Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Estudios de Postgrado
Maestría de Tecnologías de la Información y Comunicación

# PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA TEORÍA GENERAL DE DISUASIÓN

**Ing. Alicia Eugenia Ruano Aguilar**
Asesorado por el Msc. Ing. Everest Medinilla

Guatemala, mayo de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA


FACULTAD DE INGENIERÍA

# PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA TEORÍA GENERAL DE DISUASIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

**ALICIA EUGENIA RUANO AGUILAR**
ASESORADO POR EL MA. ING. EVEREST MEDINILLA

AL CONFERÍRSELE EL TÍTULO DE

**MAESTRO EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN**

GUATEMALA, MAYO  DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA


## NÓMINA DE JUNTA DIRECTIVA

| | |
|---|---|
| DECANO | Ing. Pedro Antonio Aguilar Polanco |
| VOCAL I | Ing. Ángel Roberto Sic García |
| VOCAL II | Ing. Pablo Christian de León Rodríguez |
| VOCAL III | Ing. Elvia Miriam Ruballos Samayoa |
| VOCAL IV | Br. Raúl Eduardo Ticún Córdova |
| VOCAL V | Br. Henry Fernando Duarte García |
| SECRETARIA | Ing. Lesbia Magalí Herrera López |

## TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

| | |
|---|---|
| DECANO | Ing. Pedro Antonio Aguilar Polanco |
| EXAMINADOR | Msc. Ing. Murphy Olympo Paiz Recinos |
| EXAMINADOR | MA. Ing. Marlon Antonio Pérez Türk |
| EXAMINADOR | Msc. María Elizabeth Aldana Díaz |
| SECRETARIA | Ing. Lesbia Magalí Herrera López |

## HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA TEORÍA GENERAL DE DISUASIÓN**

Tema que me fuera asignado por la Dirección de la Escuela de Estudios de Postgrados, en el mes de abril de 2014.

**Ing. Alicia Eugenia Ruano Aguilar**

FACULTAD DE
INGENIERÍA - USAC
ESCUELA DE
ESTUDIOS DE POSTGRADO

**Escuela de Estudios de Postgrado**
**Facultad de Ingeniería**
**Teléfono 2418-9142 / Ext. 86226**

Ref. APT-2016-055

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Postgrado, al Trabajo de Graduación de la Maestría en Tecnologías de la Información y la Comunicación titulado: **"PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA TEORÍA GENERAL DE DISUASIÓN"** presentado por la Ingeniera en Ciencias y Sistemas **Alicia Eugenia Ruano Aguilar**, procede a la autorización para la impresión del mismo.

IMPRÍMASE.

*"Id y Enseñad a Todos"*

Ing. Pedro Antonio Aguilar Polanco
DECANO

Guatemala, mayo de 2016.

Cc: archivo/la

FACULTAD DE
INGENIERÍA - USAC
ESCUELA DE
ESTUDIOS DE POSTGRADO

**Escuela de Estudios de Postgrado**
**Facultad de Ingeniería**
**Teléfono 2418-9142 / 24188000 Ext. 86226**

APT-2016-055

El Director de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen y dar el visto bueno del revisor y la aprobación del área de Lingüística del Trabajo de Graduación titulado **"PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA TEORÍA GENERAL DE DISUASIÓN"** presentado por la Ingeniera en Ciencias y Sistemas **Alicia Eugenia Ruano Aguilar,** correspondiente al programa de Maestría en Tecnologías de la Información y la Comunicación; apruebo y autorizo el mismo.

*"Id y Enseñad a Todos"*

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POST-GRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

MSc. Ing. Murphy Olympo Paiz Recinos
Director
Escuela de Estudios de Postgrado

Guatemala, mayo de 2016.

Cc: archivo/la

FACULTAD DE
INGENIERÍA - USAC
ESCUELA DE
ESTUDIOS DE POSTGRADO

**Escuela de Estudios de Postgrado**
**Facultad de Ingeniería**
**Teléfono 2418-9142 / 24188000 Ext. 86226**

APT-2016-055

Como Coordinador de la Maestría en Tecnologías de la Información y la Comunicación y revisor del Trabajo de Graduación titulado **"PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA TEORÍA GENERAL DE DISUASIÓN"** presentado por la Ingeniera en Ciencias y Sistemas **Alicia Eugenia Ruano Aguilar,** apruebo y recomiendo la autorización del mismo.

*"Id y Enseñad a Todos"*

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POST-GRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

MSc. Ing. Marlon Antonio Pérez Türk
Coordinador de Maestría
Escuela de Estudios de Postgrado

Guatemala, mayo de 2016

Cc: archivo/la

## ACTO QUE DEDICO A:

| | |
|---|---|
| **Dios** | Por ser mí guía en los momentos más importantes de mi vida y quien me permite ser quien soy. |
| **Mis padres** | Heber Ruano y Eugenia Aguilar, personas únicas, que sin su esfuerzo y apoyo incondicional no hubiese logrado esta meta. Gracias, por su amor, su apoyo, comprensión y motivación para seguir adelante. |
| **Mi hermano** | José Miguel Ruano Aguilar, por su apoyo incondicional y que este logro sea un ejemplo a seguir. |
| **Mi cuñada** | Liseth Ochoa, por su apoyo y para que este logro sea un ejemplo a seguir. |
| **A mi sobrina** | Ariana Ruano, por ser el angelito que trae felicidad a mi vida. |
| **A mi abuela** | Cándida Cifuentes, que en paz descanse, por todo el cariño demostrado y sus enseñanzas. |

## AGRADECIMIENTOS A:


| | |
|---|---|
| **La Universidad de San Carlos de Guatemala** | Por ser una importante influencia en mi carrera profesional. |
| **Facultad de Ingeniería** | Por brindarme los conocimiento que permitieron adicionar un título más a mi currículo profesional. |
| **Mis amigos y compañeros de la Facultad** | Que de una u otra manera me apoyaron para seguir adelante. |
| **Ing. Everest Medinilla** | Por su tiempo, seguimiento y apoyo. |

# ÍNDICE GENERAL

# ÍNDICE DE ILUSTRACIONES

## FIGURAS



## TABLAS

# GLOSARIO

| | |
|---|---|
| **Activo** | Cualquier cosa que tenga valor para la organización. |
| **Amenaza** | Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización. |
| **BMC** | Business Model Canvas (Modelo de Lienzo de Negocio). |
| **Control** | Son los procedimientos prácticas o elementos que se emplean para minimizar o eliminar un riesgo. |
| **Confidencialidad** | Propiedad de que la información esté disponible y no sea divulgada, a personas, entidades o procesos no autorizados. |
| **Disuasión** | Inducción a una persona para que desista de una idea o propósito. |
| ***Hackear*** | Acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red. |
| ***Hacker*** | Es un término que se emplea para definir a un programador habilidoso o también para definir a una |

| | |
|---|---|
| | persona que intenta acceder a los sistemas de una manera inapropiada. |
| **ISO** | *International Organization for Standarization* (Organización Internacional de Estandarización). |
| **ISO 27001** | Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. |
| **TI** | Tecnologías de Información. |
| **KMO** | Kaiser – Meyer- Olkin. |
| **GDT** | General Deterrence Theory (Teoría General de Disuasión). |
| ***Group*** | Grupo. |
| ***Phisher*** | Cualquier persona que pretende suplantar la identidad de otra persona o empresa por diferentes medios de comunicación como por ejemplo un correo electrónico, llamadas telefónicas o mensajería instantánea con el objetivo de conocer información confidencial que pueda ser usada ilícitamente. |
| ***Phishing*** | Una forma de ingeniería social que lo que pretende es adquirir información confidencial de forma fraudulenta, por medio de la suplantación de identidades. |

| | |
|---|---|
| **Política** | Intención o dirección general expresada formalmente por la gerencia o altos mandos. |
| **Riesgo** | Combinación de la probabilidad de un evento y su ocurrencia. |
| **Software** | Se refiera a programas del computador. |
| **SSI** | Sistema de seguridad de la información. |
| **TIC** | Tecnologías de la información y comunicaciones. |
| **Vulnerabilidad** | La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. |

# RESUMEN

Se entiende por información como, todo aquel conjunto de datos organizados en poder de una organización o empresa y que poseen valor para la misma (ISO, 2014). La seguridad de la información, según ISO 27001, consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos (ISO, 2014).

Debido a la importancia de la seguridad de la información, se realizó un estudio para identificar riesgos de la seguridad de la información en las organizaciones basándose en la teoría de disuasión general, que contempla como concepto fundamental la disuasión, que puede definirse como el uso de amenazas por parte de una de las partes para convencer a otra persona a abstenerse de iniciar algún curso de acción (University, 2011). Basándose en las variables que componen la teoría se elaboró una encuesta y cada pregunta se clasificó según factor de la teoría, con los datos recolectados se procedió a realizar un análisis cualitativo, agrupando y categorizando según las variables de la teoría de disuasión, detección, corrección y conocimiento sobre la

seguridad de la información, con el objetivo de identificar la relación entre cada una de ellas.

Se construyó una hipótesis con base a los constructos que comprenden la teoría de disuasión general y después de haber realizado el análisis se concluyó para la variable de conocimiento sobre seguridad de la información no presentaron relación con las variables de disuasión, detección y corrección; sin embargo, se identificó que se relacionaba directamente con las medidas preventivas.

A la hora de realizar el cálculo de la matriz de comunalidades se determinó que la variable tamaño de la organización no aportaba ningún significado en el análisis, por lo que se concluy que el tamaño de la organización o empresa no es determinante a la hora de disuadir, detectar, prevenir y corregir riesgos de seguridad de la información, según el análisis también se pudo determinar que las amenazas a la seguridad de la información se relaciona directamente con la prevención; por último, se analizó el diagrama del modelo obtenido en el análisis confirmatorio; por lo tanto, se puede observar que la prevención se relacionó también con las correcciones, sin duda son dos aspectos que van de la mano, las organizaciones tiene que definir cómo actuarán si se llega a materializar algún tipo de riesgo y qué medidas de prevención están tomando en cuenta, así mismo una de las prevenciones puede ser el factor disuasión, que se refiere al efecto que estén causando sobre los usuarios de sistemas o empleados.

Con base a lo anterior, se identificó una oportunidad de negocio en el campo de la seguridad de la información y con los riesgos identificados se estableció una serie de productos centrales a ofertar. Posteriormente, se elaboró un modelo de negocio de manera que sea la base para el

emprendimiento en el campo de la seguridad de la información para proveer diseño de soluciones a empresas u organizaciones del sector, tanto público como privado.

# PLANTEAMIENTO DEL PROBLEMA

Según consultas realizadas a sitios *web* de diferentes medios de comunicación dedicados a brindar noticias a nivel nacional, (Prensa Libre, Nuestro Diario, Siglo 21 y otros), desde el año 2012 se escucha y lee (Ver Anexo, noticias publicadas en Prensa Libre), temas relacionados con el *hackeo* de información, robo de cuentas o suplantación de identidad, dentro de entidades tanto públicas como privadas de todo tipo y ámbito.

La red de ciberactivistas Anonymous Guatemala, hackeó más de 20 páginas electrónicas nacionales, según reportajes publicados en la página *web* de Siglo 21 (diario nacional) a principios de febrero de 2013, este mismo grupo vuelve a atacar, bloqueando la página oficial del Congreso de Guatemala. Otro tema importante es el *phishing* o suplantación de identidad, la cual es una forma de ingeniería social en la que un atacante conocido como *phisher* intenta de forma fraudulenta recuperar las credenciales confidenciales o sensibles de los usuarios.

Que no exista seguridad de la información se torna un problema de impacto social, debido a que cualquier empleado o funcionario púbico está expuesto a tales amenazas, la proliferación de los delitos informáticos ha hecho que la sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de beneficio para la sociedad en general. Otro aspecto a tomarse en cuenta son las personas que no conocen nada de informática (por lo general personas de escasos recursos económicos que no cuentan con acceso a la tecnología o empleados que solo utilizan herramientas de software básicas), estas pueden ser engañadas si en un momento dado

poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como el internet, correo electrónico y otros, la educación es un factor clave en la minimización de esta problemática.

Las personas al escuchar la palabra hacker se imaginan a una persona con mucho conocimiento en temas de tecnología informática y computadores capaz de hacer daño a una red hasta robar información en la organización; sin embargo, no se toma en cuenta que dentro de la misma organización pueden existir empleados mal intencionados, y resulta que no es un ingeniero en sistemas o un experto en informática. Si alguna persona tuviera intenciones de obtener información confidencial, solamente realizando una búsqueda en internet se puede conseguir un completo manual sobre cómo práctica técnicas de *phishing o de hackeo*, así mismo como seres humanos se puede cometer errores y uno de ellos es confiarse y no creer en la posibilidad de que el peligro y las amenazas solo se encuentren fuera de la organización.

Con base a lo anterior, se plantea lo siguiente:

**Problema general**

El problema central en el que se basa el presente trabajo de graduación se fundamenta en la existencia de la seguridad de la información en las organizaciones de una manera básica y poco eficiente. Basándose en los antecedentes presentados anteriormente, surge la siguiente pregunta:

¿Qué soluciones pueden implementar las organizaciones para prevenir y mitigar los riesgos de seguridad de la información?

**Preguntas Auxiliares**

- ¿Qué es seguridad de la información?
- ¿Qué es la teoría de disuasión general y cómo puede ser aplicada a la solución de riesgos en seguridad de la información?
- ¿Qué vulnerabilidades y riesgos en seguridad de la información existen en la organización o empresa?
- ¿Es factible el emprendimiento en el área de seguridad de información por medio de servicios que ayuden a las empresas a minimizar los riesgos en seguridad de la información?

# OBJETIVOS

## General

Desarrollar el diseño de la solución a riesgos de la seguridad de la información en organizaciones tanto públicas como privadas, basado en la Teoría General de Disuasión.

## Específicos

1. Describir qué es la seguridad de la información.

2. Describir qué es la teoría de disuasión general para la solución a riesgos de seguridad de la información.

3. Identificar las vulnerabilidades y riesgos de la seguridad de la información en una organización.

4. Desarrollar un plan de negocio para el emprendimiento empresarial en el diseño de soluciones a riesgos en seguridad de la información.

# MARCO METODOLÓGICO

## Fases del estudio

### Fase 1: Revisión documental

Esta fase consiste en la investigación previa sobre conceptos relacionados con la seguridad de información, la teoría de disuasión general y análisis cualitativo, por medio de la consulta de documentos, revistas científicas, tesis que apoyen y sustenten el estudio en cuestión.

Actividades a realizar:

1. Revisión de la literatura correspondiente: detectar, obtener y consultar la bibliografía y otros materiales que pueden ser útiles para los propósitos del estudio, se debe extraer y recopilar información relevante y necesaria al problema de investigación.

2. Adopción de una teoría o desarrollo de una perspectiva teórica: descripción de la Teoría General de Disuasión.

3. Investigación sobre conceptos relacionados con la seguridad de la información.

**Fase 2: Análisis y presentación de resultados**

Para cumplir uno de los objetivos planteados, que es la identificación de riesgos de seguridad de la información es necesario conocer la percepción de las personas en cuanto al tema, para esto se requieren datos específicos para saber a qué riesgos se enfocarán las soluciones y productos o servicios a ofrecer, así mismo para identificar la factibilidad de negocio y si es aplicable la teoría de disuasión general.

Las actividades a realizar en esta fase son las siguientes:

1. Análisis cualitativo de los datos obtenidos.
2. Identificación de variables de la teoría de disuasión general que estén mutuamente relacionados que serían el punto central para identificar los riesgos.
3. Tabulación de datos, representación gráfica de datos y descripción de los mismos.

**Fase 3: diseño y solución**

Con base a la identificación de riesgos y vulnerabilidades en la seguridad de la información, en esta fase de definirán e identificarán los productos o servicios que formarán parte del emprendimiento que se pretende realizar.

**Fase 4: elaboración del plan de negocio**

Fase que establecerá la información relacionada con la empresa. El plan de negocio organiza la información y supone la plasmación de un documento

escrito de las estrategias, políticas, objetivos y acciones que la empresa desarrollará en el futuro.

Para esta fase se utilizará la herramienta de Lienzo de Negocio como guía para la elaboración del plan.

Las actividades a realizar en esta fase son las siguientes:

- Concepción de la idea de emprendimiento: consiste en el análisis de la idea, que busca identificar los elementos básicos para la transformación de la oportunidad en una actividad empresarial.

- Desarrollo del plan de negocio y descripción de elementos que conforman el plan:

    - Segmentos de clientes
    - Propuesta de valor
    - Canales
    - Relación con los clientes
    - Flujo de ingresos
    - Recursos clave
    - Actividades claves
    - Alianzas
    - Estructura de Costes

**Diseño, tipo y alcance del estudio**

El presente trabajo de graduación no se podría tipificar en un solo tipo de investigación se considera que el alcance es tanto descriptivo, exploratorio, explicativo y correlacional, ya que un estudio descriptivo permite fundamentar los estudios correlacionales. Debido a los aspectos a considerarse y las características del presente trabajo se pueden identificar los diferentes alcances investigativos en las distintas etapas de su desarrollo, como se muestra en la tabla que se presenta a continuación:

Tabla I. **Diseño, tipo y alcance de estudio**

| Tipo | Descripción | Alcance |
|---|---|---|
| **Investigación Descriptiva** | Caracteriza un fenómeno indicando sus rasgos más peculiares, la hipótesis que se plantea no se sujeta a comprobación experimental (Maya, 2014).<br>Es superficial, no llega a la esencia de las cosas para descubrir la ley que las rige (Maya, 2014). | **Descriptivo**<br>Describir el diseño de la solución que se brindará a los clientes se adaptará a las necesidades en riesgos de seguridad de la información. |
| **Investigación Exploratoria** | Las investigaciones exploratorias son utilizadas cuando el tema es poco conocido y existe poca información al respecto (De La Brouyere, 2015). | **Exploratorio**<br>Análisis Exploratorio para identificar los principales riesgos de seguridad de la información en las empresas, utilizando como herramienta de recolección de datos una encuesta y con base a los resultados desarrollar el diseño de solución. |

| | | |
|---|---|---|
| **Investigación Correlacional** | Para identificar qué variables de la teoría de disuasión están relacionadas, se aplica una investigación correlacional cuyo objetivo es evaluar en este caso la relación entre dos variables o conceptos en un contexto (De La Brouyere, 2015). | **Correlacional**<br><br>Se pretende responder a las preguntas orientadoras que integran el planteamiento del problema del presente trabajo, así como realizar comparación y el grado de correlación de las variables identificadas en el punto anterior de manera que se pueda determinar la relación que estás tienen una con la otra. |
| **Investigación Explicativa** | Conocer, explicar las causas o factores que determinan un fenómeno de la realidad a partir de un contexto teórico (Maya, 2014). | **Explicativo**<br><br>La presente investigación se lleva a cabo gracias a la investigación de teorías, ya que se pretende desarrollar el diseño de solución basado en una teoría base que es la Teoría de Disuasión General. |

Fuente: Descripción tomada del documento en sitio web Métodos y Técnicas de Investigación (Maya, 2014).

# INTRODUCCIÓN

La seguridad de la información es un tema de importancia en cualquier organización, empresa o entidad, aunque la mayoría de organizaciones ya cuentan con tecnologías de seguridad como por ejemplo: software antivirus, dispositivos de red y firewalls, estas herramientas no son suficientes porque a pesar que estos brindan cierto nivel de seguridad, no pueden brindar la protección que realmente se requiere.

El acceso no autorizado a una red informática o a equipos que en ella se encuentren puede ocasionar graves problemas, algunas de las posibles consecuencias de una intrusión son la pérdida de datos, robo de información sensible o confidencial, divulgación de información sobre clientes, ingeniería social, intercambio de contraseñas por correo electrónico, entre otros.

