

**UNIVERSIDAD RAFAEL LANDÍVAR**  
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES  
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"FUGA DE INFORMACIÓN MINISTERIAL; PROCEDIMIENTOS DE DETECCIÓN Y ENLACE DE  
RESPONSABLES"  
TESIS DE GRADO

**JELDERZÓN DEIRO TUJAB MORÁN**  
CARNET 22006-12

SAN JUAN CHAMELCO, ALTA VERAPAZ, SEPTIEMBRE DE 2017  
CAMPUS "SAN PEDRO CLAVER, S . J." DE LA VERAPAZ

**UNIVERSIDAD RAFAEL LANDÍVAR**  
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES  
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"FUGA DE INFORMACIÓN MINISTERIAL; PROCEDIMIENTOS DE DETECCIÓN Y ENLACE DE  
RESPONSABLES"  
TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE  
CIENCIAS JURÍDICAS Y SOCIALES

POR  
**JELDERZÓN DEIRO TUJAB MORÁN**

PREVIO A CONFERÍRSELE

EL TÍTULO Y GRADO ACADÉMICO DE LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

SAN JUAN CHAMELCO, ALTA VERAPAZ, SEPTIEMBRE DE 2017  
CAMPUS "SAN PEDRO CLAVER, S . J." DE LA VERAPAZ

## **AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR**

RECTOR: P. MARCO TULIO MARTINEZ SALAZAR, S. J.

VICERRECTORA ACADÉMICA: DRA. MARTA LUCRECIA MÉNDEZ GONZÁLEZ DE PENEDO

VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN: ING. JOSÉ JUVENTINO GÁLVEZ RUANO

VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA: P. JULIO ENRIQUE MOREIRA CHAVARRÍA, S. J.

VICERRECTOR ADMINISTRATIVO: LIC. ARIEL RIVERA IRÍAS

SECRETARIA GENERAL: LIC. FABIOLA DE LA LUZ PADILLA BELTRANENA DE LORENZANA

## **AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**

DECANO: DR. ROLANDO ESCOBAR MENALDO

VICEDECANA: MGTR. HELENA CAROLINA MACHADO CARBALLO

SECRETARIO: LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ

**NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN**  
MGTR. HECTOR OSWALDO CHOC XOL

**TERNA QUE PRACTICÓ LA EVALUACIÓN**  
LIC. JUAN RAMIRO SIERRA REQUENA

## **Agradecimientos.**

**DIOS**

Por darme la vida y la sabiduría para afrontar cada prueba en la vida.

**Mis padres**

Edwin Tujab y Amanda Morán por su amor incondicional y apoyo en todo momento.

**Mis hermanos**

Por ser una gran inspiración en mi trayecto académico y en mi vida.

**A mis asesores Lic. Héctor Choc y Lic. Edvard Cacao.**

Por el tiempo y dedicación extra en mi formación como profesional de principios y valores.

**Pastor Erick Ico y Familia**

Por sus sabios consejos, apoyo moral y espiritual en los momentos de luchas y pruebas.

**Compañero Erick Fernando Cruz S.**

Por su apoyo incondicional y palabras de aliento en los momentos más difíciles. Pero sobre todo por ser un verdadero amigo con quien compartí tantos buenos momentos en mi trayecto académico.

Los comentarios y opiniones realizados en la presente tesis son responsabilidad exclusiva del autor: Jelderzon Deiro Tujab Morán.

### **Listado de abreviaturas.**

DICRI	Dirección de Investigaciones Criminalísticas.
MP	Ministerio Público.
PNC	Policía Nacional Civil.
SI	Sistemas de Información.
TI	Tecnologías de Información.

## ÍNDICE

	Página No.
RESUMEN EJECUTIVO.....	I
INTRODUCCIÓN.....	II
CAPÍTULO I.....	1
INFORMACIÓN Y SEGURIDAD.....	1
1.1 Antecedentes históricos.....	1
1.1.1 Información.....	1
1.2 Que es la información ministerial e institucional.....	3
1.3 Sistemas de información.....	5
1.3.1 Tipos de sistemas de información.....	7
1.3.2 Procesos.....	10
1.3.3 Elementos que componen los sistemas de información.....	13
1.4 Seguridad de la información.....	14
1.5 Importancia de la seguridad.....	15
CAPÍTULO II.....	17
PLANEACIÓN DE SEGURIDAD.....	17
2.1 Tipos de seguridad.....	17
2.1.1 Seguridad Física.....	17
2.2 La ética y moral como principales medios de prevención.....	20
2.2.1 Principios.....	20
CAPÍTULO III.....	23
FUGA DE INFORMACIÓN, PROCEDIMIENTOS DE DETECCIÓN Y ENLACE DE RESPONSABLES.....	23

3.1 Fuga de información.....	23
3.2 Marco legal.....	25
3.2.1 Delitos y faltas.....	26
3.3 Procedimientos de detección.....	28
3.3.1 Identificación de riesgos.....	28
3.3.2 Educación del personal.....	29
3.3.3 Mecanismos de alerta.....	31
3.3.4 Focalización de controles.....	32
3.3.5 Monitoreo continuo y holístico.....	33
3.4 Enlace de responsables.....	34
IV CAPÍTULO.....	35
ANÁLISIS, DISCUSIÓN Y PRESENTACIÓN DE RESULTADOS.....	35
CONCLUSIONES.....	47
RECOMENDACIONES.....	49
REFERENCIAS.....	51
ANEXOS.....	54
Política preventiva para el resguardo y manejo adecuado de la información en materia de investigación criminal dentro del ministerio público.....	55



## **RESUMEN EJECUTIVO.**

El trabajo de monografía, “Fuga de información ministerial; Procedimientos de detección y enlace de responsables”, realizó un análisis sobre las debilidades técnicas e informáticas, dentro de las cuales se resalta el área de seguridad informática de la base de datos y fuente de información principal del Ministerio Público, empleadas como método de investigación dentro de un proceso penal. Para la obtención de resultados precisos sobre dichos factores, se realizaron entrevistas a Técnicos de la Dirección de Investigación Criminal y Forense del Ministerio Público y auxiliares fiscales de la Fiscalía Distrital de Baja Verapaz del Ministerio Público con lo cual fue posible analizar y estudiar los resultados obtenidos.

A través del análisis de resultados se logró determinar que, si bien es cierto, se cuenta hasta cierto punto con el equipo adecuado para proteger el acceso a la base de datos del Ministerio Público, en la actualidad no se cuenta con un respaldo o herramienta tecnológica que brinde seguridad sobre la información digital.

La investigación reveló la necesidad del análisis y monitoreo de la fuente de información y base de datos, ya que estas representan una prueba sólida debido a su alto grado de objetividad, de lo cual nace la premisa de la importancia de contar con un adecuado y eficiente sistema de seguridad de la información institucional.

El trabajo de investigación se encuentra estructurado por cuatro capítulos, siendo el último el análisis y discusión de resultados con respecto al eje central de investigación, el cual refleja los hallazgos encontrados mediante la correcta aplicación de los instrumentos.

## INTRODUCCIÓN.

El ministerio público es el ente encargado de la investigación de delitos y faltas que establece nuestro marco legal. Para llevar a cabo dichas investigaciones el Ministerio Público emplea procedimientos aplicables al procesamiento de escenas del crimen, tanto de delitos contra la vida e integridad de la persona, como de delitos que atenten contra el patrimonio, haciendo énfasis que dichos procedimientos deben regirse en las garantías procesales.

Según lo contenido en el artículo 107 del Código Procesal Penal: “El ejercicio de la acción penal corresponde al Ministerio Público como órgano auxiliar de la administración de justicia, tendrá a su cargo el procedimiento preparatorio y la dirección de la Policía Nacional Civil en su función investigativa dentro del proceso penal.”<sup>1</sup>Dentro del Ministerio Público existe la Dirección de Investigación Criminalística, la cual se encuentra estructurada de personal capacitado y preparado para poder realizar el procesamiento de escenas del crimen y poder aportar su trabajo como apoyo al sistema penal guatemalteco. El equipo de trabajo de dicha dirección se encuentra conformada por peritos y técnicos especializados en los diferentes campos de las ciencias criminalísticas y forenses.

Como parte de los procesos de investigación del Ministerio Público, se aplican diversas disciplinas para poder desarrollar técnicas que faciliten investigar las escenas del crimen, siendo estas, por ejemplo: la Criminalística, Dactiloscopia, Grafotécnica, Balística, Documentoscopia y Fotografía Forense entre otras.

Al existir esa variedad de disciplinas relacionadas con la investigación forense, fue necesario establecer un instrumento técnico que estandarizara el correcto procesamiento de escenas del crimen y por consiguiente, manuales de procedimientos que regularan cada una de dichas disciplinas empleadas durante una investigación o procesamiento de escena, al estudiar cada uno de ellos, no se puede negar que existen procedimientos precisos para obtener la información

---

<sup>1</sup> Código Procesal Penal. Decreto 51-92 y sus reformas del Congreso de la República de Guatemala.

necesaria para esclarecer un hecho, sin embargo, más allá del cómo obtenerlas, se observa descuidada la parte de la conservación y presentación de las mismas, así como la actualización profesional de los peritos.

Al hacer referencia de lo anterior, se puede señalar como ejemplo de lo expuesto, la falla existente en el control de calidad, seguridad y almacenamiento de la documentación realizada por el Ministerio Público, no es adecuado pensar que dichas fallas son consecuencia de errores de la institución, sino más bien, se puede notar que todo lo anterior es debido a ciertas debilidades institucionales, tales como la falta de capacitación constante a los peritos encargados de documentar, en aspectos técnicos, tecnológicos y científicos, y por otra parte, la falta de programas informáticos que faciliten el estricto control de la calidad y certeza de las pruebas objetivas.

Considerando cada uno de los puntos anteriores y sobre todo, en base a la realidad del sistema penal y judicial por la cual pasa Guatemala, es necesario velar por el respeto de las pruebas dentro de los procesos, esto únicamente se lograra al presentar pruebas realmente objetivas.

Se procedió a realizar la investigación teórica y doctrinaria en diversos libros sobre Sistemas de Información y Seguridad de los Sistemas de Información; se trazaron y aplicaron instrumentos mediante entrevistas y por último la información obtenida fue analizada y presentada a través de la interpretación de resultados, conclusiones y recomendaciones.

Para que fuera posible desarrollar la monografía se planteó un objetivo general: Analizar y describir la fuga de información ministerial para el establecimiento de procedimientos de detección y enlace de responsables.

Como objetivos específicos de la monografía se formularon:

1. Proponer planes de educación sobre amenazas, seguridad en el manejo de información sensible de carácter ministerial.

2. Formular procesos y políticas en materia de seguridad, orientada al elemento humano.
3. Identificar tanto amenazas internas como externas que atentan contra la privacidad y confidencialidad de los datos institucionales.

La investigación abarca las Instituciones encargadas de la persecución penal a través de la investigación de hechos criminales, tales como el Ministerio Público, dicha investigación se desarrolló en el municipio de Salamá, del departamento de Baja Verapaz.

Dentro de los límites que se encontraron a la hora de realizar la investigación, se pudo observar la escasa información bibliográfica sobre el tema y la falta de conocimientos técnicos por parte de los encargados de manipular la información de la institución, para poder brindar la información que se les solicitó como sujetos de investigación.

El aporte que se pretende brindar con la investigación es elaborar una Política preventiva para el resguardo y manejo adecuado de la información en materia de Investigación Criminal dentro del Ministerio Público.

Dentro de los sujetos de estudios que participaron durante la investigación, se encontraban: Técnicos en Escena del Crimen del Ministerio Público de las Fiscalías de Baja Verapaz y Auxiliares Fiscales del Ministerio Público, Fiscalía Distrital de Baja Verapaz.

Como fundamento legal se analizaron manuales, normas ordinarias, penales y leyes institucionales del sector justicia.

Los instrumentos empleados en el trabajo de investigación fueron cinco entrevistas a técnicos de la Dirección de Investigación Criminal y Forense del Ministerio Público y cinco entrevistas dirigidas a auxiliares fiscales de la Fiscalía Distrital de Baja Verapaz del Ministerio Público.

La estructura de la monografía presente se define por cuatro capítulos, fundamentados de la siguiente manera: el Capítulo I, aborda el tema de los conocimientos básicos sobre información y seguridad, el cual amplía los conocimientos del pilar fundamental del cual se sustenta la presente investigación.

El Capítulo II, ahonda en la planeación de seguridad, la cual va orientada desde los sistemas de seguridad, hasta los protocolos procedentes de la misma actividad preventiva de fuga de información o manipulación indebida de la misma. Al capítulo III, le corresponde el tema de fuga de información, procedimientos de detección y enlace de responsables.

El Capítulo IV, describe el análisis e interpretación de resultados centrándose en la regulación, resguardo y protección de la base de datos y fuentes de información del Ministerio Público, encontrando fortalezas y debilidades que posee la Institución, así mismo formulando propuestas de métodos de capacitación y el complemento de procedimientos al Manual ya establecido por el Ministerio Publico.

# **CAPÍTULO I**

## **INFORMACIÓN Y SEGURIDAD.**

La Seguridad de la Información no es un tema nuevo en Guatemala a nivel institucional, dicha concepción nació a partir del momento en el que cada ente responsable de los procesos estableció acciones para proteger la Información, sin embargo, es necesario implementar acciones bajo una concepción sistémica y debidamente estandarizada dentro de las instituciones, en este caso se hará referencia a la seguridad de la información del Ministerio Público de Guatemala.

Es importante que las acciones de seguridad de la Información sean adoptadas como actividades propias de los procesos de trabajo, en lugar de ser vistas como algo adicional, responsabilidad de terceros o de los mecanismos tecnológicos; ello refuerza la importancia de que la prioridad del Sistema de Seguridad de la Información sean los mismos colaboradores del Ministerio Público.

### **1.1 Antecedentes históricos.**

#### **1.1.1 Información.**

De acuerdo al desarrollo y constantes avances tecnológicos, la informática y el internet se han convertido en elementos indispensables para realizar la mayor parte de las actividades cotidianas, y por consiguiente su conocimiento resulta beneficioso, pero al mismo tiempo constituye una vía para delinquir, por parte de personas que valiéndose de ciertos conocimientos de orden técnico incurren en la comisión de los delitos informáticos. Desde la antigüedad el hombre ha tratado de encontrar medios para guardar información relevante, para poderla usar posteriormente, y por tal razón, toda organización requiere para su funcionamiento ciertas condiciones básicas que permitan facilidad para la realización de las tareas de una forma más efectiva y eficientes.

En las organizaciones se produce gran cantidad de información, que cualquier administrador que no cuente con sistemas bien diseñados de información, le fuese complicada la tomar las decisiones más adecuadas y oportunas para resolver los problemas que se puedan presentar.

Los sistemas de información constituyen una herramienta de suma importancia para realizar las funciones de cualquier organización por muy pequeña que esta sea, ya que este permite recopilar, clasificar, procesar interpretar y resumir cantidades de datos que permitirán la toma eficiente de decisiones.

Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implementación logra ventajas competitivas.

Los componentes anteriores conforman los protagonistas del desarrollo informático en una organización, tanto para su desarrollo como para su aplicación, además se reconoce que las tecnologías de la información constituyen el núcleo central de una transformación multidimensional que experimenta la economía y la sociedad; de aquí lo importante que es el estudio y dominio de las influencias que tal transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar.

La autora Johanna Media, en su obra asevera que “Dentro de las tecnologías de la información también se debe contemplar algunos conceptos y/o metodologías que merecen estar clasificadas como de alto impacto, ya sea para la organización, el individuo o la sociedad misma.”<sup>2</sup>

---

<sup>2</sup> Medina Iriarte, Johanna. “**Estándares para la seguridad de información con tecnologías de información**”. Chile. 2006. Tesis de Ingeniero de Control y de Gestión. Universidad de Chile. Chile. Pág. No. 11.

En la actualidad, conocer la tecnología y utilizarla ya no constituye ningún privilegio, por el contrario, es una necesidad. El uso de la tecnología es un factor determinante en los niveles de eficiencia y competitividad tanto a nivel empresarial, institucional, como personal. La informática es el tratamiento racional, automático y adecuado de la información, por medio del computador, para lo cual se diseña y desarrollan estructuras y aplicaciones especiales buscando seguridad e integridad. En el contexto de la informática, la información constituye un recurso de gran valor y se busca mantenerla y utilizarla de la mejor manera.

Todo lo anterior se enfoca a la finalidad de una adecuada utilización de los recursos existentes, para el desarrollo de las actividades orientadas a nivel institucional, tal y cual es el análisis en desarrollo, también es importante mencionar que se hace referencia a ese enfoque, debido a ser el punto de partida de la investigación, sin apartar de vista la importancia de los otros niveles organizacionales en el cual se puede aplicar o utilizar dichas herramientas.

## **1.2 Que es la información ministerial e institucional.**

La información y las bases de datos se han colocado en un buen lugar como uno de los principales recursos que poseen las empresas actualmente. Los entes que se encargan de las tomas de decisiones han comenzado a comprender que la información no es sólo un subproducto de la conducción empresarial, sino que a la vez alimenta a los negocios y puede ser uno de los tantos factores críticos para la determinación del éxito o fracaso de éstos.

Si deseamos maximizar la utilidad que posee nuestra información, el negocio la debe manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes. Los administradores deben comprender de manera general que hay costos asociados con la producción, distribución, seguridad, almacenamiento y recuperación de toda la información que es manejada en la organización. Aunque la información se encuentra a nuestro alrededor, debemos



saber que no se encuentra a una libre disposición, y su uso es estrictamente estratégico para posicionar de forma ventajosa la empresa dentro de un negocio.

La fácil disponibilidad que poseen las computadoras y las tecnologías de información en general, han creado una revolución informática en la sociedad y de forma particular en los negocios. El manejo de información generada por computadora difiere en forma significativa del manejo de datos producidos manualmente.

La Seguridad de la Información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la Seguridad de la Información es un aspecto sumamente importante en la relación que se establece entre el negocio, sus clientes, socios, proveedores y empleados.

La Seguridad de la Información es otro proceso estratégico del negocio ya que, al lograr el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información en línea con los objetivos de negocio, se estarán optimizando substancialmente las operaciones. La noción de Seguridad de la Información como un habilitador de negocios es hoy día un concepto esencial para las organizaciones de cualquier sector industrial.

Como un proceso estratégico, la Seguridad de la Información pudiera estar enfocada en proteger los activos de información de una organización contra pérdidas o uso indebido, o focalizada a brindar acceso a los activos de información apoyando los objetivos de negocio. Uniendo estos dos conceptos seguridad como **Protección** y seguridad como **Habilitador de Accesos** se define de manera integral un nuevo enfoque de Seguridad de la Información en las organizaciones.

La Seguridad de la Información hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. Si no se cuenta con reglas, lineamientos, responsabilidades y procedimientos predefinidos, y ante la ausencia de personal que es capacitado para la gestión del proceso, la inversión en tecnología quedara como una inversión onerosa ineficaz. Este concepto de Seguridad de la Información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para la institución.

A medida que el rol de Seguridad de la Información evoluciona, los directivos y ejecutivos de negocio reconocen que éste es sin duda el primer pasó en la relación entre la organización, sus clientes, socios de negocio, proveedores y empleados. En este sentido, la Seguridad de la Información acarrea enormes implicaciones para las organizaciones debido a que la confianza es la base para el intercambio, y su ausencia es una buena razón para hacer negocios con la competencia.

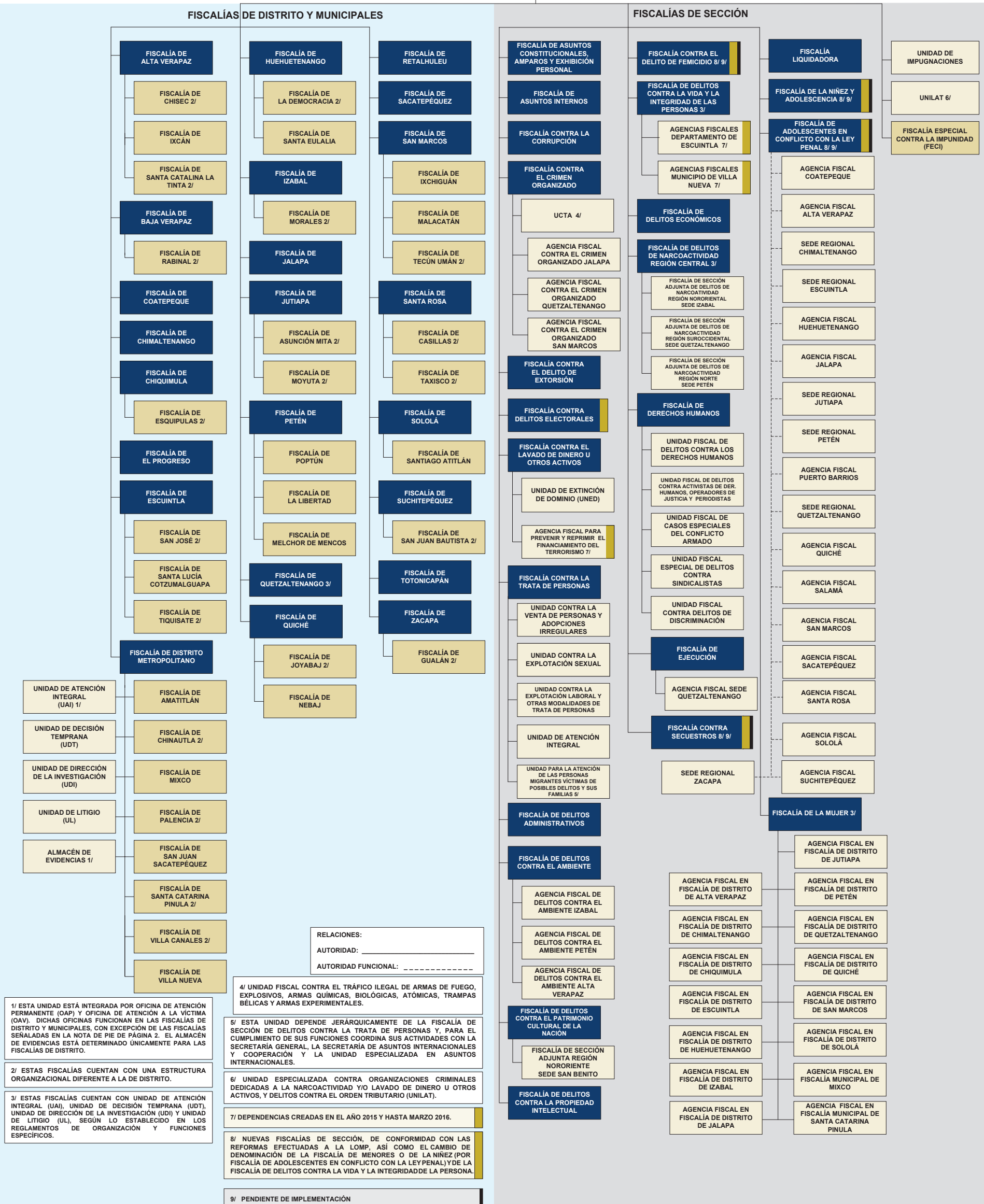
Actualmente es difícil concebir un área que no use, de alguna forma, apoyo de la informática. Una de las utilidades más importantes de la informática es facilitar información en forma oportuna y veraz, lo cual, puede facilitar entre otras cosas la toma de decisiones a nivel gerencial como permitir el control de procesos críticos.

### **1.3 Sistemas de información.**

Como lo sintetiza Medina en su estudio “Los sistemas de información son conjuntos de elementos que interactúan con el fin de dar soporte a cualquier tipo de organización o empresa. Los elementos presentes en dicho sistema corresponden al equipo computacional, el software y el hardware necesarios para apoyar el funcionamiento del sistema, y el recurso humano que interactuará con este. En un

## Estructura Funcional Área de Fiscalía

DESPACHO DEL FISCAL  
GENERAL DE LA  
REPÚBLICA



c) Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

d) Salida de información: La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo.

