APLICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV) SISTEMA INTEGRADO DE EMERGENCIAS Y SEGURIDAD (SIES) DEL MUNICIPIO DE YACUANQUER

JOSE HERNAN CORTES ROSERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2016

APLICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV) SISTEMA INTEGRADO DE EMERGENCIAS Y SEGURIDAD (SIES) DEL MUNICIPIO DE YACUANQUER

JOSE HERNAN CORTES ROSERO

Monografía de grado para optar el título de
Especialista en Seguridad Informática

Asesor
Esp. Ing. Freddy Enrique Acosta.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2016

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

San Juan de Pasto, 16 de Abril de 2016

DEDICATORIA

Dedico este trabajo a mi hijo Nicolás, que su luz ha sido parte fundamental para mi vida.

A mi familia que me brinda su compañía y apoyo cada día y me hacen saber que siempre cuento con ellos.

A Dios y la Virgen María que siempre me iluminan, para que mis esfuerzos lleguen a feliz término.

Hernán Cortés

AGRADECIMIENTOS

José Hernán expresa sus agradecimientos a:

Ing Deivis Eduardo, que me colaboro con el inicio de mi trabajo, orientándome con la parte metodológica y marco conceptual.

Ing Yarelly Torres, sus aportes me permitieron mejorar la presentación del trabajo orientándome en la redacción y contenido.

IT Juan C. Popayán Comandante de la estación de Policía de Yacuanquer, que me permitió desarrollar mis actividades en sus instalaciones.

PT Eduardo Vallejo que estuvo encargado de la sala de CCTV hasta diciembre de 2015, que con sus observaciones y recomendaciones me permitió conocer como son las labores diarias en la estación.

Ing Freddy Enrique Acosta por la asesoría aportada a este trabajo que con su conocimiento y experiencia me permitió culminarlo.

CONTENIDO

pág.

pág.

pág.

pág.

pág.

pág.

pág.

pág.

LISTADO DE TABLAS

Pág.

pág.

pág.

LISTADO DE FIGURAS

Pág.

pág.

LISTA DE GRÁFICOS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ANALÓGICO: Señales visuales o acústicas que se convierten en una tensión eléctrica variable, que se puede reproducir directamente a través de altavoces o almacenar en una cinta o disco[1].

CÁMARA PTZ: El término cámara PTZ tiene un acrónimo de pan-tilt-zoom y puede referirse sólo a las características de las cámaras de vigilancia específicas. «Cámaras PTZ» también puede describir toda una categoría de cámaras con seguimiento automático[2].

CCTV: Circuito Cerrado de Televisión[3].

CONTROL CENTER: cuenta con una interfaz de usuario integrada para administrar los videos, el control de acceso y las alarmas. Por su parte, la licencia sin restricciones le permite realizar instalaciones ilimitadas en el lugar[4].

DVR: Digital es un dispositivo interactivo de grabación de televisión y vídeo en formato digital[5].

ETHERNET: es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD)[6].

MAGERIT: es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información[7].

NETAGENT: es un producto para monitoreo por SNMP (protocolo simple de administración de red) de última generación[8].

---

[1] MASTER MAGAZINE. [En Línea]. [citado en 2016-03-12]. Disponible en Internet http://www.mastermagazine.info/termino/3850.php.

[2] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 24 agosto 2014 a las 01:39. Disponible en Internet https://es.wikipedia.org/wiki/C%C3%A1mara_PTZ.

[3] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 2 marzo 2016 a las 16:33. Disponible en Internet https://es.wikipedia.org/wiki/Circuito_cerrado_de_televisi%C3%B3n.

[4] INDIGOVISION. [En línea]. [Citado en 2016-03-12]. Disponible en Internet http://www.indigovision.com/en-us/products/video-security-management-software.

[5] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 26 octubre 2015 a las 13:42. Disponible en Internet https://es.wikipedia.org/wiki/Grabador_de_video_digital.

[6] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 4 marzo 2016 a las 16:31. Disponible en Internet https://es.wikipedia.org/wiki/Ethernet.