La seguridad de la información, según ISO 27001, consiste en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización (ISO, 2014).

El presente proyecto tiene su origen en un problema concreto que es la inseguridad de la información, el cual es enfrentado diariamente en empresas de diferentes ámbitos y se debe a la carencia de implementación de soluciones y estrategias de seguridad.

El objetivo general del trabajo de graduación es el emprendimiento empresarial en el diseño de soluciones a riesgos de seguridad de la información basado en la Teoría General de Disuasión (GDT), la cual postula que los

individuos pueden ser disuadidos de cometer actos antisociales a través de la utilización de medidas, que incluyen fuertes desincentivos y sanciones en relación con el acto delictivo (University, 2011), esto se logrará a través de la creación de un plan de negocio.

El trabajo de graduación se dividirá en nueve capítulos, los cuales se describen a continuación:

**Capítulo 1:** Antecedentes

En este capítulo se describe los antecedentes relacionados a los objetivos que se plantean en el presente trabajo, así como la descripción de la fuente principal de información que enmarca la aplicación de la teoría general de disuasión para la gestión de riesgos de seguridad de la información.

**Capítulo 2:** Justificación

En este capítulo se describe la razón por la cual se lleva a cabo el presente trabajo de investigación.

**Capítulo 3:** Alcances

El alcance contempla la descripción de las actividades que contemplan el presente trabajo de investigación y hasta dónde se llegará, definiendo así los límites y puntos centrales.

**Capítulo 4:** Marco Teórico

En este capítulo se presentarán las definiciones generales sobre seguridad de la información así como sus principios básicos, en este capítulo también se tratará el tema de la Teoría General de Disuasión que incluirá la definición, antecedentes, descripción de variables y áreas de aplicación. También se describirá el estándar de seguridad ISO/IEC 27001, aprobado y publicado como estándar internacional en octubre de 2005 por *International Organization for Standarization* y por la comisión *Internaional Electrotechnical Commision*, de manera que se pueda contar con un marco de trabajo base para dar solución a los aspectos presentados en el planteamiento del problema. En resumen presenta todos los conceptos que apoyaran y sustentarán el trabajo.

**Capítulo 5:** Diseño de la Solución a Riesgos de Seguridad de la Información en una Organización basado en la Teoría de Disuación General

Una vez comprendidos los conceptos y aspectos básicos sobre Seguridad de la Información y Teoría de Disuasión General, en este capítulo de desarrollará el diseño de la solución a riesgos de seguridad de la información, como parte del producto central que se quiere ofertar a los clientes, así mismo se describirá el estudio de campo realizado en curso de Metodologías de Investigación Cualitativa en el que se identificaron los riesgos y problemáticas de la seguridad, a través del análisis de información recabada en una encuesta dirigida a personas tanto del sector público como privado y los resultados servirán como entrada para el desarrollo del diseño de la solución.

**Capítulo 6:** Presentacón de Resultados

Este capítulo presenta los datos tabulados obtenidos de análisis cualitativo que se realizó que consistió en la realización de una serie de cálculos como parte del análisis cualitativo, con el fin de validar y descartar variables que no estuvieran estrechamente de relacionadas de la Teoría de Disuasión General.

También se describe todos los puntos a ser considerados en plan de negocio, tomando como base la herramienta de Lienzo del Modelo de Negocio.

**Capítulo 7:** Discusión de Resultados

En este capítulo se interpretarán los resultados del estudio y las conclusiones, se pretende responder a las preguntas de investigación.

# 1. ANTECEDENTES

Se tiene claro que uno de los activos más importantes para cualquier persona, empresa, institución en un ambiente laboral es la información, tiempo atrás cuando aún no se contaba con toda la tecnología que actualmente se tiene, la información únicamente podía ser recopilada de un libro, manuscrito, pergamino, etc., es decir, solo existía el medio de comunicación escrito, hoy en día el concepto fue cambiado a información digital, es decir, toda la información que antes era plasmada físicamente en una hoja de papel hoy en día se puede encontrar digitalmente en medios electrónicos y en sistemas de información, debido a la cantidad de información que se puede llegar a tener la seguridad de la información se ha convertido en punto importante que las empresas no deben pasar por alto.

Las organizaciones se han visto en la necesidad de definir e implementar estrategias que garanticen la seguridad, conservación y disponibilidad de la información. Estas estrategias pueden ser prácticas, estándares, procedimientos o políticas. Actualmente existen metodologías y estándares definidos que contienen especificaciones para identificar riesgos y establecer controles para gestionarlos o eliminarlos, un ejemplo es ISO/IEC 27001 (ISO, 2014), que ofrece lineamientos basados en la mejor continua para la gestión de la seguridad de la información, dichos lineamientos incluyen un marco metodológico para un sistema de gestión de la seguridad de la información, documentación de políticas, controles y tratamiento de riesgos, formalización y seguimiento de controles de forma periódica, tratamiento de incidentes en seguridad, uso de métricas, basado en el ciclo de mejora continua, así mismo permite cierta flexibilidad para adaptar controles en las diferentes áreas de la

empresa u organización, específicamente es aplicado para la protección de la información digital, documentos físicos y activos físicos como computadores y redes; sin embargo, no ofrece un guía exacta que indique cómo evaluar y realizar un diagnóstico en la empresa para identificar el estado actual de la misma, así mismo el objetivo principal de este tipo de implementación es llevar a la empresa a una certificación bajo este estándar y las empresas deben estar conscientes que el costo es alto, es decir debe existir un compromiso serio de parte de los alto mandos así como de todo el personal ya que se dobla el trabajo debido a todas las actividades que implica, otro aspecto a considerar es que una vez empezado el proceso de implementación no hay marcha atrás, ya que detenerlo, volvería a significar volver a realizar el esfuerzo de lanzamiento del mismo, caso contrario si se obtiene la certificación, para que la misma se mantenga en vigencia, anualmente debe ser auditada por la empresa certificadora (ISO, 2014).

También puede mencionarse COBIT (*Control Objectives for Information Systems and Related Technology*) es un modelo para la auditoría y control de sistemas de información y dentro del enfoque de control, ofrece una visión en temas de gestión y gobierno, que se complementa con guías o publicaciones adicionales, contempla Risk IT, el cual es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI, BMIS (Business Model for Information Security) orientado al negocio para la administración de la seguridad informática. Los principios en los que se basa el marco de trabajo; estos son la efectividad, eficiencia, confiabilidad, cumplimiento, confidencialidad, integridad y disponibilidad, ciertamente son las características que debe cumplir la seguridad de la información; sin embargo, este marco de trabajo ayuda a mejorar las áreas de TI desde el punto de vista solamente del gobierno corporativo, además se

requiere de un esfuerzo de la organización, para adoptar los estándares. (ISACA, 2014).

La BSA (*Business Governance Task Force)*, ha constituido un grupo de trabajo con el propósito de ofrecer una respuesta a los problemas de seguridad que se presentan en las organizaciones, como por ejemplo seguridad cibernética, haciendo énfasis en la seguridad de los sitios web corporativos, este grupo considera que una seguridad adecuada requiere la participación activa de los directivos en que se debe incluir una política de gobierno de cada organización, se entiende por gobierno a todo el conjunto de actividades y acciones que se realizan en el área de tecnologías de información y en coordinación con la alta dirección de las empresas utilizar los recursos de una forma eficiente para asegurar los objetivos estratégicos, con base a esa premisa ha publicado informes en los que resume ideas y conceptos de gobierno de seguridad, es decir todas las actividades que permiten la administración de la seguridad de la información, por medio de controles internos al negocio, empresa u organización, sin embargo no da lineamientos en cuanto al diagnóstico y gestión de la seguridad de la información el enfoque es más parecido al gobierno TI como COBIT (Rebollo Martínez, 2014).

El estándar ISO/IEC 38500, se publicó en junio de 2008 con base a la norma australiana AS8015:2005. Es la primera de una serie sobre normas de gobierno de TIC. Está dedicado al gobierno corporativo de las tecnologías de la información, a pesar de no estar específicamente orientado a la seguridad de la información, esta norma define el gobierno corporativo como el sistema, mediante el cual se controla el uso actual y futuro de las tecnologías de información (Rebollo Martínez, 2014). Esta nueva norma fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionados con los servicios de información y comunicación que suelen estar gestionados,

tanto por especialistas en TIC internos o ubicados en otras unidades de negocio de la organización, como por ejemplo proveedores de servicios externos, sus principios están orientados a informar y orientar a los directores que controlan el uso de las TIC en su organización, proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TIC (ISACA, 2014). De igual manera y como se describe anteriormente el estándar está enfocado al buen uso de las tecnologías y gobiernos y no específicamente a la gestión de riesgos.

Detmar W. Straub y Richard J. Welke ambos profesores del Departamento del Área de Sistemas de Información de la Universidad del Estado de Georgia, Estados Unidos, conciben el concepto de teoría general de disuasión aplicado a riesgos de seguridad de la información. En su investigación definen como un "sistema de riesgo" todo aquel sistema que se encuentra vulnerable a ciertas amenazas que pongan en riesgo la información. También describen que el problema de fondo con el riesgo de los sistemas es que los gerentes, por lo general no son conscientes de toda la gama de acciones que se pueden tomar para reducir el riesgo. Debido a esta falta de conocimiento, acciones posteriores para planificar y hacer frente a riesgo de los resultan que sus acciones son poco eficaces, de lo que resultan teorías y otros modelos conceptuales que ofrecen lineamientos e ideas de cómo los gerentes pueden hacer frente a riesgos de los sistemas de información. La teoría de disuasión general postula acciones genéricas que directa e indirectamente minimizan los riesgos de sistemas de información, acciones como por ejemplo si un abusador penetra con éxito al sistema de información, la organización debe tener la capacidad de detectarlo por medio de actividades preventivas, también otra de las acciones que se plantean es la elaboración de informes de actividades sospechosas y auditorías de sistemas; por último, los autores también sugieren que un programa de seguridad eficaz debe ser capaz de

poner remedio a los efectos nocivos de un acto abusivo y castigar al delincuente, todas estas acciones son fundamentadas en las cuatro variables de la teoría que son la disuasión, prevención, detección y corrección. También aseguran con base a resultados de su investigación, que ningún sistema puede ser absolutamente seguro, a pesar de este hecho, es posible formalizar partes del sistema de seguridad que aún no estén contemplados, la ventaja de dicha formalización es que se liberan recursos que se utilizan para controlar las piezas que no pueden ser formalizadas. Por lo tanto, inadecuada seguridad en muchas organizaciones es una situación que puede y debe remediarse aplicando teorías (término en inglés *theorybased)* que sirven como herramientas para la planificación de la seguridad (Straub & Welke, 1998).

Durante muchos años en estudio expertos dividieron en cuatro actividades secuenciales las siguientes estrategias para reducir riesgos de sistemas de información: (1) la disuasión, (2) la prevención, (3) la detección, y (4) recuperación, estas cuatro variables sin duda tiene fuertes bases teóricas; sin embargo, la teoría que mejor explica la eficacia de estas medidas es la teoría general de disuasión, la cual a su vez se utiliza en el estudio de los criminales y otras personalidades antisociales. Se postula que individuos con la intención fundamental de cometer actos antisociales pueden ser disuadidos por medio de sanciones pertinentes, en otras palabras se refiere a la vigilancia activa y visible convenciendo a potenciales abusadores que puede ser atrapado y castigado severamente.

Schuessler en su tesis de doctorado, indica que la Teoría General de Disuasión (GDT) postula que los individuos pueden ser disuadidos de cometer actos antisociales a través del uso de las contramedidas, que incluyen fuertes desincentivos y sanciones en relación con el acto. Schuessler también señaló a la teoría de disuasión general como una guía para la aplicación de

contramedidas podrían ponerse en práctica para eliminar amenazas o al menos mitigar algunos de los riesgos, como acceso no autorizado a ordenadores, falta de conocimiento del personal en temas de seguridad de la información y el uso incorrecto de la tecnología. En resumen Schuessler indica que la disuasión se define como "la inhibición de la conducta criminal por el miedo, sobre todo de la pena", en otras palabras, las actividades de disuasión proveen desincentivos para los posibles abusadores de ordenador. Los ejemplos de los esfuerzos de disuasión incluyen "las políticas administrativas, capacitación de los empleados, y las funciones de seguridad visibles".

La prevención se define como un estorbo o un obstáculo. Estos pueden incluir obstáculos físicos tales como guardias, puertas cerradas, y así sucesivamente y / o herramientas de software tales como dispositivos de autenticación y firewalls. La detección se define como el acto o proceso de descubrimiento. Lo que se refiere a los sistemas de información (SI), es el proceso de tratar de descubrir las violaciones de seguridad dentro de una organización mediante el examen de los registros del sistema, informes de monitoreo de actividades sospechosas, y así sucesivamente. Remedio o corrección se define como un orden jurídico de prevenir o reparar un daño o hacer cumplir un derecho, ya sea a través de sanciones internas tales como reprimendas o terminación, o externamente a través legal o sistemas de regulación. La investigación actual amplía esta visión conceptual de la teoría general de disuasión para incluir otras fuentes de amenazas como las no humanas, de esta forma, otras amenazas como los desastres naturales y fallas técnicas también pueden ser examinadas, Schuessler avala en su investigación estas otras fuentes la planificación preventiva asegura pueden ayudar a mitigar estas amenazas también. Por ejemplo, las copias de seguridad pueden reemplazar los datos perdidos después de un fallo de hardware o un desastre natural (Schuessler, 2009).

También es importante saber qué riesgos de seguridad de información son los que se presentan comúnmente en las empresas. Leticia Hernández en su tesis de grado indica que una de las principales amenazas para la seguridad informática y de la información como primer punto es la falta de conocimiento en seguridad por parte del persona, los equipos no tienen el software actualizado que proteja el computador de virus o alguna otra amenaza que provoque la pérdida de información, falta de políticas. Indica que es importante enfatizar que se tiene que concientizar a los involucrados, brindándoles políticas de seguridad y buenas prácticas; también ayudándolos con cursos de capacitación donde se proporcione información necesaria y conceptos relacionados con la seguridad de la información que se puedan poner en práctica. También indica que es necesario hacer énfasis en realizar actualizaciones en equipos, software, políticas y buenas prácticas, debido a que cualquier organización va cambiando conforme pasa el tiempo, recordar que la protección y prevención de los activos radica en el ciclo de la seguridad, así mismo resulta de gran importancia identificar las consecuencias que se tendrán si se pierde información confidencial, esto para ayudar a prevenir posibles incidentes y tener un alto grado de seguridad (Hernández Sánchez, 2014).

# 2. JUSTIFICACIÓN

El presente trabajo de investigación se desarrolla en el Área de Administración de Tecnología de la Información en la línea investigación de Tecnologías de la Información, para el apoyo al gobierno electrónico.

Las Tecnologías de la Información se refieren al conjunto de elementos tecnológicos que permiten el funcionamiento y de los sistemas de información. Debido a que las tecnologías de información y comunicaciones abarcan la utilización de medios informáticos para almacenar, procesar y difundir todo tipo de información o procesos, la seguridad de la información se incluye dentro de la línea de investigación de la Maestría en Tecnologías de Información y Comunicación.

La seguridad de la información es una necesidad presente en la actualidad, debido a los avances en tecnologías de los últimos años. Según el estudio de B2B International, titulado "*Global Corporate IT Security Risks 2013"* que se llevó a cabo entre empresas de todo el mundo en colaboración con Kaspersky Lab, sólo un 12% de las empresas tiene completamente implementadas políticas de seguridad en dispositivos móviles dentro de sus redes corporativas (Lab, 2014). Sin embargo, el número de incidentes de seguridad TI relacionados con *smartphones* y *tablets* va en aumento y la mayoría de las empresas no tiene planes de limitar el uso de los dispositivos móviles personales para asuntos relacionados con la empresa, según el estudio, el 85% de las empresas permiten a sus empleados utilizar sus propios dispositivos en el trabajo sin ningún tipo de protección. Los porcentajes indican que las empresas y organizaciones no están regulando el uso los dispositivos

móviles, lo que puede llevar a una serie de violaciones y amenazas en la seguridad de la información, cosas tan simples como esas no son tomadas en cuenta.

Si las organizaciones tuvieran protección en su información y la seguridad adecuada, podrían garantizar una efectividad en cuando a la prevención de riesgos. Las empresas actualmente manejan su información y la administran por medio de software, por lo tanto es necesario que todas implanten una evaluación de riesgos para la información con el objetivo de implantar soluciones con el propósito de proteger la integridad y cumplir con los controles de políticas de seguridad.

Con la aplicación de la identificación de los principales problemas que aquejan una institución basándose en la Teoría General de Disuasión, se podrán diseñar soluciones que se acoplen a las necesidades y problemáticas, lo que hace que este trabajo de graduación sea de importancia y de beneficio para los clientes a los que se piensa brindar el servicio.

Con base a una consulta realizada en buscadores web como Google, se encontraron escasas empresas en Guatemala que ofrecen soluciones relacionadas con el tema de Seguridad de la Información, como por ejemplo: la empresa ESET, *CheckPoit*, entre otras. Por lo que se identifica una oportunidad innovadora ofrecer al mercado este tipo de soluciones.

# 3. ALCANCES

## 3.1. Alcances investigativos

Para cubrir el aspecto investigativo del presente trabajo se abordará en el marco teórico que incluirá la descripción y definición de la seguridad de la información, así como de los principios que la conforman, descripción de los estándares más importantes de la gestión de la seguridad de la información, la descripción y definición de la Teoría General de Disuasión y su aplicación para brindar soluciones a riesgos de la seguridad de la información.

## 3.2. Alcances técnicos

Haciendo uso de herramientas de software para el análisis cualitativo de la información, se llevarán a cabo una serie de cálculos que permitirán tabular la información y presentar los resultados de manera que se puedan identificar las variables que se relacionan más de la teoría general de disuasión con el objetivo de identificar los riesgos de la seguridad de la información, el software a utilizar es “R” el cual permite realizar variedad de cálculos estadísticos por medio de “R *commander*”, cuyo lenguaje permite y facilita el uso de la herramienta.

## 3.3. Resultados esperados

Con base a los resultados obtenidos en el análisis cualitativo de la recolección de datos realizada para identificar los riesgos, se definirán los productos que ofrecerá la empresa, con base a eso, se elaborará un plan de

negocio brindará los lineamientos necesarios para el emprendimiento, así como para consolidar ideas, definir una propuesta de valor para el cliente por medio de la herramienta de lienzo de negocio.

En resumen, el resultado final será la descripción y definición de seguridad de la información, descripción de la teoría general de disuasión y aplicación a la gestión de riesgos, identificación de riesgos, el diseño a la solución de riesgos y por último, el plan de negocio.

# 4. MARCO TEÓRICO

## 4.1. Seguridad de la información

La seguridad de la información es el conjunto de medidas que se encargan de la protección, acceso, uso, divulgación, interrupción de la información y de los sistemas de información, relacionada con los riesgos procedentes de varias fuentes como por ejemplo ingeniería social, espionaje, tecnología, etc. todo lo que pueda afectar el funcionamiento de los sistemas y la recuperación de la información.

También se pueden mencionar daños como virus informáticos y ataques de intrusión o denegación de servicios volviéndose cada vez más comunes, ambiciosos y sofisticados

### 4.1.1. Antecedentes

La información es uno de los recursos más importantes de cualquier organización, la seguridad de la información surge de la necesidad de proteger dicho recurso.

Antes que se conociera la tecnología que se tiene hoy en día como por ejemplo: redes de computadores, internet, dispositivos móviles, etc. la información de importancia de una organización se guardaba de una manera física como en bodegas, archivadores, folders, etc. manteniendo siempre el material físico. En cuanto a las amenazas a la seguridad de la información, se reducía en desastres naturales o el robo de información (Montenegro, 2014).

