**INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO**

**FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS**

**ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN**

**GRUPO DE INVESTIGACIÓN FICB-PG**

# "SISTEMA DE ACCESO Y CONTROL PARA EL ÁREA DE GESTIÓN DOCUMENTAL POR SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO (HUELLA DACTILAR E IRIS)

**PRESENTA:**

**CAÑÓN, OSCAR IVÁN (172010262)**
**CUELLAR CASTRO, ALONSO (1712010164)**
**CÓDIGO**

**ASESOR TEMÁTICO:**

**JAIMES FERNÁNDEZ, WILMAR**

**ABRIL 2018**

**CONTENIDO**

PÁG.

# RESUMEN

El presente estudio propone la implementación de un sistema de control de acceso para área de gestión documental del Departamento de Policía de Mocoa (Putumayo) que funcione a través de dispositivos biométricos de huella dactilar e iris, asi como la implementación de cada opción tanto a nivel físico (instalaciones), de hardware y software. El enfoque del estudio es mixto (cualitativo y cuantitativo) abordado a partir del aspecto de la seguridad de la información. En este sentido, se establecieron unas variables que fueron vinculadas entre sí para analizar los distintos puntos de vistas de los diferentes actores que hacen vida en el departamento de policía y que tienen una relación directa con el objeto de estudio. La finalidad de las preguntas realizadas y del planteamiento en general, tenía que ver con conocer si las personas (muestra elegida) consideraban necesaria la ejecución de un sistema de seguridad que permita tener el control, seguimiento y evidencia del acceso de los tanto de los uniformados como de personal civil al área de gestión documental.

De igual manera el estudio a través de los resultados permite detectar que las fallas encontradas en seguridad no solamente recaen sobre el área de gestión documental pues hay no existen políticas de seguridad, anexas a la dependencia. siendo así los sistemas de computo. Rack, backbon, tableros eléctricos están fuera de la misma y existe un riesgo y/o amenaza en la manipulación de éstas, pues permite que cualquier persona que ingrese al edificio pueda tener acceso, no existen cuartos separados o con seguridad, resultados que fueron obtenidos a partir del uso de herramientas de diagnóstico, para la seguridad de la información en espacios físicos, (instalaciones) en equipos físicos hardware y a nivel lógico,

Muchas de las opciones de respuesta a la seguridad son el resultado de las respuestas previo análisis de la información recolectada así como la lluvia de donde se evidencia que estos resultados comprueban que la seguridad de la información es fundamental dentro del Comando de Policía y más aún en el área de gestión documental, para del departamento de policía, se debe saber que uno de los activos de mayor protección es el área de gestión documental pues ahí reposa información de carácter confidencial necesario para el buen desarrollo de las actividades institucionales, datos sensibles que pueden afectar el buen funcionamiento de los procesos internos y perjudicar la imagen de la Institución, y colocar en riesgo la vida de los funcionarios.

## ABSTRACT

This study proposes the implementation of an access control system for the documentary management area of the Mocoa Police Department (Putumayo) that works through biometric fingerprint and iris devices, as well as the implementation of each option both at the physical (facilities), hardware and software. The focus of the study is mixed (qualitative and quantitative) addressed from the aspect of information security. In this sense, some variables were established that were linked together to analyze the different points of view of the different actors that live in the police department and that have a direct relationship with the object of study. The purpose of the questions asked and the approach in general, had to do with knowing if the people (sample chosen) considered necessary the execution of a security system that allows having control, monitoring and evidence of the access of both the uniformed as of civilian personnel to the area of documentary management.

In the same way, the study through the results allows to detect that the failures found in security do not only fall on the document management area as there are no security policies, attached to the unit. thus being the computer systems. Rack, backbon, electrical boards are out of it and there is a risk and / or threat in the handling of these, because it allows anyone entering the building to have access, there are no separate rooms or with security, results that were obtained from the use of diagnostic tools, for the security of information in physical spaces, (facilities) in physical hardware and at the logical level,

Many of the security response options are the result of the responses after analyzing the information collected as well as the rainfall where it is evident that these results prove that information security is fundamental within the Police Command and even more in In the area of document management, for the police department, it should be known that one of the assets with the greatest protection is the area of document management, since there is confidential information necessary for the proper development of institutional activities, sensitive data that can be affect the proper functioning of internal processes and damage the image of the Institution, and place at risk the lives of officials.



PALABRAS CLAVE

Seguridad, Información, Control de Acceso Biométrico e iris.

KEY WORDS

Security, Information, Access Control and Biometric

## INTRODUCCIÓN

La seguridad dentro de un área, tanto física, como la seguridad en informática, debe establecer mecanismos de control y controles sobre los usuarios, personal interno y externo, procesos y procedimientos que registre cada operación llevada por el usuario como por la máquina. Esta seguridad es la piedra angular de la empresa ya que de ella dependerá la prevención del riesgo y la maximización de la vulnerabilidad.

La disposición de la información al usuario final, como su integridad dependerán de la confidencialidad que exista entre los procesos llevados a cabo por los operarios y los procesos a nivel de hardware y software que giran en torno a al uso y reusó de la información, su éxito dependerá si se considera a la información como un recurso critico dentro del desarrollo de la organización.

La carencia de personal, su tipo de vinculación y su relación directa o indirecta con la información son responsabilidad de la organización y es ésta quién debe aplicar las políticas de seguridad, políticas de seguridad claras y mecanismos de control que coadyuven al mantenimiento y resguardo tanto del espacio físico como de los datos, el acceso de personal y la manipulación de los mismos, ya sean por llaves, medios magnéticos o sistemas cloud computing

El acto de tomar acciones contra éstos riesgos o amenazas, definirá si se está preparado para desarrollar acciones que permitan establecer controles efectivos y eficientes. Uno de ellos son los sistemas biométricos por reconocimiento de huella dactilar e iris, los cuales deben ser implementados para reforzar el control de acceso y que permitirá habilitar, limitar o denegar el ingreso al área de gestión documental..

Es por ello que la intención de la presente investigación no es otro sino brindar las medidas de seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad de la información, que reposa en el área de gestión documental,

mediante la implementación de los siguientes elementos físicos, cámaras de seguridad, puertas de seguridad y un sistema de control de acceso por reconocimiento biométrico de huella dactilar e iris que minimizarán las fuentes de riesgos y protegerá al área de gestión de documental del Departamento de Policía del Putumayo, de cualquier amenaza externa o interna, que pretenda hacerse con la información de manera ilegal.

## 1. PROBLEMA

No existen políticas de seguridad asociados a la parte física y lógica que impidan el acceso de personal no autorizado del área de gestión documental

### 1.1 Descripción del problema

En el departamento de policía de Mocoa (Putumayo), no se evidencia ningún tipo de seguridad asociado a la parte física y lógica, así como un sistema de control de acceso que impida el acceso tanto a particulares como uniformados el ingreso de los uniformados al área de gestión documental, Su acceso se realiza de forma manual y sin ningún control., no existe un control de acceso ya este se realiza de forma manual (puesta de chapa)

La seguridad no es algo nuevo ni producto de los avances tecnológicos, pero sí ha cobrado mayor importancia desde la aparición de éstos cada día en todos los ámbitos, son más los elementos que debemos proteger y esto a causa de la digitalización. Antes, por ejemplo, si usted quería saber el saldo de su cuenta bancaria, debía dirigirse hasta el banco, hacer una larga fila, etc. Sin embargo, en la época actual, usted puede no sólo consultar su estado de cuenta, sino que podría hasta comprar un barco, si así lo quisiera.

