la información | Proceso | 15 |
| Inicio | Evento de inicio | 15 |
| Resuelto 1? | Compuerta | 15 |
| Incidente registrado? | Compuerta | 15 |
| Resuelto 2? | Compuerta | 3 |
| Revisar el informe | Tarea | 1 |
| Reportar incidente | Tarea | 15 |
| Documentar incidente | Tarea | 15 |
| Reportar incidente a Sistemas | Tarea | 15 |
| Informar estado de incidente | Tarea | 3 |
| Analizar el incidente | Tarea | 15 |
| Cerrar el incidente | Tarea | 15 |
| Escalar | Tarea | 3 |

*Figura 4.6*: Resultado del nivel de validación de proceso

Estos resultados se muestran en la tabla 4.2 en la ejecución No. 1, de igual forma para las demás ejecuciones seleccionadas (conformadas por grupo de procesos), se ha seguido el mismo método de trabajo.

Como se aprecia en la tabla 4.2, el grupo de control lo constituyen 30 ejecuciones seleccionadas aleatoriamente, que es el tamaño de la muestra representativa. Cada ejecución representa a un grupo de procesos, en los cuales se suscitan una cantidad de incidentes de seguridad de la información. Del total de incidentes se ha calculado la cantidad de incidentes que no fueron resueltos para las condiciones actuales, esto es, sin la aplicación del modelo sistémico de seguridad de la información. De la relación entre los incidentes de seguridad que fueron resueltas y el total de ellas, se ha calculado el porcentaje de acierto en resolver los incidentes de seguridad por cada ejecución.

**Tabla 4.2**

*Porcentaje de acierto para resolver los incidentes de seguridad del Grupo de Control*

| No. de ejecuciones | Incidentes de seguridad | | Porcentaje de acierto para resolver incidentes de seguridad |
|---|---|---|---|
| | No. de incidentes | No solucionadas | |
| 1 | 15 | 1 | 93.33 |
| 2 | 18 | 2 | 88.89 |
| 3 | 21 | 2 | 90.48 |
| 4 | 17 | 2 | 88.24 |
| 5 | 23 | 2 | 91.3 |
| 6 | 19 | 2 | 89.47 |
| 7 | 16 | 2 | 87.5 |
| 8 | 24 | 2 | 91.67 |
| 9 | 20 | 2 | 90 |
| 10 | 23 | 2 | 91.3 |
| 11 | 25 | 2 | 92 |
| 12 | 22 | 2 | 90.91 |
| 13 | 23 | 3 | 86.96 |
| 14 | 19 | 2 | 89.47 |
| 15 | 25 | 2 | 92 |
| 16 | 28 | 2 | 92.86 |
| 17 | 26 | 2 | 92.31 |
| 18 | 27 | 2 | 92.59 |
| 19 | 16 | 2 | 87.5 |
| 20 | 23 | 3 | 86.96 |
| 21 | 29 | 2 | 93.1 |
| 22 | 18 | 2 | 88.89 |
| 23 | 15 | 2 | 86.67 |
| 24 | 27 | 2 | 92.59 |
| 25 | 22 | 3 | 86.36 |
| 26 | 28 | 2 | 92.86 |
| 27 | 18 | 2 | 88.89 |
| 28 | 24 | 3 | 87.5 |
| 29 | 17 | 2 | 88.24 |
| 30 | 25 | 4 | 84 |
| | | **Promedio** | 89.82 |
| | | **Des. Standard** | 2.48 |

## 2. ANÁLISIS

De los resultados obtenidos podemos analizar que si bien, lo ideal sería resolver todos los incidentes de seguridad al 100%, la seguridad absoluta no existe, pero si se puede reducir los incidentes, de tal forma que no se tenga que escalar a un proveedor de seguridad. Por ello al calcular el promedio del total de incidentes resueltos sobre el total de incidentes reportados se obtiene como valor de 89.82%, que revela la

necesidad de capacitar y especializar al personal de sistemas en temas críticos de incidentes de seguridad, y de esta manera resolver la mayoría de los incidentes reportados.

#### 4.1.1.3. PARA EL INDICADOR: GRADO DE USO DEL RECURSO HUMANO PARA RESOLVER LOS INCIDENTES DE SEGURIDAD

1. **RESULTADOS**

Para evaluar el comportamiento del indicador es necesario el grado de uso de uno de los principales recursos en resolver los incidentes de seguridad de la información que se dan en los procesos de negocio, como es el recurso humano.

Usando el simulador de Bizagi en el nivel **Análisis de Recursos**, se define las personas que están disponibles y en qué tareas se utilizan. Para un mejor análisis se toman en cuenta dos escenarios. Para el escenario No. 1 se toman dos personas del recurso "Mesa de ayuda", una persona del recurso "Personal de sistemas "y una persona del recurso "Experto"**.** En total 4 personas, como se muestra en la figura 4.7.

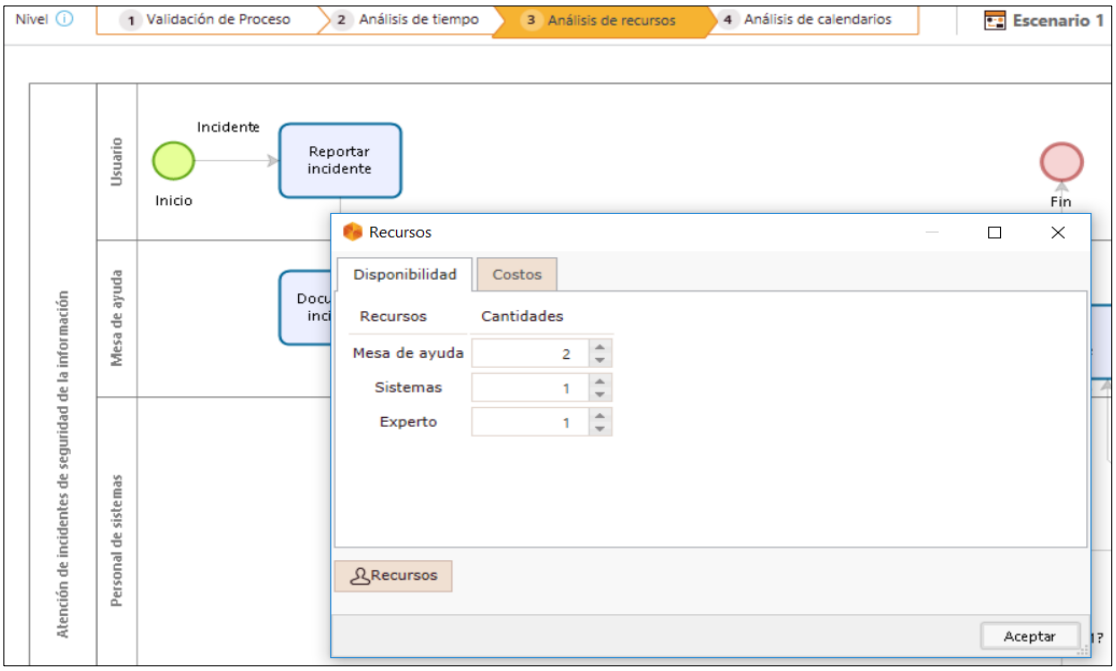



*Figura 4.7*: Disponibilidad de recursos del escenario No. 1 del Grupo de Control

Para el escenario No. 2 se toman dos personas del recurso “Mesa de ayuda”, dos personas del recurso “Personal de sistemas” y una persona del recurso “Experto”. En total cinco personas, como se muestra en la figura 4.8.

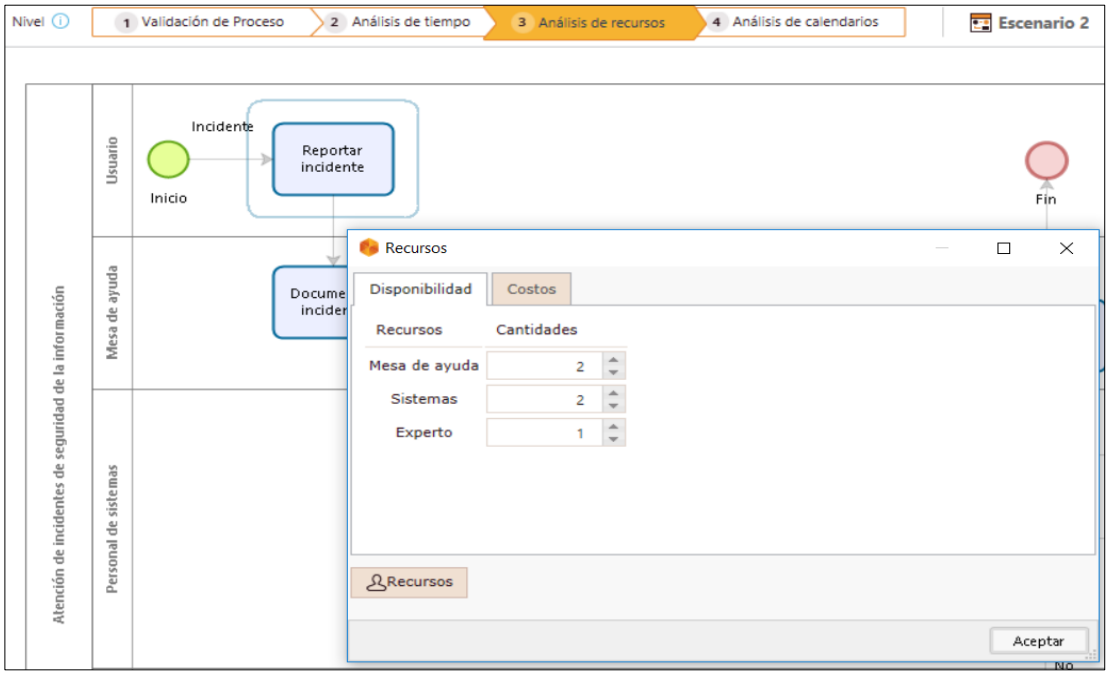



*Figura 4.8*: Disponibilidad de recursos del escenario No. 2 Grupo de Control

También se toma en cuenta la disponibilidad de los recursos en los turnos u horarios para obtener una mejor aproximación al rendimiento del proceso real. Se han definido 2 turnos: Mañana y tarde, y en el horario de refrigerio también hay personas que atienden.

En el simulador de Bizagi, en el nivel: **Análisis de calendarios** se ejecuta los 2 escenarios y los resultados se muestran en la figura 4.9.

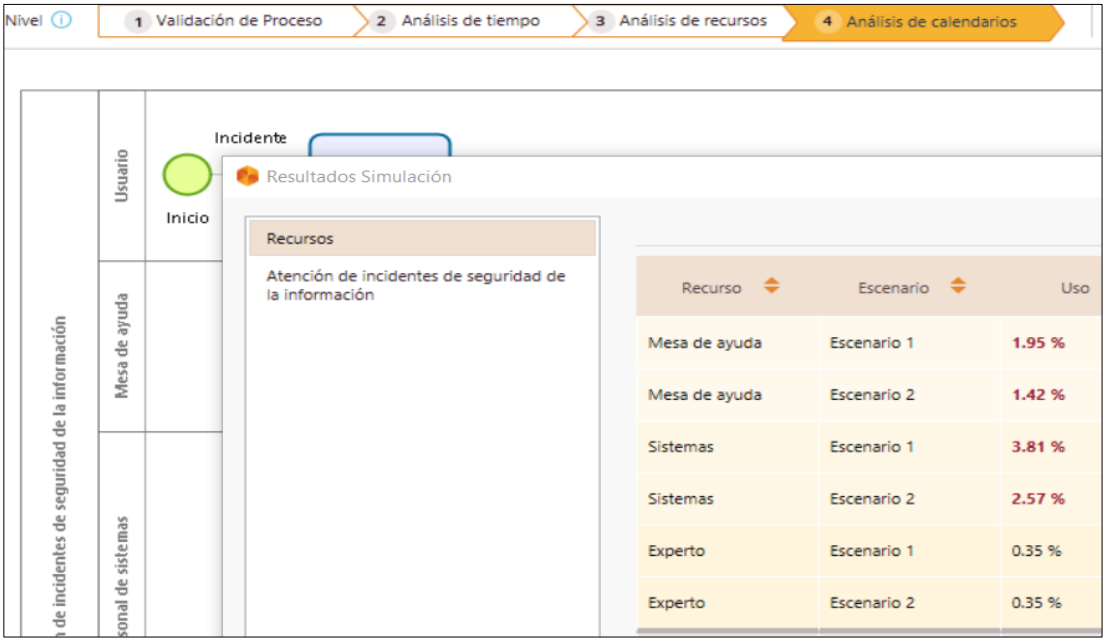



*Figura 4.9*: Resultados del uso de recurso de 2 escenarios del Grupo de Control

Se elige el escenario No. 2 porque usa un menor porcentaje de recursos. En el recurso Mesa de ayuda el porcentaje de uso de recurso es 1.42, del recurso Sistema el porcentaje es 2.57 y del recurso Experto el porcentaje es 0.35. La suma de ellos es 4.34%, y este valor se muestra en la tabla 4.3 en la ejecución No. 1. De igual forma para las demás ejecuciones seleccionadas, se ha seguido el mismo método de trabajo.