Pero hoy en día con el surgimiento de las nuevas tecnologías de la información y el auge del crecimiento del internet, la información entonces comenzó a digitalizarse de una manera impresionante, una bodega llena de archivadores con datos ahora puede almacenarse en un disco duro, memoria extraíble, disco duro externo, etc. Este avance en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de la información, trajo consigo un nuevo problema al mundo de la informática, la información en formato digital, es más fácil de transportar, por lo que las posibilidades de robarla o alterarla son altas (Montenegro, 2014).

### 4.1.2. Definición

Jorge Ramió Aguirre en su tesis de doctorado define a la seguridad de la información como la disciplina en el arte y ciencia de la protección, de los riesgos, amenazas, enfoque de análisis de escenarios, buenas prácticas y esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. Hablar de *information security* es hablar de la fuente misma de la práctica de control y cuidado de la información en cualquier medio y condición, que busca ofrecer una vista holística de su relación con procesos, personas y tecnologías. Es decir, al referirnos a seguridad de la información, ahora el enfoque es el de una disciplina orientada a la gestión de esa información como un bien y activo que requiere protección, contemplando por tanto la evaluación de las amenazas, análisis de riesgos, el uso de buenas prácticas, la adecuación a normativas y legislaciones nacionales e internacionales, controles y auditorías de esa seguridad, así como la concienciación y generación de confianza, entendiendo ese todo de manera holística como un negocio y la importancia de la continuidad del mismo (Ramió Aguirre, 2013).

En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno (Hernández Sánchez, 2014).

La seguridad de la información puede definirse como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información (Montenegro, 2014).

La seguridad de la información consiste en proteger una de las partes más importantes del negocio, la información. Sin embargo, se debe distinguir entre Seguridad Informática, que es la protección de las infraestructuras tecnológicas sobre las que funciona la empresa y Seguridad de la Información, que tiene como objetivo la protección de sistemas e información en cuanto a que estén siempre accesibles (Disponibilidad), que no sean alterados malintencionadamente o por error (Integridad) y que su acceso sea permitido sólo a personas autorizadas (Confidencialidad).

### 4.1.3. Principios de la seguridad de la información

A continuación se describen los principios de la seguridad de la información.

#### 4.1.3.1. Confidencialidad

La confidencialidad es una propiedad de la información que garantiza el acceso únicamente a las personas que estén autorizadas.

La Real Academia de la Lengua Española define “Confidencial” como: “que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas”, y “Confidencialidad” como “la cualidad de confidencial”.

Se puede dar la pérdida de la información como por ejemplo si se deja la pantalla del computador a la vista y esta no se bloquea cuando el usuario se asunta, o también cuando una laptop con información sensible sobre una empresa es robada, cuando se divulga información confidencial a través del teléfono y otros. Todos estos casos pueden constituir una violación de la confidencialidad.

#### 4.1.3.2. Integridad

Se define como la propiedad de la información que tiene como evitar que los datos sean modificados sin autorización, es decir mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. La violación de integridad se presenta cuando un empleado, programa o proceso modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad (Mifsud, 2012).

Es uno de los pilares fundamentales de la seguridad de la información.

#### 4.1.3.3. Disponibilidad

Principio de la seguridad de la información que dicta que la información debe estar disponible y recuperable en el momento que se requiera.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Así mismo, las empresas o negocios deben considerar el mantenimiento a servidores que resguardan la información así como el resguardo y acceso a los mismos.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web y otros, mediante el uso de *clusters* o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc.

### 4.1.4. Gestión de riesgos

Un riesgo se puede definir como aquellos eventos que evitan el cumplimiento de un objetivo. La norma ISO define como riesgo la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños (ISO, 2014). En otras palabras, cualquier factor que afecte parcialmente o totalmente el correcto funcionamiento de una empresa u organización es considerado un riesgo o amenaza.

El análisis y gestión de riesgos es una actividad que consiste en la selección de los mecanismos de protección, que permiten estimar las pérdidas potenciales de información por medio de la identificación de riesgos, analizarlos y evaluarlos, es decir priorizarlos y posteriormente tratarlos, con el objetivo de

prevenirlos y si ya se tienen encontrar los mecanismos necesarios para mitigarlos (López M., 2011).

Las actividades que deben considerarse en un análisis de riesgos son:

#### 4.1.4.1. Identificar los riesgos

Dentro de esta actividad se deben identificar como primer punto todos los activos de información que sean valiosos para la empresa; posteriormente, se procede a identificar las amenazas en relación a los activos identificados, seguidamente se identifican las vulnerabilidades que permitan que las amenazas se materialicen, teniendo el listado categorizar y definir el impacto que se tiene en cada uno.

#### 4.1.4.2. Analizar y evaluar los riesgos

Consiste en valuar el impacto se alguna de las amenazas llega a darse y que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información. Cuando se ha valuado el impacto se procede a evaluar la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados; por último, se estiman los niveles de riesgo y determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

#### 4.1.4.3. Tratamiento del riesgo

Esta actividad debe contemplar la aplicación de controles adecuados, aceptar los riesgos identificados y establecer planes y políticas que eviten el riesgo o en algunos casos transferirlos a terceros.

## 4.2. Ingeniería social

El término ingeniería social fue establecido por el empresario William H. Tolman en su libro "*Social Engineering*" y lo describe como una serie de técnicas psicológicas para persuadir o lograr resultados deseados, (Tolman, 1909). Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

En general, los métodos de la ingeniería social están organizados de la siguiente manera:

- Una fase de acercamiento para ganarse la confianza del usuario, haciéndose pasar por un integrante de la administración, de la compañía o del círculo o un cliente, proveedor, etc.
- Una fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo, éste podría ser un pretexto de seguridad o una situación de emergencia;
- Una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en el alerta. Ésta podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, una frase hecha o, en caso de que sea mediante correo electrónico o de una página Web, la redirección a la página Web de la compañía.

La ingeniería social puede llevarse a cabo a través de una serie de medios:

- Por teléfono
- Por correo electrónico
- Por correo tradicional
- Por mensajería instantánea
- Otros medios de comunicación

## 4.3. Teoría general de disuasión

Los defensores de la disuasión creen que las personas eligen obedecer o no violar la ley después de conocer las consecuencias de tales acciones, la disuasión es el punto central en la que se basa la teoría que se describe a continuación.

### 4.3.1. Antecedentes

La disuasión es una estrategia destinada a disuadir a un adversario de emprender una acción que aún no se ha iniciado (University, 2011).

La teoría de la disuasión ganó mayor importancia como estrategia militar durante la Guerra Fría con respecto al uso de las armas nucleares. Le tomó una connotación única durante este tiempo como una fuerza nuclear inferior, en virtud de su poder de destrucción extrema, podría disuadir a un adversario más poderoso, a condición de que esta fuerza pudiera ser protegida contra la destrucción por un ataque sorpresa. Un elemento de disuasión nuclear creíble,

Bernard Brodie escribió en 1959, siempre debe estar en la lista, sin embargo, nunca utilizado (Schuessler, 2009).

En Thomas Schelling obra clásica sobre la disuasión, se presenta el concepto de que la estrategia militar ya no puede ser definida como la ciencia de la victoria militar. En su lugar, se argumenta que la estrategia militar es ahora igualmente, si no más, el arte de la coerción, la intimidación y la disuasión. Schelling dice que la capacidad de hacer daño a otro estado ahora se utiliza como un factor de motivación para otros estados para evitarlo e influir en el comportamiento. Para ser coercitiva o disuadir otro estado, la violencia tiene que ser previsto y evitable para alojamiento. Por lo tanto, se puede resumir que el uso del poder de daño como el poder de negociación es la base de la teoría de la disuasión, y es más exitoso cuando se mantiene en reserva (Schuessler, 2009).

### 4.3.2. Definición

La Universidad de Brigham Young presenta el concepto de la disuasión como el uso de amenazas por parte de una de las partes para convencer a otra persona a abstenerse de iniciar algún curso de acción. Una amenaza funciona como un elemento de disuasión en la medida en que su objetivo no convence para llevar a cabo la acción prevista debido a los costes y las pérdidas que se dirigen incurriría. Un individuo racional se verá menos incentivado (más disuadido) de cometer un tipo de delito cuanto más larga sean la pena asociada (severidad); cuanto más grande sea la probabilidad de ser detenido y castigado por el crimen cometido (certeza), y cuanto mayor velocidad exista en la aplicación de la pena una vez detenido (celeridad). En otras palabras, existe una relación inversa entre involucramiento criminal y la severidad, certeza y celeridad del castigo al delito (University, 2011).

La disuasión puede ser de dos tipos: 1) específica, donde los individuos que cometen delitos y son efectivamente detectados y castigados, se ven disuadidos de reincidir. 2) genérica, cuando el castigo de los ofensores desestimula el involucramiento de nuevos individuos en actividades criminales (Trajtenberg & Aloisio).

### 4.3.3. Teoría General de Disuasión y la seguridad de la información

Las organizaciones necesitan determinar a detalle las medidas de seguridad que implementarán para lograr una exitosa gestión de la seguridad de la información. Dado el gran número de errores o vulnerabilidades que se producen día a día dentro de una empresa, las organizaciones tienen que personalizar sus modelos de seguridad y mejorar sus políticas, con el fin de cumplir los objetivos y estrategias que persigue la organización.

Esta teoría ha sido aplicada a seguridad de la información para investigar cómo es el control de seguridad, la aplicación de la política de empresas y la ejecución de las directrices, actualmente las medidas aplicadas a la seguridad de la información han sido poco efectivas, por ejemplo: las empresas solo se limitan a la adquisición de cámaras de seguridad, que no cumplen con el nivel de seguridad esperado, rótulos o carteles indicando cierta advertencia a la hora de entrar algún espacio físico laboral, sin embargo hoy en día este tipo de soluciones no son suficientes, la diferenciación que se propone en este trabajo de investigación es ir más allá de la implementación de medios primitivos, lo que se pretende es establecer estrategias efectivas.

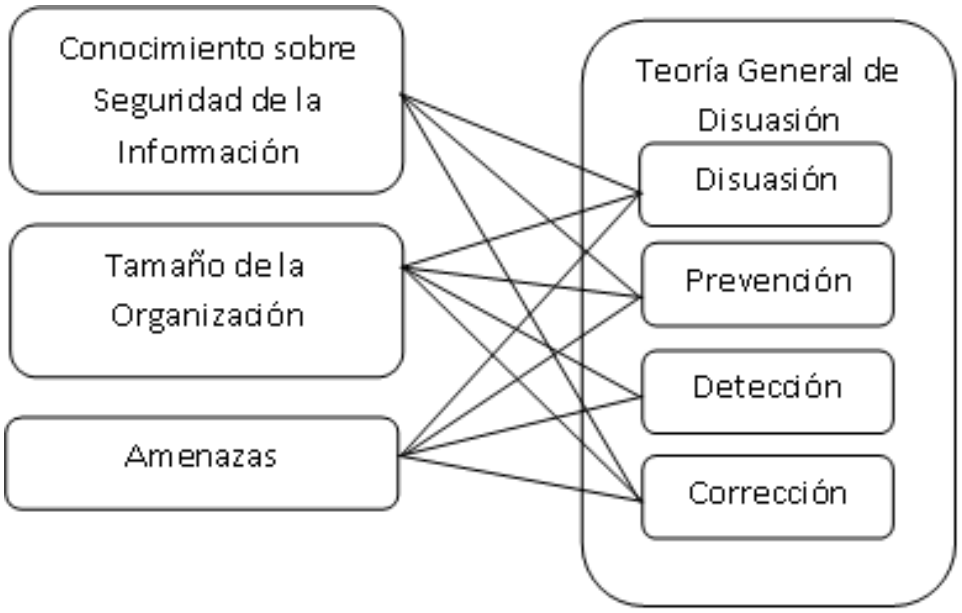
La Teoría General de Disuasión se ha utilizado para discutir temas relacionados con los sistemas de información, determinando que las medidas de seguridad de la información pueden disuadir a los posibles agresores

informáticos de cometer actos que violen la política de la organización (Schuessler, 2009).

Joseph H. Schuessler también señaló que cuando se utiliza GDT (General Deterrence Theory – Teoría General de Disuasión) como guía, contramedidas podrían ser puestas en marcha para eliminar amenazas a la seguridad o al menos mitigar algunos de los riesgos, GDT también postula que la sensibilización de los usuarios de las políticas de seguridad, la educación, la capacitación de seguridad, y programas de sensibilización y supervisión tienen un impacto directo en la percepción de los usuarios de la certeza y la severidad de la sanciones que se les aplicarían, el cual a su vez tiene un efecto directo sobre los Sistemas de Información (SI) intención de uso indebido (Schuessler, 2009).

En un sistema de información la actividad de vigilante ocurre cuando el oficial o vigilante de seguridad utiliza elementos de disuasión, para evitar que lleve a cabo un acto delictivo. La aplicación de sanciones severas por violaciones graves de seguridad se piensa para disuadir a los posibles infractores, el potencial de todo menos motivados delincuentes, de los comportamientos ilícitos.

Figura 1. **Propuesta basado en GDT y un GDT extendido**




Fuente: General Deterrence Theory: Assesin Information Systems Security Effectiveness in Large versus Smal Business por Joseph H. Schuessler, 2009

### 4.3.4. Variables de la Teoría General de Disuasión

A continuación se describen las variables que contempla la Teoría General de Disuasión aplicada a la seguridad de la información.

#### 4.3.4.1. Conocimiento sobre seguridad de la información

Se refiere al conocimiento que tengan los usuarios o empleados de la organización sobre seguridad de la información, haciendo énfasis en los términos de confidencialidad, integridad, disponibilidad y autenticación de la información (Schuessler, 2009).

#### 4.3.4.2. Tamaño de la organización

Cantidad de personas que trabajan en la institución y cantidad de departamentos que lo integran (Schuessler, 2009).

#### 4.3.4.3. Amenazas

Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad informática se refiere a los elementos de información (Schuessler, 2009).

#### 4.3.4.4. Disuasión

Diccionarios lo definen como la inducción a una persona para que desista de una idea o propósito. Aplicado a la investigación se refiere a la aplicación de desincentivos para los posibles abusadores o atacantes con el fin de disuadirlos de participar en actividades delictivas informáticas, esto incluye las políticas administrativas y capacitación de empleados.

#### 4.3.4.5. Prevención

Se define como la preparación y disposición para evitar un riesgo o ejecutar una cosa. Se refiere al uso de medidas preventivas para conducir a una mayor eficacia del SSI (Schuessler, 2009).

#### 4.3.4.6. Corrección

Medio para evitar o reparar un daño. Un remedio sirve a la organización como un camino para restituir de alguna manera ya sea por vías legales o sanciones los daños causados por faltas a la seguridad de la información tanto interna como externa a la organización (Schuessler, 2009).

## 4.4. Estándares de la seguridad de la información

### 4.4.1. Generalidades

La información es un activo fundamental para el desarrollo, operación, control y gestión del modelo de negocio o servicio de cualquier organización.

La Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel. La globalización y avances tecnológicos hoy en día, han permitido que transacciones y procesos que antes tomaban tiempo realizarse, hoy se realice en cuestión de segundos.

Los estándares se derivan en la existencia de una serie de normas aceptadas como acreditaciones de la Seguridad de la Información universalmente, y cuya implementación aporta a la organización no solo una certificación sino también un completo marco de trabajo (ISACA, 2014). Entre los aspectos que se toman en cuenta cuando se trabaja bajo un estándar pueden mencionarse:

- Mejora de la competitividad
- Mejora de la imagen corporativa

- Protección y continuidad del negocio
- Cumplimiento legal y reglamentario
- Optimización de recursos e inversión en tecnología
- Reducción de costes

### 4.4.2. Norma ISO/IEC 27001

La implantación de estándares de gestión de la seguridad de la información se ha convertido en una prioridad de las organizaciones para asegurar su continuidad, minimizar los posibles daños y maximizar el retorno de la inversión y las oportunidades de negocio (Mesquida Calafat, 2012).

En este apartado se introduce el estándar de gestión de seguridad de la información ISO/IEC 27001.

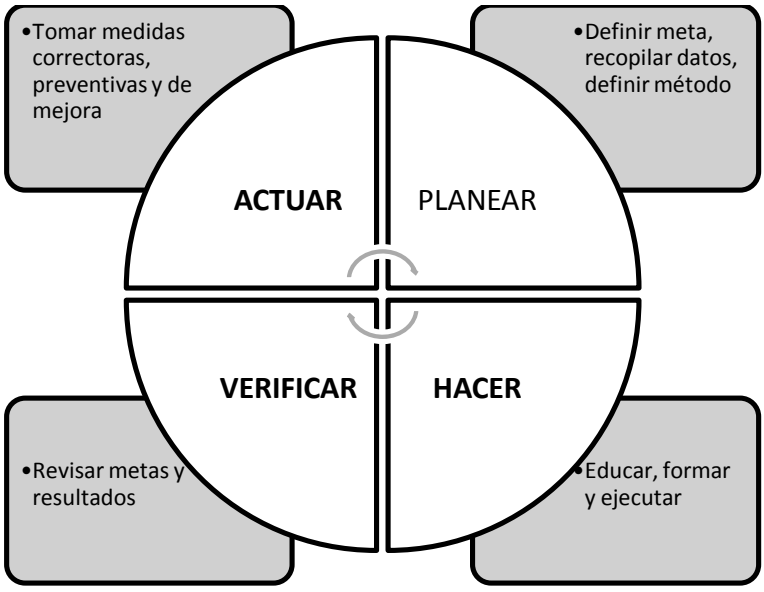
La norma ISO/IEC 27001:2005 Information Security Management Systems Requirements (ISO27000 2005a) promueve la adopción de un enfoque basado en procesos y especifica los requisitos para la creación, implantación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) documentado, dentro del contexto de las actividades empresariales de la organización y de los riesgos que ésta afronta (Mesquida Calafat, 2012).

Los requisitos establecidos en esta norma son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza. ISO 27001:2005 está estructurada en ocho cláusulas. Las tres primeras cláusulas tratan el alcance, la aplicación de la norma y las definiciones. Las cláusulas cuatro a ocho están orientadas a procesos y definen los requisitos para la implementación y mejora de un SGSI (Mesquida Calafat, 2012).

Esta norma internacional sigue el ciclo PDCA (Ver Figura 2), que se aplica para estructurar todos los procesos del sistema de gestión de seguridad de la información. La Figura 3 muestra el SGSI propuesto por la norma ISO/IEC 270001, el cual, a partir de los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida que responden a dichos requisitos y expectativas (ISO, 2014).

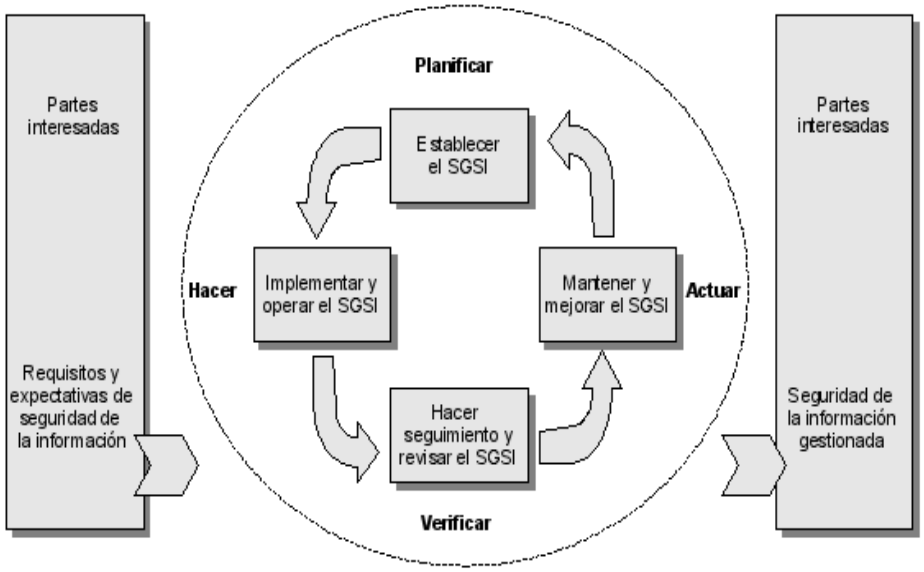
La Figura 2 representa gráficamente el ciclo de la mejora continua en la que se basa toda norma ISO.