El alcance que tienen los avances tecnológicos, gracias al poder de la red de redes cualquier dato puede estar al alcance de nosotros, a tan sólo un click de distancia. Sin embargo, esto presupone también un riesgo y todo riesgo debe ser prevenido y llevado a su mínima expresión. ¿Esto qué quiere decir? Pues

volviendo al ejemplo de la revisión de la cuenta bancaria on line, los datos personales del usuario están expuestos, son datos son sensibles de sufrir un ataque cibernético. Alguien podría hacerse con la información de la cuenta y modificar los datos (en el mejor de los casos) o hurtar el dinero del usuario.

En este sentido, las organizaciones y empresas, ya del ámbito público o privado, son conscientes del hecho de que actualmente, el mundo está siendo dominado tanto por la tecnología como por la información; siendo esta última la gran protagonista ya que, si bien la tecnología coadyuvó a que la información estuviese al alcance de todos, es esta última, el arma con la cual se pueden construir o destruir imperios. Quien controla la información, controla el mundo.

En consonancia con lo anterior, la Seguridad de la Información, pasa a ser uno de los principales objetivos de estas empresas u organizaciones, que incluso, han hecho de la seguridad, su lema principal. Llegando a vender a sus clientes, junto con todos los productos o servicios que caracterizan su marca, confianza, confidencialidad y permanencia de la información.

Hoy en día, hay organizaciones con un control de acceso estricto, que comienza desde la identificación del visitante hasta la prohibición del acceso a ciertas y determinadas zonas. Este control se realiza por medio de personas y de sistemas (controles físicos y lógicos). Las más grandes corporaciones, hacen restricciones dentro del mismo personal, éstas pueden ir, por ejemplo, desde limitar quién puede o no ingresar a una computadora, o a la restricción para navegar por determinadas páginas web. El nivel de seguridad va a depender del valor del activo que se deba cuidar. Este valor es asignado por la organización.

Cada día, son más las empresas que se suman a la adquisición e implementación de sistemas de seguridad cuya complejidad varía de acuerdo a las necesidades de la empresa. Esta seguridad puede ser lograda a través de cerraduras magnéticas que se controlan por tarjetas (HID), cerraduras tipo BEST, puertas de seguridad encriptadas; entre otros. Lo importante es, proteger la información y dar a sus usuarios la tranquilidad que necesitan para que continúen operando con normalidad.

Unas de las opciones de seguridad más recomendadas por su alta eficacia, son los sistemas por reconocimiento biométricos. Gracias al uso de este tipo de sistemas, es posible identificar a los usuarios por medio de características o rasgos que son particulares para cada individuo. Van desde lo más simple (reconocimiento de hulla dactilar) hasta lo más complejo (combinación de reconocimiento facial, iris, retina, voz; etc.)

Establecer un control de acceso con sistemas biométricos permite a quien lo aplica, mantener la información lejos de amenazas que atenten contra la integridad de la misma; es decir, que se mantenga siempre fiel y exacta, sin sufrir ningún tipo de alteración. Garantiza así mismo, que ésta pueda estar disponible para el momento que sea requerida. Y finalmente, cumple con la razón de ser de un sistema de seguridad, que es la confidencialidad de la información, que es lo que busca todo usuario, que sus datos se mantengan seguros y lejos del alcance de personas cuyas intenciones no sean las más convenientes para la organización.

Sin embargo, a pesar de que está demostrado suficientemente, que la seguridad de la información debe ser una prioridad para cualquier organización, no siempre se invierte en ésta o se aplican las medidas necesarias para que la información esté protegida. El hecho de que una organización, carezca de un sistema para controlar el acceso que tienen las personas (sean miembros o no) a la información, resulta altamente perjudicial para el desarrollo de sus actividades. Más aún cuando se trata de una entidad pública cuyo propósito principal, es brindar seguridad.

Desafortunadamente, es el caso que se presenta en el Departamento de Policía del Putumayo. Conforme a lo que se ha observado, este departamento cuenta con un área de gestión documental en la que reposa toda la información que se genera en la policía; ésta es almacenada tanto en físico como en digital, según sea el caso.

No obstante, y a pesar de que en este departamento se cuenta con una estricta política para el manejo y/o divulgación de la información, existen falencias en

cuanto a la seguridad pues no existen políticas propias de acceso y control a la seguridad de la información a nivel físico, de hardware ni lógico de software, ya que no se dispone de sistema de acceso y control que permita regular el ingreso y salida del personal y documentos al área de gestión documental, representando una fuente de riesgo que debe ser reconocida como tal y debe aplicar los correctivos necesarios para evitar que la información ahí contenida, sea manipulada (modificada, sustraída o alterada de cualquier forma) por personas cuyos fines puedan perjudicar la transparencia de las tareas y procesos llevados a diario. Por ejemplo, puede suceder que alguien tome un expediente, lo reproduzca con propósitos no honorables, como: publicación en la web, intento para favorecer a un tercero, chantaje, entre otros. Vulnerar la confidencialidad de la información y exponerla, puede ocasionar el desprestigio de todo el departamento.

En este orden de ideas, existe vulnerabilidad en la seguridad de la información, del Comando de Policía del Putumayo de ahí que se propone llevar a cabo un estudio de diagnóstico y presentación de una propuesta como salida de datos para su implementación.

Este sistema, es totalmente factible a ejecutarse en menos de un año debido a que el costo de la inversión es totalmente manejable para el Departamento. Además, entre todas las ventajas que aportaría, está el hecho de que no sólo se encargará de restringir el acceso al área de gestión documental, sino que también permitirá generar una base de datos con los rasgos de las personas que según su perfil, sean autorizadas para ingresar al área de gestión de documentos y se podrá contar con un registro que indicará quién accedió al área y por cuánto tiempo, todo en aras de mantener la trazabilidad de la información y poder establecer responsabilidades, si así fuera el caso.

**Pregunta de la Investigación:** ¿Es consciente el personal del departamento de Policía del Putumayo, de la necesidad que se tiene de la implementación de un sistema de seguridad que permita el control y acceso al área de gestión

documental, basado en el reconocimiento de huellas dactilares y seguridad de la información.?

## 2. OBJETIVO GENERAL

Proponer la implementación de un sistema de seguridad basado en políticas de seguridad a nivel externo e interno así como el reconocimiento biométrico por huellas dactilares, que permita establecer un control de acceso al área de gestión documental, en el Departamento de Policía de Mocoa -Putumayo.

### 2.1 objetivos específicos

- Levantamiento de información y diagnóstico de la situación actual del área de gestión documental del Departamento de Policía de Mocoa, Putumayo.
- Elaborar la propuesta para la implementación de un sistema de seguridad a nivel físico por reconocimiento biométrico de huellas dactilares, y lógico en el área de gestión de documentos en el Departamento de Policía de Mocoa, Putumayo.
- Concientizar a los ejecutivos de alto nivel del Departamento de Policía Mocoa – Putumayo del riesgo al que se expone la organización en caso de no tomar medidas y de que la seguridad de la información del área de gestión documental es responsabilidad de todos, a través del análisis y resultados encontrados en el presente estudio de investigación.