[7] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 26 marzo 2014 a las 15:58. Disponible en Internet https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa).

[8] SIEN ENERGIA. [En línea]. Copyright 05/2011. [Citado en 2016-03-12]. Disponible en Internet http://www.seinenergia.es/page842.html.

NVR: Grabador de vídeo en red (NVR) es grabadora de vídeo avanzado que está diseñado para grabar secuencias de vídeo comprimido a los conductores de disco duro (HDD)[9].

RAID5: «conjunto redundante de discos Independientes», hace referencia a un sistema de almacenamiento de datos en tiempo real que utiliza múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos[10].

SIES: Sistema Integrado de Emergencias y Seguridad[11].

SPANNING TREE: Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes[12].

UPS: Un sistema de alimentación ininterrumpida (SAI), por sus siglas en inglés Uninterrupted Power System[13].

VCR: (vídeo cassette recorder) videograbadora[14].

[9] TM UNIFORE Secure your home&business. [En línea]. Escrito el 04 abril 2014. [citado en 2016-03-12]. Disponible en Internet http://es.hkvstar.com/technology-news/difference-between-nvr-hd-sdi-dvr-hvr-dvr-hdcvi.html.

[10] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 7 mar 2016 a las 10:47. Disponible en Internet https://es.wikipedia.org/wiki/RAID.

[11] Alcaldía Mayor de Bogotá D.C. [En línea]. diciembre 04 de 2006. Disponible en Internet http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=22391.

[12] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 5 feb 2016 a las 00:09. Disponible en Internet https://es.wikipedia.org/wiki/Spanning_tree.

[13] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 15 mar 2016 a las 11:17. Disponible en internet https://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida.

[14] WIKIPEDIA La enciclopedia libre. [En línea]. Actualizada el 27 dic 2015 a las 19:33. Disponible en Internet https://es.wikipedia.org/w/index.php?title=Videograbadora&redirect=no

RESUMEN

El desarrollo de las tecnologías ha permitido en algunos casos la aparición de nuevos productos, en otros la evolución, como es el caso de las cámaras de vídeo vigilancia, que pasaron de enviar simples imágenes sin procesar por un cable coaxial, a ser enviadas y procesadas por otros mecanismos más eficientes en las redes de datos.

Las cámaras se han incorporado o son parte de las redes computacionales, permitiendo ejecutar diferentes procesos. La información capturada puede ser guarda en sistemas de almacenamiento, además de ser monitoreadas a distancia, estas funcionalidades son las que permiten utilizarlas en diferentes aplicaciones, como son el control de tráfico, seguridad y es esta última, donde se enfoca la presente monografía, para orientar a los usuarios que tienen a cargo un sistema de vigilancia urbana, para que sean conscientes que la información manejada es importante y se debe proteger de una forma eficiente.

La aplicación de estas cámaras en sistemas de vídeo vigilancia puede involucrar muchos dispositivos tecnológicos en redes como: switch, computadores, servidores, sistemas de almacenamiento, medios de transmisión, sistemas eléctricos, controles de acceso, sistemas de refrigeración. Es en este punto, donde un sistema de gestión de seguridad de la información entra a jugar un papel importante; la mala manipulación de estos recursos puede dejar completamente fuera de servicio los sistemas de vídeo vigilancia, colocando en riesgo la seguridad de la comunidad y la Información.

INTRODUCCIÓN

Las autoridades y dirigentes Colombianos han visto como la sociedad percibe un alto nivel de inseguridad en sus calles, estos delincuentes no son personas individuales, estas constituyen bandas criminales y organizadas, las cuales han perfeccionado sus habilidades en los diferentes delitos.

Por eso, las autoridades en su lucha, ven cada vez más indispensable la utilización de los medios tecnológicos, para poder realizar los seguimientos y capturas, las cuales en medios televisivos y escritos son resaltadas por sus detalles en las investigaciones, permitiendo desmantelas bandas organizadas, que ha permitido a las autoridades obtener resultados positivos y buena aceptación en la sociedad.