En la tabla 4.3, el grupo de control lo constituyen 30 ejecuciones seleccionadas aleatoriamente. Se ha identificado el número de personas que intervienen en responder el incidente, el porcentaje de participación o uso del recurso y los minutos por mes que el personal está disponible. Los minutos por mes se obtiene como promedio de 8 horas diarias de trabajo por 5 días por 4 semanas lo cual hace 160 horas mensual y equivalente en minutos se tiene 9600 minutos por mes.

De esta manera el grado de uso del recurso humano para resolver los incidentes de seguridad, se determina de la relación entre el número de incidentes de seguridad y el número de personas-minutos por cada ejecución (grupo de procesos).

**Tabla 4.3**

*Grado de uso del recurso humano para resolver incidentes de seguridad del Grupo de Control*

| Nro. De ejecuciones | PRODUCCIÓN | RECURSOS USADOS | | | Grado de uso de recurso humano |
|---|---|---|---|---|---|
| | Incidentes de seguridad | Personas | % Uso de Recurso | Minutos por mes | Incidentes/Persona-minuto |
| 1 | 15 | 5 | 4.34 | 9600 | 0.00720 |
| 2 | 18 | 6 | 5.50 | 9600 | 0.00568 |
| 3 | 21 | 6 | 6.44 | 9600 | 0.00566 |
| 4 | 17 | 5 | 5.70 | 9600 | 0.00621 |
| 5 | 23 | 5 | 9.81 | 9600 | 0.00488 |
| 6 | 19 | 6 | 6.35 | 9600 | 0.00519 |
| 7 | 16 | 5 | 6.24 | 9600 | 0.00534 |
| 8 | 24 | 6 | 6.88 | 9600 | 0.00606 |
| 9 | 20 | 6 | 7.07 | 9600 | 0.00491 |
| 10 | 23 | 7 | 8.00 | 9600 | 0.00428 |
| 11 | 25 | 5 | 7.34 | 9600 | 0.00710 |
| 12 | 22 | 6 | 5.66 | 9600 | 0.00675 |
| 13 | 23 | 5 | 7.47 | 9600 | 0.00641 |
| 14 | 19 | 5 | 6.67 | 9600 | 0.00593 |
| 15 | 25 | 6 | 7.54 | 9600 | 0.00576 |
| 16 | 28 | 7 | 7.25 | 9600 | 0.00575 |
| 17 | 26 | 5 | 9.39 | 9600 | 0.00577 |
| 18 | 27 | 6 | 7.76 | 9600 | 0.00604 |
| 19 | 16 | 5 | 5.47 | 9600 | 0.00609 |
| 20 | 23 | 6 | 6.74 | 9600 | 0.00592 |
| 21 | 29 | 6 | 8.53 | 9600 | 0.00590 |
| 22 | 18 | 5 | 4.41 | 9600 | 0.00850 |
| 23 | 15 | 5 | 3.71 | 9600 | 0.00842 |
| 24 | 27 | 6 | 6.11 | 9600 | 0.00767 |
| 25 | 22 | 6 | 6.16 | 9600 | 0.00620 |
| 26 | 28 | 7 | 8.93 | 9600 | 0.00467 |
| 27 | 18 | 5 | 5.78 | 9600 | 0.00649 |
| 28 | 24 | 6 | 6.55 | 9600 | 0.00636 |
| 29 | 17 | 5 | 5.36 | 9600 | 0.00661 |
| 30 | 25 | 6 | 6.75 | 9600 | 0.00643 |
| | | | | **Promedio** | 0.00614 |
| | | | | **Desv. Standard** | 0.00097 |

El promedio del grado de uso del recurso humano para resolver incidentes de seguridad es de 0.00614 incidentes/persona-minuto.

## 2. ANÁLISIS

De los resultados obtenidos podemos analizar que si disminuimos el número de personal de los recursos: mesa de ayuda, personal de sistemas y experto, el porcentaje de utilización de recursos se incrementa (ver figura 4.9), y esto afecta al personal de sistemas que siempre se encuentran bastante ocupado. Todo ello ocasiona demoras en atender los incidentes de seguridad con el riesgo de que el incidente reportado por el usuario no llegue a atenderse.

Tenemos que tener en cuenta el efecto de la disponibilidad de los recursos que intervienen en la atención de incidentes, como también sus horarios o turnos de atención, esto nos dará una mejor aproximación al rendimiento del proceso real.

### 4.1.2. GRUPO EXPERIMENTAL

Aplicando la herramienta Bizagi, se ha calculado el tiempo de espera de cada una de las actividades o tareas que conforman tal proceso. Se ha calculado el tiempo promedio de duración en responder a los incidentes de seguridad, se han eliminado tiempos improductivos e innecesarios con una mejor gestión en los recursos como son las personas. Se ha asignado en forma adecuada la cantidad de personas que deben intervenir en los recursos que son necesarios en las tareas.

En la figura 4.10 se muestra el diagrama del procedimiento mencionado conformado por los actores del negocio: los usuarios de los procesos, el equipo de manejo de incidentes, el equipo de mesa de ayuda y el proveedor, especialista en seguridad de la información; y las tareas donde intervienen.

Como se aprecia en el diagrama cuando se origina un incidente de seguridad, el usuario de una área académica o administrativa reporta el incidente de seguridad a mesa de ayuda, quiénes están preparados en un primer nivel para resolver el incidente y cerrar el incidente, sino lo resuelven, el equipo de manejo de incidentes se encarga de revisarlo a un segundo nivel, cabe resaltar que este equipo especializado se ha conformado por personas que conocen los diferentes incidentes de seguridad y están capacitados para resolverlos. Si lo resuelven, se documenta la base de conocimiento para tomarlo como una lección aprendida y cerrar el incidente, si en caso, no lo resolvieran se procede a escalar a un proveedor como tercer nivel. Si el proveedor no lo resuelve, el equipo de manejo de incidentes revisa su informe técnico, finalmente mesa de ayuda se encarga de cerrar el incidente e informar al usuario.

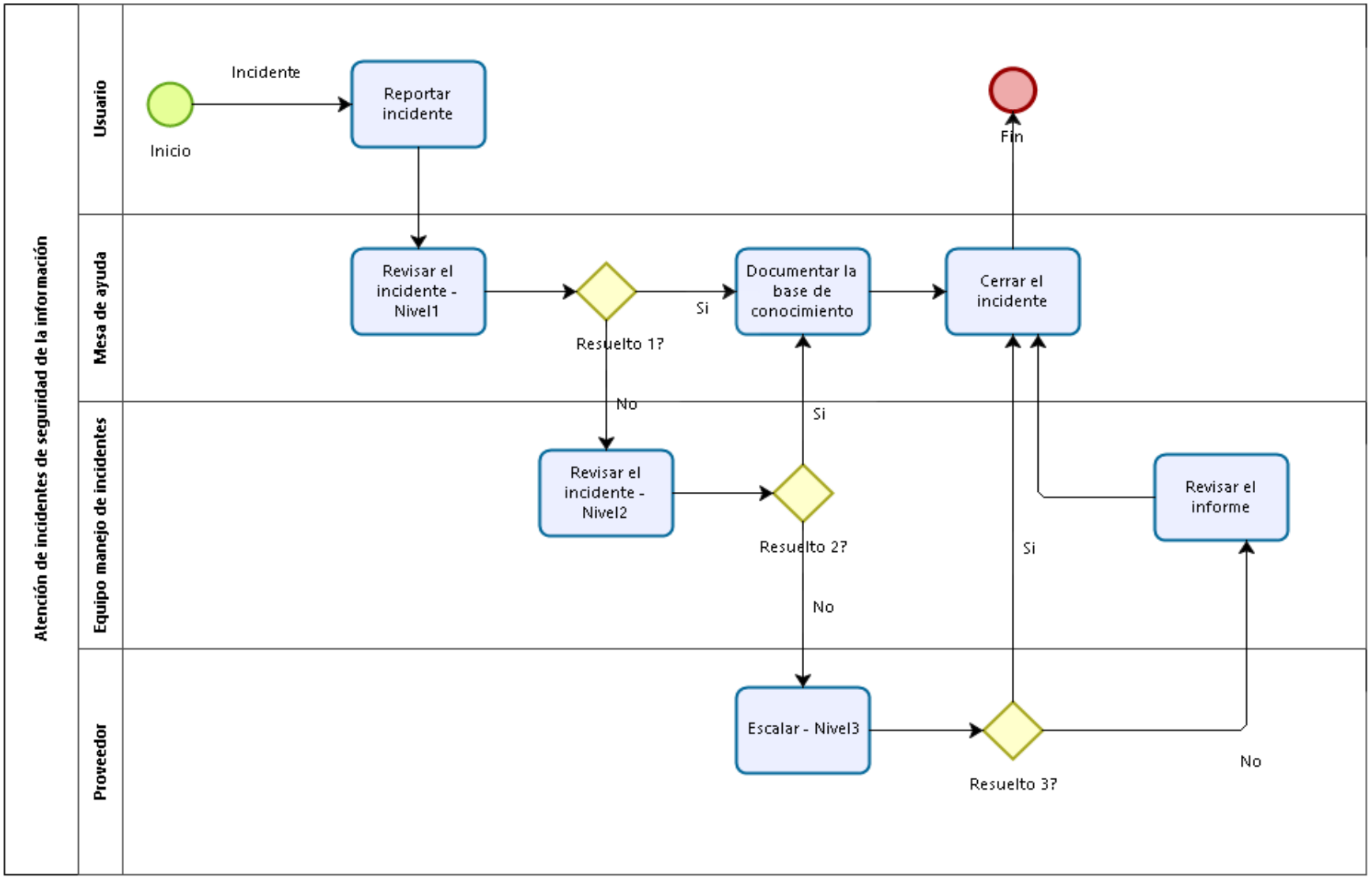



*Figura 4.10:* Atención de Incidentes de Seguridad para el Grupo Experimental.

Se procede a la presentación y análisis de resultados de los indicadores del grupo experimental.

### 4.1.2.1. PARA EL INDICADOR: TIEMPO MEDIO DE RESPUESTA ANTE LOS INCIDENTES DE SEGURIDAD

#### 1. RESULTADOS

De la misma manera que para el grupo de control, para evaluar el comportamiento del indicador, se toma la duración en minutos equivalentes de respuesta ante los incidentes de seguridad de la información que se dan en los procesos de negocio de la universidad.

Usando el simulador de Bizagi se pueden obtener el tiempo promedio del proceso, para ello ejecutamos el nivel: **Análisis de tiempo** como se muestra en la figura 4.11.