## 3. JUSTIFICACIÓN E IMPORTANCIA

Teniendo en cuenta la importancia que tiene el área de gestión documental, a través de su rol de ser de máxima seguridad por la información que ahí contiene es fácil comprender que de la seguridad de la misma depende la efectividad

dentro de los procesos llevados por la institucionalidad, dicho de otra manera en cualquier contexto, se tiene que proteger la integridad de la institucionalidad como de las personas que operan para ella “los agentes de policía” y los agentes encubierto. Ningún dato o documento en físico puede ser sustraído sin registro de la acción llevada, pues mucha información podría perjudicar al departamento de policía del Putumayo y a sus integrantes.

Seguridad en las ventanas, muros, antepechos, claraboyas, sistemas de ventilación ductos azoteas, a través de sensores de movimiento, temperatura, son inválidos sino se tiene registro de las actividades realizadas a nivel interno y externo con un sistema de monitoreo y control de acceso por reconocimiento biométrico y huella dactilar . pueden deben quedar registros, se propone también como alternativa cambiar las terminales inteligentes por terminales brutas , ninguna edificación ésta exenta de catástrofes naturales. , Un sistema de control y acceso, permitirá asignar roles de seguridad al espacio y a la información así como también es un mecanismo de prevención y control de las actividades diarias

Dentro de los múltiples beneficios que se tendrán están los siguientes:

- ✓ Integrar a todas las áreas ya que la implementación y buenos resultados de este sistema, dependerá de la disposición y grado de compromiso de cada uno de los funcionarios.

- ✓ Protección de la información, disminuyendo los riesgos relacionados la pérdida, modificación, alteración y robo de material físico como lógico..

- ✓ Resguardo de la información física y digital que se encuentre en el área de gestión documental a través del rediseño de armarios empotrados y uso de cajas fuertes para documentación de alta confidencialidad.

- ✓ Auditoria interna, médiate el monitoreo contaste del ingreso y salida de las personas que ingresan al área de gestión documental

- ✓ Permitirá tener disponibilidad e integridad de la información
- ✓ Asignación y configuración de los permisos correspondientes de acuerdo a los perfiles autorizados de cada área de Comando de policía que ingresen al área de gestión documental.
- ✓ Monitorio en tiempo real y registro de los usuarios que ingresen.

## 4. REVISIÓN DE LITERATURA

En un mundo en el que la información es el principal elemento para construir y/o desarrollar proyectos, empresas, teorías; entre otros. La seguridad de la información ha pasado de ser un simple requisito para convertirse en una necesidad y, en algunos casos, hasta una obligación. Así que es vital contar con sistemas de control que puedan protegerla, preservarla y mantenerla en el tiempo.

En este sentido, para fundamentar la situación planteada con respecto a la situación objeto de estudio, fueron consultadas diferentes fuentes tanto bibliográficas como webs gráficas, que refieren directamente al tema de seguridad de la información.

### *4.1 Información*

De acuerdo con Aguilera, Purificación [1] la información es un conjunto de datos organizados que tienen un significado; el valor de esta información puede o no ser monetario, tener un carácter estratégico y puede estar almacenada de distintas formas (física o digital).

La información es un activo intangible de la organización y como todo activo debe ser preservado y considerado, más aún, si esta información hace referencia a procesos judiciales de personas o entidades públicas o privadas.

*4.2 Vulnerabilidad*

Este concepto resulta fundamental para una mejor comprensión del tema tratado. Ha sido abordado desde diferentes escenarios; sin embargo, está íntimamente relacionado con la seguridad ya que está definida como un factor de riesgo interno de sistema expuesto a una amenaza, que es potencialmente capaz de causar daños a la organización.

Aplicando este concepto al área de gestión de documentos, que es objeto de este estudio, podemos deducir que la información que se encuentra en la referida área, al ser sensible de sufrir amenas o de ser violentada, se encuentra en condiciones vulnerables.

Esto es una razón más para elevar la propuesta de seguridad que es objeto de este estudio.

*4.3 Seguridad de la Información*

Cuando hablamos de la seguridad de la información, nos referimos directamente a que el objeto de la seguridad, es el dato en sí mismo y cuando se establece un sistema seguro para la información, se trata de evitar su pérdida, modificación y/o divulgación, non-autorizado.

La necesidad de guardad la integridad de la información es de prioridad para salvaguardar la institucionalidad, de la implementación de sus medidas, se evitará el riesgo de que personas, o grupos particulares puedan afectar la integridad de los agentes, la institución, la información causando daños materiales e inmateriales

En este mismo orden de ideas, hay varios aspectos que deben ser considerados [2]

*4.4 Confidencialidad*

De acuerdo con la definición realizada por Aguilera López, Purificación en el año 2010, [1], la confidencialidad, hace referencia a salvaguardad al conocimiento que se tiene de las personas, las entidades, los hechos , procesos y sucesos como un

mecanismo privado de información. Confidencialidad es no permitir la divulgación de información por ningún medio ya sea físico, electrónico, voz a voz, en libros, revistas, redes sociales sin previa autorización del propietario

La confidencialidad resulta fundamental en cualquier procedimiento que involucre información importante para la organización. Pueden establecerse distintos niveles de confidencialidad, de manera que el acceso a la información también es escalado dependiendo de la criticidad de la misma.

*4.5 Integridad*

Se refiere a que los datos (físicos o electrónicos) no hayan sido alterados por usuarios no autorizados; evitando la pérdida de la consistencia. Presenta dos facetas:

***4.5.1 Integridad de Datos.***

Cuando los datos se almacenan, procesan o transmiten y no han sido modificados o alterados en su integridad y contenido

***4.5.2 Integridad del Sistema***

Cuando está libre de manipulación no autorizada o deseada, un sistema debe estar construido para un fin específico y puede migrar su capacidad siempre y cuando existan políticas de por medio

*4.6 Confiabilidad*

Cuando la información presentada es de confianza en nivel de operatividad, confidencialidad, confianza, teniendo en cuenta el flujo de operaciones y/o tareas programadas. Dela confiabilidad de la información dependerá la toma de decisiones y la obtención de resultados.

*4.7 Disponibilidad*

Que tan oportuno es en tiempo y contenido la información , la garantía de un trabajo depende la prontitud con que se acepte o niege el servicio , de autorización o autorizado al uso de los recursos fisicos o del sistema. La disponibilidad es un

sistema de protección contra problemas o accidentes Por ejemplo: un documento salió y no hay control y de este depende una operación.

*4.8 Responsabilidad a Nivel Individual*

Es la capacidad que tiene un ser para afrontar una acción, de ésta depende no depende el éxito o el fracaso, pero si los resultados, Es parte de la política de la organización.

*4.9 Control de Acceso*

Este concepto fue definido por Rivas Arellano, Miguel Alejandro [3] citando a Peltier (2014). Es la forma o barrera existente para llegar al medio, método o políticas de acceso a la protección de datos, recursos físicos.

Entre los tipos de control de acceso que existen cabe destacar: administrativos, físicos y técnicos o lógicos que se refiere a los controles que se implementan para restringir el acceso a áreas de información a través de sistemas lógicos, como lo son los sistemas biométricos para nuestro estudio.