Figura 2. **Ciclo de la mejora continua de la norma ISO**




Fuente: elaboración propia.

Figura 3. **Sistema de gestión de seguridad de la información de la norma ISO/IEC**




Fuente: Documento ISO 27001 (ISO, 2014)

Entre las actividades a tomarse en cuenta en una implantación a ISO27001 pueden mencionarse las siguientes:

- Definición del alcance del SGSI;
- Definición de una política de seguridad;
- Definición de una metodología y criterios para el análisis y gestión del riesgo;
- Identificación de riesgos;
- Evaluación de los posibles tratamientos del riesgo;
- Elaboración de un declaración de aplicabilidad de controles y requisitos;
- Desarrollo de un plan de tratamiento de riesgos;
- Definición de métricas;
- Desarrollo de programas de formación y concienciación en seguridad de la información;

- Gestión de recursos y operaciones;
- Gestión de incidencias;
- Elaboración de procedimientos y documentación asociada.

Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta Norma aplican a todo tipo de Organizaciones, independientemente de su tipo, tamaño o área de actividad. Por esta basada en un trabajo por proceso y en la mejora continua es compatible e integrable con el resto de sistemas de gestión que ya existan en la organización (ISO, 2014).

## 4.5. Análisis de información

### 4.5.1. Análisis cualitativo

Por análisis de datos cualitativos se entiende el proceso mediante el cual se organiza y manipula la información recogida por los investigadores para establecer relaciones, interpretar, extraer significados y conclusiones. (Rodríguez Sabiote, Lorenzo Quiles, & Herrera Torres, 2005). El análisis de datos cualitativos se caracteriza, pues, por su forma cíclica y circular, frente a la posición lineal que adopta el análisis de datos cuantitativos (Rodríguez Sabiote, Lorenzo Quiles, & Herrera Torres, 2005).

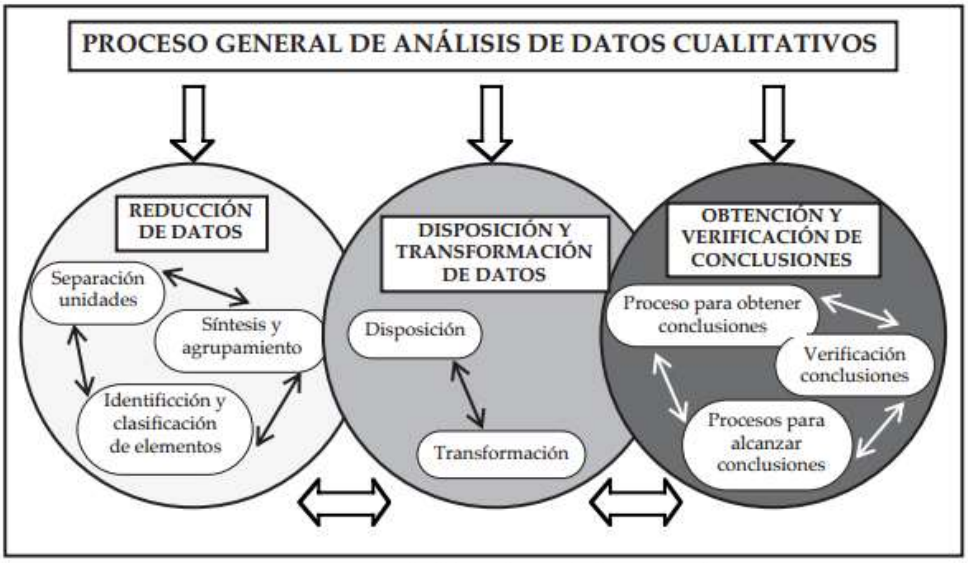
#### 4.5.1.1. Etapas del análisis cualitativo

El análisis de datos está configurado en torno a tres grandes tareas:

- Reducción de datos
- Disposición y transformación de los datos
- Obtención de resultados y verificación de conclusiones

A su vez, cada etapa está constituida por un conjunto de actividades y operaciones más específicas. Esquemáticamente, dicho entramado puede representarse de la siguiente forma (Rodríguez Sabiote, Lorenzo Quiles, & Herrera Torres, 2005):

Figura 4. **Proceso general de análisis de datos cualitativos**




Fuente: Obtenido del documentos citado (Rodríguez Sabiote, Lorenzo Quiles, & Herrera Torres, 2005).

### 4.5.2. Análisis factorial

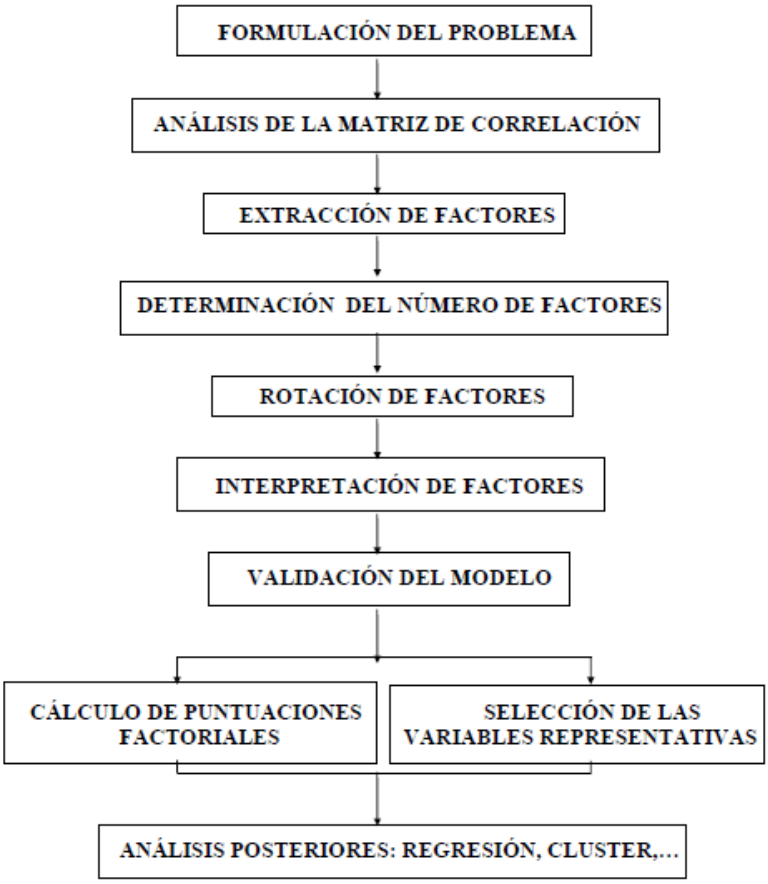
El análisis factorial es una técnica estadística multivariante cuyo principal propósito es sintetizar las interrelaciones observadas entre un conjunto de variables en una forma concisa y segura como una ayuda a la construcción de nuevos conceptos y teorías (Serrano & Gutiérrez). Para ello utiliza un conjunto de variables aleatorias inobservables llamadas factores comunes, de forma que todas las covarianzas o correlaciones son explicadas por dichos factores y cualquier porción de la varianza inexplicada por los factores comunes se asigna

a términos de error residuales a los que se les llama factores únicos o específicos (Serrano & Gutiérrez).

El análisis factorial puede ser exploratorio o confirmatorio. El análisis exploratorio se caracteriza porque no se conocen a priori el número de factores y es en la aplicación empírica donde se determina este número. Por el contrario, en el análisis de tipo confirmatorio los factores están fijados a priori, utilizándose contrastes de hipótesis para su corroboración (Serrano & Gutiérrez).

El análisis factorial se reduce a la búsqueda de estos pesos para localizar medidas distintas a partir de las variables originales, y de manera que, a poder ser, entre todas las nuevas medidas agoten o expliquen toda la varianza presente en las variables originales (De la Fuente Fernandez, 2011).

Figura 5. **Esquema de un análisis factorial**




Fuente: Obtenido del documentos citado (De la Fuente Fernandez, 2011).

#### 4.5.2.1. Análisis de la matriz de correlación

La finalidad de analizar la matriz de las correlaciones muestrales R (r) = ij, donde rij es la correlación muestral observada entre las variables (X, X) i j, es comprobar si sus características son las adecuadas para realizar un análisis factorial (De la Fuente Fernandez, 2011). Uno de los requisitos que deben cumplirse es que las variables se encuentran altamente intercorrelacionadas. También se espera que las variables que tengan correlación muy alta entre sí la tengan con el mismo factor o factores. En consecuencia, si las correlaciones

entre todas las variables son bajas, tal vez no sea apropiado el Análisis Factorial (De la Fuente Fernandez, 2011).

#### 4.5.2.2. Test de esfericidad de Bartett

Contrasta, bajo la hipótesis de normalidad multivariante, si la matriz de correlación de las p variables observadas (R) p es la identidad. Si una matriz de correlación es la identidad significa que las intercorrelaciones entre las variables son cero. Si se confirma la hipótesis nula H: R 1 o R I 0 p = p =, las variables no están intercorrelacionadas. El test de esfericidad de Barlett se obtiene mediante una transformación del determinante de la matriz de correlación (De la Fuente Fernandez, 2011).

Si la hipótesis nula es cierta, los valores propios valdrán uno, o su logaritmo será nulo y, por tanto, el estadístico del test valdría cero. Por el contrario, si con el test de Barlett se obtienen valores altos de 2x, o un determinante bajo, hay variables con correlaciones altas (un determinante próximo a cero indica que una o más variables podrían ser expresadas como combinación lineal de otras variables). En definitiva, si el estadístico del test toma valores grandes (o un determinante próximo a cero) se rechaza la hipótesis nula con cierto grado de significación. En caso de aceptarse la hipótesis nula, las variables no están intercorreladas y debería reconsiderarse la aplicación de un análisis factorial (De la Fuente Fernandez, 2011).

#### 4.5.2.3. Medidas de adecuación de la muestra

Santiago de la Fuente Hernández en su trabajo titulado Introducción al Análisis Factorial, define el análisis factorial como una técnica de reducción de datos que sirve para encontrar grupos homogéneos de variables a partir de un

conjunto numeroso de variables, dado que en algunos casos se requiere la adecuación de la muestra, se pueden aplicar varias técnicas, en este caso el coeficiente de correlación parcial es un indicador de la fuerza de las relaciones entre dos variables eliminando la influencia del resto. Si las variables comparten factores comunes, el coeficiente de correlación parcial entre pares de variables deberá ser bajo, puesto que se eliminan los efectos lineales de las otras variables, las correlaciones parciales son estimaciones de las correlaciones entre los factores únicos y deberían ser próximos a cero cuando el análisis factorial es adecuado, ya que, estos factores se supone que están incorrelados entre sí. Por lo tanto si existe un número elevado de coeficientes de este tipo distintos de cero es señal de que las hipótesis del modelo factorial no son compatibles con los datos, una forma de evaluar este hecho es mediante la KMO (Medida de Adecuación de la Muestra) propuesta por Kaiser, Meyer. KMO es un índice que toma valores entre 0 y 1 y que se utiliza para comparar las magnitudes de los coeficientes de correlación observados con las magnitudes de los coeficientes de correlación parcial de forma que, cuanto más pequeño sea su valor, mayor es el valor de los coeficientes de correlación parciales y, por lo tanto, menos deseable es realizar un análisis factorial (De la Fuente Fernandez, 2011).

Kaiser, Meyer y Olkin aconsejan que si KMO ≥ 0,75 la idea de realizar un análisis factorial es buena, si 0,75 > KMO ≥ 0,5 la idea es aceptable y si KMO < 0,5 es inaceptable.

### 4.6. Emprendimiento

La palabra emprendimiento proviene del francés *entrepreneur* (pionero), y se refiere a la capacidad de una persona para hacer un esfuerzo adicional por alcanzar una meta u objetivo, siendo utilizada también para referirse a la

persona que iniciaba una nueva empresa o proyecto, término que después fue aplicado a empresarios que fueron innovadores o agregaban valor a un producto o proceso ya existente (Frank Montesdeoca, Guillen Cuadros, Rivadeneira Mendoza, & Zambrano Dueñas, 2012).

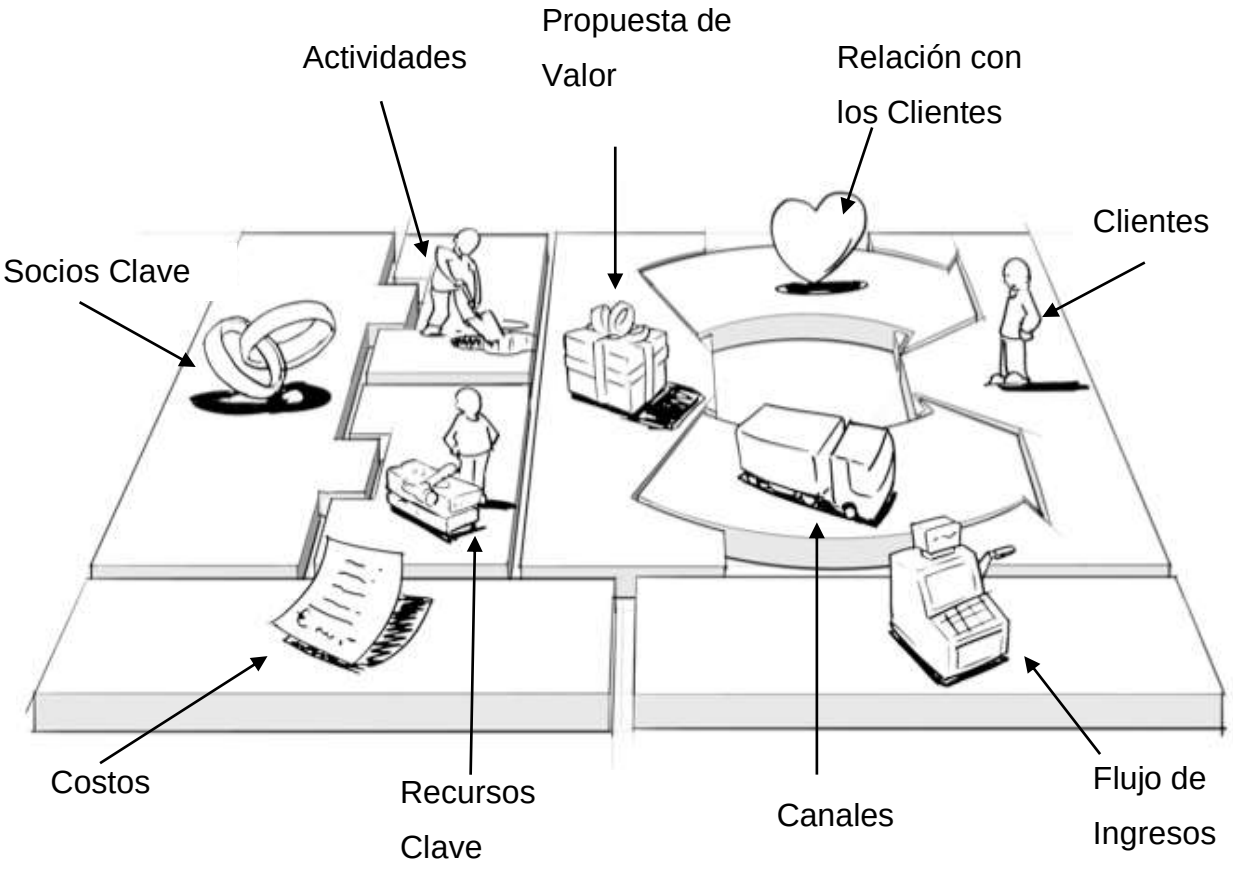
En conclusión, emprendimiento es aquella actitud y aptitud de la persona que le permite emprender nuevos retos, nuevos proyectos; es lo que le permite avanzar un paso más, ir más allá de donde ya ha llegado. Es lo que hace que una persona esté insatisfecha con lo que es y lo que ha logrado, y como consecuencia de ello, quiera alcanzar mayores logros (Frank Montesdeoca, Guillen Cuadros, Rivadeneira Mendoza, & Zambrano Dueñas, 2012).

### 4.6.1. Lienzo de modelo de negocio

El lienzo de modelo de negocio, en inglés *Business Model Canvas,* es un marco visual que incluye nueve elementos de un modelo de negocio. Por medio de este marco de trabajo, se describe la lógica sobre como una empresa que está por surgir podrá entregar valor y diferenciarse, un modelo de negocio es una descripción de cada elemento a tomar en cuenta en el emprendimiento, como por ejemplo el segmento de mercado, indicando quiénes serán los clientes, cómo se generarán las ganancias o utilidades y toda la logística que permitirá entregar a los clientes ese valor así mismo permite ver la relación que existe entre cada uno de los elementos, aclarar ideas y plasmarlas en un tablero, como se muestra en la Figura 6.

La Figura 6 muestra gráficamente cada uno de los segmentos que componen el lienzo de modelo de negocio.

Figura 6. ***Business Model Canvas*** **(Lienzo de Modelo de Negocio)**




Fuente: (Fryars, 2012)

#### 4.6.1.1. Componentes del lienzo modelo de negocio

A continuación se describen los componentes que comprenden el lienzo del modelo de negocio.

#### 4.6.1.1.1. **Segmentos de clientes**

Los clientes son elemento fundamental en el negocio, por tal motivo es importante conocerlos, ya que los clientes definen los segmentos de mercado a los que se enfocará la empresa.

#### 4.6.1.1.2. **Propuesta de valor**

Describe las soluciones que se brindarán a los clientes para resolver sus requerimientos o problemas, así mismo describe los productos o servidos a ofrecer y como se diferenciarán de otros, en este segmento también se incluye una estrategia que tome en cuenta la competencia y estrategias, es decir la definición de los precios, diseño, personalización etc.

#### 4.6.1.1.3. **Canal**

En este segmento se describe la forma en que se entregara valor los segmentos de clientes definidos, el canal es la clave para la toma de decisiones y cómo el cliente adoptará el servicio que ofrecemos.

#### 4.6.1.1.4. **Relación con los clientes**

Uno de los aspectos que debe sin duda tomarse en cuenta es la relación con los clientes, ya que son ellos quienes adquieren los productos y servicios, y es importante definir y establece estrategias para llegar a ellos.

#### 4.6.1.1.5. **Flujo de ingresos**

Se refiere al flujo de entrada y salida de efectivo en un determinado período, así mismo se incluye en este apartado las estrategias de ingresos monetarios.

#### 4.6.1.1.6. **Recursos clave**

Para implementar la propuesta de  negocio, se precisa de una serie de actividades, para lograrlo son necesarios algunos recursos, como por ejemplo, monetarios, procesos, personas, etc. En este segmento se describen los recursos y la formo como serán utilizados.

#### 4.6.1.1.7. **Actividades clave**

Son todas las actividades clave que se requieren para lograr y llevar a cabo los objetivos del negocio, abarca los proceso de marketing y producción, por medio de ellas se entrega valor haciendo uso de los canales.