Uno de esos medios tecnológicos son las cámaras de seguridad, aunque no es nuevo en nuestro entorno, en los últimos años ha tenido una gran evolución y por eso están siendo utilizadas para diferentes aplicaciones, como es el control de tráfico y vídeo vigilancia.

La vigilancia o monitoreo por cámaras es importante en el campo comercial y más cuando las autoridades pueden utilizar este medio en las calles, donde pueden monitorear las 24 horas del día, pero desplegar esta vigilancia implica un infraestructura grande en equipos tecnológicos, medios de transmisión, software y personal que pueda operarlas, para que el objetivo de las vigilancia surta los resultados esperados.

Esta monografía no se enfoca en cómo está instalado la red de vídeo vigilancia, que tecnología utiliza o capacidad tienen las cámaras, la importancia radica en el manejo de la información, lo que persigue es concientizar a las personas que están involucradas con este proyecto en el municipio de Yacuanquer, donde una buena gestión en las seguridad de la información, permitirá que el sistema obtenga los resultados esperados para el cual fue diseñado.

Para ello se aplicó el estándar ISO 27001:2013, en el circuito cerrado de televisión (CCTV), que permite mejorar su seguridad, gestión y continuidad, permitiendo que no quede inutilizado por un riesgo que pudo ser gestionado de una forma oportuna.

Para hacer la implementación del estándar ISO 27001:2013, primero se debió conocer el sistema y sus procesos, por eso en el capítulo contexto de la organización se describe como está conformado el sistema actual, su ubicación área de cobertura equipos que lo conforman, los factores a los cuales está expuesto.

El capítulo políticas de seguridad permite enmarcar al sistema en un camino a seguir para su buen funcionamiento, además se involucró a la policía en la gestión de los procesos que se deben llevar, tratando de enfocarse en puntos pertinentes al trabajo, teniendo en cuenta que el personal que labora en la estación está sujeto a traslados debido a las políticas establecidas a nivel central.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La implementación de los circuitos cerrados de televisión (CCTV), sumado al esfuerzo y el compromiso del Ministerio del Interior, la Policía Nacional y las autoridades regionales y locales, permiten visibilizar una reducción de los delitos de mayor impacto, como es el homicidio, hurto de vehículos, entre otros, mejorando la percepción de seguridad en el municipio.

Los ciudadanos son los beneficiarios directos de esta inversión, porque con el circuito cerrado de televisión (CCTV) instalado, se logra una vigilancia de 24 horas en las zonas, con altos índices de delincuencia y por ende, una reacción rápida de la Policía.

El sistema de CCTV del municipio de Yacuanquer, fue entregado a la estación de policía, para su administración y operatividad, esta responsabilidad recae sobre un grupo de patrulleros designados por el comandante, los cuales deben responder por la información que allí se genere.

El personal que allí opera el sistema tiene unos vagos conocimientos en el manejo y tratamiento de la información, la capacitación que obtuvieron estos patrulleros fueron en la utilización de estos equipos.

Cuando existe rotación de personal, y se incorpora personal nuevo a la estación de policía, algunos de los patrulleros antiguos son los encargados de orientar la capacitación sobre el manejo de los equipos, pero se omite el tratamiento que se le debe dar a la información que se genere.

La falta de capacitación y el alto volumen de rotación que tienen el personal de la policía nacional del municipio de Yacuanquer, genera un alto riesgo para la seguridad de la información que allí se produce, donde se puede incurrir en pérdida de información y un mal tratamiento a los datos, por causa del mal manejo de los equipos, por virus, por instalaciones indebidas de software, copias injustificadas de vídeos para terceros.

Así mismo se hace necesario establecer un método de autenticación a cada uno de los usuarios que manipulan el sistema de vídeo – vigilancia, con esto generar trazabilidades que permita identificar que usuarios han manipulado la información

que allí se produce, es de tener en cuenta que la información que allí se genera deben conservar su integridad debido a que está, es utilizada como pruebas en un delito, justificación de un operativo, prevención de delitos, seguimientos y vigilancia de actividades sociales.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede mejorar la gestión de seguridad y continuidad del circuito cerrado de vídeo vigilancia de la estación de policía del municipio de Yacuanquer, implementando un sistema de seguridad de la información?