*4.10 Sistema de Reconocimiento Biométrico*

El reconocimiento biométrico es una técnica que posibilita la identificación automática de individuos basándose en sus características físicas o de comportamiento. [4] [5]

Existe una gran variedad de sistemas biométricos dependiendo de la técnica a aplicar, [4] [6]

- ADN
- Geometría de la Mano
- Huella Dactilar
- Reconocimiento de la Firma
- Reconocimiento de la Retina
- Reconocimiento del Iris
- Reconocimiento del Rostro
- Reconocimiento por la Composición Química del Olor
- Reconocimiento por Voz

En el presente estudio se propone la implementación de un sistema de control por reconocimiento biométrico de huella dactilar e iris.

*4.11 Huella Dactila*

Es el espalda de la uña del dedo, que contiene líneas o crestas capilares no tiene nada que ver con la huella digital. La huella dactilar es la contiene glándulas sudoríparas, sudor que es producido en forma de aceite retenido entre lo surcos cuando hay contacto en cualquier superficie

*4.12 Terminal de Control de Acceso por Huella Dactilar (T50)*

Éste es el dispositivo seleccionado para implementar el sistema de control de acceso. Las características de este dispositivo son [9]:

- Capacidad para detectar huellas en alta resolución a gran velocidad
- A modo de un sensor óptico, es de diseño fácil y funcional adaptable a un cristal LCD
- De fácil reconocimiento a través de dispositivos con conectores RS485 o protocolos de TCP/IP
- Puede almacenar hasta 50.000 registros
- Modelo de identificación múltiple

## 5. ANTECEDENTES

En la revisión de la bibliografía, fueron halladas distintas investigaciones que tuvieron como objetivo, la implementación de un sistema de control de acceso. a continuación, se muestran las más relevantes:

- *"Implementación de un Sistema de Control de Acceso para Mejorar la Seguridad de la Información de la Empresa SNX, S.A.C"***,** Tesis presentada por Rivas Arellano, Miguel Alejandro, para optar al Título de Ingeniero en Sistemas en la Universidad Nacional Mayor de San Marcos. Aborda la importancia que tiene en la actualidad la información y por qué es pertinente implementar controles de acceso que garanticen la seguridad de

ésta a través de un sistema de control de acceso integrado al sistema de servidores de archivos que contiene la información de la empresa SNX. [3]

- *"Implementación de un Sistema de Gestión de la Seguridad de la Información del Ministerio de Defensa Nacional en el Proceso de Talento Humano",* Tesis presentada por Moreno Ciro, Jairo Andrés, para optar al Título de Ingeniero de Sistemas de la Institución Universitaria Politécnico Grancolombiano. El tema fue abordado desde la perspectiva de la seguridad de la información y la capacitación del personal para que tengan una cultura más asertiva con respecto a la importancia de la seguridad, pasando por distintos escenarios de años anteriores, donde la información ha sido empleada con fines diferentes y en prejuicio de la organización. [10]
- *"Diseño de Seguridad Física",* investigación presentada por Cuellar Castro Alonso, en la Institución Universitaria Politécnico Grancolombiano. En ella se propone un diseño de seguridad física para la firma Tirana Uribe & Michelsen, que determine los mejores procedimientos para identificar los riesgos a los que están expuestos y que puedan afectar la seguridad física de la firma. En este sentido, dentro del estudio se proponen distintas alternativas y mecanismos de control, que procuran evitar que se materialicen las amenazas. [11]
- *"Biometría y Seguridad",* libro escrito por Ortega García, Javier. En éste se exponen claramente los inicios de la biometría y la vinculación con la seguridad, describen claramente todos los sistemas biométricos que se han desarrollado, así como las ventajas y desventajas para cada caso. [4]

## 6. ESTRATEGIA METODOLÓGICA

### 6.1 Enfoque Metodológico:

Esta investigación se realizó, principalmente, desde una perspectiva de seguridad física (instalación), hardware y de la información, tiene un enfoque mixto; es decir, incluye el enfoque cualitativo y el cuantitativo (análisis y obtención de datos). De acuerdo con lo que plantea [12] el enfoque cualitativo está fundamentada en un

proceso inductivo en el que se exploran y describen distintas situaciones que van desde lo general hasta lo particular, documentado y sustentado con diferentes aportes teóricos y con la información obtenida en campo. Por su parte, el proceso cuantitativo es secuencial y probatorio, en el cual se aplica la lógica deductiva.

Todo ello, tomando como escenario, el área de Gestión Documental, del Departamento de Policía de Putumayo, Mocoa.

### 6.2 Diseño de la Investigación

Este estudio, de acuerdo con lo establecido en [12], tiene un diseño descriptivo no experimental, en el entendido de que los estudios descriptivos, donde se consultan fuentes de información, se usan métodos y metodologías acorde a las necesidades y de la recolección de datos (variables), aspectos, componentes y fenómenos que desean investigar. Y es experimental porque se observaron los fenómenos como tal y como suceden en su contexto natural, para después ser analizados.

### 6.3 Muestra

La muestra poblacional tomada fue no probabilística, con muestreo por conveniencia [12] dadas las características de este estudio, se consideraron sólo a las personas que tienen influencia directa y con poder de decisión, en el área de gestión de documentos, que es objeto de estudio.

### 6.4 Estrategia para recolección de datos:

Las estrategias utilizadas para la consecución de la información fueron las siguientes:

1. *Observación Directa e Indirecta:*

La observación en la investigación cualitativa va más allá del simple hecho de ver una realidad, de acuerdo con [12] tiene distintos propósitos, los cuáles fueron los que se persiguieron durante esta investigación:

- ✓ Explorar el ambiente y la mayoría de los aspectos importantes en torno al área de gestión documental del Departamento de Policía del Putumayo, Mocoa.
- ✓ Describir a las personas del Departamento de Policía y las principales dinámicas del interior que tienen poder de incidencia de forma directa o indirecta en el área objeto de estudio.
- ✓ Comprender los procesos, las vinculaciones de las personas y los sucesos o eventos que se presentan en el referido departamento policial; en el contexto social y cultural tal como ocurre.
- ✓ A partir de todo lo anterior, identificar los problemas y generar hipótesis que puedan servir de base para futuros estudios.

En este sentido, se tomó nota de todo lo observado que sucede en el área de gestión de documentos, del departamento de policía. Aspectos relevantes como:

- ✓ Flujo de personas que transitan alrededor del área
- ✓ Personas que ingresan al área (autorizados o no)
- ✓ Controles de seguridad para el manejo de la información
- ✓ ¿Existe algún nivel de confidencialidad de la información?
- ✓ ¿Hay listados de personas autorizadas?
- ✓ ¿Cómo se controla el acceso?

### *2. Entrevistas No Estructuradas*

En la investigación cualitativa en palabras de [12] es una reunión para intercambiar información entre el entrevistador y el entrevistado. Esto se realizó para poder indagar a fondo acerca de la situación que se estaba observando, fue necesario realizar entrevistas más bien reflexivas con los principales actores que intervienen directamente en las dinámicas que se desarrollan en el área de gestión

de documentos. Pero también se involucraron en estas entrevistas a las personas que, aunque no intervienen directamente en los procesos, pero que pueden afectarlos o participar de forma indirecta.

### 3. *Cuestionario*

Apoyándonos en lo indicado por [12], un cuestionario como un lista de preguntas para determinar una variable a medir, para el desarrollo de este se hicieron tres prototipos a fin de identificar las preguntas más relevantes en el estudio.