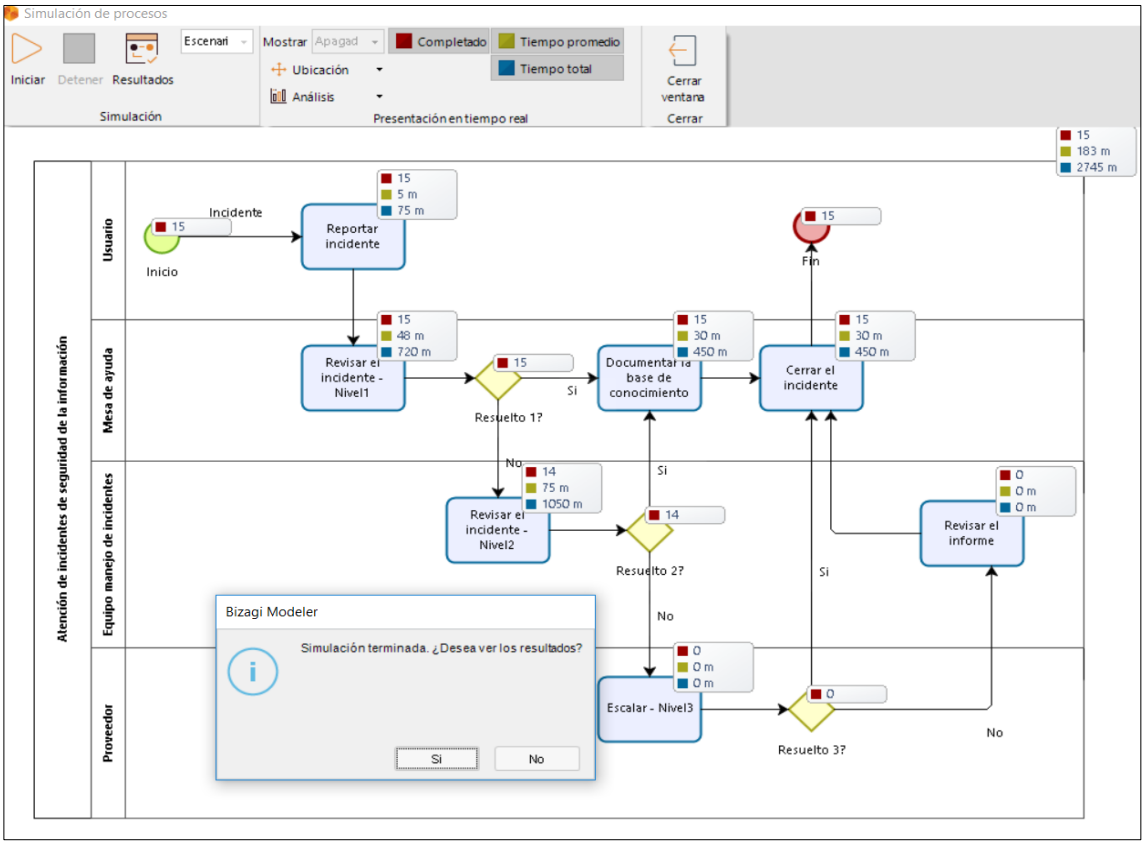
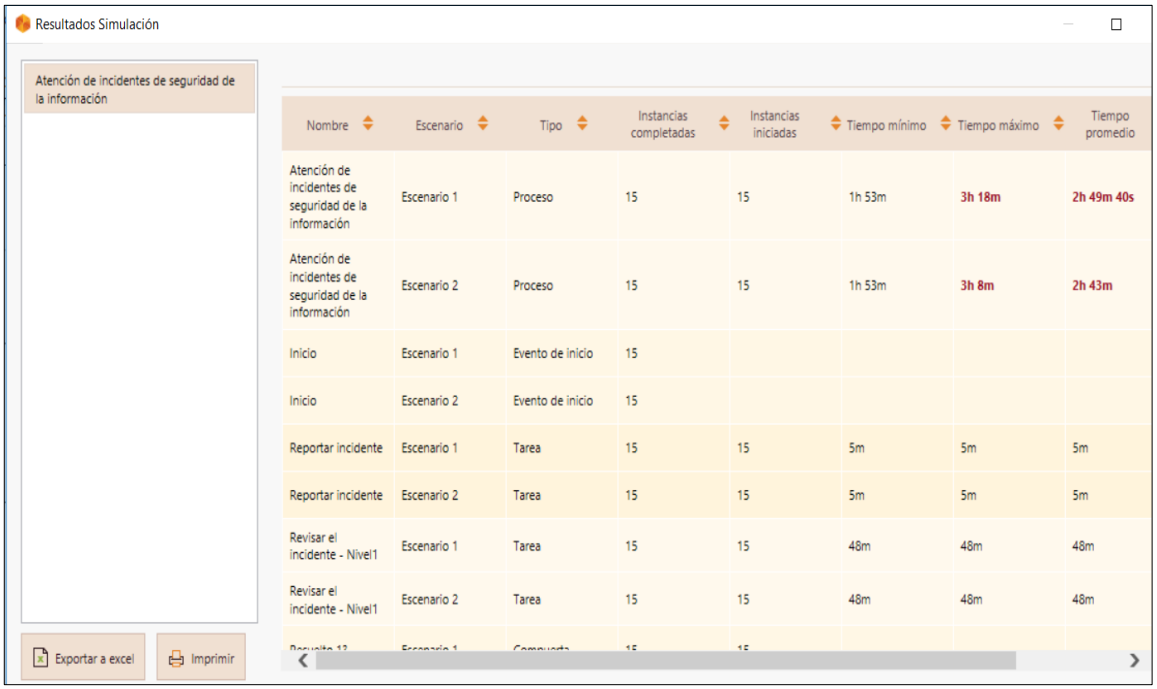



*Figura 4.11*: Análisis de Tiempo del Grupo Experimental

Para un mejor análisis en el simulador de Bizagi, se va a utilizar dos escenarios con el fin de evaluar y predecir los efectos de las decisiones en las medidas de desempeño. En la figura 4.12 se muestran los resultados: para el escenario No. 1 se obtiene un tiempo promedio de 169 minutos y para el escenario No. 2, el tiempo promedio de 163 minutos. Estos resultados se muestran en la tabla 4.4 en la ejecución No. 1, de igual forma para las demás ejecuciones seleccionadas (conformadas por grupo de procesos) en la muestra, se ha seguido el mismo método de trabajo.




| Nombre | Escenario | Tipo | Instancias completadas | Instancias iniciadas | Tiempo mínimo | Tiempo máximo | Tiempo promedio |
|---|---|---|---|---|---|---|---|
| Atención de incidentes de seguridad de la información | Escenario 1 | Proceso | 15 | 15 | 1h 53m | 3h 18m | 2h 49m 40s |
| Atención de incidentes de seguridad de la información | Escenario 2 | Proceso | 15 | 15 | 1h 53m | 3h 8m | 2h 43m |
| Inicio | Escenario 1 | Evento de inicio | 15 | | | | |
| Inicio | Escenario 2 | Evento de inicio | 15 | | | | |
| Reportar incidente | Escenario 1 | Tarea | 15 | 15 | 5m | 5m | 5m |
| Reportar incidente | Escenario 2 | Tarea | 15 | 15 | 5m | 5m | 5m |
| Revisar el incidente - Nivel1 | Escenario 1 | Tarea | 15 | 15 | 48m | 48m | 48m |
| Revisar el incidente - Nivel1 | Escenario 2 | Tarea | 15 | 15 | 48m | 48m | 48m |

*Figura 4.12*: Resultado de escenarios en el Análisis de tiempo del Grupo Experimental.

Como se aprecia en la tabla 4.4, el grupo experimental lo constituyen 30 ejecuciones seleccionadas aleatoriamente. Cada ejecución representa a un grupo de procesos, en los cuales se suscitan una cantidad de incidentes de seguridad de la información. Se han contemplado 2 escenarios y a cada uno de ellos se les ha medido la duración en responder los incidentes de seguridad bajo las condiciones de proceso funcional derivado de la aplicación del modelo sistémico de seguridad de la información. De la relación entre estas dos duraciones, se ha calculado el porcentaje del tiempo medio de respuesta ante los incidentes de seguridad por cada ejecución.

**Tabla 4.4**
*Tiempo medio de respuesta ante los incidentes de seguridad del Grupo Experimental*

| No. de Ejecuciones | No. de incidentes | Duración (minutos) | | Porcentaje de tiempo de respuesta ante incidentes (%) |
|---|---|---|---|---|
| | | Escenario No. 1 | Escenario No. 2 | |
| 1 | 15 | 169 | 163 | 96.45 |
| 2 | 18 | 167 | 163 | 97.6 |
| 3 | 21 | 166 | 159 | 95.78 |
| 4 | 17 | 165 | 155 | 93.94 |
| 5 | 23 | 172 | 157 | 91.28 |
| 6 | 19 | 168 | 149 | 88.69 |
| 7 | 16 | 164 | 154 | 93.9 |
| 8 | 24 | 173 | 158 | 91.33 |
| 9 | 20 | 169 | 159 | 94.08 |
| 10 | 23 | 172 | 150 | 87.21 |
| 11 | 25 | 170 | 156 | 91.76 |
| 12 | 22 | 167 | 153 | 91.62 |
| 13 | 23 | 172 | 157 | 91.28 |
| 14 | 19 | 168 | 153 | 91.07 |
| 15 | 25 | 170 | 156 | 91.76 |
| 16 | 28 | 172 | 154 | 89.53 |
| 17 | 26 | 171 | 159 | 92.98 |
| 18 | 27 | 171 | 160 | 93.57 |
| 19 | 16 | 164 | 152 | 92.68 |
| 20 | 23 | 172 | 164 | 95.35 |
| 21 | 29 | 173 | 161 | 93.06 |
| 22 | 18 | 167 | 145 | 86.83 |
| 23 | 15 | 163 | 152 | 93.25 |
| 24 | 27 | 171 | 160 | 93.57 |
| 25 | 22 | 167 | 156 | 93.41 |
| 26 | 28 | 172 | 161 | 93.6 |
| 27 | 18 | 167 | 154 | 92.22 |
| 28 | 24 | 165 | 158 | 95.76 |
| 29 | 17 | 165 | 151 | 91.52 |
| 30 | 25 | 170 | 159 | 93.53 |
| | | | **Promedio** | 92.62 |
| | | | **Desv. Standard** | 2.47 |

### 2. ANÁLISIS

De los resultados obtenidos podemos analizar que cuando se tiene que responder a un incidente de seguridad los tiempos de duración en el escenario No. 2 son menores que en el escenario No.1. Esto se ha logrado porque en el escenario No.2 se han eliminado tiempos improductivos e innecesarios en sus tareas, y por ello el equipo de manejo de incidentes ha mejorado en resolver con más rapidez un incidente de seguridad.

De la relación entre estas dos duraciones, se ha calculado la eficiencia de cada grupo de procesos dando lugar a un promedio de 92.65 % que revela una mejor performance del sistema.

## 4.1.2.2. PARA EL INDICADOR: PORCENTAJE DE ACIERTO PARA RESOLVER LOS INCIDENTES DE SEGURIDAD

### 1. RESULTADOS

Para evaluar el comportamiento del indicador, se toma en cuenta el número de incidentes de seguridad solucionados sobre el total de incidentes de seguridad de la información, reportados por los usuarios de los procesos de negocio de la universidad.

En este caso específico, es la diferencia entre el 100% de acierto teórico (ideal) y el porcentaje resultante entre las incidencias de seguridad no solucionadas y el total de ellas realizadas (en cada grupo de procesos seleccionados). De esta manera, la brecha entre el acierto ideal y el acierto real, constituye la eficacia del sistema.

Para conocer sobre el número de incidentes de seguridad que han sido resueltos, ejecutamos el nivel: **Validación del proceso** en el simulador de Bizagi, como se muestra en la figura 4.13.

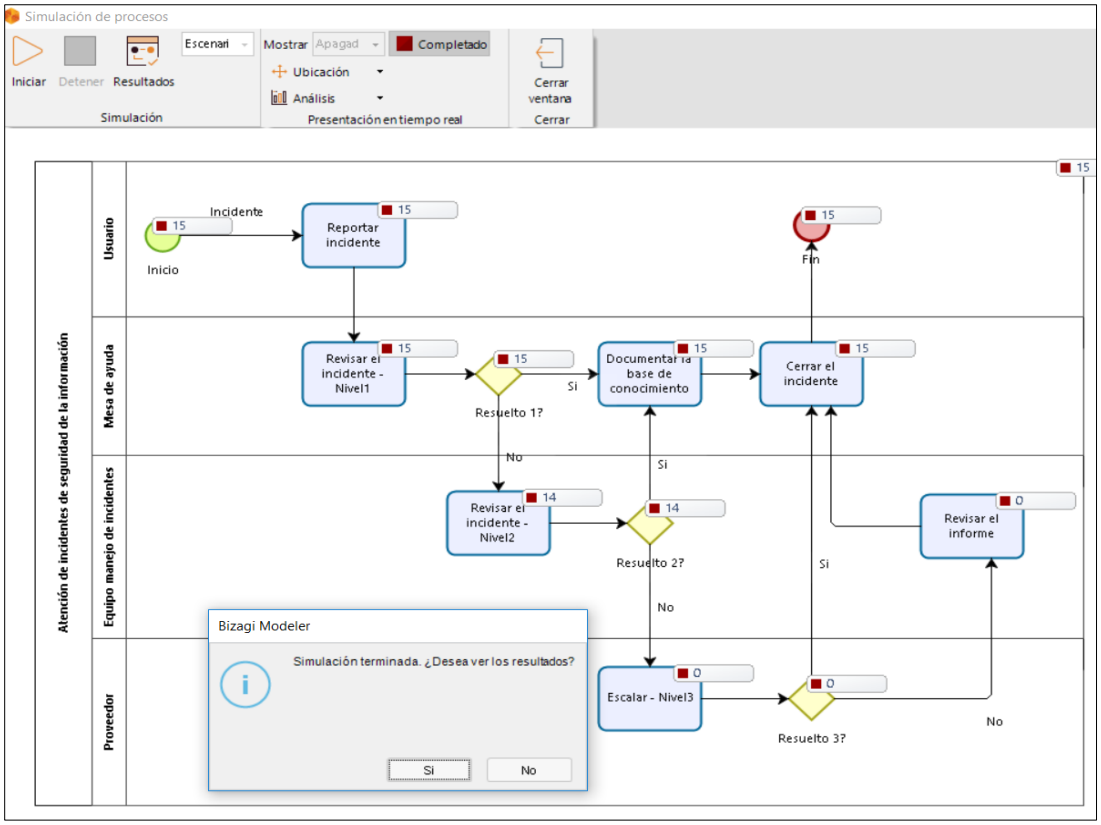
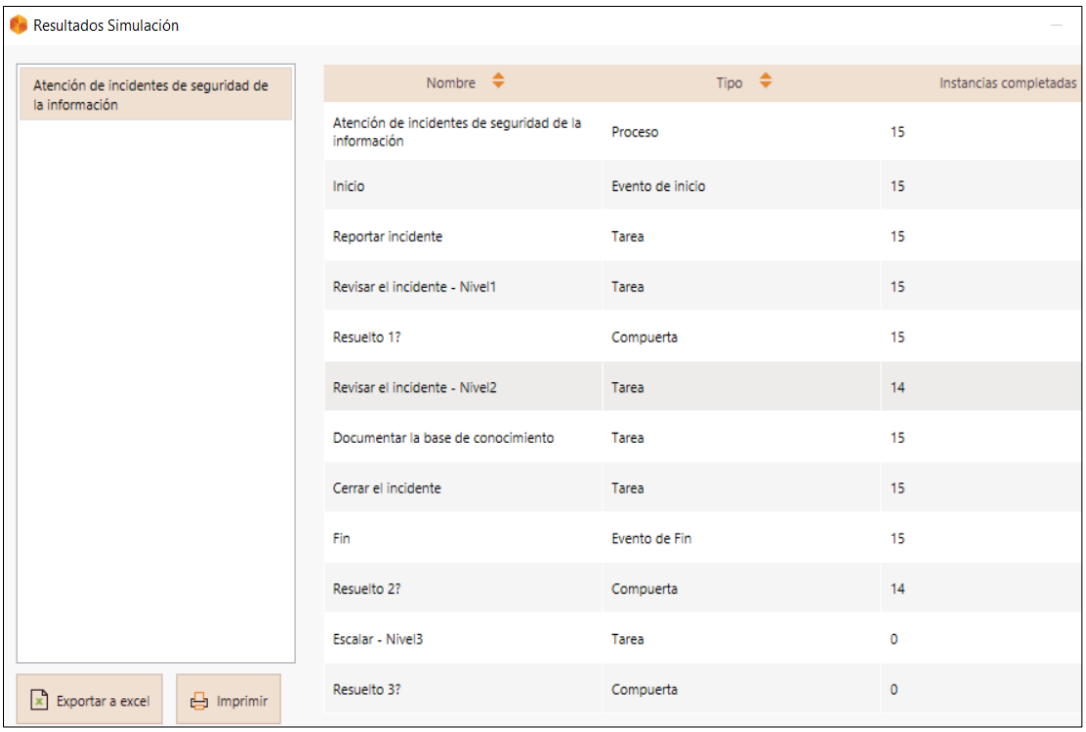