El almacenamiento de la información es una de las actividades o capacidades más importantes que tiene un sistema, ya que a través de esta propiedad el sistema puede acudir a la información guardada en un proceso anterior. La característica de procesar la información es la que permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que por ejemplo un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base. La información que sale del sistema sale procesada, con un valor agregado.

### **1.3.1 Tipos de sistemas de información.**

Para conocer de manera más precisa la tipología de los sistemas de información, es necesario detallar cada una de ellas, así mismo, identificar las principales características de cada una, las cuales se detallan a continuación:

a) Sistema Transaccionales <sup>4</sup>

---

<sup>4</sup> Ibíd. Pág. 15

Sus principales características son:

- a.1 A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas de la organización.
- a.2 Con frecuencia son el primer tipo de Sistemas de Información que se implanta en las organizaciones. Se empieza apoyando las tareas a nivel operativo de la organización.
- a.3 Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- a.4 Tienen la propiedad de ser recolectores de información, es decir, a través de estos sistemas se cargan las grandes bases de información para su explotación posterior.
- a.5 Son fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.

Se podría sintetizar este tipo de sistema, como el que podrá generar beneficios significativos para la empresa o institución, ya que sus resultados son objetivos y visibles, a su vez, aporta la generación de información a través de su base de datos.

#### b) Sistema de Apoyo de las Decisiones<sup>5</sup>

Las principales características de estos son:

- b.1 Suelen introducirse después de haber implantado los Sistemas Transaccionales más relevantes de la empresa, ya que estos últimos constituyen su plataforma de información.
- b.2 La información que generan sirve de apoyo a los mandos intermedios y a la alta administración en el proceso de toma de decisiones.
- b.3 Suelen ser intensivos en cálculos y escasos en entradas y salidas de información.

---

<sup>5</sup> Ibíd. Pág. 16

b.4 No suelen ahorrar mano de obra. Debido a ello, la justificación económica para el desarrollo de estos sistemas es difícil, ya que no se conocen los ingresos del proyecto de inversión.

b.5 Suelen ser Sistemas de Información interactivos y amigables, con altos estándares de diseño gráfico y visual, ya que están dirigidos al usuario final.

b.6 Apoyan la toma de decisiones que, por su misma naturaleza son repetitivos y de decisiones no estructuradas que no suelen repetirse.

b.7 Estos sistemas pueden ser desarrollados directamente por el usuario final sin la participación operativa de los analistas y programadores del área de informática.

b.8 Este tipo de sistemas puede incluir la programación de la producción, compra de materiales, flujo de fondos, proyecciones financieras, modelos de simulación de negocios, modelos de inventarios, etc.

Este tipo de sistemas, como su propio nombre lo dice, es el encargado de generar la información suficiente que servirá de apoyo en la toma de decisiones dentro de la organización o institución, ya que es capaz de generar información tanto cuantitativa como cualitativa que permitirá hacer un análisis previo sobre los métodos a utilizar en la obtención de un producto o beneficio final.

### c) Sistemas Estratégicos<sup>6</sup>

Sus principales características son:

c.1 Su función primordial no es apoyar la automatización de procesos operativos ni proporcionar información para apoyar la toma de decisiones.

c.2 Suelen desarrollarse in house, es decir, dentro de la organización, por lo tanto, no pueden adaptarse fácilmente a paquetes disponibles en el mercado.

c.3 Típicamente su forma de desarrollo es a base de incrementos y a través de su evolución dentro de la organización. Se inicia con un proceso o función en particular y a partir de ahí se van agregando nuevas funciones o procesos.

---

<sup>6</sup> Ibíd. Pág. 17

c.4 Su función es lograr ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores. En este contexto, los Sistema Estratégicos son creadores de barreras de entrada al negocio.

c.5 Apoyan el proceso de innovación de productos y proceso dentro de la empresa debido a que buscan ventajas respecto a los competidores y una forma de hacerlo en innovando o creando productos y procesos.

En síntesis el sistema estratégico es el encargado de generar ventajas sobre las demás organizaciones, lo cual permitirá tener procesos innovadores que generen de manera más práctica y oportuna los resultados deseados.

### **1.3.2 Procesos.**

Una gran parte de las ocupaciones profesionales está vinculada en la actualidad a la creación, procesamiento y distribución de información. Nos enfrentamos a un cambio social sin precedentes, provocado por un rápido aumento de la eficiencia de la microelectrónica, la reducción de costes en el tratamiento de la información y por la convergencia de áreas como las telecomunicaciones y la informática.

La metodología o procesos de seguridad de seguridad están diseñada para ayudar a los profesionales de la seguridad a desarrollar una estrategia para proteger la disponibilidad, integridad y confiabilidad de los datos de los sistemas informáticos de las organizaciones. Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, pues posee un valor especial para todos aquellos que intentan establecer directivas de seguridad.

La metodología ofrece un acercamiento sistemático a esta importante tarea, y como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre. Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados.

Cada organización debe analizar sus necesidades especificar y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos.

Sin embargo, los fundamentos de una buena seguridad siendo los mismos y este proyecto se centran en dichos procesos:<sup>7</sup>

a) Identificar métodos, herramientas y técnicas de ataques probables.

Las listas de amenazas, de las que disponen la mayor de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que pueden utilizar. Los métodos pueden abarcar desde virus y gusanos a la divinización de las contraseñas y la interpretación del correo electrónico. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan en forma continua.

b) Establecer estrategias proactivas y reactivas.

En cada método, el plan de seguridad debe incluir una estrategia proactiva y otra reactiva. La estrategia proactiva o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudara a desarrollar la estrategia proactiva.

---

<sup>7</sup> Seguridad Informática. Conceptos Básicos.  
[http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/lis/jerez\\_l\\_ca/capitulo1.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf). Fecha consultada: 30 de septiembre de 2016.



La estrategia reactiva o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir las funciones comerciales se normalicen lo antes posible.

c) Pruebas.

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permite evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia. Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados.

d) Equipo de respuestas a incidentes.

Es aconsejable formar un equipo de respuestas a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre estos se incluyen:

d.1 El desarrollo de instrucciones para controlar incidentes.

d.2 La identificación de las herramientas de software para responder a incidentes y eventos.

d.3 La investigación y desarrollo de otras herramientas de seguridad informática.

d.4 La realización de actividades formativas y de motivación.

d.5 La realización de investigaciones acerca del virus.

d.6 La ejecución de estudios relativos a ataques al sistema.

Estos procesos proporcionan los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

### **1.3.3 Elementos que componen los sistemas de información.**

Como se hizo referencia anteriormente, los sistemas de información están compuestos por conjuntos de atributos informáticos, los cuales a su vez se encuentran conformados por elementos sumamente importantes para lograr el funcionamiento necesario, los cuales son: la propia información materializada en diferentes soportes; el personal profesional y operativo que se constituye en enlace entre materiales documentales y usuario y en intérprete de sus particulares intereses; las instalaciones; los recursos financieros y el equipo que hacen posible la transferencia de la información.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y herramientas que resguardan el acceso a los datos, restringiendo el acceso únicamente a las personas autorizadas para hacerlo.

Los medios para conseguirlo son:<sup>8</sup>

- a) Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- b) Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

---

<sup>8</sup> Seguridad Computacional, <https://seguridad-computacional.wikispaces.com/elementos+de+seguridad+informatica?responseToken=028fc140342e081fcb2783524c4ecdb96>. Fecha Consultada: 10 de Octubre de 2016.

- c) Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- d) Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- e) Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- f) Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- g) Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

#### **1.4 Seguridad de la información.**

En la seguridad informática es necesario desarrollar técnicas para proteger los equipos informáticos individuales y conectados en una red, frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. La necesidad de Seguridad de la Información en una organización ha cambiado en las últimas décadas.

Con el uso de la computadora, y más aún con la llegada de Internet, es indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos. Estas herramientas no sólo permiten proteger a la información, sino también a los Sistemas Informáticos que son los encargados de administrar la información.

Se puede hablar de la Seguridad de la Información como el conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad de la misma, de la necesidad por proteger a la información y a los sistemas que la administran surge el término de Seguridad Informática.

Como lo sintetiza Granados Paredes en su estudio "...impedir los delitos informáticos exige también métodos más complejos para dar una mejor seguridad a las personas individuales, así como también a las personas jurídicas en sus diferentes clasificaciones, por lo tanto, es necesario tomar en cuenta las reglas para tener seguridad informática de calidad."<sup>9</sup>

### **1.5 Importancia de la seguridad.**

La seguridad informática tiene como premisa principal la conservación de la integridad de la información y el equipo en sí, debe de pensarse en los software maliciosos que tienen el principal objetivo de dañar de esta manera el sistema operativo y dejar el ordenador en condiciones vulnerables, otra cuestión a tener en cuenta es el valor de la información en sí, los datos importantes, como lo pueden ser las cuentas bancarias de los usuarios que debe ser protegido porque cabe la posibilidad de que alguien externo haga mal uso de ello.

Existen muchas amenazas en el sistema informático como podrían ser la mala utilización de las contraseñas, cuando se utilicen ciertas aplicaciones deberán de contar con parches de seguridad y actualizaciones necesarias, es importante también asegurar el equipo con el mejor antivirus del mercado; para evitar que ocurra lo anterior es importante es cumplir con la normativa anteriormente descrita, evitando caer víctimas de delitos informáticos.

---

<sup>9</sup> Granados Paredes, Gibrán. Introducción a la Criptografía, 2006, Pág. 3  
file:///C:/Users/TOSHIBA/Downloads/Introduccion%20a%20la%20criptografia.pdf. Fecha  
Consultada: 10 de Octubre de 2016.

En el proceso se deben implementar mejoras, acciones preventivas y correctivas comunicándolas a todos los interesados y que las mismas alcancen los objetivos planteados. Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso personal externo o que son procesados, comunicados o dirigidos por estas. Para lograr un eficiente sistema de seguridad de la información, se deben definir los accesos necesarios a la red, definir cargos con una adecuada capacitación, y controlar el almacenamiento de la información.

## **CAPÍTULO II**

### **PLANEACIÓN DE SEGURIDAD.**

El tema de seguridad como se ha venido desarrollando a lo largo del capítulo anterior, es de vital importancia dentro de cada una de las instituciones que posee base de datos, archivos digitales y/o genera información a través de plataformas virtuales, sin embargo también es preciso mencionar que los archivos físicos al igual que los digitales, pueden ser vulnerables en determinado momento por el personal si el acceso no se encuentra restringido.

Ese tipo de cuestionamientos han sido los que han alarmado de cierta medida a las personas encargadas de velar por el resguardo, veracidad y preservación de la información.

En el presente capítulo se hará referencia no solo de la importancia de la seguridad que debe existir en el manejo de información, sino también de los métodos que se pueden aplicar.

#### **2.1 Tipos de Seguridad.**

##### **2.1.1 Seguridad Física.**

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema, por eso necesario evaluar y controlar permanentemente la seguridad física del sistema ya que solo de esta forma se lograr integrar este atributo como función primordial del mismo. Para esto también se tiene dentro de la seguridad física distintos aspectos que pueden brindar protección tanto a las personas como a los equipamientos, además de la continuidad operacional.

Algunos de estos elementos se mencionan a continuación:

## a) Accesos Físicos<sup>10</sup>

a.1 Guardia o portero, que significaría la primera barrera de seguridad de la empresa.

a.2 Una segunda barrera serían tarjetas de visitas o magnéticas, en que indique a que piso se dirigen y les permita el acceso solamente al piso o sección indicada.

a.3 Determinar zonas con accesos restringidos.

a.4 Contar con circuitos cerrados de televisión (es necesario analizar dónde y cuántas cámaras de televisión instalar y qué y cuánto se grabará de lo que las cámaras filmen).

Las medidas de seguridad señaladas, siempre están restringidas por la cantidad de recursos monetarios que se dispongan, debiéndose realizar un análisis inversión v/s protección. Mientras la seguridad sea rentable, se invierte.

Por lo anterior es necesario establecer la seguridad física a través de un sistema informático que sea consistente en donde la aplicación enfrente amenazas físicas al hardware y software del equipo.

## b) Equipos de prevención.

Los mecanismos preventivos pueden evitar muchos problemas y ataques, pero no garantizan estar exentos de todo riesgo o daño. La seguridad tiene que comprometerse con el administrador y así evitar que ocurran incidentes o daños en el equipo. Granados Paredes argumenta en su estudio que “Los mecanismos de seguridad preventivos son todas aquellas acciones que van encaminadas a prevenir cualquier amenaza de confiabilidad, integridad, no repudio y disponibilidad de los elementos críticos del sistema. Por la propia definición de estas características, también se debe proporcionar mecanismos de autenticación y de control de acceso que garanticen la identificación, autenticación y gestión de perfiles aplicables a los

---

<sup>10</sup> Ibid. Pág. 22

recursos para determinar que usuario y bajo qué condiciones pueden o no acceder al recurso solicitado para la acción indicada.”<sup>11</sup>

Lo primero que se debe tener en cuenta es la protección física de los diferentes equipos del sistema informático. Cualquier equipo en general, y con especial atención, los servidores y hardware de red, deben situarse en recintos protegidos para que solo el personal autorizado tenga acceso a ellos.

Los mecanismos aplicables varían desde una habitación con una cerradura y llave, a los más sofisticados mecanismos de acceso por huella digital, cámaras de seguridad y guardias que reaccionen ante violaciones de la política de acceso estos dos últimos más bien se deben englobar como sistemas de detección.

Desde el punto de vista lógico, la seguridad está basada, principalmente en aplicar por un lado configuraciones, técnicas de identidad y listas de control de acceso a la información en los sistemas y las comunicaciones y por otro lado el empleo criptográfico.

Lo primero que un administrador debe de realizar a la hora de diseñar mecánicas preventivos es planificar la estrategia a seguir para cumplir la política de seguridad de la organización. Debido a la creciente importancia de los sistemas de información, no solo por la repercusión social sino también por la importancia de los datos y operaciones que se realicen con sistemas informáticos. Si se toman los procedimientos adecuados, no será necesario utilizar estas medidas, pero más de alguna falla existirá siempre, por lo cual la persona que lleva a cabo este trabajo deberá de tomarlas en cuenta.

---

<sup>11</sup> Ibid. Pág. 23



## **2.2 La ética y moral como principales medios de prevención.**

El surgimiento de la computación y de los sistemas de información aunado al desarrollo tecnológico, ha provocado un cambio radical en la sociedad en las últimas décadas. En la actualidad se puede comprobar que las computadoras se han convertido en una herramienta muy importante cuya expansión es tal que se pueden encontrar en muy diversos lugares, y es por la misma razón que es necesario que la informática haga conciencia de la importancia de velar para que se cumplan los genuinos objetivos de automatizar el procesamiento de los datos, que el desarrollo y uso de los sistemas de información respondan a principios éticos, puesto que, como lo sintetiza Isabel Benítez “El Código de Ética para todos los usuarios de la Informática se basa en principios éticos fundamentales y es aplicable a situaciones que caracterizan las actividades de esta tecnología. El código se centra en la esencia misma de lo que es ser un usuario de Informática.”<sup>12</sup>

Dicho código en la rama de la salud tiene dos componentes esenciales: uno, los principios que son relevantes para todo el personal que de una forma u otra tenga acceso a la información electrónica vinculada con la salud y el otro, reglas de conducta que describen las normas de comportamiento que se espera sean asumidas por todo el personal que se relaciona con la informática de la salud. Estas reglas son una ayuda para interpretar los principios en aplicaciones prácticas. Su propósito es guiar la conducta ética de todos los que de una forma u otra se involucre con la utilización de la tecnología informática.

### **2.2.1 Principios.**

Son muchos los principios que se vinculan con la ética informática dentro de los cuales, como pilar fundamental están los principios.

---

<sup>12</sup> Benítez Hernández, Isabel. Problemas éticos y de la seguridad informática asociados al uso de la tecnología. <http://bvs.sld.cu/revistas/inf/n809/inf1909.htm>. Fecha Consultada: 15 de Octubre de 2017.

Los principios en que se basa el código de ética para la informática son los siguientes:<sup>13</sup>

a) Principio de Accesibilidad: El sujeto de un registro electrónico tiene el derecho de acceder al registro y a exigir la exactitud del mismo con relación a su precisión, integridad y relevancia.

b) Principio de Privacidad y Disposición de la Información: Todas las personas poseen el derecho fundamental a la privacidad y, en consecuencia, a ser informadas y ejercer el derecho de autorizar la recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de la información sobre sí mismas.

c) Principio de Transparencia: La recolección, almacenamiento, acceso, uso, comunicación, manipulación y disposición de información personal debe ser revelado en tiempo y forma apropiados al sujeto de esos datos.

d) Principio de Seguridad: Todas las personas tienen el derecho a que la información que ha sido legítimamente recolectada sobre sí, sea debidamente protegida, mediante todas las medidas disponibles, razonables y apropiadas tendientes a evitar pérdidas, degradación, así como la destrucción, el acceso, uso, manipulación, modificación o difusión no autorizada.

e) Principio de Garantía: El derecho fundamental sobre el control de la recolección, el almacenamiento, acceso, uso, manipulación, comunicación y disposición de la información personal, está condicionado sólo por las necesidades legítimas, apropiadas y relevantes de información en una sociedad libre, responsable y democrática, así como por los correspondientes derechos iguales y competentes de otras personas.

---

<sup>13</sup> Loc. Cit.

f) Principio de la alternativa menos invasora: Cualquier acción legítima que deba interferir con los derechos del individuo a su privacidad o al control sobre la información relativa a ésta, deberá sólo ser efectuada de la forma menos invasora posible, tal que garantice el mínimo de interferencia a los derechos de las personas afectadas.

g) Principio de Responsabilidad: Cualquier interferencia con los derechos de privacidad de un individuo o del derecho de tener control sobre la información relativa a su persona, debe ser justificada a tiempo y de manera apropiada ante la persona afectada.

Existen muchos casos en los que se observa una conducta irresponsable y criticable moralmente por descuidos y omisiones en el desarrollo de sistemas de información, por la poca atención a la seguridad informática, errores en el código de los programas, pruebas incompletas, análisis insuficientes y a la vulnerable privacidad de la información. Para que esto no suceda las empresas al momento de contratar su personal y máximo para estos puestos deberá de tomar en cuenta que el futuro profesional informático, deberá de tener excelencia técnica y ética. Es por tal razón que se vuelve indispensable que todos los profesionales en esta área se adhieran a los principios ya expresados en este código, así como promover su difusión y práctica.

## **CAPÍTULO III**

### **FUGA DE INFORMACIÓN, PROCEDIMIENTOS DE DETECCIÓN Y ENLACE DE RESPONSABLES.**

Dentro de los riesgos a los que se encuentra expuesta la información, se puede destacar uno: la fuga de información, la cual es una amenaza silenciosa, ya que el personal de la institución puede filtrar información sensible de forma intencional o accidental, así mismo, la fuga de información puede tener serias consecuencias tanto a la institución como a las personas involucradas dentro de los casos de investigación penal.

Es muy importante que a nivel institucional, máxime dentro del Ministerio Público, se dé énfasis en la protección de la información a través de la prevención de la problemática en cuestión, por lo cual este capítulo de la investigación dará a conocer ciertos mecanismos y/o herramientas que pueden ser aplicables dentro del contexto institucional de Ministerio Público en Guatemala.

#### **3.1 Fuga de Información.**

La masificación del uso de las tecnologías y su integración en todos los ámbitos y categorías de la sociedad han creado un escenario en el que por un lado, cada vez se gestiona mayor cantidad de información y por otro, se ha convertido en un activo crítico de las organizaciones y los usuarios, además las tecnologías posibilitan un tratamiento de la información sin precedentes y a nivel global, de manera que es transmitida, procesada, copiada o almacenada con bastante rapidez y eficacia, sumado al hecho de que es posible llevar a cabo dichas acciones, desde múltiples tipos de dispositivos, no importando lo remoto del lugar. Desde el punto de vista técnico el problema radica en la dificultad de administrar y gestionar la enorme cantidad de datos que procesan las organizaciones. En este sentido, teniendo en cuenta que cada nivel de usuarios deberá acceder a distintos archivos y datos, y que estos además viajarán por las redes y se almacenarán en distintas ubicaciones

dentro y fuera del centro de cómputos; la complejidad de la situación aumenta exponencialmente. Esta diversidad de posibles ubicaciones de los datos hace que lo que se deba proteger no esté centralizado y se requieran medidas y tratamientos diferentes para cada caso. Por supuesto que todos los componentes tecnológicos forman parte de este aspecto, desde el hardware hasta el software y las redes.

El impacto y las consecuencias posteriores a un incidente de fuga de información, es uno de los aspectos que mayor preocupación despierta en las organizaciones, puesto que la filtración de información puede dañar su imagen pública y en el caso de las empresas, puede suponer un impacto negativo para el negocio, además de generar desconfianza e inseguridad en el público y generar otras consecuencias a terceros, como en el caso de que la información filtrada haga referencia a usuarios o clientes.

Por otro lado, la fuga de información es un tipo de incidente difícil de ocultar, puesto que su propia naturaleza y las motivaciones que se sitúan detrás de estos incidentes suelen terminar en muchas ocasiones con la difusión del suceso en Internet.

Abordando la relación de la fuga de información con el Ministerio Público, dicha referencia lleva consigo serias implicaciones tanto al nivel administrativo como en lo penal y jurídico, debido a la complejidad de la información que en dicha institución se maneja, los cuales van desde casos menores, hasta casos de alto impacto, sin embargo, en la actualidad, no se ha estandarizado alguna metodología o herramienta que permita el adecuado resguardo de las bases de datos del Ministerio Público, lo cual significativamente es alarmante puesto que cualquier empleado con usuario, podría acceder a las bases de datos y sustraer información.

### **3.2 Marco Legal.**

La evolución de las denominadas tecnologías de la información y comunicaciones, T.I.C, ha llevado a la humanidad a un desarrollo acelerado en cuanto a las comunicaciones, los sistemas de información, la forma en que la información se transmite; y debido a que la información se ha convertido en un bien jurídico de gran valor, se ha hecho necesario protegerlo legalmente puesto que la informática, es una de las ciencias más jóvenes en el contexto de las ramas del conocimiento humano; pero constituye una materia, cuyos avances y desarrollo constantes parecen no tener límites.

La informática tiene singular importancia en la época actual, marcada por los adelantos en materia tecnológica y sobre todo en la expansión de las economías a nivel mundial, que poco a poco han ido convirtiendo al mundo en una aldea global, con el presente proceso globalizador que permite la eliminación de las fronteras de tipo social, cultural, arancelarias, económicas y en algunos países, especialmente en los europeos, política; para la plena integración de las culturas de las naciones de los países parte.

Elmer López en su ensayo afirma que, “es tal la relevancia de la informática en la actualidad y su conexión con los diferentes ámbitos del saber y de su inserción en múltiples actividades que realiza el ser humano, que se considera necesario la realización del presente análisis, vinculado al tema del derecho informático como una de las ciencias jurídicas constituida por un conjunto de principios, doctrinas y normas jurídicas que pretendan regular el conocimiento científico y técnico que posibilita el tratamiento automático de la información por medio de las computadoras, la regulación, administración y protección de los sistemas operativo-informáticos y de los ordenadores, y de los derechos y obligaciones que los usuarios de la red deben observar en la realización de sus actos informáticos y de las

correspondientes sanciones que conlleva el incumplimiento de dichas normas obteniendo el lineamiento de la conducta humana dentro de la sociedad.”<sup>14</sup>

En Guatemala, el movimiento de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importancia mayor, no porque no se hayan cometido estos delitos, sino porque no se posee mayor conocimiento en el entorno mucho sobre esta clase de delitos a pesar del efecto de globalización que se está viviendo, y la razón de que esta nueva forma de lesión a los bienes jurídicos tutelados no sea tomada en cuenta, se debe a que se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual.