1.3 OBJETIVOS

1.3.1 Objetivo general

Implementar un sistema de gestión de seguridad de la información en el circuito cerrado de televisión (CCTV) subsistemas SIES[15] del municipio de Yacuanquer. Bajo la norma ISO 27001:2013

1.3.2 Objetivos específicos

1) Realizar un análisis del estado actual de seguridad de la información en el circuito cerrado de televisión (CCTV) del municipio de Yacuanquer - Nariño.

2) Definir políticas del sistema de seguridad de la información, para el circuito cerrado de televisión (CCTV) en la estación de policía del municipio de Yacuanquer – Nariño, basado en la norma ISO 27001:2013.

3) Determinar los activos de información mediante MAGERIT del circuito cerrado de televisión (CCTV) en la estación de policía del municipio de Yacuanquer – Nariño, y darles la clasificación de seguridad aplicable para cada uno.

4) Definir salvaguardas y plan de seguridad mediante MAGERIT para el circuito cerrado de televisión (CCTV) en la estación de policía del municipio de Yacuanquer – Nariño justificación.

[15] Sistema Integrado de Emergencias y Seguridad

1.4 JUSTIFICACIÓN

La implementación de "un sistema de gestión de seguridad de la Información, basado en la norma UNE-ISO/IEC 27001:2013, es una herramienta o metodología sencilla y de bajo coste que cualquier PYME puede utilizar. La norma le permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de su organización[16]".

La aplicación correcta de esta norma es "la respuesta a la preocupación sobre la seguridad de la información, simplifica y permite gestionarla mejor, convirtiéndose en el instrumento indispensable para compañías, particulares y grandes organizaciones partiendo del hecho de que la clave está en el contenido estructurado de la información[17]".

La Policía Nacional de Colombia entre unos de sus objetivos es brindar protección y seguridad a los ciudadanos, para lo cual se vale de diferentes métodos de vigilancia, métodos que hoy en día vienen acompañados de un sinnúmero de tecnologías, entre ellas encontramos los sistemas de circuito cerrado de televisión (CCTV).

La policía para brindar una mejor seguridad a la población de Yacuanquer ha instalado uno de estos sistemas, pero día tras día se está generando información muy valiosa, la cual, requiere que sea protegida de manera especial, debido a que mucha de esta información es utilizada para procesos de tránsito, para pruebas de delitos, entre otros, y se requiere que la información sea confiable, disponible e integra.

Por lo tanto este estudio pretende aplicar métodos que permitan proteger la información que se genera del circuito cerrado de televisión (CCTV), a través de la norma ISO 27000:2013, lo que nos permite disminuir el impacto de los riesgos que se puedan producir allí en la estación, sin necesidad de hacer grandes cambios. Para ello es necesario la planificación e implantación de ciertos controles basados en un análisis de riesgo.

---

[16] Implantación de un sistema de SGSI en la empresa. [En línea]. Pan Avanza2. [España]. (Sin fecha). [Citado en 2016-03-10]. Disponible en Internet https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf.

[17] GOMEZ, Luis y ANDRÉS, Ana. Guía de aplicación de la Norma UNE-ISO/IEC 27001sobre seguridad en sistemas de información para pymes. España, AENOR, 2009. ISBN: 978-84-8143-602-0 Citado por Las ventajas y beneficios de la implantación de un SGSI. [En línea]. España. CSO España Computerworld. 14 de abril de 2010. [citado en 2016-03-10]. Disponible en Internet http://cso.computerworld.es/defensa-perimetral/las-ventajas-y-beneficios-de-la-implantacion-de-un-sgsi.

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcance

Está monografía está ubicado en la línea de gestión de seguridad de la información, y busca la aplicación de un sistema de gestión de seguridad de la información (SGSI) en el circuito cerrado de televisión (CCTV), subsistema de emergencias y seguridad (SIES) del municipio de Yacuanquer.