*Figura 4.13*: Validación del proceso del Grupo Experimental.

Se muestra las instancias completadas cuando se ejecutan el total de incidentes de seguridad reportados. Como se puede apreciar ningún incidente de seguridad fue escalado, por lo que todos los incidentes fueron resueltos. Estos resultados se muestran en la tabla 4.5 en la ejecución No. 1, de igual para las demás ejecuciones seleccionadas, se ha seguido el mismo método de trabajo.

En la figura 4.14 se puede apreciar los resultados.




| Nombre | Tipo | Instancias completadas |
|---|---|---|
| Atención de incidentes de seguridad de la información | Proceso | 15 |
| Inicio | Evento de inicio | 15 |
| Reportar incidente | Tarea | 15 |
| Revisar el incidente - Nivel1 | Tarea | 15 |
| Resuelto 1? | Compuerta | 15 |
| Revisar el incidente - Nivel2 | Tarea | 14 |
| Documentar la base de conocimiento | Tarea | 15 |
| Cerrar el incidente | Tarea | 15 |
| Fin | Evento de Fin | 15 |
| Resuelto 2? | Compuerta | 14 |
| Escalar - Nivel3 | Tarea | 0 |
| Resuelto 3? | Compuerta | 0 |

*Figura 4.14*: Resultado de la validación de proceso del Grupo Experimental

Como se aprecia en la tabla 4.5, el grupo experimental lo constituyen 30 ejecuciones seleccionadas aleatoriamente, en los cuales se les ha medido el grado de acierto ante los incidentes de seguridad que se suscitan en cada grupo de procesos para las nuevas condiciones, esto es con la aplicación del modelo sistémico de seguridad de la información. De la relación entre los incidentes de seguridad que fueron resueltas y el total de ellas, se ha calculado la eficacia por cada ejecución.

**Tabla 4.5**

*Porcentaje de acierto para resolver los incidentes de seguridad del Grupo Experimental*

| No. de ejecuciones | Incidentes de seguridad | | Grado de acierto en resolver incidentes de seguridad (%) |
|---|---|---|---|
| | Total de incidentes | No solucionadas | |
| 1 | 15 | 0 | 100 |
| 2 | 18 | 1 | 94.44 |
| 3 | 21 | 1 | 95.24 |
| 4 | 17 | 1 | 94.12 |
| 5 | 23 | 1 | 95.65 |
| 6 | 19 | 0 | 100 |
| 7 | 16 | 1 | 93.75 |
| 8 | 24 | 1 | 95.83 |
| 9 | 20 | 1 | 95 |
| 10 | 23 | 1 | 95.65 |
| 11 | 25 | 2 | 92 |
| 12 | 22 | 1 | 95.45 |
| 13 | 23 | 1 | 95.65 |
| 14 | 19 | 1 | 94.74 |
| 15 | 25 | 1 | 96 |
| 16 | 28 | 1 | 96.43 |
| 17 | 26 | 2 | 92.31 |
| 18 | 27 | 1 | 96.3 |
| 19 | 16 | 1 | 93.75 |
| 20 | 23 | 1 | 95.65 |
| 21 | 29 | 3 | 89.66 |
| 22 | 18 | 1 | 94.44 |
| 23 | 15 | 0 | 100 |
| 24 | 27 | 1 | 96.3 |
| 25 | 22 | 2 | 90.91 |
| 26 | 28 | 2 | 92.86 |
| 27 | 18 | 1 | 94.44 |
| 28 | 24 | 2 | 91.67 |
| 29 | 17 | 1 | 94.12 |
| 30 | 25 | 2 | 92 |
| | | **Promedio** | 94.81 |
| | | **Desv. Standard** | 2.46 |

## 2. ANÁLISIS

De los resultados obtenidos podemos analizar que si bien, en algunos grupos de procesos se resolvió al 100% los incidentes de seguridad, en otros, no fue resuelto, por ello es importante que la gestión de la seguridad de la información tiene que

estar en un proceso de mejora continua, para aprender de las fallas o vulnerabilidades.

Al calcular el promedio del total de incidentes resueltos sobre el total de incidentes reportados se obtiene como valor de 94.81%, que revela una mejora significativa de la eficacia del sistema.

#### 4.1.2.3. PARA EL INDICADOR: GRADO DE USO DEL RECURSO HUMANO PARA RESOLVER LOS INCIDENTES DE SEGURIDAD

##### 1. RESULTADOS

Para evaluar el comportamiento del indicador es necesario el grado de uso de uno de los principales recursos en resolver los incidentes de seguridad de la información que se dan en los procesos de negocio, como es el recurso humano.

Usando el simulador de Bizagi en el nivel **Análisis de Recursos**, se define las personas que están disponibles y en qué tareas se utilizan. Para un mejor análisis se toman en cuenta dos escenarios.

Para el escenario No.1 se toman dos personas del recurso “Mesa de ayuda”, una persona del recurso “Personal de sistemas” y una persona del recurso “Experto”. En total cuatro personas, como se muestra en la figura 4.15.

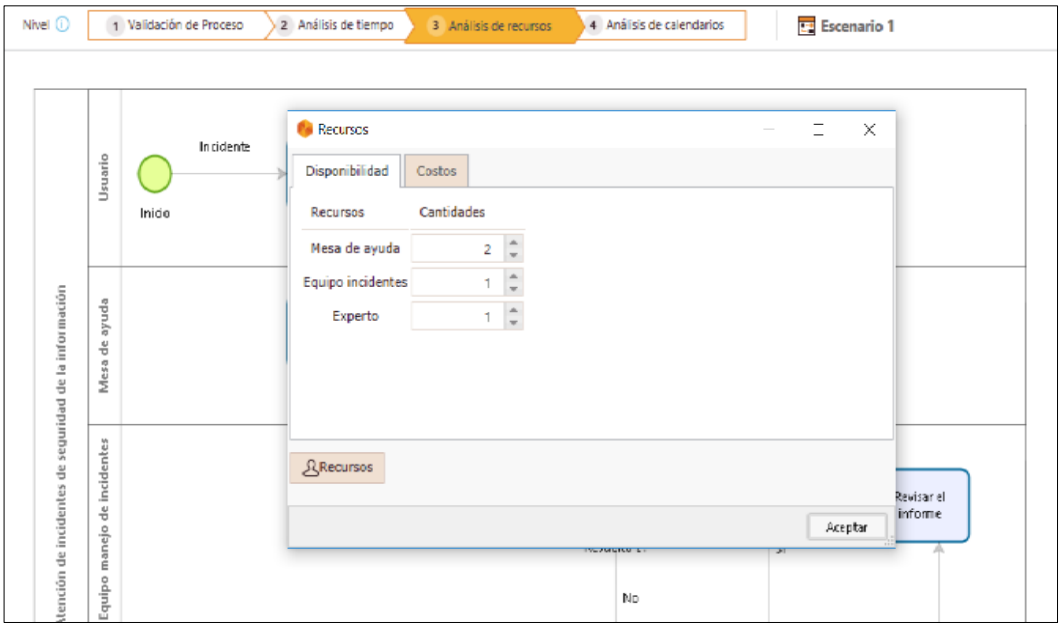



*Figura 4.15*: Disponibilidad de recursos del escenario No. 1 del Grupo Experimental

Para el escenario No. 2 se toman dos personas del recurso “Mesa de ayuda”, y se está considerando una persona más en el recurso “Personal de sistemas”, es decir ahora son dos personas y una persona del recurso “Experto”. En total cinco personas como se muestra en la figura 4.16.

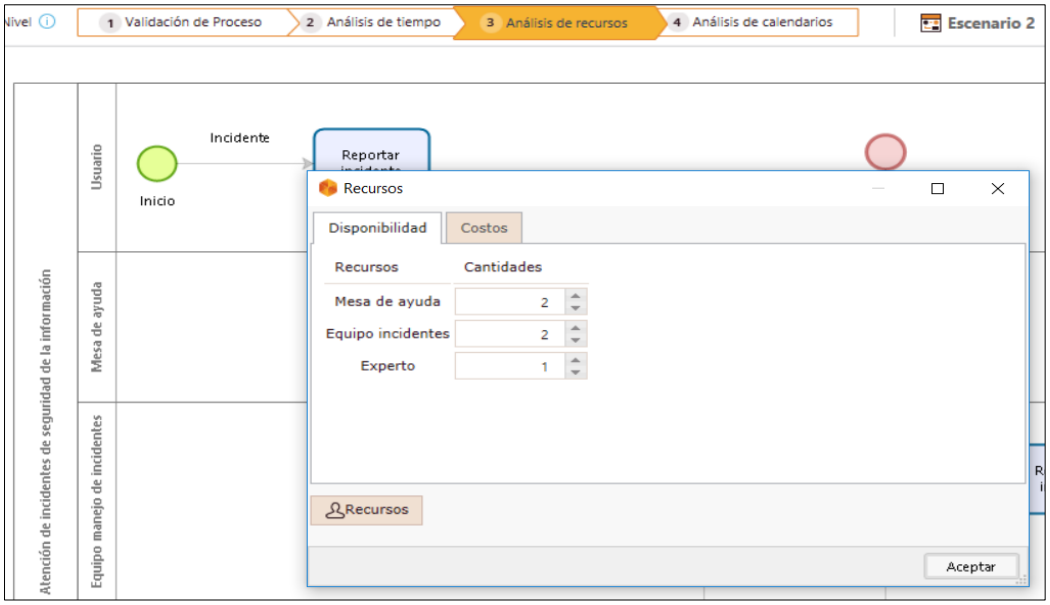



*Figura 4.16*: Disponibilidad de recursos del escenario No. 2. del Grupo Experimental

También se toma en cuenta la disponibilidad de los recursos en los turnos u horarios para obtener una mejor aproximación al rendimiento del proceso real. Se han definido 2 turnos: Mañana y tarde, y en el horario de refrigerio también se ha definido las personas que atienden.

Para un mejor análisis, en el simulador de Bizagi, en el nivel: **Análisis de calendarios** se utiliza 2 escenarios. Al ejecutar la simulación se muestran los resultados en la figura 4.17.