### **3.2.1 Delitos y faltas.**

Las dificultades que surgen al tratar de enfrentar este tipo de delincuencia a todo nivel es la tarea del Ministerio Público por mandato constitucional y por disposición legal. Ahora bien, el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados delitos informáticos.

El derecho informático, es una materia de actual concepción, cuyas normas se caracterizan por la innovación y adaptación de los cambios tecnológicos que se van suscitando en los sistemas operativos, las reglas y los sistemas de contratación informática; ya que en un país como el nuestro que no raras veces se ve rebasado por los cambios que imponen las sociedades desarrolladas; se considera de gran importancia el tratamiento, no sólo a la sustantividad de las normas penales, sino que también a las adjetivas, y en particular en lo que respecta el problema de una incipiente regulación en nuestro Código Penal, de las conductas antijurídicas que conforman los delitos informáticos.

---

<sup>14</sup> López García, Elmer Yovani. Inclusión de los Delitos Informáticos, que se comenten en Internet, dentro del código penal Guatemalteco, Guatemala, 2011, Facultad Ciencias Jurídicas y Sociales. Pág. 75

Dentro de la gran variedad de delitos informáticos que existen, se pueden mencionar entre los más frecuentes los siguientes:<sup>15</sup>

- Manipulación de los datos de entrada.
- Manipulación de los programas.
- Manipulación de los datos de salida.
- Fraude efectuado por manipulación informática.
- Sabotaje informático.
- Virus.
- Gusanos.
- Bomba cronológica.
- Acceso no autorizado a servicios y sistemas informáticos.
- Piratas informáticos.
- Reproducción no autorizada de programas informáticos.
- Infracciones al copyright.
- Intercepción de correo electrónico.
- Pesca de claves secretas.
- Estafas electrónicas.
- Estratagemas.
- Pornografía infantil.

Estos son algunos de los delitos informáticos más frecuentes que se cometen, pero en la legislación de Guatemala ninguno se encuentra regulado bajo un régimen de carácter especial, por consiguiente no constituyen delitos, lo cual deja en completa libertad a quienes realizan éste tipo de actividades.

Dentro del contexto de nuestra regulación jurado penal, se produce un gran vacío legal toda vez que en lo concerniente al Código Penal, no se da en ninguno de sus títulos la regulación de los delitos informáticos, lo cual es perjudicial, al no se

---

<sup>15</sup> Ibid. Pág. 76



protegerse de manera efectiva a las personas tanto individuales, como a nivel de la industria, de las entidades estatales, y en general a todos aquellos que manipulen de alguna forma datos a nivel informático.

La criminalidad o delincuencia informática es un problema global y necesita con urgencia la armonización legislativa y la cooperación internacional. El crimen organizado recurre a una vulnerabilidad de control de acceso a sistemas de cómputo y a una tecnología moderna de comunicación en el internet para cometer fraudes y extorsiones. Pero se debe iniciar a darle énfasis a este problema de forma interna, entender que este tipo de criminalidad ya es una realidad en Guatemala, pues existen grupos organizados que se dedican a utilizar a las computadoras, el internet, las redes sociales y en general todo la tecnología moderna para cometer delitos o bien a causar daño al software y al hardware de los equipos de cómputo de las personas o instituciones; siendo la realidad una legislación y normatividad nacional inadecuada para combatir a estos criminales.

### **3.3 Procedimientos de detección.**

#### **3.3.1 Identificación de Riesgos.**

Es importante en todas las organizaciones contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

En la Guía de gestión de fuga de información, señalan que, con el tiempo, las amenazas evolucionaron y también cambiaron algunos paradigmas de la seguridad.<sup>16</sup> La frase «el enemigo está dentro» se popularizó hace ya unos años cuando los incidentes de seguridad cuyo origen estaba en el interior de las propias organizaciones comenzaron a aumentar. Dicho aumento cambió la percepción y el

---

<sup>16</sup> Guía de Gestión de Fuga de Información, España. 2012. Instituto Nacional de Tecnologías de la Comunicación. Pág. 7

concepto de protección, puesto que hasta entonces las medidas de seguridad se centraban en crear barreras para proteger a las organizaciones de las amenazas externas.

Desde el punto de vista externo del origen de la fuga de información, la guía de gestión de fuga de información hace énfasis en que “el mapa de las amenazas externas ha cambiado enormemente en la última década, con la aparición de nuevos jugadores en el escenario de la seguridad: organizaciones criminales, activistas o terroristas, han tomado Internet y la han convertido en un verdadero campo de batalla, en el que se desarrollan todo tipo de estrategias con diversos objetivos, como conseguir beneficio económico, llevar a cabo acciones de protesta y daño de imagen, o sabotajes a instalaciones industriales”.<sup>17</sup>

Los riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Por lo tanto es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

### **3.3.2 Educación del Personal.**

Es importante que el personal que se encuentre a cargo de la información de una empresa deberá ser capacitada consecutivamente para tener la información lo más segura posible, deberá de aplicar las herramientas, técnicas y métodos de lo más actual para no vulnerar la seguridad y confiabilidad de la información institucional. Una gestión deficiente, la falta de formación y buenas prácticas, la ausencia de políticas y procedimientos o la no aplicación de mecanismos de disuasión, son causas habituales y suficientes para facilitar o desencadenar un incidente de fuga de información.

---

<sup>17</sup> Loc. Cit.

Uno de los primeros errores que se comete en relación con la protección de la información es la falta de una clasificación de la información en base a su nivel de confidencialidad, en función de diversos parámetros, como son el valor que tiene para la organización, el impacto público que puede generar su difusión, su nivel de sensibilidad o si se trata de información personal o no.

Si se desconoce el valor de la información que trata la organización, no será posible diseñar y seleccionar las medidas de protección adecuadas. En otro aspecto, el ámbito de difusión, permite establecer el perímetro dentro del cual podrá ser divulgada la información y junto con el nivel de confidencialidad, hará posible determinar quién debe de conocer la información y qué tipo de acciones puede realizar sobre esta. Los errores o la falta de conocimiento y formación son otra de las causas más comunes de la fuga de información.

En cierto sentido, el empleado debe utilizar los recursos que la organización pone a su disposición de forma responsable, como en el caso del uso del correo electrónico, la navegación Web u otros servicios y otro aspecto es que, debe disponer de ciertos conocimientos y formación en relación con su actividad diaria, siendo responsabilidad de la organización proporcionar la información y la formación necesaria de manera que el empleado pueda desempeñar su función adecuadamente.

Dentro del contenido de la guía de gestión de fuga de información, se hace referencia que “La disuasión es una herramienta muy potente si se utiliza adecuadamente y en el contexto correcto, informando a los trabajadores, pero sobre todo, dejando claro que la organización ha establecido medidas para prevenir, y en caso de que suceda un incidente, tomar la iniciativa poniendo en marcha las acciones correspondientes.”<sup>18</sup>

---

<sup>18</sup> Ibid. Pág. 8

La aseveración anterior es ampliamente confiable en algunos países, donde se considera que la preparación y enseñanza al personal de las instituciones es realmente importante, para que conozcan tanto las funciones, responsabilidades, así como implicaciones legales de no cumplir adecuadamente con sus deberes y obligaciones, lo cual puede repercutir de manera administrativa o penal sobre el empleado que incurriera en alguna actividad negativa o contraria a lo establecido dentro de la institución.

### **3.3.3 Mecanismos de alerta.**

En relación con las principales acciones (entre otras) que será necesario llevar a cabo, se indican las siguientes:<sup>19</sup>

- Determinación de las acciones destinadas a cerrar la filtración y evitar nuevas fugas de información.
- Determinación del nivel de difusión de la información y de las acciones destinadas a minimizar su difusión, en especial si esta contiene datos de carácter personal o se trata de información sensible.
- Determinación de los afectados por la fuga de información, ya sean internos o externos.
- Determinación de las consecuencias legales, posibles incumplimientos de normativa en materia de protección de datos de carácter personal, o de otra normativa, así como posibles denuncias por los afectados, otras organizaciones, etc.
- Determinación de las consecuencias económicas, que puedan afectar a la organización.
- Determinación de los activos de la organización afectados, y alcance, en relación con los activos de información, infraestructuras, personas, etc. Planificación

---

<sup>19</sup> Ibid. Pág. 18

del contacto y coordinación con fuerzas y cuerpos de seguridad, denuncia y otras actuaciones, en caso de ser necesario.

- Planificación de comunicación e información del incidente, tanto a nivel interno como externo, a medios de comunicación, y afectados, en caso de ser necesario.

Estas acciones y otras que puedan considerarse necesarias, en función del escenario, compondrán el plan de emergencia diseñado para el incidente en cuestión.

Las acciones indicadas anteriormente, podrán realizarse de forma simultánea o secuencialmente, todo dependerá del escenario, los recursos con que cuente la organización y de otras consideraciones.

#### **3.3.4 Focalización de controles.**

Las medidas adecuadas para la información deberán de aplicarse constantemente puesto los actos delictivos se encuentran latentes, pues como era descrito anteriormente, los delitos informáticos en Guatemala aun no son reconocidos por la ley, pero si se comenten en el mismo, por lo cual la persona encargada del equipo computo de la empresa u organización deberá estar en constante monitoreo que le permita detectar fisuras en los esquemas de seguridad. Dentro del plan de la guía de gestión de fuga de información, hace referencia que "...el primer paso es terminar con la brecha de seguridad y evitar que se produzcan nuevas fugas de información. Es posible que sea necesario cerrar la brecha de seguridad a costa por ejemplo, de desconectar un determinado servicio o sistema de Internet, pero cerrar la fuga es el objetivo número uno. Más adelante, se llevará a cabo la aplicación de medidas más adecuadas o menos drásticas, pero siempre garantizando la seguridad."<sup>20</sup>

---

<sup>20</sup> Ibid. Pág. 20

Al existir problemas informáticos, la persona encargada deberá dar a conocer de a los superiores y demás encargados de la seguridad de lo que acontece puesto que al no realizarse esto, la información o podría ser dañada o robada.

### **3.3.5 Monitoreo continuo y holístico.**

Deberá de existir un control exhaustivo de la herramienta que se utilice para inspeccionar la información ya que sin un monitoreo pueda que exista fuga de información por lo cual es necesario monitorearla cada determinado tiempo.

En relación con lo anterior es importante indicar que los sistemas y aplicaciones precisan de actualizaciones y revisiones constantes. Hace años, muy pocas aplicaciones eran actualizadas regularmente, incluidos los sistemas operativos. Hoy día, cualquier aplicación, dispone de actualizaciones regulares y contar con un servicio de actualizaciones se considera parte fundamental de una buena aplicación, puesto que aporta mayor seguridad y denota un trabajo de mejora continua, que redundan en beneficio para la aplicación y por extensión, para el usuario.

En la guía de gestión de fuga de información, se sintetiza que “...en la práctica es difícil separar las causas organizativas y técnicas, puesto que cada vez están más relacionadas, debido al uso intensivo de las tecnologías de la información dentro de las organizaciones para cualquier actividad, incluida la gestión de la seguridad, pero, aun así, es importante diferenciarlas, de cara a diseñar medias y detectar vulnerabilidades y mejoras.”<sup>21</sup>

Dentro del enunciado anterior se hace referencia sobre la importancia de detectar vulnerabilidades y mejorarlas, en ese aspecto importante es donde encaja significativamente el monitoreo y evaluación de las herramientas de seguridad que resguardan las bases de datos y fuentes de información de la institución.

---

<sup>21</sup> Ibid. Pág. 8

### **3.4 Enlace de Responsables.**

Los resultados que al final se persiguen luego de una serie de procedimientos rigurosos que permitirán llegar a establecer y definir la manera en que la fuga de información se llevaba a cabo.

Para ello se debe comenzar por la evaluar la conducta de los empleados, así como los riesgos asociados. Luego de acuerdo con dicha evaluación pueden diseñarse planes de educación sobre amenazas, capacitación en seguridad y procedimientos de seguridad que permita la detección y enlace de responsables para la toma de decisiones y medidas pertinentes, considerándose el momento de realizar inversiones eficientes y eficaces en tecnología de seguridad y demás medias de contingencia.

Las labores de seguridad realizadas actualmente por el área de seguridad informática son las siguientes:<sup>22</sup>

- a) Creación y eliminación de usuarios
- b) Verificación y asignación de perfiles en las aplicaciones

Las labores de seguridad realizadas por el área de sistemas son las siguientes:<sup>23</sup>

- a) Control de red
- b) Administración de firewall
- c) Administración de accesos a bases de datos.

---

<sup>22</sup> Córdova Rodríguez, Norma Edith. Plan de Seguridad Informática para una Entidad Financiera. [http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova\\_RN/Cap4.pdf](http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap4.pdf) Pág. 1

<sup>23</sup> Loc. Cit.

## **IV CAPÍTULO**

### **ANÁLISIS, DISCUSIÓN Y PRESENTACIÓN DE RESULTADOS**

En los capítulos anteriores se ha abordado la problemática derivada en la seguridad de la información y se ha hecho énfasis especialmente en la fuga de información. Cuando se habla de fuga de información, la solución más natural para contrarrestarla es empleando el concepto de cultura o educación de seguridad. No obstante, se hace muy poco dentro del país para lograrla o más bien, no se tiene conocimiento sobre la misma y en muchas ocasiones se ha dicho que la utilización de las herramientas para su detección y programas de prevención, es nula.

Para la realización de la investigación, se consultaron las diversas fuentes de estudio, necesarias para presentar en este último capítulo, los resultados obtenidos durante la investigación, mediante la utilización de entrevistas a diferentes sujetos de estudio.

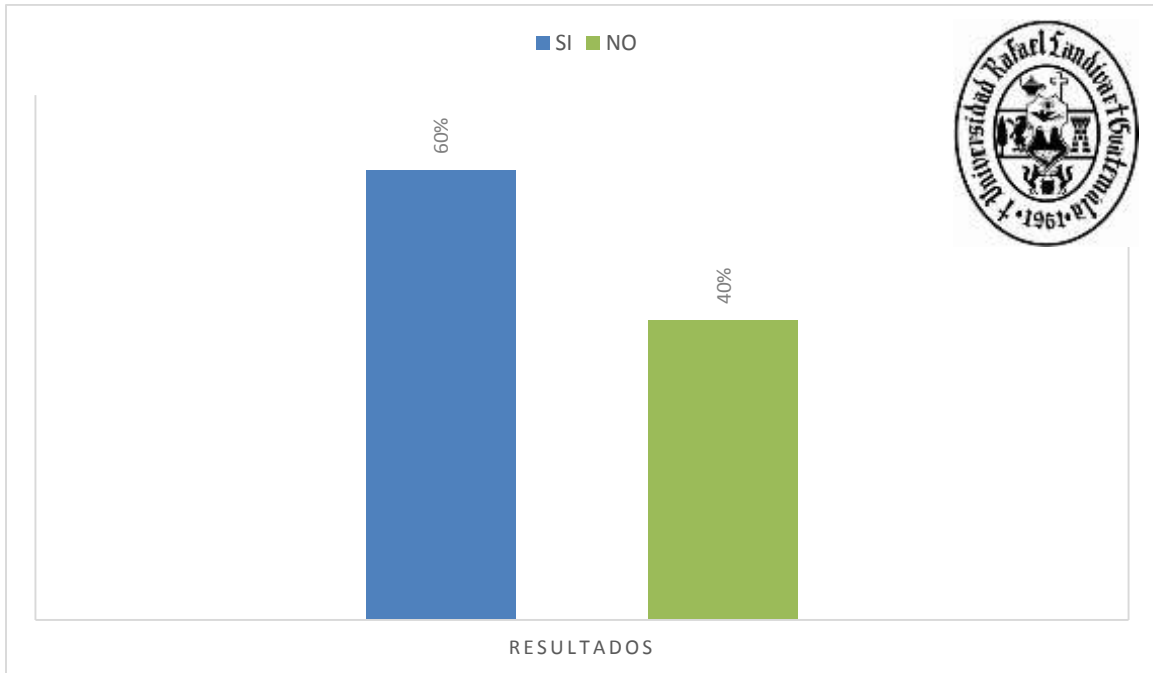
La discusión y análisis del tema de investigación, se basó en los resultados obtenidos, los cuales tenían como finalidad primordial determinar si se responde la pregunta principal de la presente tesis ¿Qué es la fuga de información ministerial y como se pueden plantear procedimientos de detección para el enlace de responsables? La presente investigación permitió responder la pregunta que la motivó; se lograron cumplir los objetivos propuestos.

Durante el desarrollo del trabajo de investigación se realizaron entrevistas dirigidas a distintos sujetos de estudio para recabar la información relacionada al tema de tesis, entre ellos: 5 técnicos en investigaciones criminalísticas de la Dirección de Investigaciones Criminalísticas del Ministerio Público y 5 auxiliares fiscales del Ministerio Público, todos ellos del Municipio de Salamá, Baja Verapaz.



### Gráfica No. 1

**¿Considera que existe la fuga de información en las instituciones encargadas de la persecución penal?**



Fuente de elaboración propia.

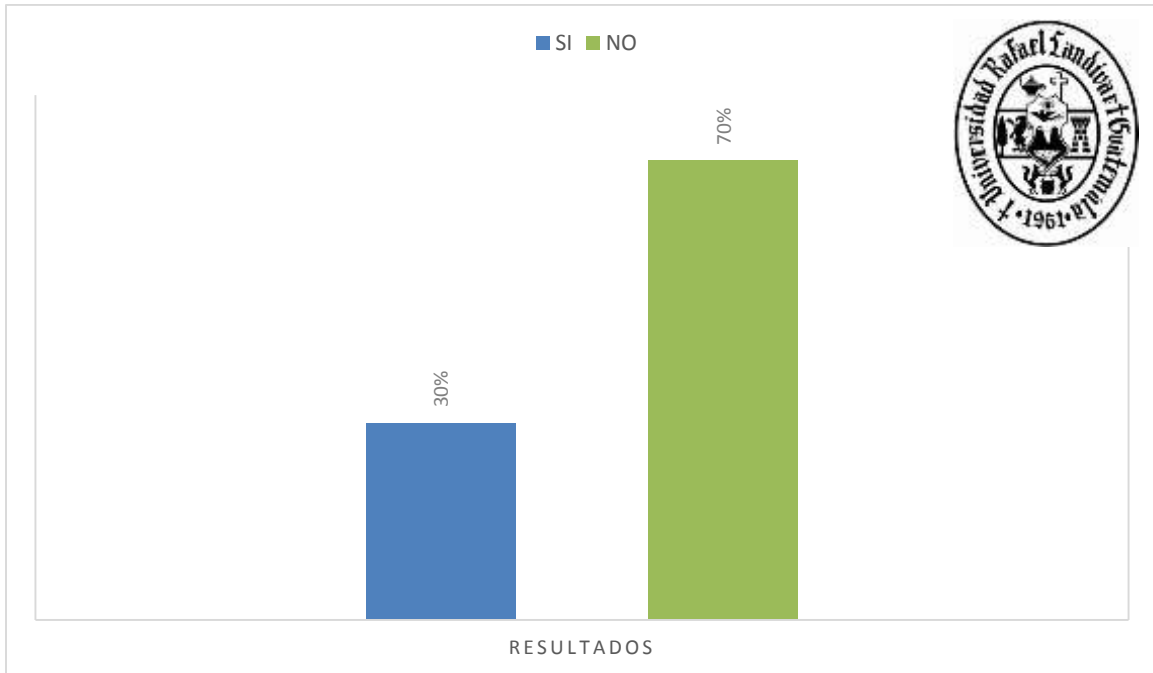
Interpretación:

De los encuestados, el 60% indicó que si considera que existe fuga de información dentro de las instituciones encargadas de realizar la persecución penal, mientras que por otro lado, el 40% de sujetos de estudio hizo referencia a la negativa sobre la existencia de la fuga de información dentro de las instituciones.

Resultados que indican que es necesario establecer métodos específicos para la prevención y detección oportuna de fuga de información ministerial.

## Gráfica No. 2

¿Conoce casos que evidencien la fuga de información en dichas instituciones?



Fuente de elaboración propia.

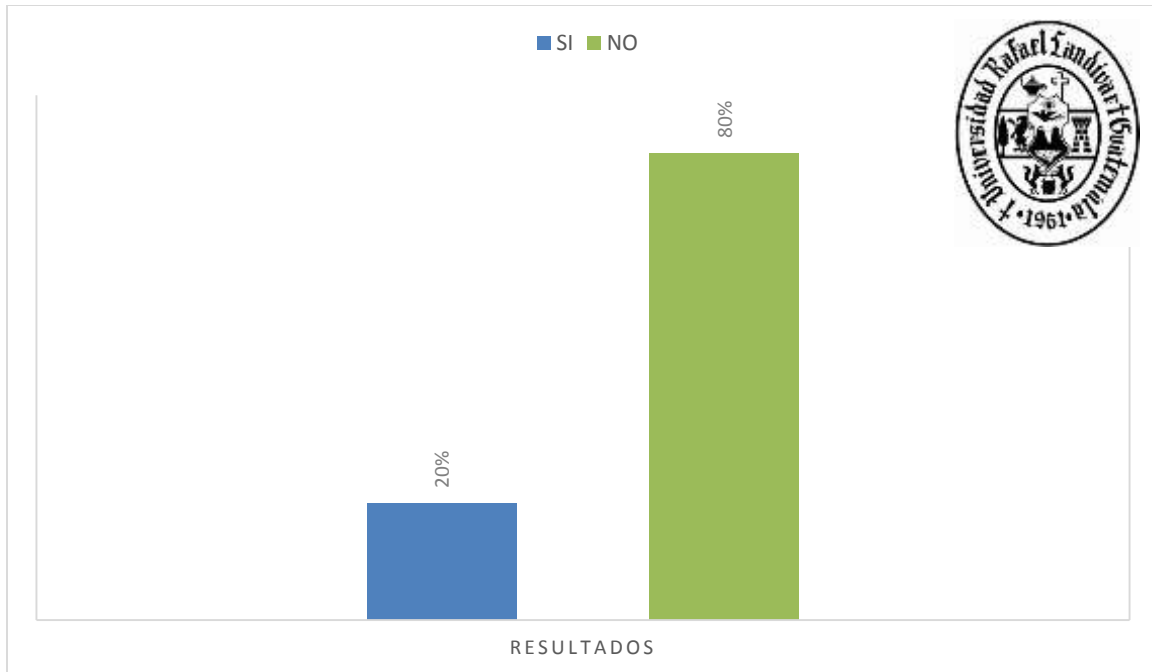
Interpretación:

De los encuestados, el 30% indicó que sí conoce casos que evidencien la fuga de información dentro de la institución, mientras que por otro lado, el 70% de sujetos de estudio hizo referencia a la negativa sobre el conocimiento de casos de ese tipo que se estuvieran dando dentro de la Institución.

Resultados que indican que es necesario fortalecer o implementar los mecanismos de prevención de fugas de información.

### Gráfica No. 3

¿Poseen las instituciones, medidas que aseguren la confidencialidad y certeza de la información?



Fuente de elaboración propia.