En este caso, fueron definidas cuatro variables a partir de las cuáles se realizaron una serie de preguntas a la parte de la población que hace vida en el departamento de policía del putumayo y que fueron seleccionadas como muestra para efectos del estudio que se realiza.

## 6.5 Variables e Instrumento de Medición

Para esta investigación, las variables a medir fueron: Seguridad, Control, Amenazas y Riesgo. Tras la definición de las cuales, se definió el instrumento de medición que se presenta a continuación para cada una de ellas:

### 1. Variable a Medir: Seguridad

Definición conceptual: Percepción que tiene usted de la seguridad que existe en torno al área de gestión de los documentos en el Departamento de Policía de Putumayo en Mocoa.

| Column a1 | Preguntas o Ítems | Completamente (mucho) | Aceptable | Regular | Poco | Nada |
|---|---|---|---|---|---|---|
| **1** | ¿Qué importancia tiene el área de gestión de documentos? | | | | | |
| **2** | ¿En qué medida considera | | | | | |

| | |
|---|---|
| | usted que es un área segura? |
| **3** | ¿Qué tan de acuerdo está usted con la política de seguridad del área? |
| **4** | ¿En qué medida piensa usted que es clara ésta política de seguridad? |
| **5** | ¿En qué medida considera usted que sus compañeros comprenden esta política de seguridad? |
| **6** | ¿En qué medida considera usted que sus compañeros están de acuerdo con esta política de seguridad? |
| 7 | ¿Cree usted que es necesario reforzar el sistema de seguridad del área? |

2. Variable a Medir: Control

Definición Conceptual: Percepción que tiene usted acerca del control o los controles existentes para gestionar el acceso al área de gestión de documentos, del Departamento de Policía de Putumayo en Mocoa.

| Columna1 | Preguntas o Ítems | Completamente (mucho) | Aceptable | Regular | Poco | Nada |
|---|---|---|---|---|---|---|
| **1** | ¿Qué importancia tiene el área de gestión de documentos? | | | | | |
| **2** | ¿En qué medida considera usted que existen controles para el ingreso al área de gestión de documentos? | | | | | |
| **3** | ¿Qué tan de acuerdo está usted con la política de control de acceso al de gestión de documentos? | | | | | |
| **4** | ¿En qué medida piensa usted que es necesario controlar el acceso al área de gestión de documentos? | | | | | |
| **5** | ¿En qué medida considera usted que sus compañeros entienden la importancia del control de acceso en el área de gestión de documentos? | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | ¿Cree usted que es necesario reforzar el sistema de control de acceso del área de gestión de documentos? | | | | | |

3. Variable a Medir: Amenazas

Definición Conceptual: Apreciación que tiene usted acerca de las posibles amenazas que puede haber en torno al área de gestión de documentos del Departamento de Policía de Putumayo en Mocoa.

| Columna1 | Preguntas o Ítems | Completamente (mucho) | Aceptable | Regular | Poco | Nada |
|---|---|---|---|---|---|---|
| **1** | ¿Tiene usted conocimiento acerca de lo que es una amenaza? | | | | | |
| **2** | ¿En qué medida considera usted que existen amenazas en torno al área de gestión de documentos? | | | | | |
| **3** | ¿Qué tan de acuerdo está usted con los mecanismos de seguridad actuales, para neutralizar las posibles amenazas? | | | | | |
| **4** | ¿En qué medida piensa usted que es necesario proteger la información contenida en el área de gestión de documentos, de las posibles amenazas que pueda haber? | | | | | |
| **5** | ¿En qué medida considera usted que sus compañeros reconozcan posibles amenazas hacia el área de gestión de documentos? | | | | | |
| 6 | ¿Cree usted que es necesario incrementar la seguridad en el área de gestión de documentos, producto de posibles amenazas a la información ahí contenida? | | | | | |

4. Variable a Medir: Riesgo

Definición Conceptual: Apreciación que tiene usted acerca de los posibles riesgos que puede haber en torno al área de gestión de documentos del Departamento de Policía de Putumayo en Mocoa.

| Column a1 | Preguntas o Ítems | Completamente (mucho) | Aceptable | Regular | Poco | Nada |
|---|---|---|---|---|---|---|
| 1 | ¿Está familiarizado usted con el concepto de riesgo? | | | | | |
| 2 | ¿En qué medida considera usted que pueden existir riesgos en torno al área de gestión de documentos? | | | | | |
| 3 | ¿Qué tan de acuerdo está usted con los mecanismos de seguridad actuales, para minimizar las posibles fuentes de riesgos sobre el área de gestión de documentos? | | | | | |
| 4 | ¿En qué medida piensa usted que es necesario proteger la información contenida en el área de gestión de documentos, de las posibles fuentes de riesgo que puede haber? | | | | | |
| 5 | ¿En qué medida considera usted que sus compañeros reconozcan posibles fuentes de riesgos con respecto al área de gestión de documentos? | | | | | |
| 6 | ¿Cree usted que es necesario incrementar la seguridad en el área de gestión de documentos, producto de posibles riesgos que pongan en peligro la integridad de la información ahí contenida? | | | | | |

## Planteamiento de Hipótesis

Hipótesis General

- El Departamento de Policía de Putumayo en Mocoa, no cuenta con un sistema de control de acceso que garantice la confiabilidad, integridad y disponibilidad de la información, dentro del área de gestión de documentos. Si se implementara un sistema de seguridad por control biométrico, esta situación podría mejorar y disminuirían considerablemente, las posibles

amenazas y se minimizarían las fuentes de riesgo de que la información fuera utilizada con fines contrarios a los designios de la organización.

### 6.6 Hipótesis Particulares

- Implementación de un sistema de control biométrico por reconocimiento de huella dactilar e iris para la optimización del acceso al recurso humano no autorizadas en al área de gestión de documentos del Departamento de Policía de Putumayo, Mocoa.
- Sustentado en esta propuesta y habiendo analizado la factibilidad de la implementación, conociendo la importancia que tiene y conscientes de las amenazas existentes, el Departamento Policial, podrá justificar la adquisición de los equipos técnicos que se requieren para la instalación del sistema.

### 6.7 Procesamiento de la Información

Para el análisis de los datos obtenidos, se usará el programa “Statistical Package for the Social Sciences” por sus siglas SPSS. Este paquete permite realizar análisis estadísticos de los datos. Mediante este programa se ingresan las variables con cada uno de sus ítems y de acuerdo a los resultados de los cuestionarios aplicados, permite hacer conclusiones acertadas.

## 7 DESARROLLO E IMPLEMENTACIÓN

### 7.1 Observación directa e indirecta:

Fueron realizadas observaciones a todos los actores que a diario tienen acceso al área de gestión de documentos. Durante unas fases, la observación fue directamente dentro del área de gestión y otras, fuera de esto.

Esto con el propósito de determinar si todas las personas que ingresaban al área tenían la autorización para hacerlo y evidenciar la manipulación de la información por parte de personal no autorizado.

### 7.2 Entrevistas No Estructuradas

En esta fase, se establecieron conversaciones en torno a la seguridad existente en torno al área de gestión de documentos y a la importancia de la información ahí contenida. La intención fue determinar si los responsables directos del área de gestión de documentos, eran de alguna manera conscientes de la carencia y a la vez de la necesidad de un sistema de control de acceso que permita restringir el ingreso del personal a esa determinada área y establecer niveles de acceso. todo ello en aras incluso de poder establecer responsabilidades en caso de que se presentase alguna eventualidad.