Se elige el escenario No. 2 porque usa un menor porcentaje de recursos. En el recurso Mesa de ayuda el porcentaje de uso de recurso es 2.73%, del recurso Sistema el porcentaje es 1.77% y del recurso Experto el porcentaje es 0.28%.

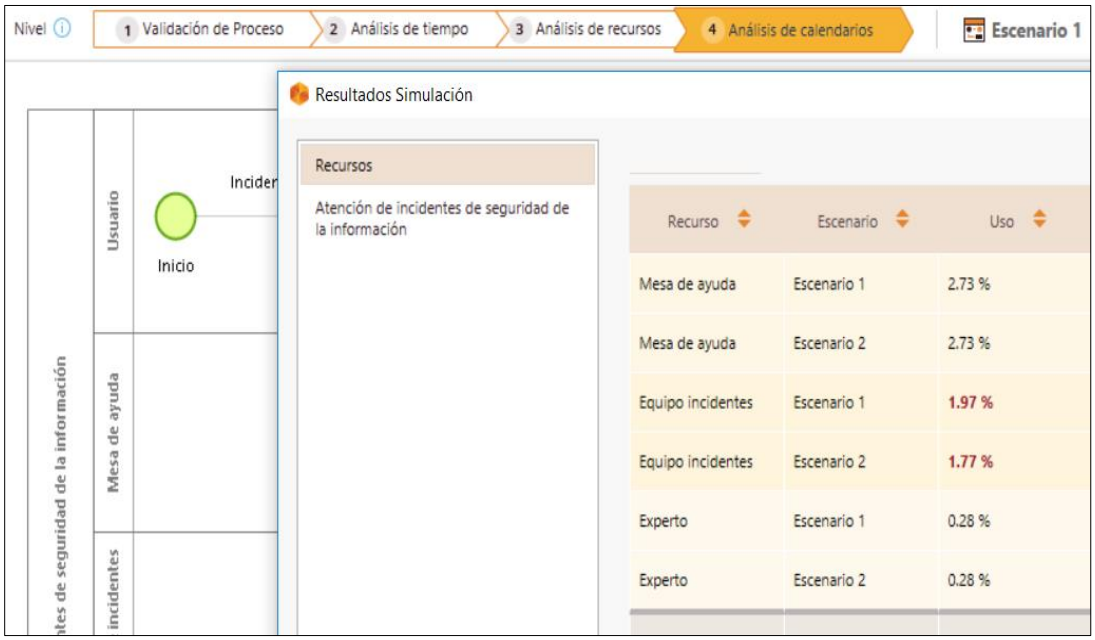



*Figura 4.17*: Resultados del uso de recurso de 2 escenarios del Grupo Experimental

La suma de ellos es 4.78%, y este valor se muestra en la tabla 4.6 en la ejecución No. 1. De igual forma para las demás ejecuciones seleccionadas se ha seguido el mismo método de trabajo. En el grupo experimental lo constituyen 30 ejecuciones seleccionadas aleatoriamente, que es el tamaño de la muestra representativa. Se ha identificado el número de personas que intervienen en responder el incidente, el porcentaje de participación o uso del recurso y los minutos por mes que el personal está disponible. Los minutos por mes se obtiene como promedio de 8 horas diarias de trabajo por 5 días por 4 semanas lo cual hace 160 horas mensual y equivalente en minutos se tiene 9600 minutos por mes.

De esta manera el grado de uso del recurso humano para resolver los incidentes de seguridad, se determina la relación entre el número de incidentes de seguridad y el número de personas-minutos por cada ejecución (grupo de procesos).

El promedio del grado de uso del recurso humano para resolver incidentes de seguridad es de 0.00836 incidentes/persona-minuto.

**Tabla 4.6**
*Grado de uso del recurso humano para resolver incidentes de seguridad del Grupo Experimental*

| Nro. de ejecuciones | PRODUCCION | RECURSOS USADOS | | | Grado de uso del recurso humano |
|---|---|---|---|---|---|
| | Incidentes de seguridad | Personas | % Uso de Recurso | Minutos por mes | Incid./Persona-minuto |
| 1 | 15 | 5 | 4.78 | 9600 | 0.00654 |
| 2 | 18 | 5 | 5.71 | 9600 | 0.00657 |
| 3 | 21 | 6 | 6.44 | 9600 | 0.00566 |
| 4 | 17 | 5 | 5.08 | 9600 | 0.00697 |
| 5 | 23 | 6 | 5.89 | 9600 | 0.00678 |
| 6 | 19 | 5 | 5.40 | 9600 | 0.00733 |
| 7 | 16 | 5 | 4.75 | 9600 | 0.00702 |
| 8 | 24 | 6 | 6.03 | 9600 | 0.00691 |
| 9 | 20 | 5 | 5.77 | 9600 | 0.00722 |
| 10 | 23 | 7 | 4.24 | 9600 | 0.00807 |
| 11 | 25 | 7 | 4.92 | 9600 | 0.00756 |
| 12 | 22 | 7 | 4.38 | 9600 | 0.00747 |
| 13 | 23 | 6 | 4.58 | 9600 | 0.00872 |
| 14 | 19 | 6 | 3.89 | 9600 | 0.00848 |
| 15 | 25 | 6 | 5.01 | 9600 | 0.00866 |
| 16 | 28 | 7 | 4.36 | 9600 | 0.00956 |
| 17 | 26 | 6 | 5.31 | 9600 | 0.00850 |
| 18 | 27 | 5 | 5.11 | 9600 | 0.01101 |
| 19 | 16 | 5 | 3.03 | 9600 | 0.01100 |
| 20 | 23 | 7 | 3.88 | 9600 | 0.00882 |
| 21 | 29 | 7 | 4.61 | 9600 | 0.00936 |
| 22 | 18 | 6 | 3.17 | 9600 | 0.00986 |
| 23 | 15 | 6 | 2.81 | 9600 | 0.00927 |
| 24 | 27 | 6 | 5.59 | 9600 | 0.00839 |
| 25 | 22 | 5 | 5.32 | 9600 | 0.00862 |
| 26 | 28 | 6 | 5.82 | 9600 | 0.00835 |
| 27 | 18 | 5 | 4.32 | 9600 | 0.00868 |
| 28 | 24 | 6 | 4.79 | 9600 | 0.00870 |
| 29 | 17 | 5 | 3.19 | 9600 | 0.01110 |
| 30 | 25 | 6 | 4.63 | 9600 | 0.00937 |
| | | | | **Promedio** | 0.00835 |
| | | | | **Desv. Standard** | 0.00137 |

## 2. ANÁLISIS

De los resultados obtenidos podemos analizar que si disminuimos el número de personal de los recursos: mesa de ayuda y equipo de incidentes, el porcentaje de utilización de recursos se incrementa (ver figura 4.17), y esto afecta el equipo de incidentes que se caracteriza por ser un equipo especializado en temas de seguridad. Para calcular el promedio de la productividad del personal se toma en cuenta el número

de personas y el grado de participación en la atención de los incidentes de seguridad, por tanto, es importante considerar el efecto de la disponibilidad de los recursos que intervienen en la atención de incidentes, como también sus horarios o turnos de atención, esto nos dará una mejor aproximación al rendimiento del proceso real.

## 4.2. CONTRASTACIÓN DE HIPÓTESIS

Conceptualmente, una hipótesis en el contexto de la estadística inferencial es una proposición respecto a uno o varios parámetros, y lo que el investigador hace a través de la prueba de hipótesis, es determinar si ésta es consistente con los datos obtenidos en la muestra, para ello, a continuación, se formula la hipótesis de investigación, la hipótesis nula y las correspondientes pruebas estadísticas.

### 4.2.1. HIPÓTESIS DE INVESTIGACIÓN

Se trata de demostrar que, la aplicación adecuada del Modelo Sistémico de Seguridad de la Información basado en BPM (variable independiente) contribuye en forma significativa en la competitividad funcional de las universidades. Desde este punto de vista, resulta razonable inferir que, se mejorará la competitividad funcional del resto de las universidades (variable dependiente).

En términos concretos, la hipótesis de investigación queda planteada en los siguientes términos:

| | |
|---|---|
| Ha = | Si se implementa un Modelo Sistémico de Seguridad de la Información basado en BPM MEJORARÁ la competitividad funcional de las universidades |

### 4.2.2. HIPÓTESIS NULA

| | |
|---|---|
| Ho= | Si se implementa un Modelo Sistémico de Seguridad de la Información basado en BPM NO MEJORARÁ la competitividad funcional de las universidades |

### 4.2.3. PRUEBA ESTADÍSTICA PARÁMETRICA UTILIZADA

Para compatibilizar el tipo de investigación y el diseño seleccionado, se ha utilizado como método de prueba estadística de la hipótesis, la denominada prueba de "t" de Student, que es una prueba estadística para evaluar si dos grupos difieren entre sí de manera significativa respecto a sus valores promedio. Su fórmula es:

$$t = \frac{\overline{x_1} - \overline{x_2}}{\sqrt{\frac{S_1^{\,2}}{N_1} + \frac{S_2^{\,2}}{N_2}}}$$

Donde:

$\overline{x}_1$= Media del grupo experimental

$\overline{x}_2$= Media del grupo de control

$S_1^2$= Desviación estándar del grupo experimental elevado al cuadrado

$S_2^2$= Desviación estándar del grupo de control elevado al cuadrado

$N_1$=Tamaño de la muestra del grupo experimental

$N_2$=Tamaño de la muestra del grupo de control

#### 4.2.3.1. PRUEBA DE HIPÓTESIS PARA EL INDICADOR: TIEMPO MEDIO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

Consolidado los valores de las tablas 4.1 y 4.4 en la tabla 4.7, se aprecia el comportamiento marcadamente diferente para el grupo de control y para el grupo experimental. Con esta información se procede a calcular el valor de t.

**Tabla 4.7**
*Resumen del tiempo medio de respuesta ante incidentes de seguridad*

| Grupo | Tamaño | Promedio (%) | Desviación Standard |
|---|---|---|---|
| De control | 30 | 88.06 | 1.98 |
| Experimental | 30 | 92.62 | 2.47 |

Grados de libertad:

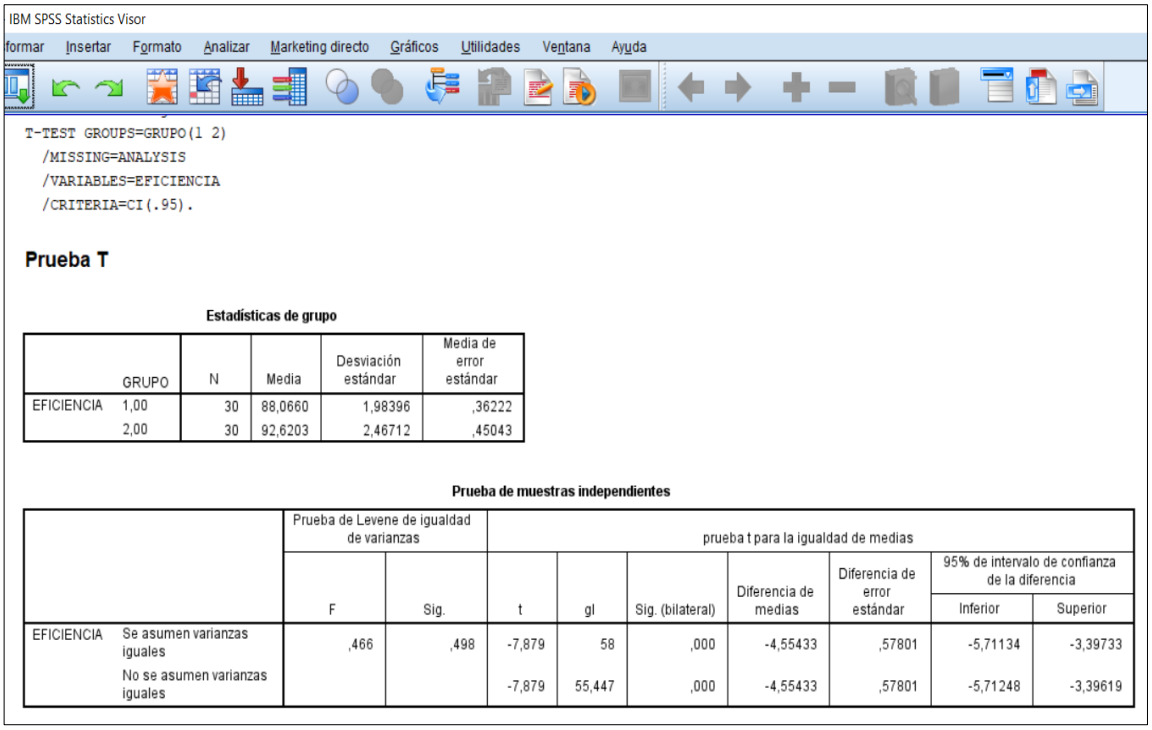
GL = (N1+N2)-2

GL = (30+30)-2

GL = 58

El valor t calculado bajo las características planteadas es de 7.879. Entonces para un nivel de confianza del 95%, un margen de error de 5% y con 58 grados de libertad, se obtiene de la tabla t de Student del Anexo 3, el valor teórico de 1.734; en consecuencia, al ser mayor el valor calculado que el valor teórico, se rechaza la hipótesis nula, por tanto, el Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el tiempo medio de respuesta ante incidentes de seguridad en los procesos críticos de las universidades.