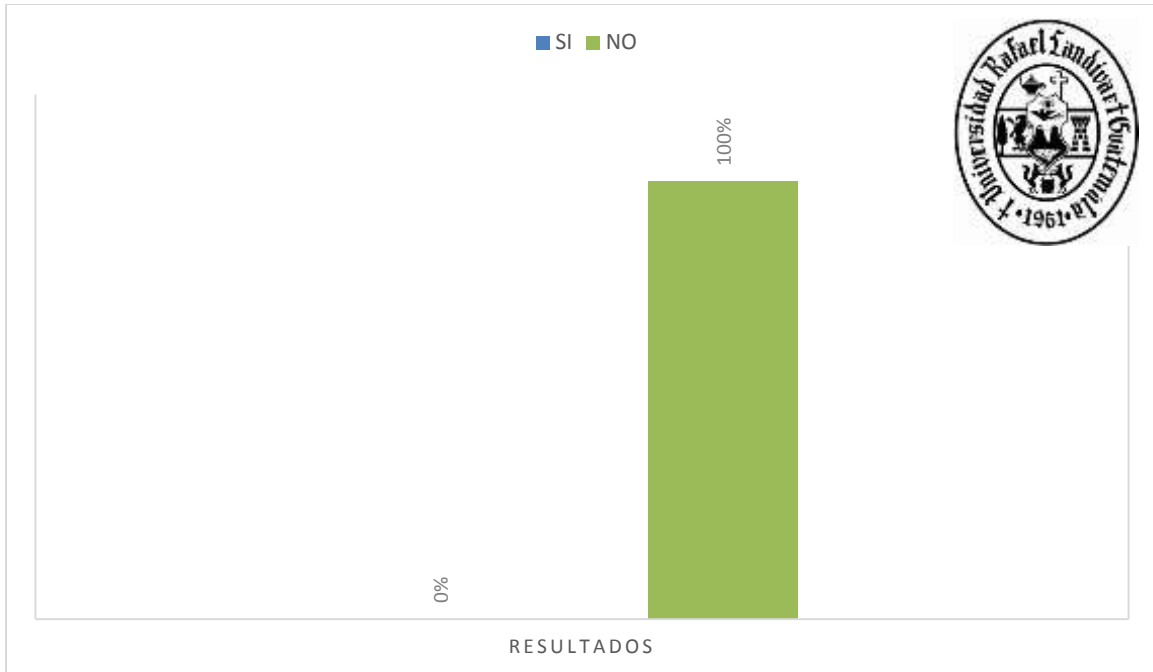
Interpretación:

De los encuestados, el 20% indicó que sí considera adecuados los procedimientos establecidos dentro de la institución para resguardar la certeza y confiabilidad de la información, mientras que por otro lado, el 80% de sujetos de estudio hizo referencia a la negativa sobre los métodos de resguardo de la seguridad de la información dentro de la Institución.

Resultados que indican que es necesario establecer métodos específicos para el resguardo de la seguridad y certeza de la información que existe dentro del Ministerio Público, tanto información digital como archivo físico.

#### Gráfica No. 4

¿Realiza el Ministerio Público test de confiabilidad a sus empleados?



Fuente de elaboración propia.

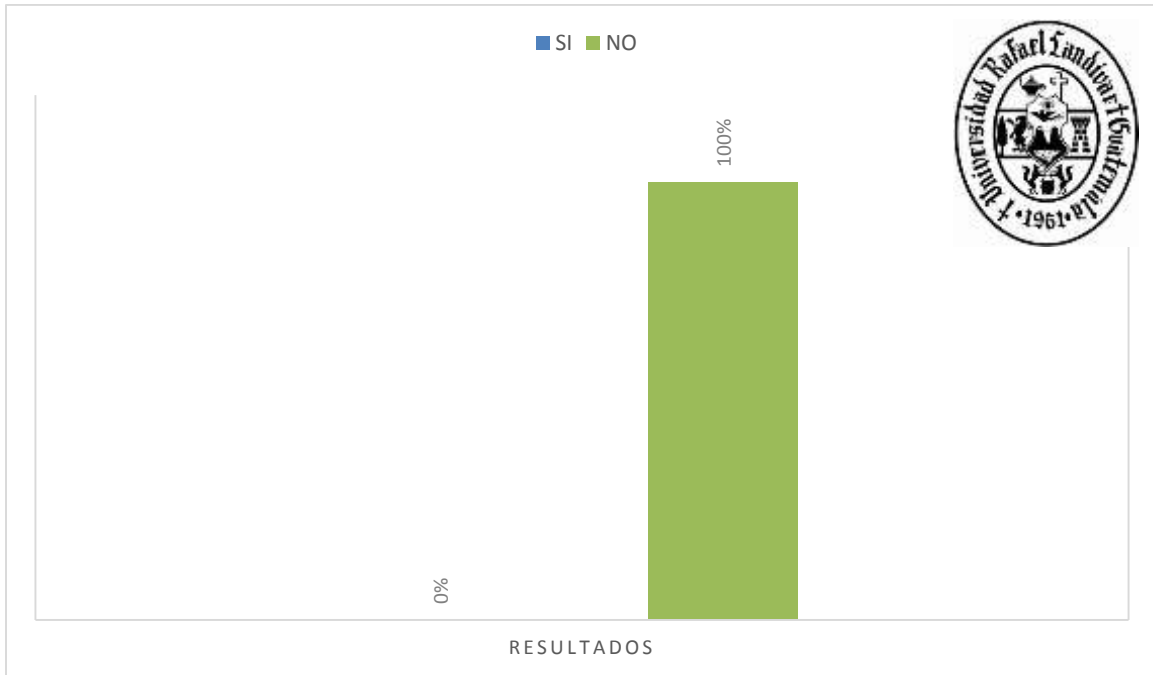
Interpretación:

De los encuestados, el 100% de sujetos de estudio hizo referencia a la negativa sobre la aplicación de test de confiabilidad del personal del Ministerio Público, especialmente las personas que tienen acceso a las bases de datos y archivos de la institución.

Resultados que indican que es necesaria la aplicación por parte del Departamento de Recursos Humanos del Ministerio Público, de test de confiabilidad dirigido a los empleados, principalmente de aquellos que tienen bajo su poder información sensible de la institución, a su vez, la mayoría de sujetos de estudio, hacen referencia a que es necesario estandarizar un modelo de contrato de confidencialidad, el cual contenga implicaciones legales de no ser respetado.

### Gráfica No. 5

**¿Conoce usted si dentro del reglamento interno del Ministerio Público, existe un apartado sobre la prevención de fuga de información?**



Fuente de elaboración propia.

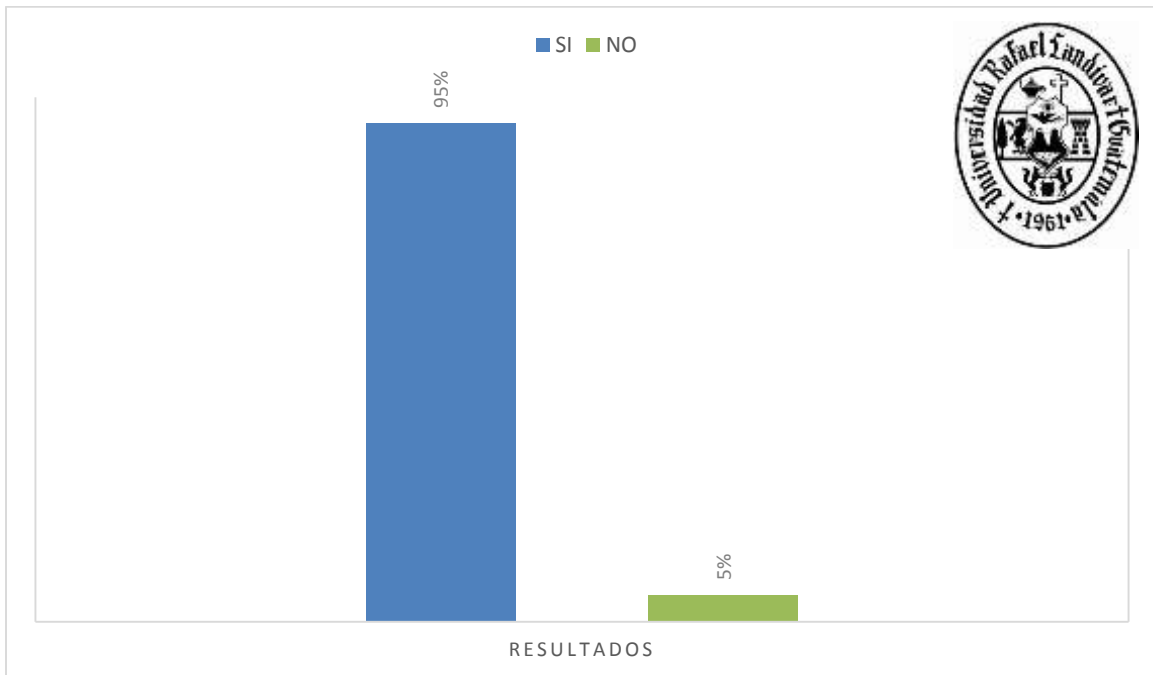
Interpretación:

De los encuestados, el 100% de sujetos de estudio hizo referencia a la negativa de conocer si el Reglamento Interno del Ministerio Público hace referencia sobre la fuga de información y su prevención.

Resultados que indican que es necesario socializar con el personal de la institución el Reglamento Interno, no únicamente sobre el tema sujeto a investigación, sino por el sano conocimiento de las normas establecidas que regula el comportamiento de los colaboradores con la finalidad de obtener resultados eficaces y eficientes.

## Gráfica No. 6

**Según su criterio y experiencia, ¿Es necesario mejorar el sistema de seguridad que resguarda la información sensible de la institución?**



Fuente de elaboración propia.

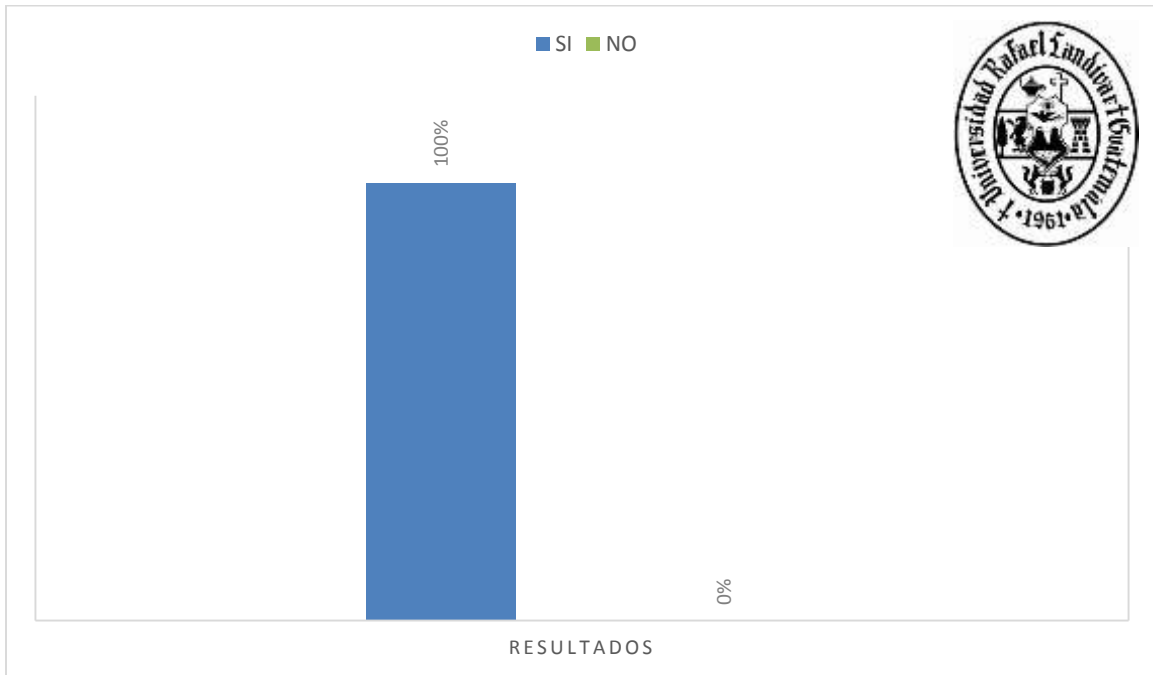
Interpretación:

De los encuestados, el 95% indicó que si considera necesario mejorar los sistemas de seguridad de la información que se maneja dentro del Ministerio Público, mientras que por otro lado, el 5% de sujetos de estudio hizo referencia a la negativa sobre el necesario mejoramiento de los sistemas de seguridad de la información.

Resultados que indican que es necesario establecer fortalecer y mejorar los sistemas actuales de seguridad y resguardo de la información.

**Gráfica No. 7**

**¿Conoce usted los riesgos a los que está expuesta la información sensible de esta institución?**



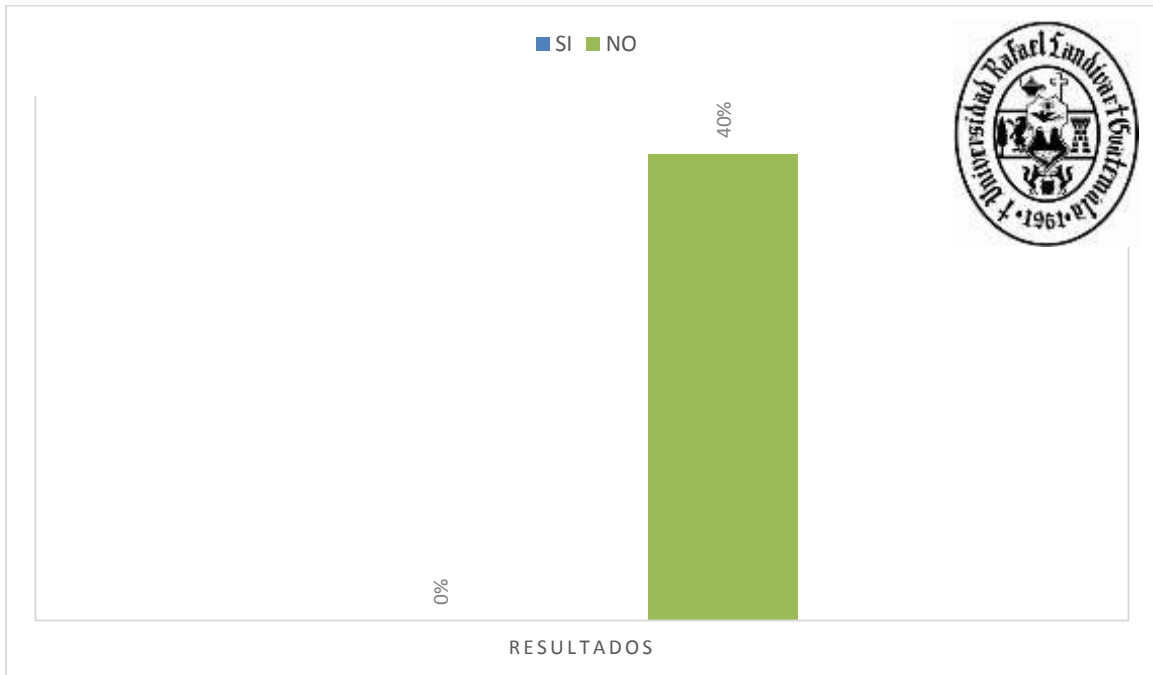
Fuente de elaboración propia.

Interpretación:

De los encuestados, el 100% indicó que si conocen los riesgos a los cuales puede estar expuesta la información que maneja la institución, especialmente en los casos de mayor impacto, los cuales tiene intereses de terceras personas de por medio.

**Gráfica No. 8**

**¿Existe un protocolo que indique la correcta manipulación de la información sensible, adicional a la cadena de custodia?**



Fuente de elaboración propia.

Interpretación:

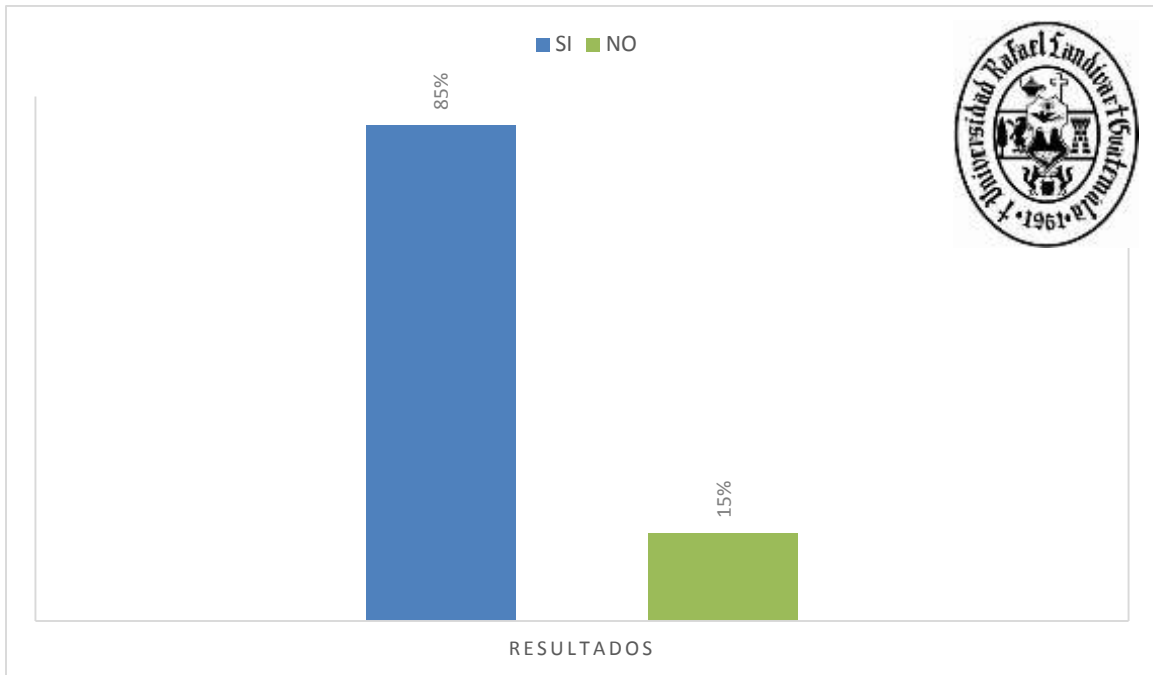
De los encuestados, el 100% de sujetos de estudio hizo referencia a la negativa sobre el conocimiento de algún protocolo que estandarice la manipulación de la información sensible del Ministerio Público, dejando en claro que la única herramienta que se utiliza actualmente es la cadena de custodia.

Resultados que indican que es necesario establecer un protocolo o policita sobre la manipulación y resguardo de la información del Ministerio Publico.



**Gráfica No. 9**

**¿Considera usted que es necesario tener más conocimientos sobre los métodos de detección y prevención de fuga de información?**

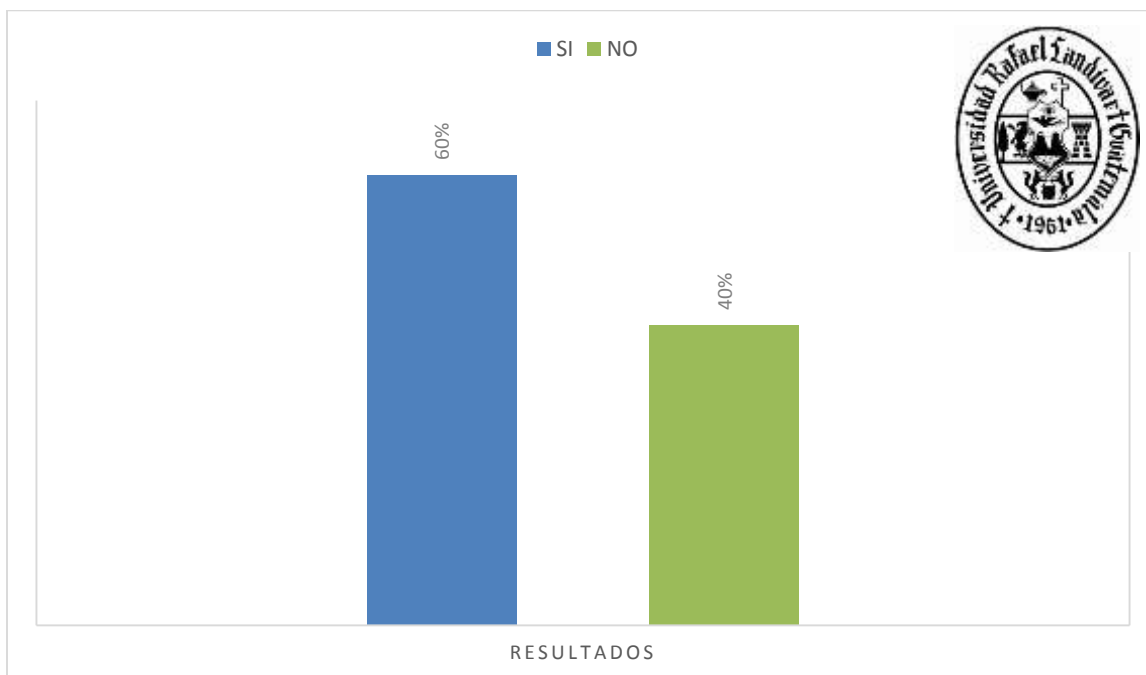


Fuente de elaboración propia.

Interpretación:

De los encuestados, el 85% indicó que sí considera necesario conocer los métodos de prevención y detección de fuga de información, mientras que por otro lado, el 15% de sujetos de estudio hizo referencia a la negativa sobre la importancia de conocer los métodos de detección y prevención de la fuga de información dentro de la Institución.

**Gráfica No. 10**  
**¿Conoce usted si existe algún tipo de sanción administrativa o penal para el empleado que incurriera en sustraer información institucional sin autorización?**



Fuente de elaboración propia.

**Interpretación:**

De los encuestados, el 60% indicó que si conoce las sanciones tanto administrativas como penales que conlleva la sustracción sin autorización de información del Ministerio Público, el 40% de sujetos de estudio hizo referencia a la negativa sobre la existencia de sanciones administrativas o penales que se dieran en caso de fuga de información dentro de la Institución.

Luego de analizar los resultados obtenidos mediante los instrumentos de estudio; se pueden determinar las deficiencias de la institución en el sentido de la seguridad proporcionada a la información y base de datos existente sobre información sensible

de la institución, es lamentable como los recursos de seguridad no se estén utilizando correctamente.

## **CONCLUSIONES.**

1. Debido al constante avance tecnológico y la creación de herramientas que permiten la edición y manipulación de la información de la base de datos, se ha vuelto realmente necesaria la implementación de técnicas capaces de detectar alteraciones al desarrollar el análisis forense a los archivos digitales constituidos.
2. En Guatemala se encuentra establecida dentro de los procesos de investigación la documentación, no obstante, ésta no se encuentra plasmada del todo en un marco jurídico vigente que la estandarice o regule dentro de la investigación criminal en el país, sin embargo, al analizar la doctrina y manuales existentes, se encontró escaso contenido referente al resguardo de información.
3. El constante avance tecnológico es consecuente al incremento del índice de violencia y delitos en Guatemala, se haciéndose emergente la implementar nuevos mecanismos de capacitación a los funcionarios, empleados y peritos que laboran dentro del ministerio público, así como la profesionalización y especialización de los técnicos en cada una de las áreas correspondientes, esto con el fin de alcanzar estándares de calidad que se vean reflejados en los resultados de las investigaciones.
4. La aplicación de nuevos procedimientos y la creación de un manual o la mejora de los ya existentes propiciar la obtención de mejores resultados antes, durante y después, en materia investigativa, a esto ampliándose la aplicación de nuevas técnicas de seguridad de los sistemas de información que va aunado con el avance tecnológico de las aplicaciones de seguridad empleadas por la institución, proporcionarían elementos de mejor calidad en el procesamiento de escena, lo cual, a su vez permitiría el desarrollo de análisis forenses basados en un estricto control de calidad.

5. En Guatemala actualmente no se cuentan con las herramientas necesarias para el resguardo y protección de las fuentes de información y base de datos que son generados a través de los casos de investigación realizados por el ministerio público, lo cual vulnera significativamente los estándares no solo de seguridad sino también de calidad, lo que a consecuencia simbolizaría la pérdida de los valores y credibilidad institucional. Implementar un método más eficaz en las sanciones, puede propiciar a una mejor filtración de empleados al ministerio público.