#### 4.6.1.1.8. **Alianzas**

Cualquier empresa, persona, que pueda formar una alianza con la empresa a emprender debería ser descrita en este apartado, las alianzas complementan la propuesta de valor y transfiriendo actividades se pueden lograr mejores resultados.

#### 4.6.1.1.9. **Estructura de costes**

Incluye y describe el costo por llevar a cabo todas las actividades definidas en el plan de negocio tomando en cuenta la escalabilidad del negocio para optimizar los costos fijos.

# 5. DISEÑO DE LA SOLUCIÓN A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN UNA ORGANIZACIÓN, BASADO EN LA TEORÍA GENERAL DE DISUACIÓN

## 5.1. Descripción del diseño

A continuación se presenta el resumen de la evaluación que se pretende ofrecer, y el diseño de la solución a los riesgos de seguridad de la información identificados por medio de una encuesta, la idea es tener un panorama inicial como empresa y saber a qué puntos centrales enfocarse para satisfacer las necesidades que las empresas actualmente están afrontando.

Parte del valor que se quiere agregar al negocio se propone la Metodología General de la Disuasión como herramienta para identificar los riesgos en seguridad de la información que una organización pueda tener y conocer en qué aspectos debe mejorar.

En la tabla que se presenta a continuación, se definen las variables e indicadores del presente trabajo de graduación, que serán tomadas en cuenta para el diseño de la solución:

Tabla II. **Variables de la Metodología Teoría General de Disuasión**

| Variable | Definición | Indicador | Tipo de Variable | Categoría | Valores /Dimensión |
|---|---|---|---|---|---|
| **Conocimiento sobre Seguridad de la Información** | Se refiere al conocimiento que tengan los usuarios o empleados de la organización sobre seguridad de la información, haciendo énfasis en los términos de confidencialidad, integridad, disponibilidad y autenticación de la información. | Que tanto conoce la persona sobre la seguridad de la información | Cualitativa | Politómica | No se conoce del tema<br>Poco<br>Conocimiento<br>del tema<br>Experto en el tema |
| **Tamaño de la Organización** | Cantidad de empleados dentro de la institución, organización o empresa. | Con base a un rango de cantidad de empleados se determina que tan grade es una organización | Cualitativa | Politómica | Pequeña<br>Mediana<br>Grande |
| **Disuasión** | Inducción a una persona para que desista de una idea o propósito. Aplicado a la investigación, se refiere a la aplicación de desincentivos para los posibles abusadores o atacantes con el fin de disuadirlos de participar en actividades delictivas informáticas, esto incluye las | Si tuviera conocimiento sobre las sanciones laborales que pueda tener si llega a cometer alguna falta en la seguridad de la información (divulgación de información confidencial o robo de documentos, etc.) se minimizaría cometer este | Cualitativa | Politómica | Totalmente de acuerdo<br>De acuerdo<br>Indeciso<br>En desacuerdo<br>Totalmente en<br>desacuerdo |

| | | | | | |
|---|---|---|---|---|---|
| | políticas administrativas y capacitación de empleados. | tipo de faltas | | | |
| **Prevención** | Se define como la preparación y disposición para evitar un riesgo o ejecutar una cosa. Se refiere al uso de medidas preventivas para conducir a una mayor eficacia del SSI. | Conocer si la organización cuenta con acciones preventivas | Cualitativa | Politómica | Ninguna acción preventiva<br>Pocas acciones preventivas<br>Existen acciones preventivas |
| **Detección** | Se refiere a identificar y reconocer los aspectos que están evitando que exista seguridad de la información. | Identificación de Riesgos | Cualitativa | Politómica | Ningún control<br>Poco control<br>Existe control |
| **Corrección** | Medio para evitar o reparar un daño. Puede ser jurídico. Un remedio sirve a la organización como un camino para restituir de alguna manera ya sea por vías legales o sanciones los daños causados por faltas a la seguridad de la información tanto interna como externa a la organización. | Conocer si la organización cuenta con acciones correctivas. | Cualitativa | Politómica | Ninguna acción correctiva<br>Pocas acciones correctivas.<br>Existen acciones correctivas |

Fuente: elaboración propia.

### 5.1.1. Importancia teórica de las variables

GDT se origina en la criminología, esto implica realizar un examen de la disuasión, prevención, detección y el uso de recursos para influir en las tasas de criminalidad, GDT sin duda es una prominente teoría criminológica contemporánea. Aplicada a los Sistemas de Seguridad de la Información, GDT sugiere que las amenazas pueden ser mitigadas a través del uso de la disuasión, prevención, detección y corrección.

## 5.2. Planteamiento de la hipótesis

Como se definió anteriormente, el modelo basado en la teoría general de disuasión consta de cuatro variables o constructores primarios: disuasión, prevención, detección y corrección; sin embargo, el planteamiento de una teoría general de disuasión extendida aplicada al estudio de la efectividad en sistemas de información brinda tres entradas más que fueron consideradas estás son: el conocimiento sobre seguridad de la información, el tamaño de la organización y las amenazas. Ya definida las entradas y los constructos a los cuales se relacionarán el objetivo es determinar cuál de los cuatro constructos es el que representa un mayor problema para las organizaciones públicas gubernamentales y enfocarse en el estudio de ese factor específicamente.

Cada una de las variables de entrada del modelo propuesto se relaciona directamente a cada uno de los constructos de la teoría, por ejemplo: el conocimiento sobre seguridad de información que pueda tener un usuario o empleado afecta directamente en la prevención sobre seguridad, gracias a este conocimiento el empleado sabrá cómo actuar, por otro lado, si se tiene una política de seguridad definida dentro de la organización y todos los empleados la conocen se convierte en un medio de disuasión para el empleado, es decir, el

empleado conoce de las posibles sanciones que pueden aplicarse en el caso que este llegue a cometer un delito o quebrantar alguna de las reglas. El tamaño de la organización es otra variable a considerarse dentro de la hipótesis, la lógica nos dice que entre más grande es una organización (cantidad de empleados) más difícil es tener un control, caso contrario en una organización pequeña (poca cantidad de empleados) el control podría llevarse de una mejor forma y tener un nivel mayor de disuasión. Y por último, las amenazas, anteriormente se ha definido como un evento que al materializarse puede provocar un impacto negativo dentro de la organización, por lo que es necesario valuar esta variable para cada uno de los constructos.

Con base a lo descrito anteriormente, se definieron las siguientes hipótesis:

**H1:** El conocimiento sobre seguridad de la información se relaciona con cada constructo de la teoría general de disuasión.

**H1a:** El conocimiento sobre seguridad de la información se relaciona con la disuasión.

**H1b:** El conocimiento sobre seguridad de la información se relaciona con la prevención.

**H1c:** El conocimiento sobre seguridad de la información se relaciona con la detección.

**H1d:** El conocimiento sobre seguridad de la información se relaciona con la corrección.

**H2:** El tamaño de la organización influye directamente con cada uno de los constructos de la teoría general de la disuasión.

**H2a:** El tamaño de la organización influye directamente con la disuasión.

**H2b:** El tamaño de la organización influye directamente con la prevención.

**H2c:** El tamaño de la organización influye directamente con la detección.

**H2d:** El tamaño de la organización influye directamente con la corrección.

**H3:** Las amenazas influyen directamente con cada uno de los constructos de la teoría general de la disuasión.

**H3a:** Las amenazas influyen directamente con la disuasión.

**H3b:** Las amenazas influyen directamente con la prevención.

**H3c:** Las amenazas influyen directamente con la detección.

**H3d:** Las amenazas influyen directamente con la corrección.

## 5.3. Presentación de resultados

### 5.3.1. Recolección de datos

Se realizó una encuesta en línea con una serie de 20 preguntas. Cada uno de los ítems representó una de las variables del constructo de la teoría general de disuasión.

La población bajo estudio la conformaron empleados del sector público y privado, comprendida entre las edades de 20 a 35 años.

Se definió la siguiente escala con la valorización correspondiente a cada respuesta (Ver encuesta en anexo):

| | | |
|---|---|---|
| Totalmente de acuerdo | = | 5 |
| De acuerdo | = | 4 |
| Neutral /Indeciso | = | 3 |
| En desacuerdo | = | 2 |
| Totalmente en desacuerdo | = | 1 |

# 6. PRESENTACIÓN DE RESULTADOS

## 6.1. Análisis factorial

El análisis factorial es una técnica de reducción de datos, que sirve para encontrar grupos homogéneos de variables a partir de un conjunto numeroso de variables (Mahía Casado). Estas variables no observables, denominadas frecuentemente constructos, son variables que no pueden medirse de manera directa: se estiman a través de variables observadas. Para este análisis se toman como variables latentes las diferentes preguntas planteadas en la encuesta descrita anteriormente tomando como base los siguientes constructos:

| | | |
|---|---|---|
| Conocimiento sobre seguridad de la información | = | CS |
| Tamaño de la Organización | = | TO |
| Amenazas | = | AM |
| Disuasión | = | DS |
| Prevención | = | PV |
| Corrección | = | CR |

## 6.2. Cálculo de KMO y prueba de Bartlett

La medida de adecuación muestral de Kaiser – Meyer- Olkin (KMO) es un índice que toma valores entre 0 y 1 y que se utiliza para comparar las magnitudes de los coeficientes de correlación observados con las magnitudes de los coeficientes de correlación parcial de forma que, cuanto más pequeño sea su valor, mayor es el valor de los coeficientes de correlación parciales y, por lo tanto, menos deseable es realizar un análisis factorial (Frank

Montesdeoca, Guillen Cuadros, Rivadeneira Mendoza, & Zambrano Dueñas, 2012).

La Tabla III presenta los cálculos resultados de la prueba de Barlett y medida de adecuación de la muestra KMO, donde CS, PV, CR, DS, AM, TO son las iniciales de los factores descritos en el punto anterior. Dado que el MSA evalúa si las mediciones son adecuadas y consistentes para la variable AM4 con un valor obtenido de 0.26900 se descartara. Se observa que el valor del KMO = 0.86874 y se encuentra arriba del valor recomendados por Kaiser, Meyer y Olkin, por lo que el análisis de factores puede realizarse. El test de esfericidad de Bartlett, sin embargo, rechaza la hipótesis de diagonalidad de la matriz de correlación indicando que sí existen relaciones significativas entre las variables.

Tabla III. **Cálculos - prueba de KMO y Bartlett**

```
    $KMO
[1] 0.86874
    $MSA
     MSA
CS1 0.63084
CS2 0.90598
PV1 0.81296
PV2 0.80342
CS3 0.92286
PV3 0.89612
CR1 0.84052
CR2 0.89438
DS1 0.93162
PV4 0.92042
CR3 0.91101
AM1 0.77145
AM2 0.92934
AM3 0.85098
PV5 0.92837
AM4 0.26900
DS2 0.76552
TO1 0.75967
DS3 0.66995
PV6 0.82848
 $Bartlett
[1] 1161.6
```

Fuente: elaboración propia.

La Tabla IV muestra las comunalidades de cada variable, es decir, la varianza de cada variable que explicada por este un único factor. Es importante verificar si cada una de las variables incluidas en el análisis son explicadas aceptablemente por el modelo. Ya que la comunalidad representa la proporción de la varianza de la variable indicadora que es explicada por los factores comunes del modelo, Hair et al. (1998/1999) proponen que las variables con una comunalidad menor a 0.5 carecen de una explicación suficiente y no deberían ser consideradas en la interpretación final del análisis. Por lo que para este análisis se descartarán también las variables CS1, PV1, AM4, DS2 y TO1. La variable TO1 trataba explicar que el tamaño de la organización es un factor que está relacionada con cada una de las variables del constructo por lo que en este punto se descartará la hipótesis **H2**. Se vuelve a recalcular sin variables descartadas.

Tabla IV. **Cálculos de comunalidades**

*$Communalities*

| | *Initial Communalities* | *Final Extraction* |
|---|---|---|
| *CS1* | *0.15715* | *0.13188* |
| *CS2* | *0.64670* | *0.55750* |
| *PV1* | *0.33137* | *0.32626* |
| *PV2* | *0.62500* | *0.55222* |
| *CS3* | *0.68633* | *0.61125* |
| *PV3* | *0.64754* | *0.53027* |
| *CR1* | *0.57360* | *0.58661* |
| *CR2* | *0.78376* | *0.77918* |
| *DS1* | *0.59236* | *0.56605* |
| *PV4* | *0.78145* | *0.74323* |
| *CR3* | *0.77237* | *0.71166* |
| *AM1* | *0.69130* | *0.57106* |
| *AM2* | *0.58901* | *0.59106* |
| *AM3* | *0.64917* | *0.69599* |
| *PV5* | *0.68794* | *0.64392* |
| *AM4* | *0.23089* | *0.22597* |
| *DS2* | *0.38886* | *0.21152* |
| *TO1* | *0.28805* | *0.14983* |
| *DS3* | *0.30839* | *0.69763* |
| *PV6* | *0.79634* | *0.75318* |

Fuente: elaboración propia.

Siguiendo los pasos del análisis factorial se continúa con la extracción de factores. El objetivo del Análisis Factorial (AF) es determinar un número reducido de factores que puedan representar a las variables originales, como se muestra en la Tabla V.

Tabla V. **Extracción de factores**

```
     [,1]       [,2]       [,3]      [,4]
CS1 -0.170185 -0.0553702  0.1027753 -0.298819
CS2 -0.745761  0.0086421  0.0203777  0.029160
PV1 -0.369853  0.0139892  0.2918117 -0.322670
PV2 -0.620792  0.3987032 -0.0715148  0.052527
CS3 -0.773124  0.1052152  0.0098517  0.048579
PV3 -0.722200  0.0438971 -0.0783535  0.025096
CR1 -0.581301  0.4895254 -0.0370883  0.087696
CR2 -0.833341  0.2711150  0.0145877 -0.104888
DS1 -0.730984 -0.0817364  0.0295211 -0.155423
PV4 -0.855885 -0.0019696 -0.0960668 -0.038217
CR3 -0.836860  0.0153741 -0.0386136 -0.097997
AM1 -0.657123 -0.3264831 -0.1718719 -0.055841
AM2 -0.690849 -0.2969392 -0.1505615  0.054261
AM3 -0.650797 -0.4474896 -0.2313819  0.136624
PV5 -0.794190 -0.0594293  0.0752832  0.063119
AM4 -0.009489 -0.1284150  0.1443767 -0.434218
D2  -0.436985 -0.0945238 -0.0782449 -0.074191
TO1  0.325838  0.1418124 -0.0269558 -0.151080
DS3 -0.274613 -0.2234215  0.7129041  0.253124
PV6 -0.820235  0.1018118  0.2330149  0.125434

$RMS
[1] 0.042561
```

Fuente: elaboración propia.

Se volvieron a realizar los caculos sin las variables descartadas, la Tabla VI muestra los resultados y se puede observar que cada factor se encuentran en el rango aceptable para seguirlos tomando en cuenta en el análisis.

Tabla VI. **Cálculos - prueba de KMO y Bartlett**

```
$KMO
[1] 0.905
$MSA

CS1 0.89546
CS2 0.93020
PV1 0.87272
PV2 0.91175
PV3 0.91286
PV4 0.93403
PV5 0.88536
CR1 0.89238
CR2 0.92953
CR3 0.91117
DS1 0.96293
DS2 0.71868
AM1 0.81648
AM2 0.93578
AM3 0.88357
$Bartlett
[1] 1036.9
```

Fuente: elaboración propia.

La tabla VIII presenta nuevamente el cálculo de comunalidades con sin las variables descartadas.

Tabla VII. **Cálculos de comunalidades**

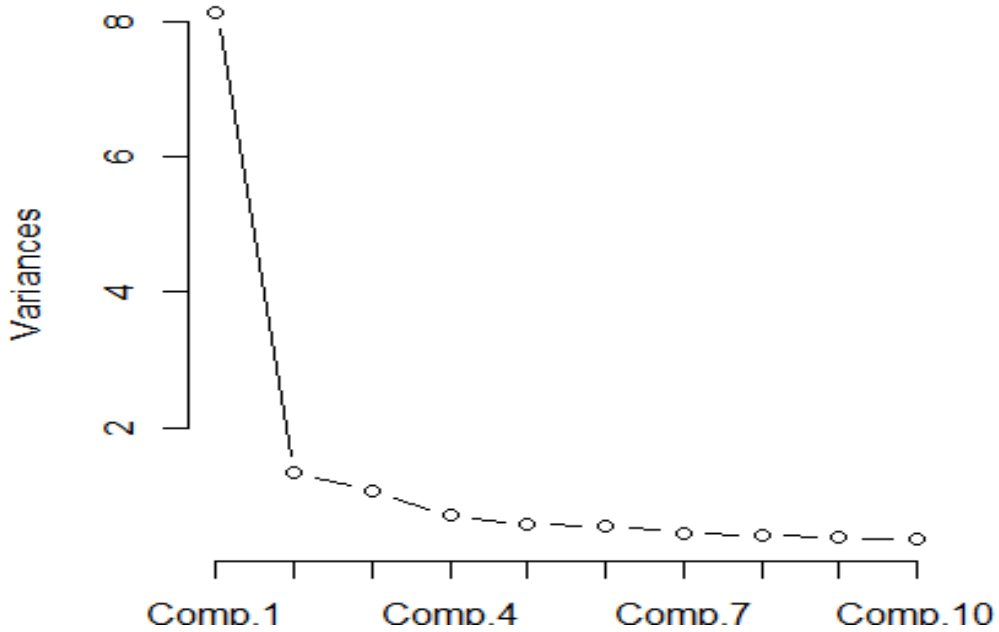
```
$Communalities
  Initial Communalities Final Extraction
CS1               0.63589          0.55495
CS2               0.66864          0.62655
PV1               0.55857          0.56955
PV2               0.61680          0.53034
PV3               0.77612          0.74810
PV4               0.67205          0.66367
PV5               0.75163          0.79443
CR1               0.52091          0.55747
CR2               0.75609          0.77743
CR3               0.76543          0.70143
DS1               0.55740          0.54791
DS2               0.24842          0.35918
AM1               0.64880          0.60882
AM2               0.56364          0.57626
AM3               0.60541          0.64008
```

Fuente: elaboración propia.

### 6.2.1. Análisis exploratorio

La Figura 7 ofrece auto valores ordenados de mayor a menor el primer auto valor es el mayor de los posibles y así sucesivamente. Si uno de los autos valores se aproxima a cero, esto significa que el factor correspondiente a ese auto valor es incapaz de explicar una cantidad relevante de la varianza total. Representación gráfica donde los factores están en el eje de abscisas y los valores propios en el de ordenadas. Los factores con varianzas altas se suelen distinguir de los factores con varianzas bajas. El punto de distinción viene representado por un punto de inflexión en la gráfica. Se pueden conservar los factores situados antes de este punto de inflexión (Frank Montesdeoca, Guillen Cuadros, Rivadeneira Mendoza, & Zambrano Dueñas, 2012).

Figura 7. **Gráfico de sedimentación**




Fuente: elaboración propia.

Para este caso, la pendiente pierde inclinación a partir del segundo valor, por lo que se considera que sólo deben extraerse dos factores, sin embargo para este análisis se quieren cuatro factores basados en la teoría general de disuasión, por lo que se realizarán varias rotaciones que nos indicarán si son suficientes para validar la hipótesis.

### 6.2.2. Rotación de factores

El resultado inicial del análisis factorial es una matriz factorial no rotada, es decir, la matriz de correlaciones de las variables con los factores. Esta matriz factorial inicial es difícil de interpretar y, en casi todos los casos donde se extrae más de un factor, es indispensable obtener una matriz adicional de factores rotados (Carroll, 1953). Por consiguiente, luego de extraer los factores iniciales, estos son sometidos a un procedimiento denominado rotación (cuando hay más de un factor en la solución).