También se ha usado la herramienta SPSS donde primero cargamos los datos de la tabla 4.1 del grupo de control y los datos de la tabla 4.4 del grupo experimental, para luego ejecutar la prueba “t” de Student para muestras independientes y los resultados se visualizan en la figura 4.18.



IBM SPSS Statistics Visor

formar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ventana Ayuda

```
T-TEST GROUPS=GRUPO(1 2)
  /MISSING=ANALYSIS
  /VARIABLES=EFICIENCIA
  /CRITERIA=CI(.95).
```

**Prueba T**

**Estadísticas de grupo**

| | GRUPO | N | Media | Desviación estándar | Media de error estándar |
|---|---|---|---|---|---|
| EFICIENCIA | 1,00 | 30 | 88,0660 | 1,98396 | ,36222 |
| | 2,00 | 30 | 92,6203 | 2,46712 | ,45043 |

**Prueba de muestras independientes**

| | | Prueba de Levene de igualdad de varianzas | | prueba t para la igualdad de medias | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% de intervalo de confianza de la diferencia | |
| | | F | Sig. | t | gl | Sig. (bilateral) | Diferencia de medias | Diferencia de error estándar | Inferior | Superior |
| EFICIENCIA | Se asumen varianzas iguales | ,466 | ,498 | -7,879 | 58 | ,000 | -4,55433 | ,57801 | -5,71134 | -3,39733 |
| | No se asumen varianzas iguales | | | -7,879 | 55,447 | ,000 | -4,55433 | ,57801 | -5,71248 | -3,39619 |

*Figura 4.18*: Resultado de prueba "t" de Student para la variable "Eficiencia"

En el primer cuadro se muestra la variable "Eficiencia" con los 2 grupos: 1 grupo de control y 2 grupo experimental, y sus valores de media y desviación estándar. En el segundo cuadro en la columna prueba t para la igualdad de medias, se muestra el valor t: 7.879 y con un valor de significancia de 0.000 menor a 0.05 que es el margen de error. Por tanto, se rechaza la hipótesis nula ya que hay una diferencia significativa en el Modelo Sistémico de Seguridad de la Información basado en BPM para mejorar el tiempo medio de respuesta ante incidentes de seguridad de los procesos críticos de las universidades.

### 4.2.3.2. PRUEBA DE HIPÓTESIS PARA EL INDICADOR: PORCENTAJE DE ACIERTO EN RESOLVER LOS INCIDENTES DE SEGURIDAD

Consolidado los valores de las tablas 4.2 y 4.5 en la tabla 4.8, se aprecia el comportamiento marcadamente diferente para el grupo de control y para el grupo experimental. Con esta información se procede a calcular el valor de t.

**Tabla 4.8**
*Resumen de porcentaje de acierto en resolver los incidentes de seguridad*

| Grupo | Tamaño | Promedio (%) | Desviación Standard |
|---|---|---|---|
| De control | 30 | 89.83 | 2.48 |
| Experimental | 30 | 94.81 | 2.46 |

Grados de libertad:

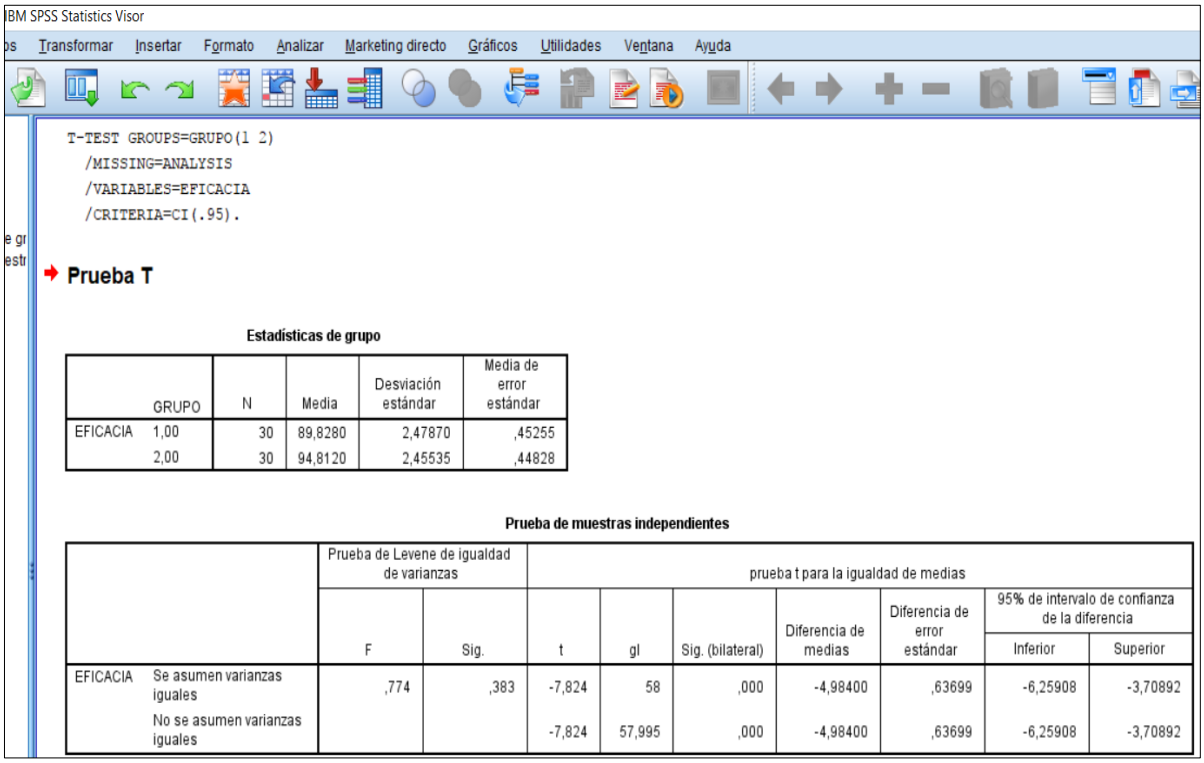
GL = (N1+N2)-2

GL = (30+30)-2

GL = 58

El valor t calculado bajo las características planteadas es de 7.824. Entonces para un nivel de confianza del 95%, un margen de error de 5% y con 58 grados de libertad, se obtiene de la tabla t de Student del Anexo 3, el valor teórico de 1.734; en consecuencia, al ser mayor el valor calculado que el valor teórico, se rechaza la hipótesis nula, por tanto, el Modelo Sistémico de Seguridad de la Información basado en BPM mejora el porcentaje de acierto en resolver los incidentes de seguridad de los procesos críticos de las universidades.

También se ha usado la herramienta SPSS donde primero cargamos los datos de la tabla 4.2 del grupo de control y los datos de la tabla 4.5 del grupo experimental, para luego ejecutar la prueba “t” de Student para muestras independientes y los resultados se visualizan en la figura 4.19.



IBM SPSS Statistics Visor

Transformar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ventana Ayuda

```
T-TEST GROUPS=GRUPO(1 2)
  /MISSING=ANALYSIS
  /VARIABLES=EFICACIA
  /CRITERIA=CI(.95).
```

**Prueba T**

**Estadísticas de grupo**

| | GRUPO | N | Media | Desviación estándar | Media de error estándar |
|---|---|---|---|---|---|
| EFICACIA | 1,00 | 30 | 89,8280 | 2,47870 | ,45255 |
| | 2,00 | 30 | 94,8120 | 2,45535 | ,44828 |

**Prueba de muestras independientes**

| | | Prueba de Levene de igualdad de varianzas | | prueba t para la igualdad de medias | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% de intervalo de confianza de la diferencia | |
| | | F | Sig. | t | gl | Sig. (bilateral) | Diferencia de medias | Diferencia de error estándar | Inferior | Superior |
| EFICACIA | Se asumen varianzas iguales | ,774 | ,383 | -7,824 | 58 | ,000 | -4,98400 | ,63699 | -6,25908 | -3,70892 |
| | No se asumen varianzas iguales | | | -7,824 | 57,995 | ,000 | -4,98400 | ,63699 | -6,25908 | -3,70892 |

*Figura 4.19*: Resultado de prueba "t" de Student para la variable "Eficacia"

En el primer cuadro se muestra la variable "Eficacia" con los 2 grupos: 1 grupo de control y 2 grupo experimental, y sus valores de media y desviación estándar. En el segundo cuadro en la columna prueba t para la igualdad de medias, se muestra el valor t: 7.824 y con un valor de significancia de 0.000 menor a 0.05 que es el margen de error. Por tanto, se rechaza la hipótesis nula ya que hay una diferencia significativa en el Modelo Sistémico de Seguridad de la Información basado en BPM para mejorar el porcentaje de acierto en resolver los incidentes de seguridad de los procesos críticos de las universidades.

### 4.2.3.3. PRUEBA DE HIPÓTESIS PARA EL INDICADOR: GRADO DE USO DE RECURSO HUMANO EN RESOLVER LOS INCIDENTES DE SEGURIDAD

Consolidado los valores de las tablas 4.3 y 4.6 en la tabla 4.9, se aprecia el comportamiento marcadamente diferente para el grupo de control y para el grupo experimental. Con esta información se procede a calcular el valor de t.

**Tabla 4.9**
*Resumen del grado de uso de recurso humano en resolver los incidentes de seguridad*

| Grupos | Tamaño | Promedio (%) | Desviación Standard |
|---|---|---|---|
| De control | 30 | 0.00614 | 0.00097 |
| Experimental | 30 | 0.00835 | 0.00137 |

Grados de libertad:

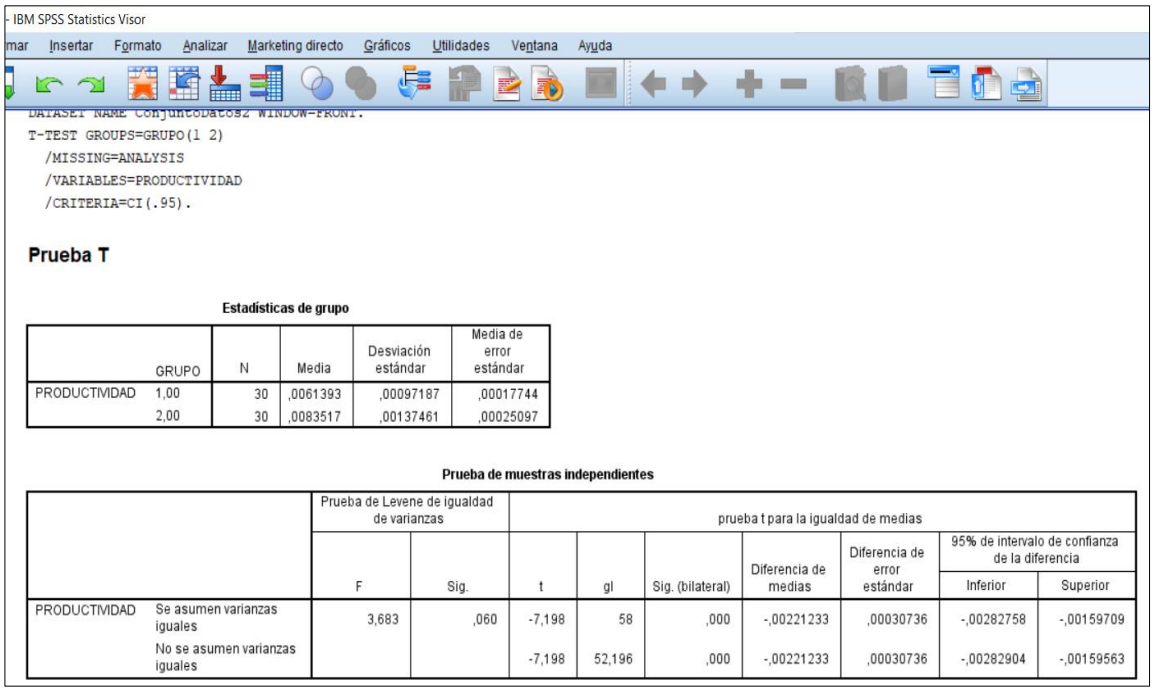
GL = (N1+N2)-2

GL = (30+30)-2

GL = 58

El valor t de calculado bajo las características planteadas es de 7.198. Entonces para un nivel de confianza de 95%, un margen de error de 5% y con 58 grados de libertad, se obtiene de la tabla de t de Student del Anexo 3, el valor teórico de 1.734; en consecuencia, al ser mayor el valor calculado que el valor teórico, se rechaza la hipótesis nula, por tanto, el Modelo Sistémico de Seguridad de la Información basado en BPM mejora el grado de uso de recurso humano en resolver los incidentes de seguridad de los procesos críticos de las universidades.