6. Si se previene el manejo adecuado de la información se va evitar la fuga de la misma, iniciando con la implementación de nuevos procedimientos de reclutamiento y evaluación.

## **RECOMENDACIONES.**

1. Implementar la aplicación de la Política preventiva para el resguardo y manejo adecuado de la información en materia de Investigación Criminal dentro del Ministerio Público.
2. Propiciar la ampliación o mejoramiento de los lineamientos establecidos en el Manual de normas y procedimientos para el procesamiento de escena del crimen en casos de delitos contra la vida e integridad de la persona, esto con el fin de fortalecer las debilidades que radican en el desde la perspectiva de las responsabilidades de cada uno de los técnicos para el desarrollo de sus actividades, en especial el fortalecimiento de las áreas técnicas de investigación.
3. Considerar la implementación de herramientas tecnológicas dentro del Ministerio Publico, con las cuales se pueda realizar un análisis y monitoreo de los estándares de seguridad de la información generada en las investigaciones del Ministerio Publico.
4. Ofrecer constante capacitación y actualización a los técnicos del Ministerio Público, sobre los conocimientos y técnicas básicas de seguridad de la información, al igual que aplicar evaluaciones de desempeño basados en los resultados obtenidos de confiabilidad y responsabilidad.
5. Instruir al personal del Ministerio Publico que participa en la investigación criminal, siendo estos Auxiliares Fiscales y Técnicos en escena del crimen, sobre la importancia de cumplir con responsabilidad sus funciones, haciendo referencia en el acceso a los sistemas de información y base de datos, con la finalidad de disuadirlos en el tema de fuga de información o manipulación indebida de la misma. Ejecución de sanciones disciplinarias acorde a lo establecido en el pacto colectivo de condiciones de trabajo y de más leyes especiales para que en la institución se

encuentre solo personal idóneo que cumpla a cabalidad con las normas y estándares de seguridad.

6. Incluir dentro del procedimiento de selección de nuevo personal una etapa de evaluación ética y moral donde psicólogos evaluaran a través de test, el nivel de confiabilidad del personal hacia la institución, previendo la protección y buen manejo de información sensible.

## REFERENCIAS.

### 1. Referencias bibliográficas.

Carrillo Medrano, Patricia. *Manual de Procesos Alternativos*. México, UNAM, 2007.

Fleita, Benito Amílcar. *Sistemas actuales de análisis de criminalística*. Argentina, Ediciones La Rocca, 2005.

Getty Trust, J. Paul. *Introducción a los Metadatos: vías a la información digital*. Estados Unidos, Sin Editorial, 1999.

Guzmán, Carlos A. *Manual de Criminalística*. Argentina, Ediciones La Rocca, 2003.

Sin autor. *Manual de normas y procedimientos para el procesamiento de escena del crimen en casos de delitos contra la vida e integridad de la persona*. Guatemala, Ministerio Publico, 2009.

### 2. Referencias normativas.

Asamblea Nacional Constituyente. Constitución Política de la República de Guatemala.

Congreso de la República de Guatemala. Decreto 17-73 Código Penal.

Congreso de la República de Guatemala. Decreto 40-94. Ley Orgánica del Ministerio Público

Congreso de la República de Guatemala. Decreto 51-92.y sus reformas. Código Procesal Penal.

Ministerio Público. Acuerdo 3-96. Reglamento de la Carrera del Ministerio Público



### 3. Referencias electrónicas.

Benítez Hernández, Isabel. Problemas éticos y de la seguridad informática asociados al uso de la tecnología. <http://bvs.sld.cu/revistas/infd/n809/infd1909.htm>. Fecha Consultada: 15 de Octubre de 2017.

Córdova Rodríguez, Norma Edith. Plan de Seguridad Informática para una Entidad Financiera.

[http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova\\_RN/Cap4.pdf](http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap4.pdf). Fecha consultada: 28 de Octubre 2017.

Granados Paredes, Gibrán. Introducción a la Criptografía, 2006, Pág. 3  
file:///C:/Users/TOSHIBA/Downloads/Introduccion%20a%20la%20criptografia.pdf.  
Fecha Consultada: 10 de Octubre de 2016.

Seguridad Computacional, <https://seguridad-computacional.wikispaces.com/elementos+de+seguridad+informatica?responseToken=028fc140342e081fcb2783524c4ecdb96>. Fecha Consultada: 10 de Octubre de 2016.

Seguridad Informática. Conceptos Básicos.  
[http://catarina.udlap.mx/u\\_dl\\_a/tales/documentos/lis/jerez\\_l\\_ca/capitulo1.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf).  
Fecha consultada: 30 de septiembre de 2016.

### 4. Otras referencias

Guía de Gestión de Fuga de Información, España. 2012. Instituto Nacional de Tecnologías de la Comunicación.

López García, Elmer Yovani. Inclusión de los Delitos Informáticos, que se comenten en Internet, dentro del código penal guatemalteco, Guatemala, 2011, Facultad Ciencias Jurídicas y Sociales.

Medina Iriarte, Johanna. "Estándares para la seguridad de información con tecnologías de información". Chile. 2006. Tesis de Ingeniero de Control y de Gestión. Universidad de Chile. Chile.

# ANEXOS

## Anexo 1:

MP MINISTERIO PÚBLICO  
Ciencia • Verdad • Justicia

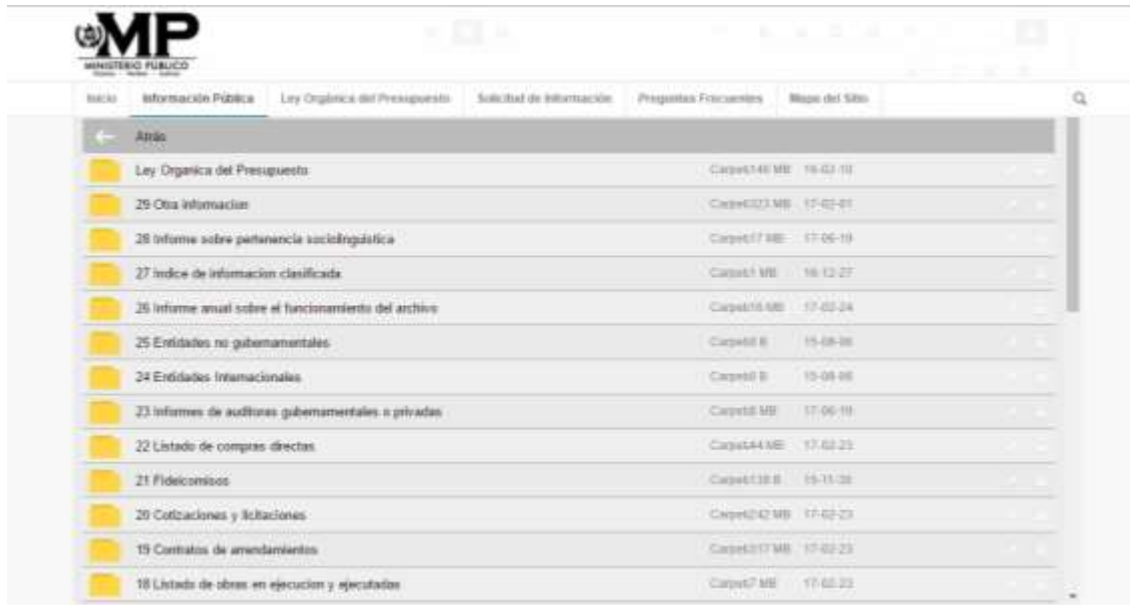
Inicio Información Pública Ley Orgánica del Presupuesto Solicitud de Información Preguntas Frecuentes Mapa del Sitio

1-6'

1. Estructura Orgánica, Funciones y Marco Normativo
2. Directorio de la entidad
3. Directorio de empleados y servidores públicos
4. Número y nombre de funcionarios, servidores públicos, empleados y asesores que laboran en el sujeto Obligado
5. Misión, Objetivos y Plan operativo Anual

Acceso a la información pública/ Portal Ministerio Publico de Guatemala

## Anexo 2:



Inicio	Información Pública	Ley Orgánica del Presupuesto	Solicitud de Información	Preguntas Frecuentes	Mapa del Sitio
← Atrás					
		Ley Orgánica del Presupuesto	Carpet6140 MB	16-02-10	
		25 Otra Información	Carpet6023 MB	17-02-01	
		26 Informe sobre pertenencia sociolingüística	Carpet17 MB	17-05-19	
		27 Índice de Información clasificada	Carpet1 MB	16-12-27	
		26 Informe anual sobre el funcionamiento del archivo	Carpet16 MB	17-02-24	
		25 Entidades no gubernamentales	Carpet0 B	15-08-06	
		24 Entidades Internacionales	Carpet0 B	15-08-06	
		23 Informes de auditorías gubernamentales o privadas	Carpet0 MB	17-06-16	
		22 Listado de compras directas	Carpet44 MB	17-02-23	
		21 Fideicomisos	Carpet128 B	15-11-26	
		20 Cotizaciones y licitaciones	Carpet202 MB	17-02-23	
		19 Contratos de arrendamientos	Carpet317 MB	17-02-23	
		18 Listado de obras en ejecución y ejecutadas	Carpet7 MB	17-02-23	

Acceso a la información pública/ Portal Ministerio Publico de Guatemala

**Anexo 3:**

**Política preventiva para el resguardo y manejo  
adecuado de la información en materia de  
Investigación Criminal dentro del ministerio  
público.**

## ÍNDICE

	Página No.
1. Principios orientadores que rigen esta política.	4
1.1 Declaración universal de los derechos humanos en el ámbito laboral.	5
1.2 Derechos humanos constitucionales.	6
1.3 Instituciones de Justicia de Guatemala.	11
1.4 Transparencia y rendición de cuentas.	13
2 Ministerio Público.	16
2.1 Historia del Ministerio Público.	16
2.2 Misión.	17
2.3 Visión.	17
2.4 Estructura Funcional.	19
2.5 Funciones.	20
2.6 Fiscalías.	20
2.7 Casos de mayor sensibilidad.	21
2.8 Métodos especiales de investigación.	24
2.9 Consejo Superior del Ministerio Público – Reformas.	25
2.10 Pacto Colectivo.	26
2.10.1. Sanción.	27
2.11 Grupos de presión.	28
2.11.1 Sindicato ministerio público.	28
2.12 Renglones de Contratación	28
3 Marco legal para sancionar la mala actuación profesional de los empleados y funcionarios públicos.	29
3.1 Código penal.	29

3.2 Entorno de seguridad en Guatemala.	30
3.3 Opinión sobre el resguardo de la información dentro de la institución.	30
3.4 Contexto de los niveles de seguridad en la información sensible.	31
3.5 Ejemplos a nivel mundial sobre el mal resguardo de la información.	33
3.5.1 Su efecto en el entorno social.	36
3.6 Métodos más usados en el pasado para filtrar información.	37
3.7 NSA (Agencia de Seguridad Nacional) – Estados Unidos.	38
3.8 Desafíos en materia de seguridad en Guatemala.	41
3.9 Prevención.	43
3.9.1 Ejes de trabajo.	43
3.10 Investigación.	48
3.10.1 Sistemas de seguridad de la información.	48
3.11 Inserción.	52
3.11.1 Clasificación de las áreas del ministerio público por niveles de acceso.	52
3.12 Resultados en perspectiva sobre la aplicación de esta política.	52
4 Conclusiones.	54

## **1. Principios orientadores que rigen esta política.**

- **Legalidad:** Actuar bajo los límites de la Ley, y al derecho consuetudinario con base a él bien común y servicio a la sociedad.
- **Transparencia:** Condición en la que las gestiones y demás actos están a disposición de todo aquel que tenga interés en saber al respecto, facilitando el libre acceso a toda la información, en todas las fases del proceso y actividades.
- **Justicia:** Propiedad de aquellas personas que tiene un valor moral de dar y tratar a cada persona como le corresponde por derecho, manteniendo la igualdad ante todo.
- **La verdad:** La verdad se ha fomentado siempre y quien la cultiva es considerada como una persona de alta calidad humana.
- **Eficiencia:** Capacidad que demuestra una persona o institución competente en el desenvolvimiento de sus funciones asignadas.
- **Igualdad:** Ausencia de todo pensamiento y limitante discriminatorio respecto a las oportunidades que toda persona debe tener en su calidad de ser humano.
- **Integridad:** Condición que indica la rectitud que muestra una persona en el desenvolvimiento de sus actividades de su entorno pues será equilibrado, honesto y justo.



- La responsabilidad y el deber: La responsabilidad es la virtud humana de responder con formalidad de ser capaz para tomar decisiones de dirigir una actividad de organizar a un grupo o de coordinar un todo. También se trata de tomar con seriedad toda.
- Honestidad: Característica de una persona que hace que sus acciones y palabras tengan credibilidad, expresando coherencia y sinceridad en el actuar.
- Ética: Aspecto que surge como tal en la interioridad de una persona, como resultado de su propia reflexión y su propia elección, determinando qué es lo bueno y cómo se debe actuar.
- Moral: La moral es un conjunto de normas de conducta y convivencia, íntimamente ligada a la ética, establecidas en el seno de una sociedad.
- Respeto: Actitud ante la vida que implica aceptar y comprender a los demás, así como acatar su autoridad y considerar su dignidad. Se asocia mucho a la verdad.

### **1.1 Declaración universal de los derechos humanos en el ámbito laboral.**

- a. Artículo 23. “Toda persona tiene derecho al trabajo”<sup>1</sup>, teniendo la libre elección del mismo, bajo las mismas condiciones (prestaciones, salarios, etc.), así como a la protección contra el desempleo injustificado.
- b. Los trabajadores poseen el derecho a una retribución igualitaria que proporcione a su persona y su familia un existencia bajo los estándares

---

<sup>1</sup> Declaración Universal de los Derechos Humanos. <http://www.derechoshumanos.net/normativa/normas/1948,DeclaracionUniversal.htm?gclid=CLzF0eScjaACFUxahgodZKgFsg>. Página consultada el 03-11-2016.

básicos de vida, siendo estos apoyados por otros medios de protección social.

- c. “Toda persona tiene derecho a fundar sindicatos y a sindicarse para la defensa de sus intereses”<sup>2</sup>.
- d. Artículo 24: “Toda persona tiene derecho al descanso”<sup>3</sup>, pudiendo disponer a su parecer de su tiempo libre, a límites justificables del periodo que dure su trabajo, así como a las vacaciones periódicas pagadas como retribución por su labor.

## **1.2. Derechos humanos constitucionales.**

Artículo 1. Protección a la persona. “El estado de Guatemala se organiza para proteger a la persona y a la familia”<sup>4</sup>; teniendo como fin otorgar un entorno con las condiciones de vida requeridas.

Artículo 2. Deberes del estado. “Es deber del Estado garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona”<sup>5</sup> permitiéndoles tener las cauciones necesarias para progresar.

Artículo 3. Derecho a la Vida. “El estado garantiza y protege la vida humana”<sup>6</sup>, desde su etapa inicial de vida garantizando su protección tanto física como psicológica.

---

<sup>2</sup> *Loc. Cit.*

<sup>3</sup> *Loc. cit.*

<sup>4</sup> Constitución Política de la República de Guatemala. Acuerdo Legislativo 18-93. Emitido el 14 de enero de 1986.

<sup>5</sup> *Loc. cit.*

<sup>6</sup> *Loc. cit.*

Art. 4.- Libertad e Igualdad. “En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos”<sup>7</sup>. Toda personas con el simple hecho de constituirse como ser humano posee los mismos derechos y/o privilegios que cualquier otra persona, no importando sus respectivas características distintivas (raza, sexo, estatus social, etc.), por lo que no concierne el proceder de la persona, esta gozara lo que por ley le corresponde.

Art. 5.- Libertad de acción. “Toda persona tiene derecho a hacer lo que la ley no prohíbe”<sup>8</sup>; y esta radica en realizar cualquier acción siempre y cuando estas no se encuentren tipificados como delitos o faltas.

Artículo 6.- Detención legal. “Ninguna persona puede ser detenida o presa, sino por causa de delito o falta”<sup>9</sup>, será detenido o preso de manera legal y conforme a lo que la ley establece. En caso contrario se incurrirá en delito por parte de la autoridad competente.

Artículo. 12.- Derecho de defensa. “La defensa de la persona y sus derechos son inviolables”<sup>10</sup>. Toda persona residente en el territorio guatemalteco posee bienes jurídicos tutelados que deben ser respetados ante el poderoso estado.

Artículo 14.- Presunción de inocencia y publicidad del proceso. “Toda persona es inocente, mientras no se le haya declarado responsable judicialmente, en sentencia debidamente ejecutoriada”<sup>11</sup>. Toda persona que se encuentre ligada a proceso debe ser tratada como inocente hasta que haya sido vencido y probado su culpabilidad mediante pruebas contundentes del delito en el que se le vincula

---

<sup>7</sup> *Loc. cit.*

<sup>8</sup> *Ibid.*, Pág. 6.

<sup>9</sup> *Ibid.*, Pág. 6.

<sup>10</sup> *Ibid.*, Pág. 7.

<sup>11</sup> *Ibid.*, Pág. 7.

Artículo 23.- Inviolabilidad de la vivienda. “La vivienda es inviolable Nadie podrá penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente”<sup>12</sup>. Salvo en casos en los que la ley lo tipifique, la morada de una persona es inviolable y solo se podrá ingresar bajo una orden de juez correspondiente en un parámetro de horario determinado.

Artículo 26.- Libertad de locomoción. Toda persona tiene libertad de entrar, permanecer, transitar y salir del territorio nacional”<sup>13</sup>, siempre se esté circulando en la vía publica bajo las normas de convivencia no se impedirá tal acción.

Artículo 27.- Derecho de asilo. “Guatemala reconoce el derecho de asilo y lo otorga de acuerdo con las prácticas internacionales”<sup>14</sup>. Al ratificarse ciertas normas internacionales Guatemala es reconocido como lugar de asilo, salvo en extradiciones que cumplan con lo que está establecido para que se lleve a cabo.

Artículo 28.- Derecho de petición. “Los habitantes de la República de Guatemala tienen derecho a dirigir, individual o colectivamente, peticiones a la autoridad”<sup>15</sup>, pues son trabajadores que fueron electos por el pueblo y por lo consiguiente están para garantizar el bienestar social.

Artículo 29.- Libre acceso a tribunales y dependencias del Estado. “Toda persona tiene libre acceso a los tribunales, dependencias y oficinas del Estado”<sup>16</sup>. Donde puede realizar sus gestiones necesarias para que sus derechos se cumplan y se respeten tal como lo describe nuestro marco legal.

---

<sup>12</sup> *Ibid.*, Pág. 9.

<sup>13</sup> *Ibid.*, Pág. 9.

<sup>14</sup> *Ibid.*, Pág. 9.

<sup>15</sup> *Ibid.*, Pág. 10.

<sup>16</sup> *Ibid.*, Pág. 10.

Artículo 33.- Derecho de reunión y manifestación. “Se reconoce el derecho de reunión pacífica y sin armas”<sup>17</sup>. Los derechos por medio de los cuales la sociedad puede salir a las calles de manera individual o colectiva a manifestar no deben restringirse siempre y cuando se respete el orden social.

Artículo 34.- Derecho de asociación. “Se reconoce el derecho de libre asociación”<sup>18</sup>. Toda persona tiene a su libre elección la pertenencia a un grupo social o no, excepto la colegiación profesional, la cual es obligatorio y necesario para el ejercicio de la profesión.

Artículo 35.- Libertad de emisión del pensamiento. “Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa”<sup>19</sup>. Ninguna persona particular o jurídica podrá impedir que los ideales de otros circulen libremente siempre y cuando estos no dañen la imagen ni su moralidad pues se estaría incurriendo en un hecho punible, exceptuándose los casos en los que se trate de funcionarios y empleados públicos.

Artículo 36.- Libertad de religión. “El ejercicio de todas las religiones es libre”<sup>20</sup>. Toda persona indistintamente del grupo religioso al que pertenezcan es libre de practicarlo pública o privadamente teniendo únicamente en cuenta el debido respeto al orden público y a los otros cultos y sus seguidores.

Artículo 39.- Propiedad privada. “Se garantiza la propiedad privada como un derecho inherente a la persona humana”<sup>21</sup>. Toda personas podrán realizar lo que mejor les convenga con las propiedades que posea legalmente.

---

<sup>17</sup> *Ibid.*, Pág. 10.

<sup>18</sup> *Ibid.*, Pág. 11.

<sup>19</sup> *Ibid.*, Pág. 11.

<sup>20</sup> *Ibid.*, Pág. 12.

<sup>21</sup> *Ibid.*, Pág. 12.

Artículo 43.- Libertad de industria, comercio y trabajo. “Se reconoce la libertad de industria, de comercio y de trabajo, salvo las limitaciones que por motivos sociales o de interés nacional impongan las leyes”<sup>22</sup>. Toda persona tiene plena libertad buscar desarrollo económico a través de la industria o el comercio siempre y cuando sus hechos no incurran en delitos que tipifica la ley.

Artículo 47.- Protección a la familia. “El Estado garantiza la protección social, económica y jurídica de la familia”<sup>23</sup>. A través de sus diversas organizaciones y ministerios el estado tiene bajo su tutela a la familia buscando otorgarles un entorno adecuado para su crecimiento y desarrollo a cada miembro.

Artículo 57.- Derecho a la cultura. “Toda persona tiene derecho a participar libremente en la vida cultural y artística de la comunidad”<sup>24</sup>. Como parte de la sociedad se tiene el derecho de ser partícipes en las actividades culturales y artísticas que se organicen.

Artículo 71.- Derecho a la educación. “Se garantiza la libertad de enseñanza y de criterio docente. Es obligación del Estado proporcionar y facilitar educación a sus habitantes sin discriminación alguna”<sup>25</sup>. Independientemente del grupo étnico, estatus social, raza o lugar de origen, toda persona tiene el derecho a una educación de calidad que garantice su desarrollo y preparación académica.

Artículo 93.- Derecho a la salud. “El goce de la salud es derecho fundamental del ser humano, sin discriminación alguna”<sup>26</sup>. Toda persona sin distinción alguna tiene pleno derecho a exigir que se garantice su salud, así como el cuidado de los problemas médicos q pueda a desarrollar, siendo atendido en hospitales preparados tanto en insumos como en infraestructura.

---

<sup>22</sup> *Ibid.*, Pág. 13.

<sup>23</sup> *Ibid.*, Pág. 13.

<sup>24</sup> *Ibid.*, Pág. 14.

<sup>25</sup> *Ibid.*, Pág. 16.

<sup>26</sup> *Ibid.*, Pág. 20.

Artículo 101. Derecho al trabajo. “El trabajo es un derecho de la persona y una obligación social. El régimen laboral del país debe organizarse conforme a principios de justicia social”<sup>27</sup>. Bajo los tratados internacionales con la Organización Internacional del Trabajo (OIT), Guatemala está obligada a proporcionar fuentes de empleo a las personas que requieren de un ingreso digno, seguridad en el lugar del trabajo así como mejores perspectivas de desarrollo persona e integral.

### **1.3 Instituciones de Justicia de Guatemala.**

El Sistema judicial en la República de Guatemala está formada por organismos, entidades descentralizadas, autónomas y semiautónomas del Estado, que son descritos en la Constitución Política de la República de Guatemala y demás leyes de la nación que lo regulan.

a. Organismo Judicial.

Es el encargado de impartir justicia de conformidad con la Constitución Política de la Republica y las leyes del país.

Su fundamento legal está regulado en los Artículos 203 al 222 de la C.P.R.G. en la ley del organismo judicial, sus reformas y otras leyes ordinarias.

b. Corte de Constitucionalidad.

Es un órgano independiente de los demás que integran el estado. Este tribunal permanente posee la principal función de defender el orden constitucional de Guatemala, así como otras que le asigna la constitución y su ley orgánica.

c. Fiscalía especial contra la impunidad - Ministerio público.