1.5.2 Limitaciones

Es de resaltar que el desarrollo del presente proyecto, no enmarca temas como los que se definen a continuación:

1) Las etapas de operar, verificar, y actuar un sistema de seguridad Informática, Únicamente abarcara el estudio al circuito cerrado de televisión (CCTV) del municipio de Yacuanquer.

2) Se entregara la propuesta de seguridad de la información para el circuito cerrado de televisión (CCTV), al comandante de la estación de policía del municipio de Yacuanquer, pero no será implementa.

1.6 DISEÑO METODOLÓGICO

1.6.1 Tipo de investigación

Investigación cualitativa "Los autores Blasco y Pérez (2007:25), señalan que la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas[18]".

Utiliza variedad de instrumentos para recoger información como las entrevistas, imágenes, observaciones, en los que se describen las rutinas y las situaciones problemáticas.

[18] BLASCO, Eugenia; PEREZ José Antonio. Metodologías de la Investigación en las ciencias de la actividad Física y el Deporte. Editorial Club universitario. San Vicente (Alicante). 2007. p. 25

Se toma este enfoque, porque se estudia un sistema implementado y funcional, se pretende dar una respuesta a una situación problema que tiene en su ejecución.

1.6.2 Método de investigación

Investigación – acción: Lomax (1990) define la investigación-acción como «una intervención en la práctica profesional con la intención de ocasionar una mejora[19]».

Se toma una realidad y se busca mejorarla con la implementación de un estándar de seguridad que se ha venido aplicando en diferentes ámbitos empresariales, este estándar aplicado a un sistema de vídeo vigilancia, que busca concientizar a los funcionarios de la importancia de la seguridad y que mejore su desempeño.

1.6.3 Población

La presente monografía tiene como población objetivo el circuito cerrado de televisión implementado por la policía Nacional.

1.6.4 Muestra

La muestra en el cuál se enfocó la monografía, fue el circuito cerrado de televisión (CCTV) del municipio de Yacuanquer – Nariño.

1.6.5 Variables

1) **Gestión**: desde la dirección, en este caso el comandante asume una posición de pertenencia asía el sistema e involucre en su funcionamiento al personal designado.

2) **Seguridad**: que la información procedente de cada cámara esté disponible, se asegure su confidencialidad y la integridad.

3) **Continuidad**: el proceso de SGSI permite también la continuidad del sistema.

[19] Ibíd., p. 121.

1.6.6 Recolección de datos

1.6.6.1 La observación

"Es el método por el cual se establece una relación concreta e intensiva entre el investigador y el hecho social o los actores sociales, de los que se obtienen datos que luego se sintetizan para desarrollar la investigación[20]".

Los diferentes mantenimientos realizados al sistema, brindo una oportunidad de interacción con los diferentes recursos, como son los equipos que están instalados y el recurso humano que labora diariamente en la sala de monitoreo, esto permitió observar cómo se realizan los diferentes procesos que se llevan a cabo.

Para recolectar la información se realizó a través de un formato que se diligencio en unas visitas y permitió documentar los hallazgos encontrados.

1.6.6.2 Revisión de documentación

El contratista al momento de la entrega y puesta en marcha del sistema de vigilancia, dejaron una documentación, que se encuentra en el archivo de la Policía, esto permite consultar los equipos instalados, planos que se realizaron, diagrama de red, recorridos de fibra.

1.6.6.3 Entrevistas individuales y/o colectivas

Las entrevistas se utilizan para recabar información en forma verbal, a través de preguntas. Quienes respondieron fueron el Comandante y Patrulleros, los cuales son operadores actuales del sistema existente.

1.6.6.4 El cuestionario

Para conocer más sobre el sistema, desde el punto de vista de las personas que intervienen diariamente en él, se realizó una encuesta donde cada individuo lleno un formato que no tomo más de 20 minutos en contestarlo.