También se ha usado la herramienta SPSS donde primero cargamos los datos de la tabla 4.3 del grupo de control y los datos de la tabla 4.6 del grupo experimental, para luego ejecutar la prueba “t” de Student para muestras independientes y los resultados se muestran en la figura 4.20.



IBM SPSS Statistics Visor

mar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ventana Ayuda

```
DATASET NAME ConjuntoDatos2 WINDOW=FRONT.
T-TEST GROUPS=GRUPO(1 2)
  /MISSING=ANALYSIS
  /VARIABLES=PRODUCTIVIDAD
  /CRITERIA=CI(.95).
```

**Prueba T**

**Estadísticas de grupo**

| | GRUPO | N | Media | Desviación estándar | Media de error estándar |
|---|---|---|---|---|---|
| PRODUCTIVIDAD | 1,00 | 30 | ,0061393 | ,00097187 | ,00017744 |
| | 2,00 | 30 | ,0083517 | ,00137461 | ,00025097 |

**Prueba de muestras independientes**

| | | Prueba de Levene de igualdad de varianzas | | prueba t para la igualdad de medias | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% de intervalo de confianza de la diferencia | |
| | | F | Sig. | t | gl | Sig. (bilateral) | Diferencia de medias | Diferencia de error estándar | Inferior | Superior |
| PRODUCTIVIDAD | Se asumen varianzas iguales | 3,683 | ,060 | -7,198 | 58 | ,000 | -,00221233 | ,00030736 | -,00282758 | -,00159709 |
| | No se asumen varianzas iguales | | | -7,198 | 52,196 | ,000 | -,00221233 | ,00030736 | -,00282904 | -,00159563 |

*Figura 4.20*: Resultado de prueba “t” de Student para la variable “Productividad”

En el primer cuadro se muestra la variable” Productividad” con los 2 grupos: 1 grupo de control y 2 grupo experimental, y sus valores de media y desviación estándar. En el segundo cuadro en la columna prueba “t” para la igualdad de medias, se muestra el valor t: 7.198 y con un valor de significancia de 0.000 menor a 0.05 que es el margen de error. Por tanto, se rechaza la hipótesis nula ya que hay una diferencia significativa en el Modelo Sistémico de Seguridad de la Información basado en BPM para mejorar el grado de uso de recurso humano en resolver los incidentes de seguridad de los procesos críticos de las universidades.

.

# CAPÍTULO V
# CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONES

1. El Modelo Sistémico de Seguridad de la Información contribuye a las universidades obtener información más relevante y medible, y a la vez retroalimentar los procesos de seguridad para determinar las falencias de seguridad y aplicar las propuestas de solución, para así lograr la mejora en la gestión de seguridad de la información.

2. El Modelo Sistémico de Seguridad de la Información permite incrementar la confianza y la reputación corporativa de las universidades hacia los estudiantes, egresados, docentes, investigadores y empleados.

3. Al construirse el Modelo Sistémico de Seguridad de la Información basado en BPM en las universidades, el rendimiento del indicador tiempo medio de respuesta ante incidentes de seguridad, mejora favorablemente, pasando de 88.06% para el grupo de control a 92.62% para el grupo experimental.

4. La construcción y aplicación del Modelo Sistémico de Seguridad de la Información basado en BPM en las universidades mejora el rendimiento del indicador porcentaje de acierto ante incidentes de seguridad de la información de los procesos de negocio. Se pasa de 89.83% a 94.81%.

5. Al construirse el modelo sistémico seguridad de la información basado en BPM en las universidades mejora el rendimiento del indicador de grado de uso de recurso humano ante incidentes de seguridad. Los resultados demuestran un incremento de la intervención del recurso humano para resolver los incidentes de seguridad con 0.00614 incidencias/persona-minutos para el grupo de control,

contrastado con el valor de 0.00835 incidencias/persona-minutos para el grupo de experimental.

6. El valor t calculado para el indicador tiempo medio de respuesta ante incidentes de seguridad es 7.879, el mismo que al compararse con su valor teórico correspondiente a 58 grados de libertad (1.734), se observa que el primero es mayor, ello permite concluir que se acepta esta hipótesis de investigación y, por contraposición, se rechaza la hipótesis nula. Concretamente, la tesis enunciada es la siguiente: Si se implementa un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el tiempo medio de respuesta ante incidentes de seguridad de los procesos críticos de las universidades.

7. El valor t calculado para el indicador porcentaje de acierto ante incidentes de seguridad es 7.824, el mismo que al compararse con su valor teórico correspondiente a 58 grados de libertad (1.734), se observa que el primero es mayor, ello permite concluir que se acepta esta hipótesis de investigación y, por contraposición, se rechaza la hipótesis nula. Concretamente, la tesis enunciada es la siguiente: Si se implementa un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el porcentaje de acierto ante incidentes de seguridad de los procesos críticos de las universidades.

8. El valor t calculado para el indicador grado de uso de recurso humano ante incidentes de seguridad es 7.198, el mismo que al compararse con su valor teórico correspondiente a 58 grados de libertad (1.734), se observa que el primero es mayor, ello permite concluir que se acepta esta hipótesis de investigación y, por contraposición, se rechaza la hipótesis nula. Concretamente, la tesis enunciada es la siguiente: Si se implementa un Modelo Sistémico de Seguridad de la Información basado en BPM mejorará el grado de uso de recurso humano ante incidentes de seguridad de los procesos críticos de las universidades.

9. Podemos afirmar que el Modelo Sistémico de Seguridad de la Información basado en BPM contribuye a mejorar la competitividad funcional de las universidades y,

por generalización a la gestión académica y administrativa de todas las instituciones educativas que la apliquen.

10. El Modelo Sistémico de Seguridad de la Información también es aplicable a toda clase de organización, sin importar su tipo, el tamaño y la naturaleza del negocio

## 5.2. RECOMENDACIONES

1. Alinear los objetivos del Modelo Sistémico de Seguridad de la Información con los objetivos de la universidad y que no sea visto como un gasto sino como una inversión.

2. Crear una cultura de trabajo y gestión a través de un Modelo Sistémico de Seguridad más transversal no sólo en los actores ligados a la tecnología de la información sino con todas las partes interesadas.

3. Se tiene que prestar principal atención a los eventos de seguridad de la información, para ello se debe establecer los niveles de atención de incidentes de seguridad en la universidad.

4. Implementar acciones que garanticen un cambio de comportamiento en las personas con respecto a la seguridad que es lo que se tienen que medir, no sometiéndolas a capacitaciones y actividades de sensibilización interminables.

5. Mejorar las prioridades de los modelos de seguridad de la información en no solo darle máxima oportunidad al aspecto documental dejando de lado el cumplimiento de los objetivos como es el apoyo al objetivo del negocio; perspectiva que deben ser corregidas tanto por los implementadores como los auditores.

## REFERENCIAS BIBLIOGRÁFICAS


Alexander, A. G. (2007). Diseño de un Sistema de Gestión de Seguridad de la Información. Bogotá, Colombia: Alfaomega Colombiana.

Alberts, C. y Dorofee, A. (2003). *Managing Information Security Risk.* Addison Wesley.

Arjonilla, S. y Medina, J. (2010). *La gestión de los sistemas de Información en la empresa.* Madrid, España: Pirámide.

Campbell, S. y McCarthy M. (2002). *Seguridad digital: Estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía.* España: Mcgraw-Hill / Interamericana de España

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática.* México: Alfaomega Grupo Editor.

Gonzáles, M. y Codagnone T. (2004). La organización universitaria. IV Coloquio Internacional sobre Gestión Universitaria en América del Sur. Coloquio llevado a cabo en Florianópolis, Brasil.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (1997). *Metodología de la Investigación*. México: Mc Graw – Hill

Ísmodes, Eduardo. (2014). *Cambiar la universidad en el Perú: una contribución a partir de la experiencia E-quipu.* Lima, Perú: Fondo Editorial de la Asamblea Nacional de Rectores.

ISACA (2009). An Introduction to the Business Model for Information Security. Recuperado de: http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf

ISO 9000:2005. Sistemas de gestión de la calidad – Fundamentos y vocabulario. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-3:v1:es

ISO 9001:2008. Sistemas de gestión de la calidad Requisitos. Recuperado de: https://www.iso.org/obp/ui#iso:std:iso:9001:ed-4:v2:es

ISO/IEC 27000:2016. Information technology-Security techniques-Information security management systems-Overview and vocabulary. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

ISO 31000:2009. Risk Management-Principles and guidelines. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

ISO/IEC Guide 73:2002. Risk Management-Vocabulay-Guidelines for use in standards. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Lane, J. y Owens, T. (2012). *Higher Education and Economic Competitiveness.* Measuring Higher Education's Role in Economic Development (pp. 205-237). New York: Suny Press.

Laudon, K. y Laudon, J. (2012). *Sistemas de Información Gerencial*. México: Pearson Educación.

Leavitt, Harold J. (1965). *Applied organizational change in industry: structural, technological and humanistic approaches in: Handbook Organizations*, J.G. March. IL, USA:Chicago, Rand McNally.

López, S. (2016). Competitividad de la educación superior en cuatro países de América Latina: perspectiva desde un ranking mundial. *Revista de la Educación Superior*, 45 (178),45-59. Recuperado de: http://www.sciencedirect.com/science/article/pii/S0185276016000121

NTP-ISO/IEC 17799:2007. Tecnología de la información. Código de buenas prácticas para la gestión de seguridad de la información. Recuperado de: http://www.ongei.gob.pe/bancos/banco_normas/archivos/P01-PCM-ISO17799-001-V2.pdf

Peltier, T. (2001). *Information Security Risk Analisys*. Auerbach. London.

Porter, Michael (1991). *La ventaja competitiva de las naciones*. Buenos Aires. Vergara.

Pallas Mega, G.(2009). *Metodología de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) en un grupo empresarial jerárquico*. (Tesis de maestría, Universidad de la República). Recuperado de: https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PCM (2016). Resolución Ministerial (N° 004-2016-PCM). Recuperado de: http://www.pcm.gob.pe/wp-content/uploads/2016/01/RM_N_04-2016-PCM.pdf

Rainer, R. y Cegielski C. (2013). *Introduction to information Systems.* New York, USA: Wiley.

Rayme Serrano, R.(2007). *Gestión de Seguridad de la Información y los Servicios Críticos de las Universidades. Un estudio de tres casos en Lima Metropolitana.* (Tesis inédita de maestría). Universidad Nacional Mayor de San Marcos, Lima, Perú.

Rebollo Martínez, O. (2014). *Marco para el Gobierno de la Seguridad en Servicios de Cloud Computing*. Recuperado de: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/4121/TESIS%20Rebollo%20Mart%C3%ADnez.pdf?sequence=1

Ribagorda, A. (2004). *Avances en Criptología y Seguridad de la Información*. España: Editorial Díaz de Santos.

Ruiz Larrocha, E. (2010). *MISITILEON (metodología que integra seguridad en ITIL evolucionada y orientada a la Normalización*. (Tesis doctoral, Universidad Nacional de Educación a Distancia). Recuperado de: http://e-spacio.uned.es/fez/eserv/tesisuned:IngInf-Eruiz/Documento.pdf

Senge P. (1992). *La Quinta Disciplina.* Barcelona, España: Ediciones Granica.

Shinder, D. (2003). *Prevención y Detección de delitos informáticos.* Madrid: Ediciones Anaya Multimedia.

Trani, Eugene y Holsworth, Robert (2010). The indispensable University. Lanham: Rowman & Littlefield Publishers, Inc.

Viloria, O. y Blanco, W. (2009). Modelo sistémico de la seguridad de la información en las universidades. *Revista Venezolana de Análisis de Coyuntura*, XVI, (1), 219-240.

Villegas, M. (2008). *Modelo de madurez para la gestión y administración de la seguridad informática en las universidades.* Recuperado de: http://mendillo.info/seguridad/tesis/Villegas2.pdf

Wissema J. (2009). T*owards The Third Generation University*. Massachusetts: Edward Elgar Publishing.