Departamento del ministerio público que investiga los casos que en conjunto con CICIG seleccionan para ser asignados a esta Fiscalía de

---

<sup>27</sup> *Ibid.*, Pág. 22.

conformidad con el marco de competencia. “Dichos casos deben llenar los requisitos establecidos en el mandato conferido a la CICIG, y en común acuerdo entre el/la Fiscal General de la República y el Comisionado contra la Impunidad en Guatemala”<sup>28</sup>.

d. Procuraduría General de la Nación.

Es la entidad que legalmente tiene asignada la representación del Estado, brindando asesoría a asuntos que sean de su interés. Este es también considerado también el máximo órgano en la representación de los menores e incapaces, entre otros procesos que realiza buscando que todo se cumpla conforme a la nuestro marco legal.

e. Procurador de los Derechos Humanos:

“Es un comisionado del congreso de la república de Guatemala asignado para garantizar el cumplimiento de los derechos humanos establecidos en nuestra constitución, la declaración universal de los derechos humanos, convenios y tratados suscritos y ratificados por el país sobre dicha materia”<sup>29</sup>.

Entre otras de sus funciones principales que se mencionan están, la fiscalización en la administran publica de los recursos del estado, la recepción e investigación de denuncias, etc.

f. Ministerio de Gobernación:

Uno de los principales sectores del gobierno comprometidos en la seguridad del país pues se encuentra inmerso dentro de la “formulación de políticas y velar por el estricto cumplimiento del régimen legislativo referente al mantenimiento de la paz y el orden público, la seguridad de las personas y de sus bienes, la garantía de sus derechos, la ejecución de las órdenes y

---

<sup>28</sup> CICIG. <http://www.cicig.org/index.php?page=preguntas-frecuentes>. Página consultada el 03-11-2016.

<sup>29</sup> Procurador de Los Derechos Humanos. <http://www.pdh.org.gt/procurador/quien-es.html> Página consultada el 03-11-2016.



resoluciones judiciales, el régimen migratorio y refrendar los nombramientos de los Ministros de Estado”<sup>30</sup>, no dejando de lado su función como rector y supervisor del sistema penitenciario y dirección general de la policía nacional civil.

g. Instituto de la Defensa Pública Penal.

Se encarga de prestar el servicio de asistencia penal a las personas a las cuales se les señala de haber cometido un delito, así mismo brinda apoyo legal a las mujeres víctimas de violencia intrafamiliar. En ambos casos un abogado defensor los acompaña durante el proceso sin cobro alguno.

#### 1.4 Transparencia y rendición de cuentas.

Gráficas tomadas de: Informe anual memoria administración mayo 2015 – 2016. (<https://www.mp.gob.gt/noticias/memoria-administracion-mayo-2015-2016/>).

tabla 23

Región	Fiscalía	Personas condenadas	personas absueltas	Total de personas
<b>Total</b>		<b>8,795</b>	<b>2,098</b>	<b>10,893</b>
<b>Metropolitana</b>	Guatemala	893	155	1,048
	Mixco	254	56	310
	Villa Nueva	251	100	351
	Palencia	10	0	10
	Villa Canales	72	12	64
	San Juan Sacatepequez	26	6	31
	Amatitlan	66	21	69
	Santa catarina pinula	23	1	24
	Chinautla	16	1	17
	<b>Central</b>	Chimaltenango	305	35
Escuintla		186	19	205
Santa Lucía cotzumalguapa		76	26	102
San José		56	13	71

<sup>30</sup>[http://www.deguate.com/artman/publish/politica\\_ministerios/Ministerio\\_de\\_Gobernaci\\_n\\_1049.shtm#WTowzPmGPIU](http://www.deguate.com/artman/publish/politica_ministerios/Ministerio_de_Gobernaci_n_1049.shtm#WTowzPmGPIU)

	Tiquisate	51	11	62
	Sacatepequez	180	27	207
<b>Noroccidental</b>	Huehuetenango	73	2	95
	La Democracia	22	13	35
	Santa Eulalia	40	10	50
	Quiché	40	27	67
	Ixcán	26	18	44
	Nebaj	40	23	63
	Joyabaj	34	27	61
<b>Nororiental</b>	Chiquimula	68	33	101
	Esquipulas	36	5	41
	El Progreso	81	14	95
	Izabal	64	73	137
	Morales	27	17	44
	Zacapa	82	18	100
	Gualán	43	5	48

**tabla 23**

Región	Fiscalía	Personas condenadas	personas absueltas	Total de personas
<b>Suroriental</b>	Jalapa	101	39	140
	Jutiapa	69	15	84
	Asuncion Mita	46	7	53
	Moyuta	32	4	36
	Santa Rosa	236	28	264
	Taxisco	65	7	92
	Casillas	34	6	40
<b>Suroccidental</b>	Solola	103	31	134
	Santiago Atitlan	39	10	49
	Suchitepequez	122	28	150
	San Juan Bautista	17	0	17
	Retalhuleu	71	36	107
	Quetzaltenango	142	43	185
	Coatepeque	116	43	159
	San Marcos	32	6	38
	Ixchiguán	8	4	12
	Malacatan	41	14	55
	Tecún umán	27	8	35
	Totonicapan	119	24	143
<b>Norte</b>	Alta Verapaz	37	36	73

	Santa Catalina la Tinta	2	4	6
	Chisec	13	4	17
	Baja Verapaz	75	27	102
	Rabinal	27	17	44
<b>Petén</b>	Petén	111	61	172
	Poptun	56	41	97
	La libertad	32	16	48
<b>Sección A</b>	Administrativo	72	43	115
	Asuntos Internos	10	3	13
	Económicos	44	2	46
	Anticorrupción	63	3	66
	Propiedad Intelectual	10	1	11
	Lavado de dinero	34	2	36
	Patrimonio	7	1	6
	Trata de personas	47	11	5
	Extorsiones	2260	35	295
	Mujer	1,362	455	1,617
	Menores	642	13	655
	Vida	368	31	399
	<b>Sección B</b>	Narcoactividad	494	23
Ambiente		29	7	36
Derechos Humanos		31	1	32
Crimen Organizado		365	120	505

<b>TABLA 24</b>	<b>Delito</b>	<b>Personas Condenadas</b>	<b>personas absueltas</b>	<b>Total</b>
	<b>Total</b>	<b>7,113</b>	<b>1,569</b>	<b>8,682</b>
	Violencia contra la mujer	1,649	506	2,155
	Robo agravado	604	119	723
	Extorsión	572	91	663
	Portación ilegal de armas de fuego de uso civil y/o deportiva	474	122	596
	Asesinato	461	80	541
	Robo	420	31	451
	Encubrimiento propio	417	51	468

Homicidio	319	101	420
Promoción o estímulo a la drogadicción	315	4	319
Violación	306	119	425
Robo de equipo terminal móvil	239	38	277
Hurto agravado	195	19	214
Agresión sexual	177	53	230
Violación agravada	172	53	225
Negación de asistencia económica	154	16	170
Posesión para el consumo	144	14	158
Asociación ilícita	142	93	235
Lesiones leves	129	15	144
Lesiones graves	115	12	127
Maltrato contra personas menores de edad	109	32	141

## **2. Ministerio público.**

### **2.1 Historia del ministerio público.**

En 1929 se institucionalizó el Ministerio Público y con ello, la figura del Procurador General y Agentes Auxiliares. El 25 de mayo de 1948 a través del Decreto No. 512 del Congreso de la República, se define en la Ley Orgánica del Ministerio Público, la estructura básica para su funcionamiento, determinando las funciones propias y de las secciones de Procuraduría, Fiscalía y Consultoría, así como las atribuciones del Procurador General de la Nación como Jefe del Ministerio Público. En 1992 por medio del Decreto 51-92 del Congreso de la República, Código Procesal Penal, se establece el juicio oral y público como un medio para el fortalecimiento de los derechos humanos y el proceso democrático, para determinar la inocencia o culpabilidad de la persona imputada, sustituyendo el sistema inquisitivo por uno acusatorio con el cual el Ministerio Público asumió una serie de funciones y responsabilidades como la facultad de dirección de la investigación y el ejercicio de la persecución penal. En 1993 con las reformas al artículo 251 de la Constitución Política de la República de Guatemala, se establece al Ministerio Público como una institución auxiliar de la administración

pública. La consolidación de la nueva institución responsable de la acción penal pública, permitió que el Ministerio Público adquiriera el rango constitucional en la Reforma de 1993 y obtuvieron la aprobación de su ley orgánica en 1994, incorporándose así en el marco del retorno a la institucionalidad democrática y la firma de los Acuerdos de Paz para cumplir con los compromisos asumidos por el Estado guatemalteco, que incluían cambios profundos en el sistema de justicia; y mediante el Decreto 40-94 se define a la institución con funciones autónomas que promueve la persecución penal y dirige la investigación de los delitos de acción pública, velando por el estricto cumplimiento de las leyes del país.

Ministerio Público. “El ministerio Público es una institución auxiliar de la administración pública y de los tribunales con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país. Su organización y funcionamiento se regirá por su ley orgánica”<sup>31</sup>.

El encargado de la acción pública penal es la Fiscal General, quien debe cumplir con los mismos requerimientos que un magistrado de la corte suprema de justicia, siendo nombrado por el presidente entre 6 candidatos seleccionados por una comisión de postulación, quien luego estará dirigiendo por cuatro años dicha institución teniendo a su favor los mismos privilegios e inmunidades que los magistrados de la C.S.J., pudiendo ser removida únicamente por causa justificada por el presidente de la república.

## **2.2 Misión.**

“Promovemos la persecución penal, dirigimos la investigación de los delitos de acción pública y velamos por el estricto cumplimiento de las leyes del país. En el

---

<sup>31</sup> Constitución Política de la República de Guatemala. Acuerdo Legislativo 18-93. Emitido el 14 de enero de 186. Art. 251.

ejercicio de esa función, el MP perseguirá la realización de la justicia, y actuará con autonomía, objetividad, imparcialidad y con apego al principio de legalidad”<sup>32</sup>.

### **2.3 Visión.**

“Ser una institución que ejerce su mandato constitucional con excelencia, eficacia y transparencia, defensora e impulsora de la constitución del Estado de Derecho e integrada por un equipo humano de profesionales comprometido con el logro de la misión institucional, particularmente con la realización de la justicia”<sup>33</sup>.

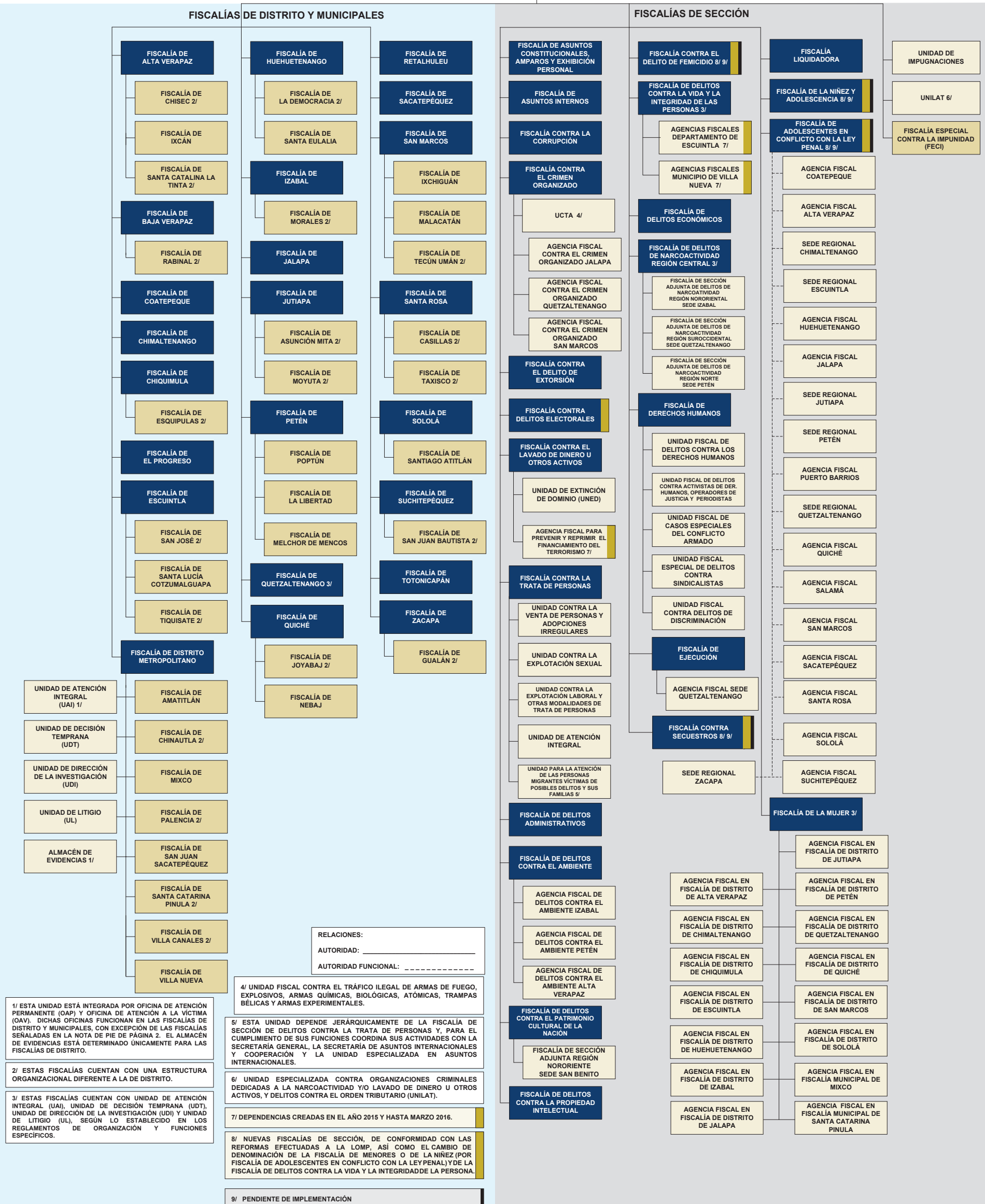
---

<sup>32</sup> Informe anual memoria administración mayo 2015 – 2016. <https://www.mp.gob.gt/noticias/memoria-administracion-mayo-2015-2016/>. Página consultada el 05 de Junio de 2017.

<sup>33</sup> *Loc. cit.*

## Estructura Funcional Área de Fiscalía

DESPACHO DEL FISCAL GENERAL DE LA REPÚBLICA



## 2.5 Funciones.

- “Investigar los delitos de acción pública y promover la persecución penal ante los tribunales, según las facultades que le confiere la Constitución, las leyes de la República y los tratados y convenios internacionales.
- Garantizar los derechos a la víctima dentro del proceso penal.
- Dirigir a la policía y demás cuerpos de seguridad del Estado en la investigación de hechos delictivos.
- Preservar el Estado de Derecho y el respeto de los derechos humanos, efectuando las diligencias necesarias ante los tribunales de justicia”<sup>34</sup>.

## 2.6 Fiscalías.

- “Fiscalía de Asuntos Constitucionales, Amparos y Exhibición Personal
- Fiscalía Contra la Corrupción
- Fiscalía Contra el Crimen Organizado
- Fiscalía Contra el Lavado de Dinero u Otros Activos
- Fiscalía de Delitos Administrativos
- Fiscalía de Delitos Contra el Ambiente
- Fiscalía de Delitos Contra el Patrimonio Cultural de la Nación
- Fiscalía de Delitos Contra la Propiedad Intelectual
- Fiscalía de Delitos Contra la Vida y la Integridad de la Persona
- Fiscalía de Delitos Económicos
- Fiscalía de Delitos de Narcoactividad
- Fiscalía de Derechos Humanos
- Fiscalía de Ejecución
- Fiscalía de Menores
- Fiscalía de la Mujer
- Fiscalía Contra el Delito de Extorsión

---

<sup>34</sup> *Loc. cit.*



- Fiscalía de Delitos Contra la Trata de Personas
- Fiscalía de Asuntos Internos
- Fiscalía Liquidadora
- Fiscalía Especial Contra la Impunidad - FECl-
- Fiscalía de Delitos Electorales”<sup>35</sup>.

## **2.7 Casos de Mayor sensibilidad.**

### a. Cisne blanco.

En el transcurrir del tiempo, las instituciones guatemaltecas han pasado por problemas de confidencialidad, pues se ha visto vulnerada la información sensible, cayendo en manos de personas que muchas veces buscan fines ilícitos, tal es el caso de la estructura criminal denominada El Cisne Blanco, en el cual “Tres trabajadores del Ministerio Público (MP), y dos abogados fueron capturados por las fuerzas de seguridad, mediante el operativo "ORION" acusados de filtrarle información clasificada a miembros de estructuras criminales, para alertarlos acerca de las acciones que estaba realizando el ente investigador”<sup>36</sup>, evidenciando un claro ejemplo de parámetros que deben ser implementados o reestructurados, pues se ha mostrado como personal interno ha llegado a burlar dichas medidas de seguridad de la institución.

---

<sup>35</sup> <sup>35</sup> *Loc. cit.*

<sup>36</sup> Nota: Génesis Agustín, Fotos: Roberto López. CAPTURADOS EMPLEADOS DEL MP POR FUGA DE INFORMACIÓN. [http://www.pnc.gob.gt/index.php?option=com\\_k2&view=item&id=3495:capturados-empleados-del-mp-por-fuga-de-informaci%C3%B3n&Itemid=414](http://www.pnc.gob.gt/index.php?option=com_k2&view=item&id=3495:capturados-empleados-del-mp-por-fuga-de-informaci%C3%B3n&Itemid=414). Página consultada el 07 de marzo de 2015.



<https://cerigua.org/article/capturan-a-trabajadores-del-mp-y-abogados-por-filt/>

Las diligencias sobre el caso dieron inicio por parte del área de asuntos internos al tenerse fragmentos de información certera sobre un grupo de personas estaba extrayendo información de la base de datos interna sin previa autorización.

“Hasta el momento se tienen documentados siete casos en los que existió fuga de información, entre éstos un operativo contra la trata de personas que se realizó en San Marcos el 27 de agosto de este año, que puso en peligro la integridad del personal y el éxito de la operación”<sup>37</sup>. Lo que evidencia por completo el peligro al tener fisuras en los esquemas de seguridad que pueden convertirse en problemas de proporciones inimaginables, sobre todo cuando datos confidenciales pasan a manos de personas no autorizadas, ocasionando no sólo un grave incidente, sino un daño irreversible puesto que quienes la posean pueden darle un mal uso al

<sup>37</sup> CAPTURAN A TRABAJADORES DEL MP Y ABOGADOS POR FILTRAR INFORMACIÓN CONFIDENCIAL. <https://cerigua.org/article/capturan-a-trabajadores-del-mp-y-abogados-por-filt/>. Página consultada el 15 de mayo de 2017.

utilizarla para la comisión de ilícitos penales, sin mencionar la mala reputación y falta de credibilidad que se irá tomando de la institución.

- b. Se esperan capturas por fuga de información confidencial del ministerio público.

Guatemala, Junio 8 del 2016.- Miembros trabajadores del Ministerio Público (MP) señalan que en los próximos días se podrían efectuar capturas de trabajadores de esa institución que se encuentran involucrados en la fuga de información y otros ilícitos.

Trabajadores del ente investigador se dedican a filtrar información confidencial a cambio de dinero o favores de otras personas, lo que ha puesto en amenaza el trabajo contra la corrupción que realiza el MP.

Fuentes que prefirieron no ser identificadas indican que se evidencia tres problemas siendo la fuga de información que resulta ser perjudicial y en esos casos se pudo haber originado la fuga de implicados en casos de alto impacto como **Luis Mendizábal** y **Juan Carlos Monzón**.

El segundo se trata de cohecho pasivo, donde los trabajadores reciben dinero y se registra desde los operadores que reciben las denuncias hasta fiscales que desestiman pruebas, además se suman pérdidas de evidencia y filtración de información.

Y el tercero se trata de la sustracción de evidencia física, digital y documental. Los casos se han reportado en los departamentos de Petén, Izabal, Santa Rosa y la sede central en la capital. Lo sustraído ha sido dinero en efectivo y teléfonos de última generación.

Nota periodística:  
REPORTAJE DE. <http://reportajede.news/?p=6168>

## 2.8 Métodos especiales de investigación.

Artículo 21. Operaciones encubiertas. “Se entenderá por operaciones encubiertas, aquellas que realizan agentes encubiertos con la finalidad de obtener información o evidencias”<sup>38</sup>. Toda agente tiene el primordial objetivo de obtener evidencia suficiente para procesar a los sospechosos de los cuales se sospecha su participación en organizaciones delictivas, buscando la disolución de la misma con la utilización de métodos que producirán resultados positivos para el ente investigador que se encuentra a cargo de la dirección de las pesquisas (ministerio público).

Se tiene únicamente dos observaciones para que la investigación en cubierto se realice sin altercados posteriores los cuales son: la inducción al delito e investigaciones que estén fuera del plan de acción.

Artículo 35. Entregas vigiladas. “Se entenderá por entrega vigilada el método de investigación que permite el transporte y tránsito de remesas ilícitas o sospechosas, así como de drogas o estupefacientes y otras sustancias, materiales u objetos prohibidos o de ilícito comercio, que ingresen, circulen o salgan del país, bajo la estricta vigilancia o seguimiento de autoridades previstas en la presente Ley”<sup>39</sup>.

El control y seguimiento de material sospechoso o ilícito es una estrategia donde se busca identificar las vías por donde circula, personas involucradas y puntos estratégicos del trayecto que darán un panorama amplio sobre todo el movimiento que se realizan los productos ilícitos, dando como resultado a las autoridades a quienes la ley asigna esta tarea, la desarticulación de la red de tráfico ilegal.

Artículo 48. Interceptaciones. “Cuando sea necesario evitar, interrumpir o investigar la comisión de los delitos regulados en los artículos 2, 3, 4, 5, 6, 7, 8, 9, 10 y 11 de la presente ley, podrá interceptarse, grabarse y reproducirse con

---

<sup>38</sup> Ley contra la delincuencia organizada. Decreto Número 21-2009. Emitido el 04 de agosto de 2009.

<sup>39</sup> *Ibid.*, Pág. 22.

autorización judicial, comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares”<sup>40</sup>. La violación a los diversos medios de comunicación privada de una persona se dará únicamente bajo ciertas normas y criterios establecidas por la presente ley y debidamente autorizada por la autoridad competente quien estimara si es necesario tal medida.