### 7.3 Cuestionarios

Fueron aplicados una serie de cuestionarios a razón de cuatro variables que se pretendía analizar. Éstas variables fueron: seguridad, control, riesgo y amenaza. Estos cuestionarios fueron aplicados al personal que tiene inherencia directa sobre el área de gestión documental y al jefe del departamento, quien es el responsable de la seguridad a nivel general.

### 7.4 Análisis de Datos

El análisis de los datos cuantitativos obtenidos se realizó por medio del programa estadístico SPSS, en el cual se configuraron las variables y las respuestas obtenidas para cada ítem.

## 8. PROPUESTA DE MEJORAMIENTO DE LA SEGURIDAD A LA OFICINA DE GESTIÓN DOCUMENTAL DEL DEPARTAMENTO DE POLICÍA MOCOA – PUTUMAYO.

15 de MAYO de 2018

Señores

COMANDO DE POLICÍA PUTUMAYO

Director comunidad del anillo

Ciudad

Cordial saludo.

**Nosotros**: CAÑÓN, OSCAR IVÁN Y CUELLAR CASTRO, ALONSO, Agentes de policía, adscritos al departamento con perfiles de ingeniero de sistemas y patrulleros próximamente a recibir el grado de especialización en seguridad de la información", presentamos a usted una propuesta que busca mejorar la seguridad dentro del área de gestión documental del Departamento de Policía Mocoa.

En respuesta a la problemática encontrada, nos complace presentar una propuesta de servicios profesionales que va orientada tanto a la seguridad física como lógica de la instalación.

### NUESTRAS PROPUESTA.

El presente estudio propone la implementación de un sistema de control de acceso que funcione a través de dos dispositivos biométricos de huella dactilar e iris, así como la identificación de posibles fallas entorno espacio físico y lógico del área de gestión documental del Departamento de Policía de Mocoa (Putumayo).

La responsabilidad del archivo no solo recae sobre los operadores, sino que es un asunto de todos, Pues de las políticas generadas a nivel superior van acorde a la respuesta de las necesidades encontrados en los subniveles. El estudio se hará

bajo un enfoque mixto. (cualitativo y cuantitativo) haciendo uso la recolección de información para llegar un diagnostico utilizando las herramientas estadísticas del Muestreo no probabilístico “muestreo por conveniencia”. Dado que no existe un control de acceso al espacio físico dentro del área.

Identificar las fallas y posibles errores cometidos dentro del área de gestión documental que incluye desde **el espacio físico**: sus áreas de trabajo, seguridad en puertas, ventanas, techos, pisos, paredes, sistemas de aireación, ingreso a la dependencia, políticas de seguridad para el ingreso de personal autorizado o no autorizado, seguridad en documentación y carpetas, archivadores, escritorios y de **la parte lógica** y **seguridad física de hardware:** Ubicación de los equipos de cómputo, condiciones climáticas, seguridad en torres y periféricos, control y seguridad a portátiles, condiciones de acceso a equipos y dispositivos de red, rack y armarios, cajas de computadoras, equipamiento de equipos, Chek list de entrada y salida de equipos, Ups, alojamiento físico de máquinas backup, concentradores y puertos rj45 libres y **seguridad lógica del software.** Pasword en Bios, servidores de almacenamiento, terminales brutas e inteligentes, redundancia de la información y almacenamiento cíclico, manejo de contraseñas para dominios y grupos de trabajo, Katchers, Keylogers y otros sistemas de captura de datos, conectividad, dispositivos para capturas de datos “Tap”, sistemas Monitorización del hardware, sistemas de grabación de datos, aceptación o anulación de sistemas por wireless, radiofrecuencia o bluetooth.

Tenemos el compromiso de ayudar a nuestros clientes, para que crezcan en sus equipos de trabajo haciéndolos más exitosos, Nuestra propuesta guiará a tomar mejores decisiones y será un punto de garantía tanto del acceso al personal, como acceso a información y otros que derive de ésta que mejorarán indudablemente el rendimiento de los funcionarios dentro de la dependencia.

## 8.1 Nuestro enfoque

Estamos convencidos de que la presente propuesta será estudiada y analizada, pues utilizamos las últimas técnicas en recolección de información y auditoria, nuestro muestrea va acorde a las necesidades identificadas más las que nos presente el cliente, como profesionales en seguridad de la información conocemos los diferentes métodos y metodologías para recolectar información y del juicio impartido será basado en la experiencia como especialistas.

Apoyados en herramientas estadísticas y software asistido por computador Independientemente de los resultados obtenidos, se profundizará en temas que requieran buscando debilidades a nivel de espacios de infraestructura fisicia y

hardware asi como lógicos o de software. Nuestro trabajo no solo llevará al diagnóstico sino a una posible solución previa determinación de los requerimientos y presupuestos asignados para tal fin.

En resumen, podemos afirmar que por la capacidad y experiencia daremos respuesta a sus necesidades y estas serán atendidas oportunamente con el compromiso de ofrecer un valor agregado en cada uno de nuestros procesos.

**8.2 Nuestros honorarios**

Ocho millones más gastos de impuestos, en caso de que requiera inversión adicional por adición de tiempo, su empresa será notificada con un mes de anticipación.

Si una vez expuesta ésta a su entera satisfacción y cumple con los requerimientos. Le agradecemos hacerlo saber para empezar a asignar el personal adecuado y empezar a trabajar previa cronograma planificado

Muy atentamente,

Oscar Iván Cañón Rodríguez Alonso Cuellar Castro

**9. RESULTADOS**

- Mediante la observación directa e indirecta, así como entrevistas y encuestas, se comprobó que:

  La oficina que pertenece al **área de gestión documental** , Ubicada en el 5to piso del edificio de la Policía – Mocoa, en la calle 8 con 8. No tiene seguridad más que la entrada al Edificio que si eres convincente puedes pasar sin identificarte previamente.

**La entrada principal** Debe contar un interfono (video-portero), Cambiar la puerta de madera a puerta de metal, cuya cerradura debe ser electrónica y mecánica (puesto que en mocoa, se la energía es muy intermitente), también se propone colocar una inclusa en la puerta de entrada asi solo se podría abrir desde el interior , Esto sería de gran medida preventiva al ingreso de visitan tanto del personal interno como externo, limitando el acceso a cierto número de personas, previniendo así intrusos, y si logra entrar, pues no podría salir. Un dato importante de el Video, es que podría tener EVIDENCIAS, de registra o saca documentación con o sin previa autorización, Se hace necesario también colocar cámaras externas para evaluar el entorno a fin de detectar situaciones no normales. La puerta debe tener un mínimo de 2m de altura, Con mirilla de 180º de Angulo de visión(a veces ingresan archivadores que no son cómodos al hora del ingreso)

**Las chapas de seguridad.** Son chapas ordinarias marca “Pajarito”, se propone unas con pasadores de 1” de largo, cambio de bisagras por acero con separaciones no mayores a 45 Cm, su adhesión debe ser puerta marco y muro,

**Las ventanas**. Por ser ventanas corredizas pueden ser levantadas fácilmente, a fin de escatimar gastos, se deben asegurar con tornillos y pernos de fijación el muro en contra lamina (no deja ver donde quedo el tornillo), y porta guía para que no corra el riel, adicional a eso deben tener reja de seguridad que no sirva como escalera.