#### 6.2.2.1. Método promax

Consiste en alterar los resultados de una rotación ortogonal hasta crear una solución con cargas factoriales lo más próximas a la estructura ideal. Dicha estructura se supone que se obtiene elevando las cargas factoriales obtenidas en una rotación ortogonal.

La Tabla VIII muestra los resultados de la rotación realizada, se resaltan los resultados de los factores con los valores más altos.

Tabla VIII. **Matriz de factores rotados con el método promax**

| | Factor1 | Factor2 | Factor3 | Factor4 |
|---|---|---|---|---|
| CS1 | 0.145 | 0.172 | 0.515 | |
| CS2 | | 0.274 | 0.716 | |
| PV1 | | 0.709 | 0.133 | |
| PV2 | 0.194 | 0.227 | 0.534 | |
| PV3 | 0.581 | 0.479 | | |
| PV4 | 0.343 | 0.199 | 0.181 | 0.242 |
| PV5 | | 0.453 | | 0.839 |
| CR1 | -0.205 | 0.689 | 0.204 | |
| CR2 | | 0.637 | 0.177 | 0.173 |
| CR3 | 0.558 | 0.568 | -0.266 | 0.159 |
| DS1 | 0.447 | 0.248 | | 0.116 |
| DS2 | | -0.131 | | 0.501 |
| AM1 | 0.881 | | | -0.124 |
| AM2 | 0.620 | | 0.248 | |
| AM3 | 0.847 | -0.190 | 0.109 | |

Fuente: elaboración propia.

Con base a resultados obtenidos, se procede a renombrar los factores. Los nombres se derivan de la agrupación de combinaciones lineales con valores propios de mayor peso.

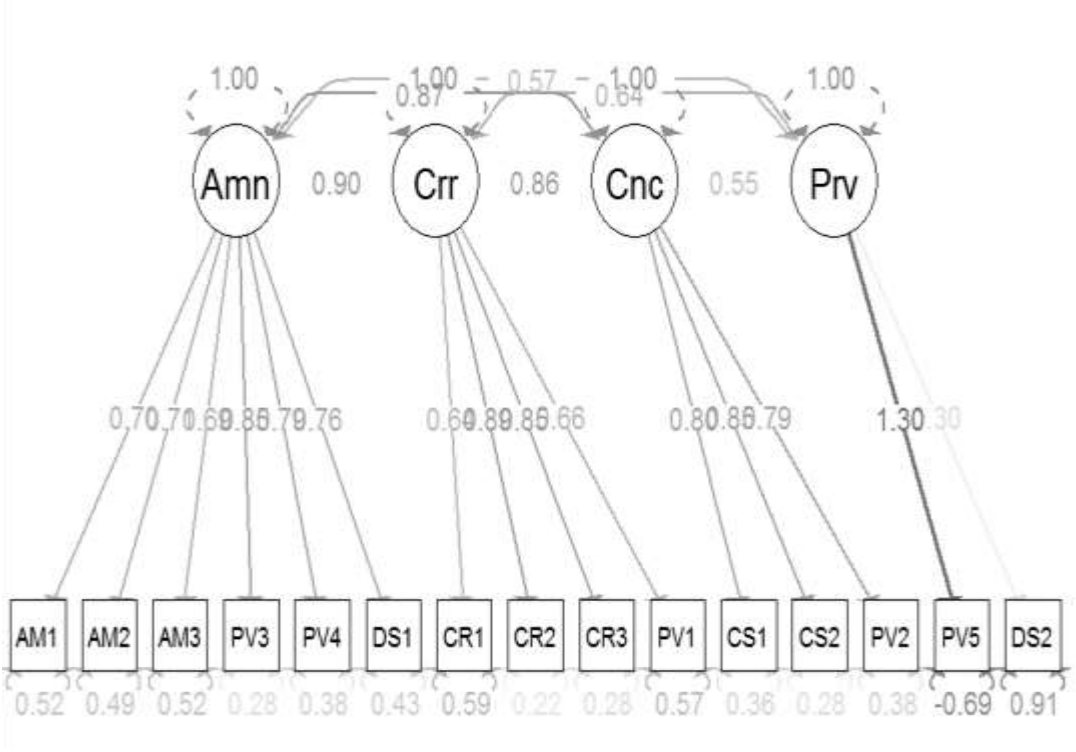
Factores renombrados:

Factor 1: se denomina amenaza, ya que los valores propios con mayor peso únicamente se ven reflejadas en las variables de amenazas; el Factor 2: se denomina prevención y corrección, los valores propios con mayor peso se relación con la prevención y corrección; el Factor 3: se denomina conocimiento sobre seguridad de la información, ya que los únicos valores con mayor peso

se ubicaron en las variables de corrección y, por último, al Factor 4: se denomina prevención.

La Figura 8 representa gráficamente cómo están relacionados los constructos que conforman la teoría con cada enunciado de la encuesta realizada que a su vez fue clasificada, según el aspecto a evaluar.

Figura 8. **Representación gráfica del modelo**




Fuente: elaboración propia.

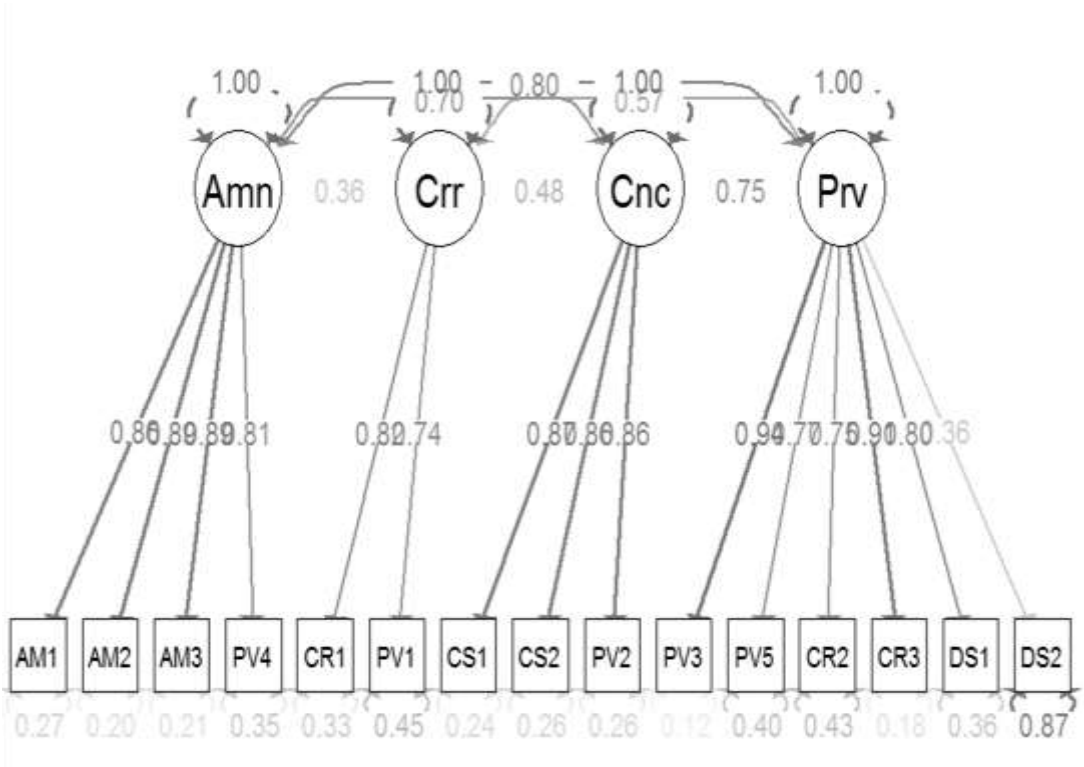
### 6.2.3. Análisis confirmatorio

Para una muestra de 50 encuestas de 20 preguntas cada una, se realiza de nuevo el cálculo de factores con el método de rotación promax que fue el

que mejor se ajuste a la búsqueda de factores de manera que se obtuvo el siguiente resultado:

La Figura 9 muestra las relaciones con cada constructo de la teoría y la relación entre las preguntas de la encuesta, donde Amn, son las amenazas, Crr, corrección, Cnc, conocimiento sobre la seguridad de la información y Prv, prevesión.

Figura 9. **Representación gráfica del modelo para análisis confirmatorio**




Fuente: elaboración propia.

## 6.3. Plan de negocio de emprendimiento empresarial

A continuación se describe el plan de negocio para una empresa individual, que ofrecerá consultoría en soluciones a riesgos de la seguridad de la información.

### 6.3.1. Estructuración del plan de negocio

Debido a que el presente trabajo no implica el desarrollo de software, no se cuenta con una arquitectura de éste tipo, sin embargo por medio de la herramienta Lienzo de Modelo de Negocio, se definió una estructura la cual se utilizó para definir el plan de negocio de emprendimiento los puntos principales que se tomaron en cuenta son:

- Actividades clave
- Propuesta de valor
- Relación con los clientes
- Socios clave
- Clientes
- Costos
- Recursos clave
- Canales
- Flujo de ingreso

### 6.3.2. Plan de negocio

El presente proyecto empresarial surge de la experiencia personal y profesional en diferentes áreas laborales, identificando las oportunidades de

negocio en torno a las nuevas tecnologías y el manejo de la información que es uno de los recursos más importantes para cualquier empresa.

Los altos mandos en las empresas están conscientes que las Tecnologías de la Información y la Comunicación (TIC) son un elemento muy importante para la consolidación y crecimiento de sus empresas, por otra, el coste económico en la pérdida de datos o falta de controles en el acceso a la información y gestión de la seguridad hace que las empresas o instituciones se preocupen de la pérdida de información confidencial

Los empresarios y gerentes de las pequeñas empresas, obviamente no son expertos en TIC y tampoco en temas de seguridad de información, por tal razón, se ven en la necesidad de adquirir asesoría que les ayude a implantar soluciones que les ayude a tener un mejor control de su información, así como también de definir políticas y concientizar a los empleados.

Esta realidad puede percibirse propiamente en el ambiente laboral en el que se desenvuelve cualquier profesional en el área tecnológica en cualquier sector, tanto público o privado.

Guatemala ofrece un nicho de mercado para la empresa que se propone, enfocándose en prestar servicios a pequeñas, grandes y medianas empresas que deseen buscar algún tipo de certificación o establecer el estado actual de su empresa en cuanto a seguridad de la información y mejor continua del negocio.

La empresa se pretende crear como una firma de consultoría especializada en servicios de ingeniería, tecnologías de información y seguridad informática.

Una oficina en casa se establecerá el primer año de operaciones para reducir los costos de inicio.

Se contará con una inversión inicial para los gastos de puesta en marcha, se presenta el siguiente plan de negocio con el cual se espera un retorno de esta inversión inicial producto del capital de trabajo que será manejado en una cuenta empresarial.

La empresa se especializará en la prestación de servicios en el diseño de soluciones riesgos de la seguridad de la información para empresas públicas y privadas.

### 6.3.3. Definición del problema

El problema central en el que se basa el presente plan de negocio se fundamenta en que no existe seguridad de la información en las organizaciones.

Con base a lo anterior, se plantea la siguiente pregunta principal:

¿Qué soluciones pueden implementar las organizaciones para prevenir y mitigar los riesgos de seguridad de la información?

Así mismo, se plantean las siguientes preguntas que complementan a la principal:

- ¿Cuáles son los riesgos en seguridad de la información dentro de la empresa?
- ¿Existen pérdidas de información en la empresa u organización?

- ¿Los ejecutivos o empleados conocen las medidas de prevención a posibles ataques?
- ¿Los ejecutivos o empleados protegen su información?
- ¿Cuenta la empresa u organización con un documento que brinde los lineamientos a seguir contra riesgos y amenazas de seguridad?
- ¿Cuál son los puntos débiles dentro de la empresa en cuanto a la seguridad de la información?

### 6.3.4. Misión

Generar un valor constante a clientes y sociedad en general, proveyendo soluciones integradas que mejoren y faciliten la gestión de los procesos de la seguridad de la información y comunicación. Para conseguir estos niveles de servicio se toma como base estándares y mejores prácticas.

### 6.3.5. Visión

Ser la empresa líder a nivel nacional en el diseño de soluciones a riesgos de seguridad de la información.

### 6.3.6. Lienzo de modelo de negocio

#### 6.3.6.1. Segmentos de mercado

Los segmentos de mercado a los cual apuntará el negocio se describen a continuación:

- **Sector público:** es el conjunto de organismos administrativos mediante los cuales el Estado cumple, o hace cumplir, la política o voluntad

expresada en las leyes del país, es decir todas las instituciones gubernamentales del Estado.

Este sector se divide en:

- Administración Central
- Entidades descentralizadas, autónomas y de seguridad social
- Gobiernos locales
- Empresas pública

- **Sector privado:** es aquella parte de la economía que busca el ánimo de lucro en su actividad y que no está controlada por el Estado, es decir, toda empresa privada.

- **Sector financiero:** el sistema financiero de Guatemala tiene dos segmentos. El sector financiero formal (regulado), que está conformado por instituciones cuya autorización es de carácter estatal, bajo el criterio de caso por caso, y que están sujetas a la supervisión de la Superintendencia de Bancos, órgano facultado para tal fin (Guatemala, 2014).

  El sector financiero a su vez se divide en:

  - **Sector bancario:** incluye a los bancos comerciales y a las sociedades financieras, estas últimas, definidas por ley como instituciones especializadas en operaciones de banca de inversión (Guatemala, 2014);
  - **Sector no bancario:** incluye a las compañías de seguros y de fianzas (Guatemala, 2014).

#### 6.3.6.2. Propuesta de valor

Los modelos de seguridad tradicionales se enfocan en mantener alejados a los atacantes externos. La realidad es que existen amenazas tanto dentro como fuera de la organización. La tecnología móvil, computación en nube, las redes sociales y el sabotaje por parte de los empleados son solo algunas de las amenazas internas que enfrentan las empresas.

La propuesta es brindar una evaluación diagnóstica basada en la teoría general de disuasión para identificar los riesgos que hay que enfrentar y con base a eso hacer el diseño de la solución a esos riesgos.

Lo que se busca es ayudar al cliente a identificar sus debilidades y que exista un proceso de cambio y mejora continua.

#### 6.3.6.3. Canales

Lo que se busca es una buena fidelización de clientes y redes de comunicación de tal forma que, por medio de un cliente se obtenga otro. Contar con un conocimiento estructurado del cliente permitirá realizar procesos de segmentación efectivos y establecer programas de relacionamiento óptimos de acuerdo con las necesidades y posibles comportamientos del cliente.

##### 6.3.6.3.1. Canales principales

- **Web corporativa:** la página será el escaparate de los servicios que se prestan y de la profesionalidad, la seriedad y el compromiso de con el cliente, a través de este medio y resolver sus dudas a la vez de pedir información sobre las diferentes gestiones que necesiten llevar a cabo.

Así mismo, se tomará como lineamiento el ciclo de proceso de atracción de clientes que se muestra a continuación que será el medio para la adquisición y crecimiento del número de clientes de la empresa.

- **Alianzas:** Serán necesarias las alianzas con otras empresas con el objetivo de compartir información, experiencia, clientes, llegar a otro mercado, reducir los costos, aumentar las ventas, crear barreras de entrada y dar solución a necesidades de los clientes. Fundamentalmente permitirá la expansión, sin perder independencia y flexibilidad. Así al trabajar en cooperación con otra empresa es probable que se alcancen los objetivos esperados.

Algunas de las organizaciones a tomar en cuenta son:

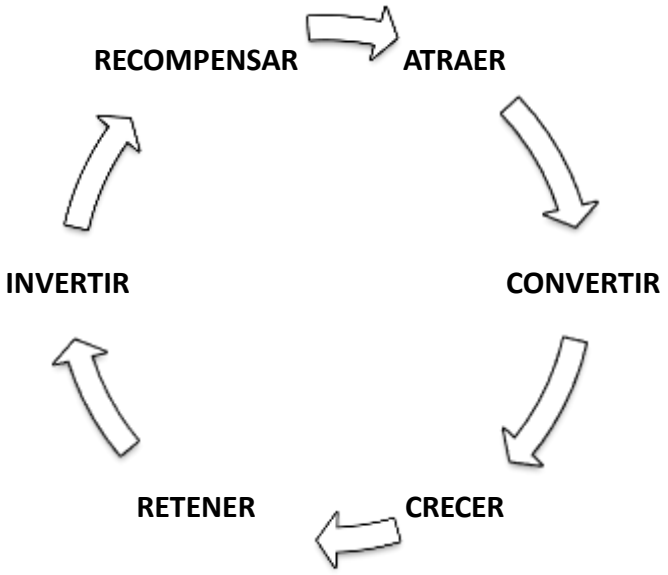
**ISACA**

ISACA Guatemala está conformado por un grupo de profesionales interesados en el desarrollo de las Tecnologías de Información en Guatemala, la organización se ha constituido como una Asociación no lucrativa cuyos objetivos principales son el de promover la educación, ayudando a expandir el conocimiento y habilidades de sus integrantes en los campos relacionados con la auditoría, seguridad, control y gestión de sistemas de información, además de promover las certificaciones profesionales entre sus asociados proveyendo de personal calificado a la industria, el comercio y cualquier otro organismo u organización interesado en contar con personal certificado.

**ESET**

Es una empresa que brinda soluciones tecnológicas de seguridad para todo tipo y tamaño de empresas. Se considerará esta empresa para formar alianzas que permitan la colaboración para la prestación y adquisición de servicios.

Figura 10. **Ciclo de proceso de atracción del cliente**




Fuente: elaboración propia.

Herramientas de marketing a ser utilizadas:

- **Publicidad**: para dar a conocer la empresa y servicios así como para distinguirse de la competencia y potenciar una buena imagen;
- **Promociones**: tienen como objetivo estimular la venta a corto plazo;

- **Relaciones públicas**: esencial para cualquier nuevo negocio como en éste caso, el objetivo es crear una buena imagen, tanto dentro de la empresa como de cara al exterior;

- **Directorios empresariales:** la empresa figurará en las guías telefónicas y directorios relacionados con esta actividad, tanto en papel como en internet. Además, Google *Maps* Negocios ofrece la posibilidad de suscribirse de forma gratuita;

- **Tarjetas corporativas:** tarjetas de reducido tamaño y en horizontal, tendrán como característica principal la portada, que será la imagen o logotipo de la empresa. En las contraportadas se incluirán los datos de página web, contacto y localización de la empresa;

- ***Mailing*:** es otra herramienta de comunicación también muy adecuada para este tipo de empresas, puesto que permite ofrecer al cliente los servicios de forma personalizada, pero sin el coste de la visita comercial.

#### 6.3.6.4. Relación con el cliente

Es importante fomentar una buena relación con el cliente para fidelizarlo. La satisfacción del cliente favorecerá el impulso de las ventas y la atracción de nuevos clientes. Para alcanzar estos resultados se debe conocer cómo se están satisfaciendo sus necesidades y cómo esto puede ayudar a mejorar los aspectos claves y de éxito de la entrega del servicio, el proceso de venta, etc.

Para lograr una buena relación con el cliente se tomarán en cuenta los siguientes aspectos:

- **Relación personal:** es la interacción entre el cliente y el consultor; normalmente se produce en el momento de la oferta de los servicios a través de medios telefónicos, chat en línea, por correo, etc.

- **Relación personal dedicada:** se brindará atención personal dedicada a cada proyecto que se implemente.