## 2.9 Consejo Superior del Ministerio Público – Reformas.

Reformas a la ley orgánica del ministerio público. Decreto 18-2016 realizadas el 18 de marzo de 2016

1)	<b>SECCIÓN III Consejo del Ministerio Público</b>	<b>Se reforma el nombre de la sección III, del título II del decreto número 40-94 del congreso de la república, ley orgánica del ministerio público. “FISCALES DE DISTRITO Y DE SECCION”</b>
02)	Artículo 17. Integración. El Consejo del Ministerio Público estará integrado por: 1) El Fiscal General de la República quien lo presidirá; 2) Tres fiscales electos en asamblea general de fiscales, de entre los fiscales distritales, de sección y los agentes fiscales; 3) Tres miembros electos por el Organismo Legislativo, de entre los postulados a Fiscal General de la República. El Consejo podrá acordar que durante el tiempo en que se reúnan, los fiscales miembros no ejercerán sus funciones, excepto respecto del Fiscal General.	DEROGADO
03)	Artículo 18. Atribuciones. Corresponde al Consejo del Ministerio Público las siguientes funciones: 1) Proponer al Fiscal General el nombramiento de los fiscales de distrito, fiscales de sección, agentes fiscales y auxiliares fiscales, de acuerdo a la carrera del Ministerio Público. 2) Ratificar, modificar o dejar sin efecto las instrucciones generales o especiales dictadas por el Fiscal General, cuando ellas fueren objetadas conforme el procedimiento previsto en esta ley, así como las demás establecidas conforme al régimen disciplinario, los traslados y sustituciones. 3) Acordar a propuesta del Fiscal General la división del territorio nacional, para la determinación de la sede de las fiscalías de distrito y el ámbito territorial que se les asigne; así como la creación o supresión de las secciones del Ministerio Público. 4) Asesorar al Fiscal General de la República cuando él lo requiera. 5) Las demás establecidas por la ley.	DEROGADO
	Artículo 19. Elección. El Congreso de la República, una vez nombrado el Fiscal General, elegirá a tres miembros, de entre los postulados a dicho cargo, para el período que corresponda al Fiscal General de la República. La elección deberá efectuarse dentro de los cinco días siguientes de haberse nombrado el Fiscal General. Los fiscales del Consejo del Ministerio Público serán electos en asamblea	

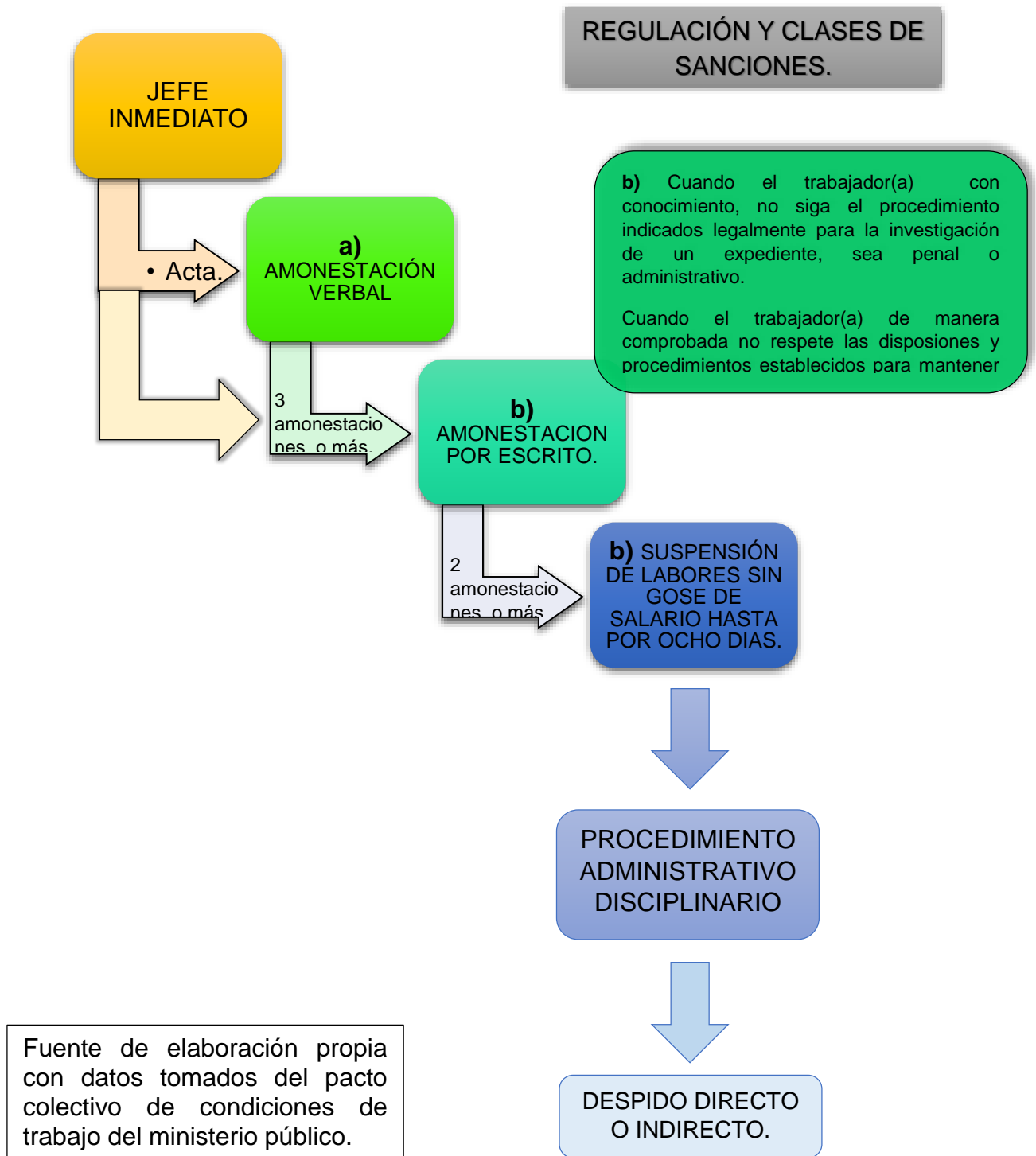
<sup>40</sup> *Ibid.*, Pág. 28.

04)	general de fiscales, para un período de dos años, pudiendo ser reelectos. La elección deberá efectuarse, treinta días antes de concluido el período anterior. La Asamblea General de fiscales será convocada por el Fiscal General y se integra con los fiscales de distrito, fiscales de sección, agentes fiscales y auxiliares fiscales. Cada uno de ellos tendrá un voto. Cada uno de los miembros del Consejo, será electo por mayoría absoluta, y la votación será para cada candidato en particular	DEROGADO
05)	Artículo 20. Sesiones. El Consejo del Ministerio Público deberá reunirse, por lo menos, dos veces al mes. Las sesiones serán convocadas por el Fiscal General de la República o quien lo sustituya. El Secretario del Consejo será el Secretario General del Ministerio Público. El Consejo sesionará válidamente con la asistencia de, por lo menos, cuatro de sus miembros y el funcionario que lo preside. El Fiscal General de la República está obligado a convocar a sesión extraordinaria del Consejo cuando se lo solicitaren por lo menos tres miembros.	DEROGADO
06)	Artículo 21. Informes y opiniones. El Consejo podrá citar al Director de la Policía Nacional y a los funcionarios de los demás órganos de seguridad del Estado para que rindan informes y opiniones. Estos funcionarios están obligados a asistir ante el llamado del Consejo. Los funcionarios que incumplan el requerimiento incurrirán en el delito de desobediencia y serán sancionados de conformidad con la ley. También podrá invitar a los directores de los centros penitenciarios o a cualquier otra persona calificada para que participe en sus deliberaciones, con voz, pero sin voto.	DEROGADO
07)	Artículo 22. Imperatividad. Todos los miembros del Consejo del Ministerio Público están obligados a concurrir a las sesiones del Consejo, salvo causa justificada presentada a los miembros del Consejo. Cada uno de los miembros del Consejo desempeñará el cargo con independencia absoluta. Serán responsables de las resoluciones adoptadas por el Consejo, salvo que hubieren razonado en contra su voto	DEROGADO
08)	Artículo 23. Remuneraciones. La presencia de los miembros en las sesiones del Consejo dará derecho a dietas, que serán determinadas en el reglamento respectivo.	DEROGADO

## 2.10 Pacto colectivo de condiciones de trabajo del Ministerio Público.

Este acuerdo negociado entre el sindicato del ministerio público y los trabajadores no afiliados a los sindicatos, por lo que sus efectos solo cobijan a quienes lo suscriban o se adhieran a él; la Organización Internacional del Trabajo (OIT) le ha recomendado al Gobierno que prohíba la celebración de dichos pactos cuando exista un sindicato.

## 2.10.1 Sanción.



## **2.11 Grupo de Presión.**

Dentro del Ministerio Público se establecieron grupos sindicales que regulan aspectos como: condiciones de trabajo, despidos y demás sanciones, regularizando los lineamientos administrativos para cada trabajador, otorgando un mejor ambiente para enfrentar los procesos y llegar a una mejor resolución del caso.

### **2.11.1 Sindicato ministerio público.**

Artículo 4- Sindicato. “El Sindicato es la persona jurídica integrada por trabajadores afiliados del Ministerio Público, constituida para el estudio, mejoramiento, defensa de sus intereses económicos, sociales y culturales, cuya denominación es la de sindicato de Trabajadores del Ministerio Público – S.T.M.P.”<sup>41</sup>.

Los grupos de personas organizadas dentro de las instituciones como lo son los sindicatos, buscan representar los intereses de cada trabajador así como la defensa de sus prestaciones que por ley le son conferidos, buscando en común acuerdo la celebración de acuerdos o pactos colectivos de condiciones de trabajo.

## **2.10 Renglones de contratación dentro del ministerio público.**

011 Personal permanente. Comprende las remuneraciones en forma de sueldo a los funcionarios, empleados y trabajadores estatales, cuyos cargos aparecen detallados en los diferentes presupuestos analíticos de sueldos.

022 Personal por contrato. Contempla los egresos por concepto de sueldo base a trabajadores públicos, contratados para servicios, obras y construcciones de carácter temporal, en los cuales en ningún caso los contratos sobrepasarán el

---

<sup>41</sup> Pacto Colectivo de Condiciones de Trabajo del Ministerio Público. Guatemala. Resolución Número 90-2005. Emitido el 24 de Septiembre de 2012.



período que dura el servicio, proyecto u obra; y, cuando éstos abarquen más de un ejercicio fiscal, los contratos deberán renovarse para el nuevo ejercicio.

029 Otras remuneraciones de personal temporal. En este renglón se incluyen honorarios por servicios técnicos y profesionales prestados por personal sin relación de dependencia, asignados al servicio de una unidad ejecutora del Estado, y que podrán ser dotados de los enseres y/o equipos para la realización de sus actividades, en periodos que no excedan un ejercicio fiscal.

031 Jornales. Comprende los egresos por concepto de salario diario que se paga a los obreros, operarios y peones, que presten sus servicios en talleres, principalmente en mantenimiento y similares; así como en la ejecución de proyectos y obras públicas, que no requieren nombramiento por medio de Acuerdo y cuyo pago se hace por medio de planilla y la celebración del contrato que establece la ley.

- Tomado del manual de clasificación presupuestaria para el sector público de Guatemala (Acuerdo ministerial 215-2004. Emitida el 30-12-2004).

### **3. Marco legal para sancionar la mala actuación profesional de los empleados y funcionarios públicos.**

#### **3.1 Código penal.**

**Artículo 422.** “El funcionario o empleado público que revelare o facilitare la revelación de hechos, actuaciones o documentos de los que tenga conocimiento por razón del cargo y que por disposición de la ley deben permanecer en secreto, será sancionado con multa de doscientos a dos mil quetzales”<sup>42</sup>. Ya se trate de errores u omisiones humanas, estos pueden producir daños significativos a la institución, por lo que es importante comprender y conocer el marco legal que vela por el estricto cumplimiento de las buenas prácticas profesionales, tal es el caso

---

<sup>42</sup> Código Penal. Decreto Número 17-73. Emitido el 27 de julio de 1973.

del artículo citado que describe la sanción por la revelación de documentos o información que únicamente conoce el personal autorizado.

### **3.2 Entorno de la seguridad en Guatemala.**

Según reportes del INACIF (Instituto Nacional de Ciencias Forenses) en el año 2016 se realizaron un total de 5459 necropsias asociadas a hechos delictivos por lo que Guatemala sigue siendo catalogado como uno de los principales países con más altos índices de violencia del triángulo norte de centro américa.

El secretario general de la ONU se pronunció al respecto ratificando esta información, lo que demuestra que la inseguridad y la violencia que afecta a todos los ciudadanos que ven dañados constantemente su integridad física y material prevalecen desde años atrás.

### **3.3 Opinión sobre el resguardo de la información dentro de las instituciones.**

Metodología utilizada: Entrevista.

- T.U. Mario Guzmán Vidaure, Técnico de escena del crimen del Ministerio Público.

Fiscalía de La Tinta Alta Verapaz

“La información de carácter sensible es un punto que mucho ha sido vulnerado dentro del ministerio público pues cualquiera tiene acceso a la información, partiendo principalmente del compadrazgo de la población con el personal de la fiscalía, influyendo mucho en la fuga de información pues las mismas personas que trabajan en la institución son del lugar donde se ubica y eso la mayoría de veces hace que haya fisuras por las cuales pasan los datos

La falta de medidas de seguridad implementadas hace que también sea difícil tener un control en la institución, sugiriendo a mi criterio la rotación del personal a diferentes áreas, lo cual es complicado por el pacto colectivo pero eficiente en

casos de gran impacto por los antecedentes en otras fiscalías donde se ha tomado dicha medida”.

- Lic. Daniel Mayen, Técnico de escena del crimen del Ministerio Público.  
Fiscalía de Salamá Baja Verapaz.

“Actualmente existen plataformas que registran cada acción dentro del sistema del Ministerio Público, con datos como la contraseña de quien la extrajo información, lo que lleva al usuario y la hora, dando una referencia de quien pudo haber realizado la consulta. Pero que a pesar de ello hay casos que evidencian la fuga de información que ha resultado en investigaciones por parte del departamento de asuntos internos”.

**Análisis:** Según la información que pude recabar durante mis entrevistas el nivel alto de confiabilidad no se respeta, dejando en claro la ineficacia de los sistemas de seguridad actuales. Si bien no se trata de una problemática nueva, su creciente difusión ha permitido tomar mayor conciencia sobre el valor de su información y la importancia de la confidencialidad y la privacidad de la misma.

### **3.4 Contexto de los niveles seguridad en la información sensible.**

Ninguna persona tiene derecho únicamente por virtud de su grado o posición a tener acceso o estar en posesión de información o material clasificado. El material clasificado se confiará sólo a aquellas personas cuyos deberes oficiales requieren el acceso o su posesión. Por lo tanto, todas las personas que requieran el acceso tendrán que ser autorizadas primero para poder recibir material o información clasificada. Todos los individuos autorizados deben ser de una lealtad, integridad y discreción indudable, de excelente carácter y de tales hábitos y asociaciones que no habrá duda de su discreción y sano juicio en el manejo del material o información clasificada.

### Clasificación de seguridad:

Las informaciones y materiales clasificados tendrán las siguientes categorías de clasificación para fines de seguridad:

a) Alto Secreto:

Esta clasificación debe dársele a toda aquella información o material cuya revelación no autorizada causaría un peligro extremadamente grave para la nación.

b) Secreto:

La clasificación de Secreto, debe darse a toda aquella información o material cuya revelación no autorizada pondría en peligro la seguridad nacional, que pueda causar daños serios a los intereses o prestigio de la nación, o que pueda resultar de gran ventaja para una nación extranjera.

c) Confidencial:

La clasificación de Confidencial, deberá dársele a toda aquella información o material cuya revelación no autorizada resultaría perjudicial para los intereses y prestigio de la nación, o pueda ser ventajosa para una nación extranjera, o que pueda causar daños a la institución.

d) Reservado:

La clasificación de Reservado, deberá dársele a toda aquella información o material cuya revelación no autorizada resultaría perjudicial para los intereses o prestigio de la institución.

### Marcaje:

La clasificación asignada deberá estar siempre marcada o impresa, y no escrita a máquina; ésta se debe hacer en la parte superior e inferior de todas las páginas que contengan dicha información clasificada.

El tamaño de las letras, que sean grandes, diferentes a las que contengan el documento, sobresalientes a simple vista y de ser posible de color diferente a la empleada en el mencionado documento.

Cobertura de los documentos clasificados:

Los documentos que sean clasificados como “alto secreto”, deberán ser cubiertos con una hoja de cartulina blanca de tamaño oficio, cuyos márgenes de 25 milímetros de ancho serán de color “Anaranjado”, en la parte superior e inferior llevará en letras de 20 milímetros de alto, la clasificación de “Alto Secreto” y en el centro la siguiente inscripción: “Esta es una hoja para cubrir la información de alto secreto”, tanto la clasificación como la inscripción deberán ser del mismo color del margen de la hoja.

Los documentos que hayan sido clasificados como “Secretos”, “Confidenciales” y “Reservados” deberán cubrirse con hojas de cartulina blanca tamaño carta, cuyos márgenes de 23 milímetros de ancho deben ser de color rojo para cubrir los documentos clasificados como “Secretos”, en azul los clasificados como “Confidencial” y en negro los clasificados como “Reservado”; en la parte superior e inferior de la hoja llevarán la clasificación correspondiente en el mismo color del margen, así como también la inscripción en el centro que indicará: “Esta es una hoja para cubrir información de carácter Secreto (Confidencial o Reservado).

- Proporcionado por Licenciado Marvin Dubon. Ex militar.

### **3.5 Ejemplos a nivel mundial sobre el mal resguardo de la información sensible en materia de seguridad.**

#### a. Vatileaks

Escándalo que tuvo lugar en el vaticano teniendo como principal personaje del caso al papa Benedicto XVI quien fue cuestionado en su gestión como guía de la iglesia católica al filtrarse información al exterior al punto de ser publicados en el

libro denominado **Sua Santita** donde se encontraban numerosos documentos privados como correspondencias personales, planes, confabulaciones, etc.

“El VatiLeaks se desató a primeros de 2012 cuando una televisión italiana publicó unas cartas enviadas por el actual nuncio en Estados Unidos, Carlo María Vigano, al papa en las que denunciaba la "corrupción, prevaricación y mala gestión" en la administración vaticana”<sup>43</sup>, dejando en evidencia la falta de seguridad en las líneas de comunicación, pues incluso circularon rumores sobre el asesinato del papa el mismo año.

Ante tal situación se crearon comisiones pesquisidoras buscando es esclarecimiento el caso que posterior a investigaciones e interrogatorios llevaría a los culpables, siendo estos el ex mayordomo del papa, Paolo Gabriele y el hacker Claudio Sciarpelletti.

#### b. Wikileaks

Se trata de una organización social sin fines de lucro que permitió en su momento publicar información (religiosa, corporativa o gubernamental) de carácter sensible de contribuyentes que mantendrían su seguridad y anonimato al proporcionar datos al sitio web que tendría gran trascendencia e impacto en la sociedad, pues mediante dicha página se dio a conocer en la red un enorme set de más de 250,000 textos de carácter diplomático a cerca de lo que realizaba el departamento de Estados Unidos y sus embajadas por el mundo. La publicación de tal información dejó por primera ocasión a la sociedad conocer a detalle las actividades del gobierno y el contexto en el que se desarrollan las relaciones internacionales, evidenciando sus debilidades y planes.

---

<sup>43</sup> El caso vatileaks, el mayor escándalo del papado de Benedicto XVI. <http://www.abc.es/sociedad/20130211/rc-caso-vatileaks-mayor-escandalo-201302111248.html>, Página consultada el 19 de Junio de 2017.

c. Edward Snowden.

El espionaje es un tema que desde tiempos antiguos se ha llevado a cabo por muchos países que en la actualidad sigue su curso sobre el análisis de fuentes externas e internas de información, por lo que el tema en cuestión es catalogado a nivel mundial como prueba fáctica de ello.

Las manifestaciones sobre el espionaje de la NSA (Agencia Nacional de Seguridad) de los Estados Unidos, hechas por el ex empleado de la CIA Edward Snowden representan para la seguridad una nueva fase, en la que la tecnología es la herramienta principal de espionaje hacia los demás países del exterior e incluso interior.

El interceptar todo elemento de comunicación era una suposición que no tenía fundamento certero y verídico, hasta la gran revelación de programas secretos de vigilancia y demás información clasificada contenidos en más de 15,000 documentos secretos según indico el columnista del diario británico The Guardian, que fueron saliendo a la luz pública, dejando evidencia: el poder ilimitado que puede tener un estado, el atropello a los derechos fundamentales de una persona y la violación de la soberanía del estatal.

d. Panamá papers.

En años de existencia del bufete de abogados Mossack Fonseca, funciono sin represalias ni persecuciones legales por parte de las autoridades, hasta ser descubierto una red creada con la finalidad de ocultar fortunas y evadir impuestos por parte de grandes funcionarios de gobiernos, artistas famosos, jugadores de renombre y empresas a nivel mundial .

“Una enorme filtración de documentos confidenciales ha revelado cómo personas adineradas y poderosas usan los paraísos fiscales para ocultar su riqueza. Once millones de documentos fueron filtrados de una de las compañías más reservadas del mundo, la firma legal panameña Mossack Fonseca. Dichos documentos muestran cómo Mossack Fonseca ha ayudado a clientes a lavar dinero, esquivar

sanciones y evadir impuestos, dejando al descubierto a más de 140 políticos de 50 países, 100 medios en 78 países y 11.5 millones de documentos en paraísos fiscales”<sup>44</sup>. Y todo ello a partir de las fisuras que permiten la fuga de información detectada por una organización de periodistas que realizaron las investigaciones correspondientes hasta llegar a los orígenes e implicados de tal compleja red.

### **3.5.1 Su efecto en el entorno social.**

Los efectos y consecuencias posteriores que puede ocasionar la fuga de información pueden ser varios y de diferente tipo, dependerá de algunos factores como la intencionalidad del hecho, los objetivos que tenía el hechor, entre otros.

En primer plano resaltaría el efecto negativo que tuvo, puesto que se reveló una serie de ilícitos e irregularidades por parte de autoridades superiores y órganos del estado que claramente en los casos anteriormente citados y expuestos deja al descubierto muchos sucesos secretos.

En un segundo plano cabría mencionar las fisuras que evidencian debilidades en la estructura de seguridad de determinada institución pueden convertirse en daños de grandes proporciones, sobre todo cuando datos privados llegan a personas ajenas a la información ocasionando no solo un hecho grave, sino un daño irreparable puesto que quienes la adquieran pueden darle un mal uso, para beneficio personal de algunos que con malas intenciones utilizan la información, hasta el punto de cometer ilícitos penales, así como la mala imagen que buscan que se tenga de la institución al notarse las claras deficiencias.

Al divisarlo desde otra perspectiva, como lo son los incidentes intencionales, “el impacto está más claro: esa información puede ser utilizada para realizar un ataque a la organización, para venderse, para hacerse notorios, para afectar la reputación o imagen de la organización y así mismo puede generar consecuencias a terceros: como pueden ser grupos externos de usuarios y otras organizaciones

---

44 EL TREMENDO ESCÁNDALO DE PANAMA PAPERS RESUMEN Y PRINCIPALES IMPLICADOS. <http://theguiltycode.com/el-tremendo-escandalo-de-panama-papers-resumen-y-principales-implicados/>. Página consultada el 19 de Junio de 2017.



cuyos datos se hayan hecho públicos. En cualquiera de los casos la fuga de información se caracteriza por ser un incidente que difícilmente pueda ser reparado o realizar algún procedimiento que permite volver atrás la situación”<sup>45</sup>.

### **3.6 Métodos más usados en el pasado para filtrar información.**

Espionaje.

El espionaje está constituida como la actividad que se realiza con el fin de obtener información de forma secreta, es decir dar seguimiento a un objetivo en particular con el fin de recabar información de una manera secreta. La persona dedicada a este tipo de actividades es catalogada como espía.

Los orígenes de estas acciones datan de más de 500 años atrás, siendo descritos en la obra liberaría El Arte de la Guerra de Tzu Sun.

Los espías utilizan la técnica de la **infiltración** la cual consiste en introducir a uno de los suyos al lado de los enemigo, ubicándolos en puntos estratégicos que les permita extraer información sobre las actividades, capacidades, planes, proyectos, etc., para fines lucrativos o destructivos.

Otra habilidad utilizada por los espías es la técnica de la penetración, la cual consiste en la colaboración consiente o inocente de un miembro de la organización o grupo contrario con el fin de que proporcione datos e información confidencial del grupo al que éste pertenece. Así mismo resaltan los sobornos como herramienta para la compra de la información requerida

Actualmente existen dos tipos de espionajes a los que se recurre consistentemente, los cuales son:

Espionaje industrial; el cual consiste en la obtención ilícita de información relativa a la investigación, desarrollo y fabricación de prototipos, mediante las cuales las

---

<sup>45</sup> ¿Qué es la fuga de información?. <http://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/>. Página consultada el 30 de Mayo de 2015.

empresas pretenden adelantarse a sus competidores en la puesta en el mercado de un producto novedoso.