**Los muros**. Los muros rústicos se prestan para subir como escaleras, además no son muros reforzados, se propone alisar o pulir los muros, y quitar las bancas que están en el pasillo como descansaderos. Las seguridad debe ir más allá del muro., al ser un muro muy bajo, con ventana de aireación, colocar un cerco eléctrico o en su defecto sellarlo.

**Al ser el último piso**. **azotea.** Tiene vulnerabilidad por el aire. Se sugiere colocar sensores de moviento, aumentar la azotea con una reja o en su defecto colocar muros… se sugiere colocar seguridad a la reja y puerta que eta en el pasillo que dirige a la azotea en forma de un portón automatizado

**Con respecto a la Iluminación,** el área de gestión documental no cuenta con dispositivos o mecanismos de alerta de inundación e incendio. Se deben cambiar las lámparas de lugar , puesto que en caso de accidente pueden quemar el área de archivo, se propone colocarlas en la pared con una malla de seguridad a fin de que no puedan ser apagadas manualmente (Si fallará el sistema de video vigilancia principal o fuera desconectado el Sistema interno sigue funcionando). Las lámparas deben funcionar con baterías pues en caso de que corten el fluido ellas seguirán encendidas. Deben haber lámparas de emergencia
El encendido de las lámparas e ingreso al área debe ser con horarios establecidos. Como en varias ocasiones la oficina queda sola. Debe contar con un sistema de luces automáticas que simulen que existe personal internamente laborando.

**Los tableros eléctricos.** Si bien no están dentro del área en estudio, pueden ser objeto de la delincuencia se tienen que camuflar pues están a la vista de todos, No se deben tener bajo llave de emergencia.

**Los archivadores y gabinetes de archivos,** a fin de protegerlos en un 99.9% deben estar empotrados, y se debe tener en cuenta que deben estar protegidos contra inundaciones o desastres, como primera medida, Adquirir una caja fuerte para documentación importante, caja que debe ser instalada por personal preferiblemente de otra ciudad sin conocimiento del lugar donde la ésta instalando.

Él área de gestión documental. No cuenta ningún tipo de blindaje, los únicos equipo de comunicación con que cuenta son los celulares de los operadores y radioteléfonos. No existen botón pánico (sonoro o electrónico), en caso de una catástrofe no tienen dispensa de alimentos, nevera. agua, botiquín de primeros auxilios una cama. Mejor dicho No

existe un plan de seguridad a nivel interno ni conocen sus responsabilidades en caso de tragedia

Instalación de un CCTV. 24/7, que funcione todo el año, ubicado estratégicamente donde el servidor de grabación este lejos de las instalaciones (fuera del edificio), que llegan y se lo roban el servidor.? Se recomienda cámaras IP con resolución HD. O pueden ser Cámaras con video análisis procesal, cámaras que detectan objetos sustraídos, incluso movimientos no autorizados.
E instalación de sistemas de alarma en todos los sectores (puertas, ventanas, muros, ductos, tragaluz, lámparas, sistema de aire acondicionado) con barreras fotoeléctricas o sensores de proximidad y movimiento

Debe haber un identificador de llamadas para el número 4294682,

**Adicionalmente a la parte física**
Debe existir un código de comunicación a nivel interno. (Un agente puede ser secuestrado su familia y es obligado a sustraer documentación). Mantener la puerta cerrada, no permitir que otras dependencias coloquen publicidad en la cartelera destinada al área de gestión documental y no dormirse en la oficina con la puerta abierta. (ya se han dado casos), que llegan los agentes cansados y se han dormido.

No se cuenta con una póliza de seguro ante todo riesgo, así como tampoco se ha logrado culminar el proceso de digitalizar el archivo físico en archivo digital, se propone. Crear un plan de riesgo a fin de contratar más operadores para hacer digitalizar todo el archivo.

Como mecanismo de control de ingreso se propone un sistema de ingreso de control y un sistema de lector de retina así como los dispositivos que puede encontrar en [14]

**Armarios y archivadores.** No poseen llaves de seguridad o protección alguna, aquí está toda la información de hojas de vida de los agentes, de casos atentados cometidos, oficios llegados y entregados, remisorios. Casos de seguimiento nombres de agentes en cubierto y toda la parte secreta del Departamento del Policía de Putumayo. , No hay copias de los mismos y como se manifestó. La tarea de digitar esos documentos físicos no avanza, por sobrecarga laboral en los 2 agentes encargados del área

**Siguiendo con la seguridad a nivel físico (hardware)**

**Electricidad para equipos de radio y sistemas de cómputo.** Es indispensable usar UPS (sistemas de suministro ininterrumpido de energía), que a su vez son regulares de tensión, el diagnostico arrojo que existen UPS que duran máximo 15 minutos., debe hacerse un estudio de los sistemas de automatización de energía, el centro de cómputo y rack o armario.

**Revisión de redes (eléctricas y de datos).** a simple vista el cableado electico cumple con la norma, pero el sistema electico tiene ya 50 años de funcionamiento, y la red de datos 9 años. La revisión de la estructura de redes (no de sus dispositivos) determina que la carga eléctrica no corresponde a la cantidad que equipos que se maneja no existen cajas separadas de distribución y a nivel lógico no existen varios enrutadores lo que significa que si se ataca la red principal sufrirá la dependencia en estudio también.

**Redes de datos.** No existe un software asociado a detectar fallas o niveles de fallas, entre maquinas ni puntos de conexión de ahí el áre de gestión documental en varias ocasiones se ha quedado sin conectividad

**Las torres (CPU) Y Portátiles tienen puertos de interconexión abiertos.** No se han desactivado puertos usb, paparalelos y com dentro de los dispositivos de computo, lo que permite que el uso de grabadoras de Cd y Usb de usuarios externos pueden albergar cualquier tipo de información. Se trabaja sobre terminales inteligentes.. Se propone tener terminales brutas. Las terminales inteligentes pueden ser objeto de robo en su totalidad o integridad.

**Rack y armarios**. Dentro del área de gestión documental no existen estos elementos, Pero cabe aclarar que donde se encuentran ubicadosn (en la oficina de sistemas, Existen puertos rj45 abiertos sin deshabilitar. Lo que implica que un intruso conecte un cable y se conecte a toda la red.

**Las cajas de las CPU**. Las cajas encontradas no tienen ningún tipo de seguridad, fácilmente con destornillador se pueden destapar, incluso se evidencio que una de las torres abre sin ningún tipo de seguridad, donde fácilmente se podría extraer el disco duro o cualquier elemento interno. Se propone que los tornillos deben ser sellados con estaño o en su defecto silicona, no se realiza mantenimiento correctivo ni preventivo con un cronograma de actividades. También se propone asegurar las torres a la pared y sujetar los portátiles con guayas o cableado en 00 cero, se tiene acceso total a la máquina, sin tener seguridad en las BIOS.