#### 6.3.6.5. Recursos clave

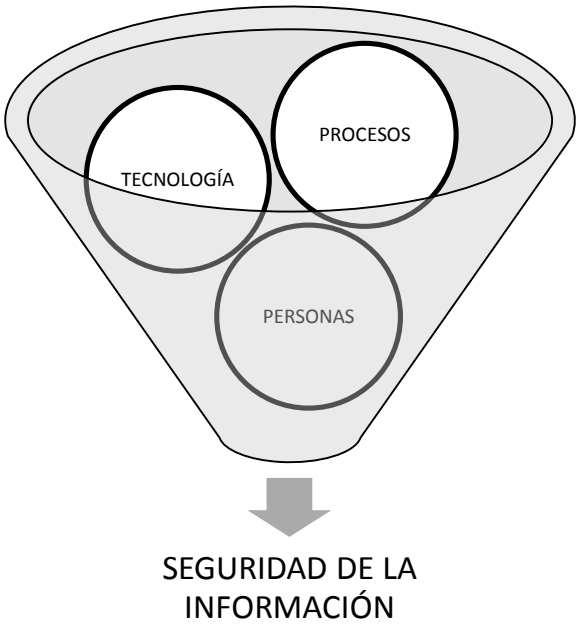
Los recursos que se consideran claves para el éxito de este emprendimiento son:

- **Tecnología:** se define como el conjunto de conocimientos y técnicas que, aplicados de forma lógica y ordenada, permiten al ser humano modificar su entorno material o virtual para satisfacer sus necesidades, esto es, un proceso combinado de pensamiento y acción con la finalidad de crear soluciones útiles;

- **Procesos:** actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado;

- **Personas:** empleados y clientes involucrados en los procesos.

Figura 11. **Recursos claves**




Fuente: elaboración propia.

#### 6.3.6.5.1. **Cobertura**

En sus comienzos, la empresa prestará sus servicios en el departamento de Guatemala, pensando en un corto plazo expandirse a nivel república, todo esto dependerá de las ganancias obtenidas durante de los primeros dos años, así como la demanda del servicio y nuevos clientes.

### 6.3.6.6. Socios clave

Se considerará la comunicación con empresas como ESET, que son líderes en la industria de seguridad, de manera que se pueda obtener alguno de los servicios que esta empresa ofrece como parte de la soluciona a brindar de parte de la empresa  a nuestros clientes.

También se considerará la adquisición de servicios como parte de la solución de la empresa *Wide Defense,* quienes brindan servicios especializados para la detección y manejo de situaciones de riesgo existentes en la red y en los sistemas que soportan el negocio. Contempla servicios asociados a *Governance, risk and compliance, ethical hacking*, continuidad del negocio, consultoría, entre otros.

Así mismo, los socios clave también serán nuestros propios clientes que a su vez podrán recomendar nuestros servicios a otras empresas.

#### 6.3.6.7. Actividades clave

Las actividades claves en las que se desenvolverá la empresa serán:

- Evaluación diagnóstica
- Desarrollo de la política de seguridad de la información
- Campaña disuasiva
- Capacitación y concientización
- Mejores prácticas
- Mejora continua

Las actividades anteriormente descritas se trabajarán en función a los siguientes factores que se consideran claves para el éxito:

- Calidad en los trabajos y satisfacción de los clientes;
- Integrar los servicios que se presten dentro del funcionamiento diario de la empresa;
- Personalizar los servicios para lograr el objetivo de la integración, esto requiere conocer en profundidad la empresa del cliente y mantener una relación fluida durante el proceso de prestación del servicio;

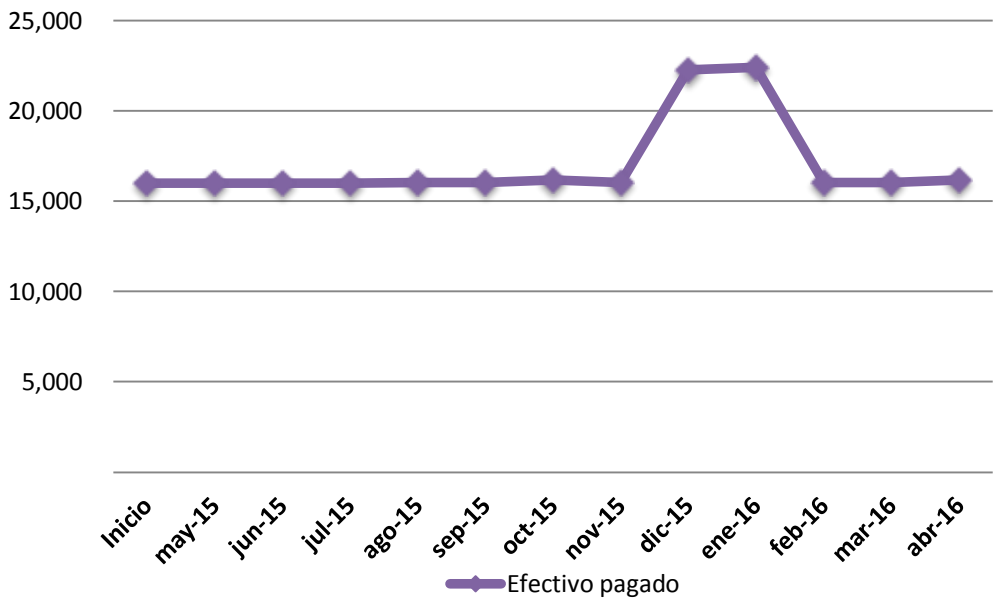
- Servicios complementarios. Servicio postventa de atención de incidencias, asesorar a los trabajadores de la empresa-cliente, capacitación, mejora continua de procesos, definición de políticas y documentación.

#### 6.3.6.8. Estructura de costes

La financiación total del proyecto en sus inicios será de Q.30, 000.00, el cual será proveído por el socio mayoritario y dueño fundador de la empresa. La factibilidad de contar con este monto es inmediata.

Como se puede observar en la tabla de flujo de efectivo, que el primer mes se utilizará como estrategia de ventas que permita crear la cartera inicial de clientes, ofreciendo una evaluación gratuita que incluirá una propuesta para la solución de los problema identificados en la evaluación que será el diseño de la solución, la cual tendrá un costo aproximado de Q2,000.00. Esperando un crecimiento de clientes y ventas en el sexto mes.

Figura 12. **Resumen de Flujo de Efectivo (sumas expresadas en quetzales)**




Fuente: elaboración propia.

La tabla IX contiene todos los aspectos a tomar en cuenta para operación de la empresa y flujo de efectivo en el primer año de funciones. Se considera el alquiler de un local básico, un aproximado de ingresos por servicios y se contempla el salario para un único consultor.

Tabla IX. **Flujo Efectivo**

**FLUJO DE EFECTIVO A DOCE MESES**

Valores expresados en Quetzales (Q.)

| | Inicio | may-15 | jun-15 | jul-15 | ago-15 | sep-15 | oct-15 | nov-15 | dic-15 | ene-16 | feb-16 | mar-16 | abr-16 | Promedio mensual |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Efectivo disponible (a principio de mes) | 30,000 | 14,005 | 24,005 | 24,005 | 24,005 | 24,005 | 24,005 | 24,005 | 24,005 | 24,005 | 26,005 | 26,005 | 26,005 | 23,672 |
| Ingreso por Servicios | | 10,000 | 10,000 | 10,000 | 10,000 | 10,000 | 10,000 | 10,000 | 10,000 | 12,000 | 12,000 | 12,000 | 12,000 | 10,667 |
| Posición de efectivo (a fin de mes) | 14,005 | 7,990 | 7,990 | 7,990 | 7,985 | 7,985 | 7,835 | 7,985 | 1,735 | 1,585 | 9,985 | 9,985 | 9,835 | 6,575 |
| **Efectivo pagado** | | | | | | | | | | | | | | |
| Compras | 521 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 |
| Salarios brutos | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 | 12,500 |
| Suministros (de oficina y operativos) | 350 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| Reparaciones y mantenimiento | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| Publicidad | 150 | | | 150 | | | 150 | | | 150 | | | 150 | 50 |

Continúa tabla IX.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alquiler | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 | 2,500 |
| Servicios (Agua, luz, teléfono, internet) | 600 | 600 | 620 | 625 | 625 | 625 | 625 | 625 | 625 | 625 | 625 | 625 | 625 | 623 |
| Hosting(Servicio de Pagina Web en Internet) Anual | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 | 45 |
| Bonos extras (Bono14 y Aguinaldo) | . | . | . | 12,500 | . | . | . | . | 6,250 | 6,250 | . | . | . | 8,333 |
| Compra de capital (especificar) | | | | | | | | | | | | | | |
| Otros gastos iniciales | 400 | | | | | | | | | | | | | |
| Reserva o depósito | | | | | | | | | | | | | | |
| Retirada del propietario | | | | | | | | | | | | | | |
| **Total de efectivo pagado** | **15,995** | **15,995** | **16,015** | **16,015** | **16,020** | **16,020** | **16,170** | **16,020** | **22,270** | **22,420** | **16,020** | **16,020** | **16,170** | **17,096** |

Fuente: elaboración propia.

# 7. DISCUSIÓN DE RESULTADOS

Tomando como base el modelo obtenido en el análisis confirmatorio se concluye lo siguiente:

Para:

**H1:** El conocimiento sobre seguridad de la información se relaciona con cada constructo de la teoría general de disuasión.

**H1a:** El conocimiento sobre seguridad de la información se relaciona con la disuasión.

**H1b:** El conocimiento sobre seguridad de la información se relaciona con la prevención.

**H1c:** El conocimiento sobre seguridad de la información se relaciona con la detección.

**H1d:** El conocimiento sobre seguridad de la información se relaciona con la corrección.

Conclusiones para H1:

Se descarta H1a, H1c y H1d y se concluye entonces que el conocimiento sobre seguridad de la información se relaciona directamente con las medidas preventivas que se manejen dentro de la organización, empresa o institución.

Para:

**H2:** El tamaño de la organización influye directamente con cada uno de los constructos de la teoría general de la disuasión.

**H2a:** El tamaño de la organización influye directamente con la disuasión.

**H2b:** El tamaño de la organización influye directamente con la prevención.

**H2c:** El tamaño de la organización influye directamente con la detección.

**H2d:** El tamaño de la organización influye directamente con la corrección.

Conclusiones para H2:

Esta hipótesis se descartó desde un inicio cuando se determinó por medio de cálculo de matriz de comunalidades, donde se observó que esta variable no aportaba ningún significado en el análisis. Algunas personas consideraron en las respuestas que el tamaño de la organización no siempre va a afectar que se tenga una buena gestión de la seguridad.

Para:

**H3:** Las amenazas influyen directamente con cada uno de los constructos de la teoría general de la disuasión.

**H3a:** Las amenazas influyen directamente con la disuasión.

**H3b:** Las amenazas influyen directamente con la prevención.

**H3c:** Las amenazas influyen directamente con la detección.

**H3d:** Las amenazas influyen directamente con la corrección.

Conclusiones para H3:

Se descarta entonces H3a, H3c y H3d, concluyendo entonces que las amenazas se relacionan directamente con la prevención que se tenga o medidas que se tengan ante las amenazas.

Otras conclusiones:

Analizando el diagrama del modelo obtenido en el análisis confirmatorio, en se puede observar que la prevención se relaciona también con las correcciones y sin duda son dos aspectos que van de la mano, las organizaciones tiene que definir cómo actuarán si se llega a materializar algún tipo de riesgo y qué medidas de prevención están tomando en cuenta, así mismo una de las prevenciones puede ser el factor disuasión, que se refiere al efecto que estén causando sobre los usuarios de sistemas o empleados.

En una de las preguntas de respuesta abierta para la primera encuesta entregada a una pequeña muestra de personas, coincidieron que una de las principales razones por las que existen riesgos en la seguridad es porque los empleados no tienen conocimiento del tema y otra razón es que las organizaciones no cuentan con políticas de seguridad establecidas.

Siguiendo la línea de investigación y basado en los antecedente presentados, el argumento base de este trabajo, se enfoca en que las acciones de seguridad de la información que se apliquen puede disuadir a potenciales abusadores informáticos de cometer actos que violen implícita o explícitamente la política de la organización, la aplicación específica de la teoría se basa en la relación entre las actividades de los altos mandos y los posibles abusadores, en primer lugar debería ser los directivos la clave para disuadir con éxito y

garantizar la prevención y detección del abuso, así como contar con los recursos que permiten castigar a los delincuentes. Cabe señalar que estos constructos y sus interrelaciones están implícitos en la teoría general de disuasión específicamente en los efectos de la actuación policial. Una cierta porción de potencial de abuso es disipado mediante técnicas de disuasión, como las políticas y directrices para el uso adecuado de sistema de información y recordatorios a los usuarios a cambiar sus contraseñas. Dependen totalmente de la voluntad de los usuarios del sistema cumplir con todas las directrices plasmadas en una política de seguridad eficaz.

Programas de concientización de seguridad son una forma de contramedida disuasiva que no se debe obviar, es decir, la educación a los usuarios, así como a sus superiores acerca de la seguridad, produce grandes beneficios. Estas sesiones educacionales transmiten conocimiento sobre los riesgos en la organización, como por ejemplo: dar a conocer las políticas y las sanciones por violaciones, revelar las amenazas a los sistemas locales y su vulnerabilidad a los ataques y enseñar al usuario como debe actuar ante ataques, para lograr el objetivo que se persigue que es la seguridad.

## 7.1. Propuesta de diseño

Para este trabajo especial de graduación se dará la propuesta de diseño de solución a las problemáticas de los riesgos de seguridad de la información identificados en la evaluación y análisis realizado en el punto anterior, los puntos a dar solución son los siguientes:

- Conocimiento sobre seguridad de la información
- Política de seguridad de la información

La solución estará basada bajo las premisas de la norma internacional ISO/IEC 27001, tecnología de la Información, técnicas de seguridad y código para la práctica de la gestión de la seguridad de la información.

### 7.1.1. Conocimiento sobre seguridad de la información

#### 7.1.1.1. Solución a la ingeniería social

Para lograr defender al sistema de información es necesario cubrir puntos importantes: formar y concientizar, la primera es explicar a los empleados como consigue un hacker engañarle y como reconocer un ataque, es decir que se limite a utilizar el sistema como herramienta de trabajo, es decir, no compartir con nadie accesos, como usuarios y contraseñas, ya que son para uso personal.

Concientizar, es demostrarles a los empleados que este tipo de ataques es cada vez más frecuente y por lo general es el primer recurso que se utiliza cuando se quiere corromper la seguridad. Además es necesario retroalimentar esta información y recordar periódicamente a los usuarios, esta medida es recomendada por muchos autores sobre seguridad de la información ya que respalda el trabajo previo de la ingeniería social, por eso es recomendable informar constantemente a los usuarios.

#### 7.1.1.2. Conocimiento en seguridad de la información

A continuación se describe el diseño de la solución basado en la Norma ISO 27001.

- **Control**

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral (ISO/IEC, 2005).

- **Lineamiento de implementación**

La capacitación y el conocimiento debería comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios (ISO/IEC, 2005).

La capacitación constante debe incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales, así como la capacitación en el uso correcto de los medios de procesamiento de información; por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los proceso disciplinarios (ISO/IEC, 2005). En este punto los procesos disciplinarios entran a ser parte del factor disuasivo.

Las actividades de conocimiento, educación y capacitación debieran ser adecuados y relevantes para el rol, responsabilidades y capacidades de la persona, y debieran incluir información sobre amenazas conocidas, a quién contactar para mayor consultoría sobre seguridad y los canales apropiados para reportar los incidentes de seguridad de la información (ISO/IEC, 2005).

### 7.1.2. Política de seguridad de la información

Una política de seguridad de la información es un conjunto de reglas aplicada a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma (Rodríguez Córdova, 2014).

El propósito de contar con una política de seguridad de la información en las organizaciones es proteger la información y los activos de datos. Las políticas son guías para asegura la protección, confidencialidad e integridad de los datos dentro de los diferentes sistemas con que cuente una organización como por ejemplo correo, software y procedimiento manuales.

#### 7.1.2.1. Documento de la política de seguridad de la información

A continuación se describe el diseño de la solución basado en la Norma ISO 27001.

- **Control**

El documento de la política de seguridad de la información debería ser aprobado para la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes (ISO/IEC, 2005).

- **Lineamiento de implementación**

El documento de la política de seguridad de la información debe enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información (ISO/IEC, 2005).

Puntos que deberían ser considerados dentro del documento:

- Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información;
- Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;
- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;
- Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización incluyendo:
- Gestión de la continuidad del negocio.
- Consecuencias de las violaciones de la política de seguridad de la información (disuasión).
- Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información;
- Referencias a la documentación que fundamente la política.

Es importante que está política sea comunicada a toda la organización de una forma accesible y entendible para el lector.

### 7.1.3. La disuasión como solución

A continuación se describe el diseño de la solución basado en la Norma ISO **27001**.

- **Control**

Debiera existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad (ISO/IEC, 2005).

- **Lineamiento de implementación**

El proceso disciplinario no debiera iniciarse sin una verificación previa de la ocurrencia del incumplimiento de la seguridad (ISO/IEC, 2005).

El proceso disciplinario formal debiera asegurar el tratamiento correcto y justo para los empleados sospechosos de cometer incumplimientos de la seguridad (ISO/IEC, 2005). El proceso disciplinario debe proporcionar una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio, si esta es la primera ofensa, si el culpable fue apropiadamente capacitado, la legislación relevante, contratos comerciales y otros factores que se puedan requerir.

Definitivamente contar con procesos disciplinarios y sobre todo que los empleados estén enterados de las posibles sanciones que se puedan aplicar e inclusive una remoción de sus labores, pueden ser utilizados como un disuasivo

para evitar que las personas violen las políticas y procedimiento de seguridad organizacionales y cualquier otro incumplimiento de la seguridad.

## 7.2. Definición de los productos

Con base a las conclusiones y al análisis realizado en los puntos anteriores, a continuación se describen los productos que se ofertarán con base a las problemáticas identificadas.

### 7.2.1. Evaluación diagnóstica

La evaluación diagnóstica consiste en identificar las debilidades que tienen una empresa u organización, basado en la Teoría General de Disuasión. Es el acto de investigar y analizar los riesgos asociados a los procesos del propio negocio y su entorno.

Objetivos:

- Conocer los activos y recursos a proteger, los puntos vulnerables de cada proceso y las amenazas asociadas;
- Evaluar la viabilidad y efectividad de los controles de reducción a la exposición de amenazas que se están desarrollando;
- Identificar el nivel de riesgo aceptable para que la organización pueda existir;
- Calcular el coste del impacto de materialización de las amenazas identificadas;
- Valorar la capacidad de recuperación frente a incidentes y la probabilidad de continuidad de los procesos del negocio;

- Elaborar planes de acción para la mejora y solución de los puntos críticos;
- Entrevistar y encuestar a los empleados para evaluar el conocimiento de seguridad de la información.

Aspectos a evaluar, según estándar ISO 27001:

- Sistema de gestión, políticas, planes de seguridad y base reglamentaria;
- Inventario de Hardware, Software y la evaluación de su valor real y de pérdida;
- Seguridad de la red e Internet;
- Accesos remotos y uso de servicios de acceso a aplicaciones de la organización;
- Publicaciones de la organización;
- Ordenadores de mesa y estaciones de trabajo en red;
- Seguridad física y ambiental de la edificación;
- Fronteras de responsabilidades y disciplina tecnológica de la red;
- Conocimiento en seguridad de la información de los empleados.

### 7.2.2. Política de seguridad de la información

Se brindará a la empresa el servicio de elaboración de la política de seguridad de la información con base a la evaluación brindada sobre seguridad de la información.

Las políticas contienen el compromiso de la alta gerencia con la seguridad de información, así como también el estricto cumplimiento por parte de los empleados.