## ANEXOS

## ANEXO 1. DECLARACIÓN JURADA DE CONFIDENCIALIDAD

| | | | |
|---|---|---|---|
| | **UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA**<br>**Gerencia de Recursos Humanos** | Código: | RHU-FR-05 |
| | | Versión: | 1.3 |
| | | Documento de Aprobación: | |
| | | Fecha de Aprobación: | 15.01.2015 |
| | **DECLARACIÓN JURADA DE CONFIDENCIALIDAD** | N° de página: | **1** de **1** |

DECLARACIÓN JURADA DE CONFIDENCIALIDAD

Conste por el presente documento, el conocimiento y la adhesión al ACUERDO DE CONFIDENCIALIDAD, que suscribe el personal de la UPSJB; que establece lo siguiente:

1. Toda Información relacionada a la operación de la Institución es confidencial y constituye secreto de esta, permanecerá como propiedad y negocio de la Institución.

   Los trabajadores están prohibidos de revelar y/o difundir y/o divulgar y/o publicar información confidencial. En esta prohibición se incluyen:

   - Información, Normas y Reglamentos que aún no sean comunicados fuera de la Institución.
   - Planes y estrategias de la Institución.
   - Información de Clientes y Proveedores.
   - Programas de computadoras.
   - Bases de datos e información en ellas contenidas.
   - Códigos de acceso (passwords) a redes de computadoras, equipos, sistemas o informaciones similares.
   - Información Operativa.

2. No se podrá hacer uso de ninguna información de la institución para propósitos personales ni de terceras personas.
3. Toda información confidencial impresa a ser desechada, será destruida de manera total, evitando que esta pueda ser reconstruida de los restos que quedan de ella.
4. Toda Información acerca de la Infraestructura Tecnológica de la Institución es CONFIDENCIAL y de carácter RESTRINGIDO.
   - La Plataforma Tecnológica de la Institución la constituye los elementos de red LAN/WAN, las direcciones IP, los nombres de Servidores, los Sistemas Operativos, las Bases de Datos, Sistemas de Información, Aplicaciones y planos de red LAN/WAN.
   - La ubicación, función, distribución y configuración de los elementos mencionados constituye información confidencial de la Institución.
   - La información parcial o total de esta plataforma sólo puede ser entregada a terceros por la Oficina de Sistemas de Información con autorización de la Dirección Ejecutiva.

5. Cualquier incumplimiento al acuerdo de confidencialidad será sancionado de acuerdo a lo establecido en el Reglamento Interno de Trabajo de la AUPSJB y el Código Penal vigente.

Ciudad y Fecha: …… _ FIRMA: ……..

Apellidos y Nombres: …… DNI N°: ……

## ANEXO 2. GUÍA DE CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD

1. Uso indebido de información:

   - ✓ Para fines personales, publicitarios, políticos o religiosos.
     Uso de la información y/o activos de información
   - ✓ Suplantación de identidad
     (Ejemplos: envío de correos a nombre de otra persona o Dependencia, el estudiante ha ingresado con el usuario y clave del docente para modificar sus calificaciones)

2. Destrucción no autorizada de información de la institución:

   - ✓ Formateo sin permiso y/o respaldo.
   - ✓ Eliminación de archivos sin permiso y/o respaldo.

3. Daño de dispositivos con información institucional

   - ✓ Daño físico de dispositivos que contengan información institucional.
     (Caída de líquidos, golpes, pérdida de información por aplicación de garantías)
   - ✓ Daño de la información contenida en dispositivos como memoria portátil, disco duro, discos ópticos, discos magnéticos, cintas, celulares, computadoras, etc.

4. Robo o pérdida de activo de información

   - ✓ Robo o pérdida de dispositivo (memoria portátil, disco duro, discos ópticos, discos magnéticos, cintas, celulares, computadoras, PDA, etc.) que contenga información institucional

5. Divulgación no autorizada de información personal

- ✓ Divulgación por cualquier medio de: domicilios, parentescos, teléfonos, bienes, estado de salud, creencias o preferencias sin autorización del dueño de la información, conforme a la Ley de Protección de datos personales y/o Reglamento de Transparencia y acceso a la Información de la Universidad Privada San Juan Bautista.
- ✓ Engaño (Ingeniería Social), Fraude y/o Extorsión.

6. Daño a activos de información por Acceso no autorizado a equipo informático

- ✓ Acceso físico a una computadora, servidor, celular y/o equipo de red.
- ✓ Acceso remoto a la información contenida en una computadora, servidor, celular y/o equipo de red.
- ✓ Acceso o intento no autorizado a un sistema informático, aplicación y/o base de datos.
- ✓ Servicio ftp no autorizado

7. Denegación del servicio
   - ✓ Cualquier actividad maliciosa tendiente a dificultar el acceso a un servicio

8. Modificación o eliminación no autorizada de un sistema, sitio o página web.

- ✓ Cambio o eliminación de cualquier dato contenido en un sistema, sitio, página web y/o base de datos.
- ✓ Cambio o eliminación de la programación del sistema, sitio, página web y/o base de datos.

9. Anomalía o vulnerabilidad técnica de sistemas.

- ✓ Encontrar una vulnerabilidad en la seguridad de un sistema informático.
- ✓ Encontrar un mal funcionamiento u operación de un sistema.
  Ejemplo: El docente registró las notas en el aula virtual pero no se grabó en el sistema

10. Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)

- ✓ Detección de un equipo informático (computadora o servidor) produciendo ataques a uno o varios equipos.
- ✓ Detección de un equipo (computadora o servidor) que está siendo atacado o colapsado.
- ✓ Destrucción, corrupción o filtración de información por infección de virus, gusanos, troyanos, etc.;
- ✓ Detección de alteración del usuario a la configuración o desactualización del antivirus.

11. Daños a la infraestructura;
    - ✓ Cortes eléctricos
    - ✓ Daños por agua
    - ✓ Sismos
    - ✓ Incendios
12. Creación de usuarios no autorizados
13. Cambios no autorizados en las configuraciones del equipamiento
14. Amenaza o acoso por un medio electrónico

## ANEXO 3. TABLA t DE STUDENT PARA P DE UNA SOLA COLA

| Grados de libertad | 0.25 | 0.1 | 0.05 | 0.025 | 0.01 | 0.005 |
|---|---|---|---|---|---|---|
| 1 | 1.0000 | 3.0777 | 6.3137 | 12.7062 | 31.8210 | 63.6559 |
| 2 | 0.8165 | 1.8856 | 2.9200 | 4.3027 | 6.9645 | 9.9250 |
| 3 | 0.7649 | 1.6377 | 2.3534 | 3.1824 | 4.5407 | 5.8408 |
| 4 | 0.7407 | 1.5332 | 2.1318 | 2.7765 | 3.7469 | 4.6041 |
| 5 | 0.7267 | 1.4759 | 2.0150 | 2.5706 | 3.3649 | 4.0321 |
| 6 | 0.7176 | 1.4398 | 1.9432 | 2.4469 | 3.1427 | 3.7074 |
| 7 | 0.7111 | 1.4149 | 1.8946 | 2.3646 | 2.9979 | 3.4995 |
| 8 | 0.7064 | 1.3968 | 1.8595 | 2.3060 | 2.8965 | 3.3554 |
| 9 | 0.7027 | 1.3830 | 1.8331 | 2.2622 | 2.8214 | 3.2498 |
| 10 | 0.6998 | 1.3722 | 1.8125 | 2.2281 | 2.7638 | 3.1693 |
| 11 | 0.6974 | 1.3634 | 1.7959 | 2.2010 | 2.7181 | 3.1058 |
| 12 | 0.6955 | 1.3562 | 1.7823 | 2.1788 | 2.6810 | 3.0545 |
| 13 | 0.6938 | 1.3502 | 1.7709 | 2.1604 | 2.6503 | 3.0123 |
| 14 | 0.6924 | 1.3450 | 1.7613 | 2.1448 | 2.6245 | 2.9768 |
| 15 | 0.6912 | 1.3406 | 1.7531 | 2.1315 | 2.6025 | 2.9467 |
| 16 | 0.6901 | 1.3368 | 1.7459 | 2.1199 | 2.5835 | 2.9208 |
| 17 | 0.6892 | 1.3334 | 1.7396 | 2.1098 | 2.5669 | 2.8982 |
| 18 | 0.6884 | 1.3304 | 1.7341 | 2.1009 | 2.5524 | 2.8784 |
| 19 | 0.6876 | 1.3277 | 1.7291 | 2.0930 | 2.5395 | 2.8609 |
| 20 | 0.6870 | 1.3253 | 1.7247 | 2.0860 | 2.5280 | 2.8453 |
| 21 | 0.6864 | 1.3232 | 1.7207 | 2.0796 | 2.5176 | 2.8314 |
| 22 | 0.6858 | 1.3212 | 1.7171 | 2.0739 | 2.5083 | 2.8188 |
| 23 | 0.6853 | 1.3195 | 1.7139 | 2.0687 | 2.4999 | 2.8073 |
| 24 | 0.6848 | 1.3178 | 1.7109 | 2.0639 | 2.4922 | 2.7970 |
| 25 | 0.6844 | 1.3163 | 1.7081 | 2.0595 | 2.4851 | 2.7874 |
| 26 | 0.6840 | 1.3150 | 1.7056 | 2.0555 | 2.4786 | 2.7787 |
| 27 | 0.6837 | 1.3137 | 1.7033 | 2.0518 | 2.4727 | 2.7707 |
| 28 | 0.6834 | 1.3125 | 1.7011 | 2.0484 | 2.4671 | 2.7633 |
| 29 | 0.6830 | 1.3114 | 1.6991 | 2.0452 | 2.4620 | 2.7564 |
| 30 | 0.6828 | 1.3104 | 1.6973 | 2.0423 | 2.4573 | 2.7500 |
| 31 | 0.6825 | 1.3095 | 1.6955 | 2.0395 | 2.4528 | 2.7440 |
| 32 | 0.6822 | 1.3086 | 1.6939 | 2.0369 | 2.4487 | 2.7385 |
| 33 | 0.6820 | 1.3077 | 1.6924 | 2.0345 | 2.4448 | 2.7333 |
| 34 | 0.6818 | 1.3070 | 1.6909 | 2.0322 | 2.4411 | 2.7284 |
| 35 | 0.6816 | 1.3062 | 1.6896 | 2.0301 | 2.4377 | 2.7238 |
| 36 | 0.6814 | 1.3055 | 1.6883 | 2.0281 | 2.4345 | 2.7195 |
| 37 | 0.6812 | 1.3049 | 1.6871 | 2.0262 | 2.4314 | 2.7154 |
| 38 | 0.6810 | 1.3042 | 1.6860 | 2.0244 | 2.4286 | 2.7116 |
| 39 | 0.6808 | 1.3036 | 1.6849 | 2.0227 | 2.4258 | 2.7079 |
| 40 | 0.6807 | 1.3031 | 1.6839 | 2.0211 | 2.4233 | 2.7045 |
| 41 | 0.6805 | 1.3025 | 1.6829 | 2.0195 | 2.4208 | 2.7012 |
| 42 | 0.6804 | 1.3020 | 1.6820 | 2.0181 | 2.4185 | 2.6981 |
| 43 | 0.6802 | 1.3016 | 1.6811 | 2.0167 | 2.4163 | 2.6951 |
| 44 | 0.6801 | 1.3011 | 1.6802 | 2.0154 | 2.4141 | 2.6923 |
| 45 | 0.6800 | 1.3007 | 1.6794 | 2.0141 | 2.4121 | 2.6896 |
| 46 | 0.6799 | 1.3002 | 1.6787 | 2.0129 | 2.4102 | 2.6870 |
| 47 | 0.6797 | 1.2998 | 1.6779 | 2.0117 | 2.4083 | 2.6846 |
| 48 | 0.6796 | 1.2994 | 1.6772 | 2.0106 | 2.4066 | 2.6822 |
| 49 | 0.6795 | 1.2991 | 1.6766 | 2.0096 | 2.4049 | 2.6800 |
| 50 | 0.6794 | 1.2987 | 1.6759 | 2.0086 | 2.4033 | 2.6778 |
| 51 | 0.6793 | 1.2984 | 1.6753 | 2.0076 | 2.4017 | 2.6757 |
| 52 | 0.6792 | 1.2980 | 1.6747 | 2.0066 | 2.4002 | 2.6737 |
| 53 | 0.6791 | 1.2977 | 1.6741 | 2.0057 | 2.3988 | 2.6718 |
| 54 | 0.6791 | 1.2974 | 1.6736 | 2.0049 | 2.3974 | 2.6700 |
| 55 | 0.6790 | 1.2971 | 1.6730 | 2.0040 | 2.3961 | 2.6682 |
| 56 | 0.6789 | 1.2969 | 1.6725 | 2.0032 | 2.3948 | 2.6665 |
| 57 | 0.6788 | 1.2966 | 1.6720 | 2.0025 | 2.3936 | 2.6649 |
| 58 | 0.6787 | 1.2963 | 1.6716 | 2.0017 | 2.3924 | 2.6633 |
| 59 | 0.6787 | 1.2961 | 1.6711 | 2.0010 | 2.3912 | 2.6618 |