Espionaje cibernético; consistente en la práctica u obtención de información privada de usuarios por medio del internet, teniendo como principal herramienta los virus informáticos.

### **3.7 NSA (Agencia de Seguridad Nacional) – Estados Unidos.**

Área anexa al departamento de defensa de los Estados Unidos cuyo objetivo principal es la interceptación de la información que fluye entre otros países, protegiendo la información de carácter sensible y las líneas de comunicación propias, tanto internas como externas.

Fundada por el entonces presidente Harry Truman el 04 de noviembre de 1952 durante el desarrollo de la guerra fría donde se desconocía por el mundo de su fundación y existencia hasta su revelación que sucedió con el pasar de los años, la desclasificación de información secreta y el mejor control por parte del gobierno estadounidense.

“Teóricamente la NSA solamente vigilaría conversaciones de sospechosos con algún interlocutor extranjero pero, al final, parece que el programa se terminó convirtiendo en una grabadora masiva de conversaciones de todos los ciudadanos con la intromisión en las redes de AT&T, Verizon y Bell South y ahora con PRISM también en los players de la red como Google o Facebook”<sup>46</sup>. Por lo consiguiente en torno a la NSA circundan una serie de interrogantes acerca de sus verdaderas actividades y planes ocultos, al no saber con certeza datos básicos como su número de empleados, la ubicación geográfica de sus sedes y divisiones, así como el presupuesto anual que están enmarcados bajo la resaltada palabra **información clasificada**.

---

46 Claves para entender qué es la NSA y a qué se dedica. <https://hipertextual.com/2013/06/que-es-la-nsa>, Página consultada el 01 de mayo de 2017.

## Otros servicios de inteligencia.

- a. Estados Unidos - CIA (agencia central de inteligencia).
  - Posee la principal función de recopilar información de los demás gobiernos por quienes tienen intereses personales, también se enfocan en personas, asociaciones, actividades que se realizan en segundo o tercer plano y seguridad del estado.
  - Fue fundada en 1947, tras el fin de la Segunda Guerra Mundial.
- b. Reino Unido - MI6 o SIS (servicio de inteligencia).
  - Agencia de inteligencia que junto otros organismos de seguridad de la nación operan de manera secreta realizando trabajo de espionaje tal y como su lema lo dice (siempre ocultos) con la finalidad de mantener sus fines en materia de seguridad.
  - Fue fundada en 1992.
- c. Rusia – SVR (servicio de inteligencia exterior).
  - División del servicio de seguridad encargada de velar por la seguridad exterior del país. Esta es la continuidad de la controversial policía secreta KGB, que realizo sin fin de actividades que hasta la fecha son historias de las cuales no se tiene certeza verídica.
  - Fue fundada en 1991.
- d. China – MSS (ministerio de seguridad del estado).
  - Organización de seguridad considerada como el más importante puesto que posee la suficiente autonomía como para realizar sus actividades sin mayor restricción, siempre y cuando corresponda a su competencia.
  - Fue fundada en 1983.

- e. Israel – Mossad (instituto para la información y las operaciones especiales).
  - Agencia en la que las acciones que la caracterizan se realizan en cubierto, pues su trabajo de espionaje va incluso a actividades paramilitares que atentan contra la seguridad estatal.
  - Fue fundada en 1949.
  
- f. India – RAW (ala de investigación y análisis).
  - Dedicada de igual manera a actividades de recolección de información que permita tomar medidas contra el terrorismo y demás amenazas del estado y sus habitantes.
  - Fue fundada en 1968.
  
- g. Pakistán – ISI (directorío para la inteligencia inter servicios).
  - Posee objetivos más centrados de interés pakistaníes, como lo es la constante vigilancia y análisis de acontecimientos políticos, también le corresponde el monitoreo de actos militares de los países aledaños.
  - Fue fundada en 1948.
  
- h. Alemania – BND (servicio federal de inteligencia).
  - Agencia de inteligencia que en conjunto a otros órganos internos de seguridad, realizando actividades preventivas estableciendo mecanismo de alerta para la gestión de contramedidas hacía el peligro latente de grupos terroristas u otros que posean los mismos fines.
  - Fue fundada en 1956.
  
- i. Australia – ASIS (servicio secreto de inteligencia australiano).
  - Al denominarse como servicio secreto es claro que sus acciones también están encaminadas a realizan de manera oculta trabajo en

la interceptación de las fuentes de información que fluyen en el exterior.

➤ Fue fundada en 1952.

j. Francia – DGSE (dirección general de seguridad exterior).

➤ Realiza primordialmente acciones de contrainteligencia y paramilitares en el exterior previendo actos que atenten contra la seguridad nacional y demás intereses propios.

➤ Fue fundada en 1982.

### **3.8 Desafíos en materia de seguridad en Guatemala.**

El contexto de la seguridad en Guatemala está relacionado directamente con su posición geográfica, la poca presencia de instituciones del Estado en todo el territorio nacional, la porosidad de sus fronteras terrestres, la falta de capacidad de control de su espacio aéreo y marítimo, la narcoactividad, el lavado de activos, el terrorismo, la trata de personas, el tráfico de armas, municiones y explosivos y el contrabando. En relación con la frontera con México, es relevante mencionar el desplazamiento de los carteles de la droga mexicanos hacia nuestro territorio con el propósito de controlar las rutas logísticas para el trasiego hacia el norte, al provocar que ciertas zonas territoriales cuenten con fuerte presencia de dichas organizaciones, ejercer presión para el control social e incentivar acciones de ingobernabilidad para limitar la presencia de la autoridad del Estado.

➤ **Conflictividad social.** El nivel de desarrollo desigual e insuficiente, aunado a la incertidumbre jurídica de la tenencia de la tierra; la poca disponibilidad de tierra cultivable; la degradación y explotación de los recursos naturales y estratégicos, generan conflictividad constante por los diferentes enfoques de atención y solución a las demandas y necesidades de la población.

- **Deterioro de la Gobernabilidad.** Se produce cuando, por la ineficiencia del actuar del Gobierno en el cumplimiento de los Objetivos Nacionales, en la población se erosiona la legitimidad de la autoridad pública, se pierde la confianza y el apoyo al sistema político.
  
- **Debilidad institucional.** Guatemala presenta características de Estado débil. Las instituciones del Sistema Nacional de Seguridad y Justicia están desacreditadas por los rasgos de ineficiencia, corrupción e impunidad, lo cual ha reducido la confianza de la población y ha propiciado la evolución criminal. La ausencia del Estado en algunas regiones del territorio nacional, propicia un ambiente de caos favorable para que las organizaciones criminales se desarrollen y ejerzan el poder local. Fronteras porosas. El flujo migratorio de indocumentados y el contrabando. Desastres naturales, sociales y tecnológicos. El territorio nacional es altamente vulnerable por su ubicación geográfica, que se agrava por la situación social, económica y los bajos niveles de desarrollo, altos índices de pobreza, inequidad y exclusión social. En este campo, el país tiene como problema principal la falta de ordenamiento territorial que provoca invasiones ilegales y conflictos sociales, que obliga la intervención de las fuerzas de seguridad. Pandemias, epidemias y endemias.

La situación de inseguridad prevaleciente en el Estado de Guatemala, descrita en párrafos anteriores, plantea al Gobierno y a los diferentes Organismos estatales retos y desafíos importantes, destacando entre otros: REFORMAS LEGALES Los cambios estructurales que se deben realizar en las instituciones del Sistema Nacional de Seguridad, parten de las reformas a las siguiente leyes: Ley de la Policía Nacional Civil (reforma de la PNC, crear la Policía de Investigación Criminal), Ley del Sistema Penitenciario (creación del Instituto Nacional de Cárceles y Rehabilitación) y Dirección General de Migración (crear el Instituto Nacional de Migración y Naturalización). Estos cambios deben realizarse en consonancia con el Pacto para la Paz, la Seguridad y la Justicia y el Acuerdo para

el Nacional para el Avance de la Seguridad y la Justicia, propuesto para ser suscrito por los tres organismos de Estado y el Ministerio Público.

### **3.9 Prevención.**

#### **3.9.1 Ejes de trabajo.**

a. Individual:

- Dentro de las fases de contratación se debe implementar una etapa de evaluación ética y moral donde psicólogos evaluarán a través de test, el nivel de confiabilidad del personal hacia la institución, previendo la protección y buen manejo de información sensible.

Ejemplos de Test de confiabilidad.

#### **Test grafico de conductas desadaptativas (GRACODE)**

Factores de Medición

Inteligencia, Autoconcepto, Creatividad, Independencia, Sociabilidad, Productividad, Energía, Agresividad, Superación, Organización, Toma de Decisiones, Calidad de Trabajo, Estabilidad Emocional, Satisfacción, Conflicto y Pronóstico Laboral ( Mentira por maldad ).

#### **Dicha evaluación maneja 2 niveles de interpretación:**

El primero de ellos se basa en la exclusiva interpretación de las conductas negativas del evaluado, es decir, solo aquello que perjudique su adecuada interacción social y su estabilidad emocional.

El segundo nivel interpreta de manera más completa al evaluado ya que integra al primer nivel y adiciona todo el recurso y/o potencial que usa la persona para su dinámica social, personal y familiar, además de poder indicarnos todas las capacidades dormidas del sujeto, es decir, el potencial que el mismo evaluado puede desconocer que posee.

## **Clasificación**

Es una evaluación de tipo proyectiva de la rama descriptiva, sin embargo, su metodología de calificación en el primer nivel le permite ser calificada de una forma cuantitativa por ausencia – presencia

## **Tiempo de aplicación**

En promedio la prueba se aplica en 20 minutos, sin embargo, no maneja tiempos mínimos ni límites.

## **Áreas de aplicación**

Selección y evaluación de personal, evaluación psicométrica clínica, autoconocimiento de conductas desadaptativas, en el caso de la interpretación de segundo nivel la prueba puede ser aplicada para un sinnúmero de objetivos: Orientación vocacional, Promociones laborales, estudios de personalidad, peritajes, etc.

## **Material de aplicación**

- Hojas blancas tamaño carta, blancura estándar
- Bolígrafo marca BIC de punto mediano color negro
- Lápiz con punta, del número 2

## **Instrucciones de aplicación**

Se le proporciona al sujeto evaluado el lápiz y una hoja blanca en sentido vertical, dando la siguiente indicación: “por favor dibuje a una persona de cuerpo completo”, en caso de existir algún cuestionamiento por parte del sujeto se le responderá: “como usted guste”, “no es para un concurso de dibujo”, “dibuje como a usted más le plazca”.

Una vez finalizado el dibujo movemos dicha hoja hacia el costado izquierdo del evaluado, le proporcionamos una nueva hoja (con la misma orientación que la primera) y el bolígrafo, retirando de la mesa el lápiz. Es importante verificar que el



primer dibujo del sujeto este visible al evaluado, ya que este le servirá como referencia gráfica, la cual nos elevara el nivel proyectivo de la grafología.

Una vez colocada en la mesa la segunda hoja y el bolígrafo se le dará la siguiente instrucción: “ahora en esta hoja, quiero que por favor me redacte una historia de la persona que usted dibujo (señalando el dibujo que se encuentra a un costado)”

En caso que el sujeto llenase la primera página de la hoja con su historia y necesite continuar escribiendo; se le proporcionara otra hoja para continuar su historia, tratemos de evitar su escritura en ambos lados de la hoja, ya que puede decrementar el nivel de interpretación de nuestra prueba.

Una vez terminada la historia se le pide al sujeto que firme la hoja, en caso de existir algún cuestionamiento se contestará: “donde usted guste”.

Una vez realizada la firma se le indica que escriba su nombre (en la hoja de la historia), en caso de existir algún cuestionamiento se contestará: “donde usted guste”.

Finalizando la evaluación, agradecemos al sujeto su tiempo y colaboración.

### **Aspectos a considerar durante la realización de la prueba**

Teniendo conocimiento del nivel proyectivo de los dibujos y grafismos, se toma en consideración ciertas conductas y/o actitudes tomadas por el sujeto evaluado, ya que estas son sin duda una expresión de los mecanismos de defensa utilizados.

1. Actitud ante la prueba
2. Conducta durante la prueba
3. La rapidez con que se dibuja
4. Sombreados, retoques, borraduras.
5. Las omisiones

## **Instrucciones de calificación**

Para la calificación se cuenta con 4 hojas de puntuación por presencia.

Las hojas de calificaciones cuentan con tablas de 3 columnas: ÍTEM, TIPO Y P/A, para iniciar la puntuación tomamos en primer lugar la hoja de dibujo y marcamos (con plumón) en las hojas de calificación en la columna de P/A los ítems presentes en la prueba del evaluado, una vez calificado el dibujo continuamos con la hoja de grafología con el mismo procedimiento.

Una vez calificada toda la prueba se giran nuestras hojas de calificación para poder visualizar la interpretación de cada uno de los ítems puntuados, los cuales ya se encontrarán marcados automáticamente, esta información nos será útil para poder realizar la integración del reporte, para poder enriquecer el mismo a continuación se describe de forma detallada la interpretación y los puntos principales a considerar.

<https://www.gestiopolis.com/seleccion-de-personal-como-medir-la-honestidad-productividad-y-responsabilidad/>

Por favor, responda con franqueza a las siguientes cuestiones.

		Totalmente de acuerdo	De acuerdo	Ni a favor ni en contra	En desacuerdo	Totalmente en desacuerdo
1	Recelo de los demás	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	No confío en la gente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	Creo en la bondad humana	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	Confío en los demás	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	Sospecho que los demás esconden motivos ocultos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	Me fío de lo que la gente dice	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	Pienso que todo funcionará	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	Creo en las buenas intenciones de los demás	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	Creo que la gente básicamente sigue una moralidad	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	Creo que la gente es fundamentalmente malvada	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Restablecer

<http://www.psicologia-online.com/test/confianza/>

Evaluar

- Implementación esporádica de pruebas que evalúen la capacidad y desempeño de cada empleado a fin de monitorear y mantener un rendimiento eficiente.

b. Institucional: ¿Como la institución reservan los casos de gran impacto?

Trabajando cada caso de manera reservada por parte de un departamento en específico de la institución que puede llevar a cabo los análisis herméticamente teniendo como herramienta principal un servidor exclusivo donde toda la información fuera centralizada. Cada computadora estaría configurada para ser una estación de trabajo donde toda la información fuera directamente al servidor en la nube, teniendo en cuenta que la fluidez de los datos fuese hacia el servidor únicamente y no viceversa. Parte de la protección estaría asignada a cortafuegos y demás software de defensa de tal manera que solo el administrador de bases de datos pudiera acceder a ella con permisos especiales.

c. Social: ¿Cómo la información no debe fluir a los medios de prensa cuando es demasiado sensible?

La implementación de una unidad de monitorio mantendría informada a la institución a cerca de la información que está fluyendo en el exterior, permitiendo tomar medidas como lo pueden ser los comunicados de prensa donde estaría dándose información veraz y certera del acontecer de ciertos casos.

### **3.10 Investigación.**

#### **3.10.1 Sistemas de seguridad de la información.**

“**La seguridad** es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como **peligro o daño**

todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen”<sup>47</sup>.

A diario las amenazas que ponen en peligro la integridad de la información y con ello la viabilidad de sus funciones en la circulación que este tiene dentro de la estructura de determinada institución, son latentes y se mantienen constantes, pues los riesgos provienen no solo del exterior sino también del interior.

Con ello surge la pregunta, ¿Por qué es tan importante la seguridad de la información?, un cuestionamiento muy frecuente que lleva a pensar en los debidos parámetros de seguridad que se deben de manejar, pues mantener la información segura otorga una buena reputación y credibilidad ante la sociedad que confía en que sus datos y demás procesos que se manejan internamente, permanezcan de la misma manera.

#### a. Sistemas informáticos.

Un sistema es un proceso y actividad particular que desarrolla la empresa con cuya finalidad será resguardar la información de la empresa. La importancia de los sistemas informáticos es que los elementos de la misma estén bajo ciertos métodos de prevención y monitores continuo.

Algunos sistemas informáticos de protección son:

- Firewalls: Sistema ubicado estratégicamente entre dos redes que tiene como objetivo el cumplimiento de una política establecida. En otras palabras su finalidad se enfoca a la protección contra amenazas que se encuentra en redes desconocidas.

---

<sup>47</sup> Asociación Española Para La Calidad. Seguridad de la Información. 2016. <http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion>. Página consultada el 17 de abril de 2016.

- Contraseñas robustas: Para el resguardo la información sensible de la institución, teniendo en cuenta el cambio periódico de ellas así como el uso de una serie de números y símbolos que dificulten su vulneración.
- Lista de Control de accesos: “Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios”<sup>48</sup>, proporcionando así un historial de todas las actividades realizadas por el personal en su estación de trabajo.
- Criptografía: En la prevención contra la posibilidad de que información de carácter sensible llegue a terceras personas con malas intenciones, se utiliza este método para la codificación de los mensajes e información, dando como resultado datos que solo están visibles a personal autorizado.
- Antivirus: Aplicaciones con filtros de seguridad dentro de su funcionamiento de escaneo y muro cibernético que impide el ingreso de virus o bombas informáticas capaces de extraer información, espiar y nadar los sistemas informáticos.

b. Sistemas físicos.

Está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema, por eso necesario evaluar y controlar permanentemente la seguridad física puesto que solo de esta forma se logra integrar la seguridad como función primordial del mismo. Para esto también se tiene dentro de la seguridad física, distintos aspectos que pueden brindar seguridad tanto a las personas como a los equipamientos,

---

<sup>48</sup> SEGU.INFO, <http://www.segu-info.com.ar/proteccion/proteccion.htm>, Página consultada el 20 de Junio de 2017.

además de la continuidad operacional. Algunos de estos elementos se mencionan a continuación:

#### Accesos Físicos.

- Guardia, que estaría catalogado como el primer filtro de seguridad.
- La segunda etapa de seguridad estaría constituida por tarjetas de visitas o magnéticas, en que indique a que piso se dirigen y les permita el acceso solamente al piso o sección indicada.
- Identificación e identificación de áreas restringidas y áreas públicas.
- Circuitos cerrados de televisión y sensores de movimiento que mantendrían vigilancia continua mientras crean una prueba en su tiempo de grabación de cualquier suceso anómalo.

Estas medidas de seguridad se encuentran al alcance de las instituciones tengan los recursos económicos necesarios, pues tiende a ser onerosa la inversión, debiéndose analizar la rentabilidad y el nivel de seguridad a ser obtenido.

Por lo anterior es necesario establecer la seguridad física un sistema informático que sea consistente en donde la aplicación enfrente amenazas físicas al hardware y software del equipo.

Lo primero que se debe tener en cuenta es la protección física de los diferentes equipos del sistema informático. Cualquier equipo en general, y con especial atención, los servidores y hardware de red, deben situarse en recintos protegidos para que solo el personal autorizado tenga acceso a ellos.

Los mecanismos aplicables varían desde una habitación con una cerradura y llave, a los más sofisticados mecanismos de acceso por huella digital, cámaras de seguridad y guardias que reaccionen ante violaciones de la política de acceso estos dos últimos más bien se deben englobar como sistemas de detección.

### 3. 11 Inserción.

#### 3.11.1 Clasificación de las áreas del ministerio público por niveles de acceso.

Se contempla dentro de esta política la clasificación de las áreas del ministerio público que resguarden información de carácter sensible, con el objetivo de poseer una mejor estructura de seguridad que permita más control y un registro de quien interactúa con la información.

Bajo.	Medio.	Alto.
- Delitos con penas menores a 8 años de prisión.	- Estructuras criminales.	- Casos de gran impacto social.
Se someterá a la persona autorizada a ingresar a esta área un registro físico en busca de teléfonos, u otros dispositivos.	Todo trabajador que tenga acceso a esta área deberá ser sometido a un filtro de seguridad donde será ingresado a una cámara que permita la detección de dispositivos electrónicos que pueden ser utilizados para la extracción de información.	
- A partir de la calificación de las áreas de la institución, se hará de igual manera con el personal, otorgándoles tarjetas magnéticas con información individual y grados de acceso a ciertas áreas con determinada información.		

#### 3.12.1 Resultados en perspectiva sobre la aplicación de esta política.

- Mejores empleados: El cual da inicio con la selección del personal, puesto que son sometidos a una rigurosa etapa de filtros que garantizan su idoneidad en los puestos que desempeñarán, seguido de la orientación, cuyo proceso es de vital importancia puesto que son considerados como uno de los principales pilares de una institución en cuanto a la protección que pueden brindar, iniciando por el conocimiento y comprensión profunda de la información que cada empleado tiene a su cuidado. Por lo que se considera



urgente su inmersión dentro de las políticas de seguridad y demás medidas, desde el primer día, no olvidando el monitoreo continuo de los tipos de datos que genera y utiliza en su área, como también el conocimiento acerca de los encargados de gestionar los distintos tipos de información.

- Mayor seguridad en el trabajo: Puntos débiles en las políticas de seguridad pueden convertirse en problemas de proporciones inimaginables, sobre todo cuando datos confidenciales pasan a personas no autorizadas, por lo que la implementación de esta política proporcionara un grado mayor en los esquemas de seguridad.
- Reducción en el índice de investigaciones internas por fuga de información dentro de la institución.
- Mayor credibilidad en la institución que será capaz de trabajar los casos con de manera más cautelosa y privada, manteniendo el hermetismo al no dejar fluir la información de carácter sensible al exterior.
- Mejor estructura y orden en los esquemas de seguridad al clasificarse las áreas de la institución que requieren de cierto grado mayor o menor de autorización.

#### 4. Conclusiones.

Mejorar los parámetros de seguridad para ser considerados de vital importancia dentro del contexto de la fuga de información, dándole un valor alto de confiabilidad al individuo que manipula los datos de carácter sensible, lo cual propiciaría la creación de entorno confiables, siempre y cuando se implementen políticas que atacaran los diferentes enfoques (físico, informático y administrativo) de la problemática.

Fortalecer y empoderar al **elemento humano**, evitando que por negligencia u omisión cometa algún delito dentro de la institución. “De cualquier manera, dada la imposibilidad de monitorear a las personas más allá de la esfera laboral, es estrictamente necesario que exista un alto grado de concientización y que las políticas de seguridad estén correctamente aplicadas para garantizar que quienes manejen información confidencial tengan asumidos los riesgos relacionados con su filtración”<sup>49</sup>.

Se definen tácticas efectivas que aseguren un manejo adecuado de los procesos que se realizan con la información a fin de darle mayor resguardo y al mismo tiempo un constante control, con la finalidad de mejorar los sistemas establecidos, actualizándolos constantemente pese al crecimiento exponencial de las tecnologías que día con día van en constante desarrollo.

Actualizar estándares, códigos de buenas prácticas, desarrollos de políticas en seguridad, desempeño y confiabilidad, entre otros, con motivo de resguardar unos de los elementos más valiosos de la institución, como lo es su información, elemento clave para su funcionamiento eficaz y eficiente, mejorando así la prevención, investigación y persecución penal.

---

<sup>49</sup> Federico Pacheco, Gerente de Investigación y Educación de ESET Latinoamérica **Fuga de información: ¿una amenaza pasajera?**. [http://www.welivesecurity.com/wpcontent/uploads/2014/01/fuga\\_de\\_informacion.pdf](http://www.welivesecurity.com/wpcontent/uploads/2014/01/fuga_de_informacion.pdf). Página consultada el 01 de Junio de 2017

Incluir dentro del informe de labores anual del ministerio público los resultados de la auditoria sobre las capacidades y desempeño del personal, permitiendo esto la consideración de una depuración o capacitación de los mismos, así como el mejoramiento de los filtros de contratación de nuevos trabajadores.