### 7.2.3. Campaña disuasiva

La disuasión es la “acción y efecto de disuadir”, y disuadir significa “inducir, mover a alguien con razones a mudar de dictamen o a desistir de un propósito”; básicamente, la disuasión consiste en convencer a alguien, de una u otra forma, para que cambie su manera de actuar. Cuando hablamos de seguridad, las medidas de disuasión son las que tratan de “convencer” a alguien hostil para que cese su actitud.

Pero no es suficiente contar con medidas disuasivas tan simples como por ejemplo colocar unos letreros en la empresa que digan que las personas están siendo grabadas por cámaras de seguridad o un mensaje dentro de la página web corporativa que advierta al usuario a utilizar correctamente el equipo, etc… es necesario montar una verdadera campaña disuasiva que incluya más aspectos.

El servicio a ofrecer como campaña disuasiva con enfoque al personal interno el cual incluirá las siguientes características:

- Dar a conocer las políticas de seguridad de la información de la empresa u organización;
- Hacer de conocimiento al empleado de las posibles sanciones o repercusiones que podrían tener a la hora de cometer una falta a la seguridad de la información.

### 7.2.4. Programas de capacitación y concientización del personal

Capacitación a personas con distintos niveles de conocimiento tanto técnico como administrativo. Estas capacitaciones pueden ser con base a uno o

varios temas relacionados con la seguridad de la información. Con respecto a la ingeniería social se incluirán pruebas especializadas para establecer el nivel de preparación del personal ante estos ataques.

### 7.2.5. Mejores prácticas

Verificación del cumplimiento con las mejores prácticas del mercado sin llegar a una certificación.

### 7.2.6. Mejora continua

Desarrollo e implementación de un plan que permita mantener la funcionalidad de una organización, a un nivel mínimo aceptable, durante una contingencia.

### 7.2.7. Evaluación de herramientas para la gestión del riesgo

Como parte del diseño de la solución a riesgos también se brindará una evaluación de herramientas de *software* que ya se encargan del manejo y gestión de los riesgos, algunas de estas herramientas son de licencia libre y otras pagadas; sin embargo, con base a la evaluación se pueden dar una recomendaciones para que a su vez las puedan adquirir e implementar.

# CONCLUSIONES

1. La propuesta de diseño desarrollada contempla los siguientes aspectos: el uso de medios disuasivos, diagnósticos periódicos, los lineamientos para generar una política de seguridad de la información, capacitaciones al personal, el uso de la seguridad informática y gestionar la seguridad de la información de forma permanente.

2. La seguridad de la información tiene como fin la protección de la información e incluye todo el conjunto de medidas que permitan garantizar los principios de la seguridad que son: la confidencialidad, disponibilidad e integridad de la información, toma en cuenta aspectos funcionales y de procesos de una organización que incluye identificar los riesgos, establecer controles para gestionarlos o eliminarlos; establecer estrategias para prevenir y mitigar riesgos y establecer políticas o normas que la gestionen la seguridad.

3. La Teoría General de Disuasión postula que los individuos pueden ser disuadidos de cometer actos antisociales, a través del uso de contramedidas que incluyan falta de incentivos y sanciones firmes en relación con el acto, y se aplica a la seguridad de la información, haciendo uso de medidas o herramientas disuasivas, como por ejemplo: video vigilancia, definiendo normas, reglas o políticas que indiquen las consecuencias de las faltas a la seguridad y que sean conocidas por todo el personal.

4. Con base a resultados obtenidos en la encuesta y análisis realizado, se concluye que los dos principales riesgos en seguridad de la información es la falta de conocimiento en seguridad de información por parte de los empleados y falta de una política de seguridad de información que sea conocida por el personal, el riesgo es enfocado directamente al empleado en la organización, quien no sabría cómo prevenir o actuar en caso de un ataque o si alguien quisiera robar información confidencial.

5. Basado al plan de negocio elaborado, se concluye que es factible el emprendimiento empresarial para el diseño de soluciones de seguridad de la información. Los aspectos más relevantes que se incluyen en el plan de negocio son: una evaluación diagnóstica basada en la teoría general de la disuasión, identificación de los riesgos, elaboración del diseño de la solución, la creación de una política de seguridad de la información, la creación de un marco referencial para establecer los objetivos de control, la estructura de evaluación y gestión del riesgo, la definición de principios, estándares y consecuencias de las violaciones de la política y por último la definición de las actividades para la gestión de la mejora continua del negocio.

# RECOMENDACIONES

1. A organizaciones y público en general, la utilización de la teoría de disuasión general puede ser utilizada no sólo para la identificación y solución de riesgos en seguridad de la información, que puede ser aplicada a otros temas, donde se requieran métodos disuasivos para llevar el control de determinado evento, proceso o problema.

2. A organizaciones en general, la utilización de herramientas o medios disuasivos dentro de la empresa como prevención.

3. A cualquier persona que desee emprender, el uso de la herramienta de lienzo de negocio, ya que facilita comprender y ordenar las ideas para elaborar de una manera sencilla un plan de negocio.

4. A empresas que comienzan operaciones, establecer canales informativos que proporcionen a los emprendedores los conocimientos u orientaciones necesarias, para incorporar la seguridad de la información y la continuidad de negocio como áreas de la estrategia empresarial.

5. A estudiantes de la carrera de maestría en Tecnologías de la Información y Comunicación, el uso del análisis estadístico en caso que el trabajo de investigación requiera un estudio de campo, facilita la interpretación de los datos para fundamentar soluciones, conclusiones o argumentos en el trabajo de investigación.

# REFERENCIAS BIBLIOGRÁFICAS


1. Baltazar Gález, J. M., & Compuzano Ramírez, J. C. (Febrerto de 2011). Diseño e Implementación de un Esquema de Seguridad Perimetral para Redes de Datos. Caso Práctico: Dirección General del Colegio de Ciencias y Humanidades. *Diseño e Implementación de un Esquema de Seguridad Perimetral para Redes de Datos. Caso Práctico: Dirección General del Colegio de Ciencias y Humanidades*. Distrito Federal, Mexito: Universidad Nacional Autónoma de México.

2. Cohen, D., & Asin, E. (2000). *Sistemas de Información* (3 era. ed.). Mc. Graw Hill.

3. De La Brouyere, J. (2015). *Universidad Nacional Abierta y a Distancia de Colombia*. Recuperado en enero de 2015, de http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin__exploratoria_descriptiva_correlacional_y_explicativa.html

4. De la Fuente Fernandez, S. (2011). *Portal Fuente Rebollo.* Recuperado en febrero de 2015, de http://www.fuenterrebollo.com/Economicas/ECONOMETRIA/MULTIVARIANTE/FACTORIAL/analisis-factorial.pdf

5. De Salvador, L. (18 de octubre de 2011). *Instituto Español de Estudios Estratégicos.* (I. E. Estratégicos, Ed.) Recuperado en enero de

2015, de ieee.es: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

6. Diaz, A. (2010). *Sistema de Gestión de la Seguridad de la Información UNE-ISO/IEC 27001.* Artículo.

7. Frank Montesdeoca, M. V., Guillen Cuadros, J. E., Rivadeneira Mendoza, J., & Zambrano Dueñas, G. J. (Enero de 2012). *Diseño y ejecución de un plan de capacitación sobre Emprendimiento.* Obtenido de https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CDcQFjAEahUKEwj764vIhY7GAhWyLYwKHX1oAP0&url=http%3A%2F%2Frepositorio.utm.edu.ec%2Fbitstream%2F123456789%2F956%2F1%2FTESIS%2520-%2520EMPRENDIMIENTO.pdf&ei=PNp8VfvdE7LbsAT90IHoDw&usg=AF

8. Fryars, N. (27 de 04 de 2012). *Zebra Management Consulting*. Obtenido de http://www.zebramc.com/introduction-to-the-business-model-canvas/

9. Guatemala, B. d. (2014). *Banco de Guatemala.* Obtenido de http://www.banguat.gob.gt/inc/ver.asp?id=/publica/doctos/bgdoc005/2

10. Hernández Sánchez, L. (2014). *Buenas Prácticas para la Implementación de la Seguridad en un Centro de Cómputo.* Universidad Nacional Autónoma de México. Obtenido de

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/3735/Tesis.pdf?sequence=1

11. ISACA. (2014). *Control Objectives for Information an Related Technology.* Recuperado el 14 de marzo de 2014, de ISACA: https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=SEM&gclid=CPyKgfyTpb0CFe99OgodpCQA1w

12. ISO. (2014). *Estándar ISO/IEC 27001.* (I. O. Standardization, Ed.) Recuperado el 15 de febrero de 2014, de ISO: http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

13. ISO/IEC. (2005). *Tecnología de la Información - Técnicas de Seguridad - Código para la práctica de la gestión de la seguridad de la información* (Vol. 2da. edición). (ISO, Ed.) Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

14. Lab, K. (2014). *Media Kaspersky.* (K. Lab, Ed.) Obtenido de IT Security Risks Survey 2015: A Business Approach to Managing Data Security Threats: http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf

15. López M., A. A. (Julio de 2011). *Biblioteca de Ciencias y Tecnología de la Universidad Centrooccidental Lisandro Alvarado de Venezuela.* Obtenido de http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TGMQA76.9.A25L662011.pdf

16. Mahía Casado, R. (s.f.). Analisis Factorial. *Universidad Autónoma de Madrid.* Recuperado el 26 de mayo de 2014, de Universidad Autónoma de Madrid: http://www.uam.es/personal_pdi/economicas/eva/pdf/factorial.pdf

17. Maya, E. (2014). *Sitio Web Facultad de Arquitectura.* Recuperado en enero de 2015, de http://arquitectura.unam.mx/uploads/8/1/1/0/8110907/metodos_y_tecnicas.pdf

18. Mesquida Calafat, A. L. (Mayo de 2012). *Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros.* Recuperado el 2 de abril de 2014, de Tesis Doctorales en Red: http://www.tdx.cat/

19. Mifsud, E. (26 de marzo de 2012). *Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado.* (G. d. España, Ed.) Recuperado el 12 de febrero de 2014, de INTEF: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?format=pdf

20. Montenegro, L. (2014). *Seguridad de la Información: Más que una actitud, un estilo de vida.* Obtenido de TechNet: http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

21. Ramió Aguirre, J. (Octubre de 2013). *Bibiloteca Buleria.* Recuperado en diciembre de 2015, de

http://buleria.unileon.es/bitstream/handle/10612/3277/Seguridad_TIC.PDF?sequence=1

22. Rebollo Martínez, O. (2014). *Las amenazas son eventos que pueden causar alteraciones a la información, ocasionándole.* https://ruidera.uclm.es/xmlui/bitstream/handle/10578/4121/TESIS%20Rebollo%20Mart%C3%ADnez.pdf?sequence=1, España. Recuperado en enero de 2015, de https://ruidera.uclm.es/xmlui/bitstream/handle/10578/4121/TESIS%20Rebollo%20Mart%C3%ADnez.pdf?sequence=1

23. Rodríguez Córdova, N. E. (2014). *UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS.* Obtenido de UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS: http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap6.PDF

24. Rodríguez Sabiote, C., Lorenzo Quiles, O., & Herrera Torres, L. (2005). *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal.* (E. Universidad de Granada, Ed.) Recuperado en enero de 2015, de http://www.redalyc.org/pdf/654/65415209.pdf

25. Schuessler, J. H. (2009). *General Deterrence Theory: Assesin Information Systems Security Effectiveness in Large versus Small Business.* Obtenido de http://nsl.cse.unt.edu/~dantu/cae/attachments/JosepthSchuesslerDissertation.pdf

26. Serrano, C., & Gutiérrez, B. (s.f.). *iFinanzas.* (U. d. España, Ed.) Recuperado en enero de 2015, de iFinanzas: http://ciberconta.unizar.es/LECCION/factorial/FACTORIALEC.pdf

27. Straub, D., & Welke, R. (1998). *http://misq.org/.* Obtenido de http://paul-hadrien.info/backup/LSE/IS%20490/utile/Straub%20G%20DT.pdf

28. Tolman, W. H. (1909). *Social Engineering .* New York: New York: McGraw Publishing Company.

29. Trajtenberg, N., & Aloisio, C. (s.f.). *Sitio de la Facultad de Ciencias Sociales de la Universidad de la República Uruguay.* Obtenido de http://www.fcs.edu.uy/archivos/Nicol%C3%A1s%20Trajtenberg%20-%20Carlos%20Aloisio%20La%20racionalidad%20en%20las%20teor%C3%ADas%20criminol%C3%B3gicas%20contempor%C3%A1neas.pdf

30. University, B. Y. (2011). *IsTheory.* Recuperado en noviembre de 2013, de IsTheory: http://istheory.byu.edu/wiki/General_deterrence_theory

## ANEXOS

PRENSA LIBRE.com | Justicia

24/09/13 - 10:30 JUSTICIA

# Hackers atacan página del Ministerio Público

**El Ministerio Público informó que en la mañana de este martes, la página de internet de esa dependencia fue objeto de ataques cibernéticos.**


Página del Ministerio de Finanzas sin funcionamiento. (Foto Prensa Libre: Internet)

CIUDAD DE GUATEMALA - Por medio de un comunicado, la Fiscalía General indicó que "el Departamento de Sistema Informático Integrado se encuentra trabajando para restaurar la página", con lo cual se dará continuidad al servicio de la población, concluye el mensaje.

El boletín se identifica con el número 135-2013, difundido a las 8:32 horas. Al ingresar al portal, solo se lee el mensaje: "This page is under construction. Please come back soon!" (La página está en construcción. Por favor regrese pronto).

En el sitio web se puede encontrar información sobre los casos que investiga el ente encargado de la persecución penal, fotografías de personas con orden de captura, así como otras actividades de relaciones públicas.

Durante el 2012 se registraron ataques cibernéticos en los portales del **Arzobispado** y del **Ministerio de Finanzas**.



Fuente: imagen obtenida del sitio web de Prensa Libre
http://www.prensalibre.com/noticias/justicia/Hackers-atacan-pagina-internet-MP_0_998900223.html?print=1.

PRENSA LIBRE.com | Tecnología

14/12/13 - 18:01 TECNOLOGÍA

# Anonymous Guatemala lanza concurso para hackear páginas web del Gobierno

**La célula de piratas informáticos Anonymous que opera en el país anunció esta semana el Hacking Fest 2013, que consiste en hacer un desfase (modificación de una página web sin permiso) a cualquier sitio del Gobierno o embajadas de Guatemala en el extranjero.**

Imagen de Facebook de Anonymous Guatemala.

CIUDAD DE GUATEMALA - La convocatoria para participar en el concurso se lanzó el miércoles pasado en la **fanpage de Anonymous Guatemala**, donde indican que los participantes tendrán del 15 de diciembre al 15 de enero para realizar el ataque informático, según informó el blog tecnológico **Retico**.

La agrupación ofrece dinero en efectivo al ganador, sin embargo no indican el monto. Además, indican que el primer lugar también recibirá una máscara representativa del colectivo, fabricada con material PVC, que está valorada en US$50.

En la imagen que publicita el concurso se aclara que el participante debe vivir en Guatemala y el desfase debe ser registrado en zona –H para su validez, pueden hacer uso del XSS y deben agregar la imagen de Anonymous Guatemala.

El grupo de piratas informáticos aclaró en un comentario en Facebook que este concurso no se hizo porque ellos no puedan hackear páginas, si no porque creen que hay mucha gente que le gustaría participar.



Fuente: imagen obtenida del sitio web de Prensa Libre
http://www.prensalibre.com/tecnologia/Anonymous_Guatemala_lanza_concurso_para_hackear_sitios_web_del_Gobierno-seguridad_informatica-piratas_informaticos-hackers_0_1047495435.html#.

PRENSA LIBRE.com | Comunitario

25/09/13 - 06:30 COMUNITARIO

# Alertan sobre la exposición al cibercrimen

**Los errores usuales de ingresar a cualquier correo electrónico sin saber su procedencia o indicar en redes sociales a dónde van las personas de viaje, pueden pagarse caro, porque eso convierte a una persona en blancos de oportunidad para el cibercrimen.**

es importante no proporcionar datos personales por la web.

CIUDAD DE GUATEMALA - Durante el **Congreso Internacional de Ciencia, Tecnología e Innovación** que desde ayer se realiza en el hotel Tikal Futura, la conferencia sobre esa modalidad de violentar la ley hizo abrir los ojos a decenas de estudiantes que la presenciaron.

El coronel Ronald Morales, experto en el tema, disertó sobre los tipos de cybercrimen y delitos informáticos y sus modalidades, así como los usuarios de internet pueden evitar ser víctimas de hackers o delincuentes, y de manera simple.

Morales indicó que el 79 por ciento de víctimas de cibercrimen son blancos de oportunidad, es decir, personas que no fueron buscadas por quienes buscan aprovecharse de ellas, sino que fueron "encontradas" por descuidos propios de los usuarios. Ejemplificó que colocar en redes sociales "me fui al puerto" pude servir como alerta a que se piense que su vivienda estará sola por un día. También se cae en el error de abrir correos electrónicos de dudosa procedencia, por lo que recomienda leer mensajes sólo de gente conocida.

Fuente: imagen obtenida del sitio web de Prensa Libre
http://www.prensalibre.com/noticias/comunitario/Cibercrimen-Pirateria-Tecnologia-Robo-Identidad_0_998900364.html.

# ENCUESTA

1. ¿El conocimiento que tengo sobre el tema de seguridad de información es?


2. Existe en mi empresa u organización un documento que incluye la política de la seguridad de la información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

3. Dadas las tendencias actuales hacia el uso de redes sociales y dispositivos personales móviles en su organización o empresa, se percibe cambios en el ambiente de riesgos que enfrenta su organización.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

4. Mi empresa u organización cuenta con un programa de administración de riesgos de tecnología e información establecido, que maneja los riesgos derivados del uso de redes sociales y dispositivos personales móviles.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

5. Se hacen de conocimiento al personal de la empresa u organización las políticas de seguridad de la información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

6. La organización o empresa tiene acuerdos con el personal sobre la confidencialidad de la información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

7. Los empleados o usuarios reciben capacitación actualizada en temas de seguridad de la información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

8. En mi empresa u organización existen procedimientos de respuesta a incidentes y anomalías en materia de seguridad informática para ser aplicados por los usuarios.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

9. Mi empresa u organización cuenta con controles de ingreso del personal a las áreas físicas donde se encuentran los sistemas de información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

10. Mi empresa u organización cuenta con procedimientos y responsabilidades operativas del uso y acceso a los sistemas informáticos.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

11. Mi organización o empresa tiene procedimientos para afrontar incidentes de las comunicaciones de datos y operaciones de los sistemas informáticos.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

12. Tienen establecidos controles en la red de datos contra software malicioso (antivirus antispyware etc.).

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

13. Se tienen establecidos controles de seguridad para el sistema de correo electrónico de la empresa u organización.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

14. Mi empresa u organización cuenta con una administración de las contraseñas de usuarios para los sistemas informáticos.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

15. En mi empresa o institución se realizan auditorías a los sistemas informáticos.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

16. Conozco sobre algún caso o casos de robo de información o incidentes en la seguridad de la información dentro de mi empresa u organización.


17. Considera que si tuviera conocimiento sobre las sanciones laborales que pueda tener si llega a cometer alguna falta en la seguridad de la información (divulgación de información confidencial o robo de documentos, etc.) evitaría que usted las cometiera.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

18. En mi empresa u organización existe poco control debido a que la cantidad de empleados es muy grande.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

19. En mi empresa u organización hay cámaras de seguridad en las estaciones de trabajo y pasillos para el control de empleados y personas que ingresan al edificio.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo

20. Mi empresa u organización cuenta con un departamento dedicado a la gestión de la seguridad de la información.

- Totalmente de acuerdo
- De acuerdo
- Neutral
- En desacuerdo
- Totalmente en desacuerdo