**Seguridad en la BIOS.** El operador de la máquina supone que tener seguridad en la BIOS pues no es muy seguro puesto que por el calor, las CPU deben estar destapadas, que en una ocasión estuvieron con pasword en la BIOS pero que personal con pocos conocimientos hizo puente entre

esta y elimino el pasword, que por eso ahora está sin pasword en la BIOS. Esto es un error fatal.. Lo que se propone es cambiar de cajas para la CPU, cajas de seguridad empotradas con pasword en la BIOS, y si la temperatura del ambiente es alta, colocar sistemas de refrigeración a fin de evitar abrir la caja innecesariamente.

**Acceso al interior de la máquina.** Se debe colocar accesorios físicos a dispositivos como unidad Usb o CD-ROM A fin de que no sean abiertos y si lo hacen que estén habilitados por contraseñas. Si bien la estructura del Pc no es modificable sus cajas de protección son poco resistentes, cualquiera puede llevarse un disco duro y hacerle clonación con un Norton gost por ejemplo. Debe existir solo personal autorizado para hacer mantenimiento y administración de las maquinas. De ahí que proponemos usar terminales brutas.

**Duplicidad de información.** No existe un software de gestión documental , todo se lleva manualmente mediante la Suite de Microsoft. En varias ocasiones un archivo es llevado de un lado a otro , sin tener control sobre sus modificación y generando duplicidad de contenidos. Existen programas que se encargan de evitar estos sucesos que además de garantizar el contenido de la información solicitan acceso para su edición o eliminación. Además de crear un backup del archivo.

**Sistemas de backus**

Una forma de proteger el archivo de gestión documental físico , es haciendo una copia de seguridad digital, un sistema confiable de Backup , es cuando las instalaciones donde se encuentra son físicamente seguras , no es factible tener un sistema de backup en la misma área donde se tiene los equipos que es lo que se encuentra actualmente.

**UPS**. No es recomendable tener las Ups debajo del computador o al lado. Una por el magnetismo que éstas producen y otra, porque en caso de hurto de información y bajen los braker's pues la maquina seguirá operando . Las ups. Deben estar en un circuito y fuera de las instalaciones, no pueden estar al acceso del operador.

**Redes Bluetooh y Wireless**. Para este caso si existe protección desde el centro de mando.. No se permiten la creación de redes alternas o vpn por dependencia.. el inconveniente se presenta cuando no se tiene registrados los equipos por Mac. Lo que quiere decir que cualquier que tenga la clave podrá acceder a la red en forma remota. Se propone la adquisición de un firewall ya sea físico o lógico como es el caso de Endian Firewall.

**Sistemas de captación de datos.** existen dispositivos para captar las pulsaciones de los teclados como son los dongles, programas como los keyloger's muchas veces no son detectados por los antivirus si estos no son licencias compradas, un dongle o keycatchers o keyloger tiene la capacidad de detectar claves y enviarlas directamente a los correos electrónicos de los intrusos. Las pruebas que se hicieron no permitieron detectar rastro de dispositivos de este tipo a nivel físico o lógico.

**Seguridad física en el cableado.** Las conexiones fast Ethernet 802.x si cumplen con la norma en cuanto a cableado vertical y horizontal. No se tiene recomendaciones.

**No existe un centro remoto de hardware.** Los equipos de cómputo , no son manejados por servicios como Webmin, ssh, telenet o similares. Todo se hace desde el punto físico. La preocupación sería entonces. Que hacer en caso de que se tome un terrorista las instalaciones con los equipos dentro.?

**No contratar personal ajeno al personal de policía para mantenimiento.** Existe la falencia de que en ocasiones de contrata una empresa de la ciudad para hacer mantenimiento de los equipos, si bien por la empresa no puede haber inconvenientes, son muchos los casos de equipos que son asaltados o accidentados en el transcurso de la Oficina al centro de diagnóstico y reparación.

Toda la información recogida es producto de las encuestas, entrevistas al personal auxiliar como oficial de la Policía Nacional Putumayo y muchas de las sugerencias surgen a partir de la investigación y metodologías de lluvias de ideas propias para cada situación.

La evaluación de resultados permite como primera medida gestión un presupuesto para la adquisición de que se debe implementar un sistema de control de acceso por reconocimiento dactilar y biométrico

## 10. DISCUSIÓN Y CONCLUSIONES

A la luz de toda la investigación realizada, tanto en los aspectos metodológicos como en la revisión de la literatura, efectivamente la información juega un papel determinante para el Departamento de Policía del Putumayo. El hecho de no contar con un sistema de control de acceso, es motivo de preocupación ya que reconocen las fuentes de riesgo que están presentes y las posibles amenazas.

En ese sentido, es factible la aceptación de la propuesta que aquí se hace para la implementación de un sistema para el control de acceso que pueda realizarse a través del dispositivo T50 (descrito en el apartado anterior)

Estos resultados sirven de base para futuras investigaciones y aplicable a otras áreas que incluso en el mismo departamento existen en condiciones vulnerables.

## 11. REFERENCIAS


[1] P. Aguilera López, Seguridad Informática, Editex, 2010.

[2] Markus Erb, «Blog sobre Gestión del Riesgo en Seguridad Informática,» [En línea]. Available: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/). [Último acceso: 10 04 2018].

[3] M. A. Rivas Arellano, «Implementación de un Sistema de Control de Acceso para Mejorar la Seguridad de la Información de la Emoresa SNX, S.A.C,» Lima, Perú, 2016.

[4] J. Ortega García, F. Alonso Fernandez y R. Belmonte Coomonte, Biometría y Seguridad, Madrid, España: Fundación Rogelio Segovia, 2008.

[5] A. Giraldo y D. Gómez, «Estado del Arte de la Seguridad en Sistemas Biométricos,» Bogotá, 2017.

[6] F. Serratosa, La Biometría para la Identificación de las Personas, Catalunya, España: UOC.

[7] A. Arrieta, J. Gómez, L. García , L. Alonso Romero, Á. Sánchez y V. López, Gestión y Reconocimiento Óptimo de los Puntos Característicos de Imágenes de Huellas Dactilares, Salamanca, España, 2016.

[8] C. Tolosa y Á. Giz, «Sistemas Biométricos,» España, 2015.

[9] [En línea]. Available: file:///C:/Users/FERNANDO/AppData/Local/Temp/control_de_accesos_huellas_digitales_T50.pdf.

[10] J. Moreno Ciro, «Implementación de un Sistema de Gestión de la Seguridad de la Información del Ministerio de Defensa Nacional en el Proceso de Talento Humano,» Bogotá, Colombia, 2016.

[11] A. Cuellar Castro, «Diseño de Seguridad Física,» Bogotá, 2017.

[12] Dr. Hernández Sampieri, Roberto; Dr. Fernández, Collado, Carlos; Dra. Baptista, Lucio, Pilar;, Metología de la Investigación, México: Mc Grow Hill, 2008.

[13] Colciencias, «Modelo de Medición de Grupos, de Investigacion, Desarrollo Tecnológico o de Innovación y reconocimiento de investigadores del Sistema

3] Nacional de Ciencia, tecnología e Innovación 2014,» Colciencias, 2014. [En línea]. Available: http://www.colciencias.gov.co/sites/default/files/ckeditor_files/files/DOCUMENTO MEDICI%C3%93N GRUPOS - INVESTIGADORES VERSI%C3%93N FINAL 15 10 2014 (1).pdf. [Último acceso: 01 2015].

14 Disposicitivos para el control de acceso a sistemas de seguridad http://enlacesdelcaribe.com/categoria-producto/control-de-acceso-en-bogota/