[20] Prof. FABBRI, María Soledad. Las técnicas de investigación: la observación. [En línea]. [citado en 2016-03-10]. [35 renglones]. Disponible en Internet http://www.fhumyar.unr.edu.ar/escuelas/3/materiales%20de%20catedras/trabajo%20de%20campo/solefabri1.htm.

1.6.6.5 Diagrama de flujo

Es una representación gráfica de los pasos que se llevan para realizar una actividad. Útil para determinar cómo funciona realmente el proceso para producir un resultado.

Esto fue un resultado de una observación en sitio, sobre las actividades que se realizan, también de las experiencias que se han obtenido en el trascurso de los mantenimientos que se han realizado.

1.6.7 Metodología a utilizar del SGSI

La norma 27001 está diseñada para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información[21]. Para alcanzar los objetivos propuestos en el sistema de vídeo vigilancia del municipio de Yacuanquer se propuso un enfoque basado en procesos[22]. Se puede considerar como proceso cualquier actividad que use un recurso.

El enfoque basado en procesos hace énfasis en la importancia de:

1) Comprender los requisitos de seguridad de la información.

2) La necesidad de establecer la política y objetivos en relación con la seguridad de la información.

3) Implementar y operar controles para mejorar los riesgos de la seguridad de la información.

4) El seguimiento, revisión del desempeño y eficacia del SGSI.

1.6.7.1 Planificar

Establece la política, los objetivos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, (ver figura 1).

[21] ICONTEC. Compendio Seguridad de la Información. Técnicas de Seguridad .. Editada en 2006-04-03. Colombia, Icontec, Marzo de 2013, p. I. ISBN: 978-958-8585-37-6
[22] Ibíd.,

Figura 1: Etapa de Planificación

Fuente: CORTI, María Eugenia. Metodología para la Implementación de SGSI. [Online]. Uruguay. AGESIC. 24/06/2010. Pg.; 20. Disponible en Internet http://www.agesic.gub.uy/innovaportal/file/1065/1/primera.pdf

1.6.7.2 Hacer

Implementar y operar la política, los controles, procesos y procedimientos del Sistema de Gestión de la Información (SGSI), (Figura 2).

Figura 2: Etapa de Implementación

Fuente: Ibíd.; p. 30

2. MARCO TEÓRICO

2.1 MARCO CONCEPTUAL

2.1.1 Sistemas de información

"Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para para conseguir sus objetivos[23]".(Ver figura 3)

En la actualidad las empresas, tienen funcionando un sistema de información, la cual permita dar respuesta a una determinada solicitud; no se puede concebir en la actualidad, que una empresa u organización no implemente esta herramienta dentro de su organización, esta puede estar formada por:

Recursos: sus elementos físicos como son los ordenadores, periféricos o lógicos como son los programas que esté utilizando para realizar sus actividades.

Equipo humano: está conformada por las personas que laboran en la empresa u organización y cumplen una función específica para alcanzar los objetivos.

Información: toda actividad realizada interna o externa produce información, la cual la empresa debe de guardarla, puede ser considerada importante o relevante según el trato que tenga, pero esta debe ser organizada, para que en cualquier momento pueda ser consultada.

Actividades: son las actividades que realiza la organización para alcanzar los objetivos que se ha propuesto.

[23] AGUILAR, Purificación. Seguridad informática, España, Editex S.A, 2010. p. 8. ISBN 978-84-9771-4

Figura 3: Sistemas de información

Fuente: AGUILAR, Purificación. Seguridad informática. [En línea]. Madrid. Editorial Editex. 1/06/2010. p. 8. Disponible en Internet https://books.google.com.co/books?id=Mgvm3AYIT64C&printsec=frontcover&hl =es#v=onepage&q&f=false

2.1.1.1 Actividades de un sistema de información

"Un conjunto de elementos interactivos, que puedan ser diseñados para que, en forma cooperativa, logren cumplir una función dada, o alcanzar propósitos determinados[24]".

Los procesos que se desarrollan dentro de una organización, por pequeña que sean, producen información las cuales son para toma de decisiones, controlar procesos, crear productos o servicios (ver figura 4).

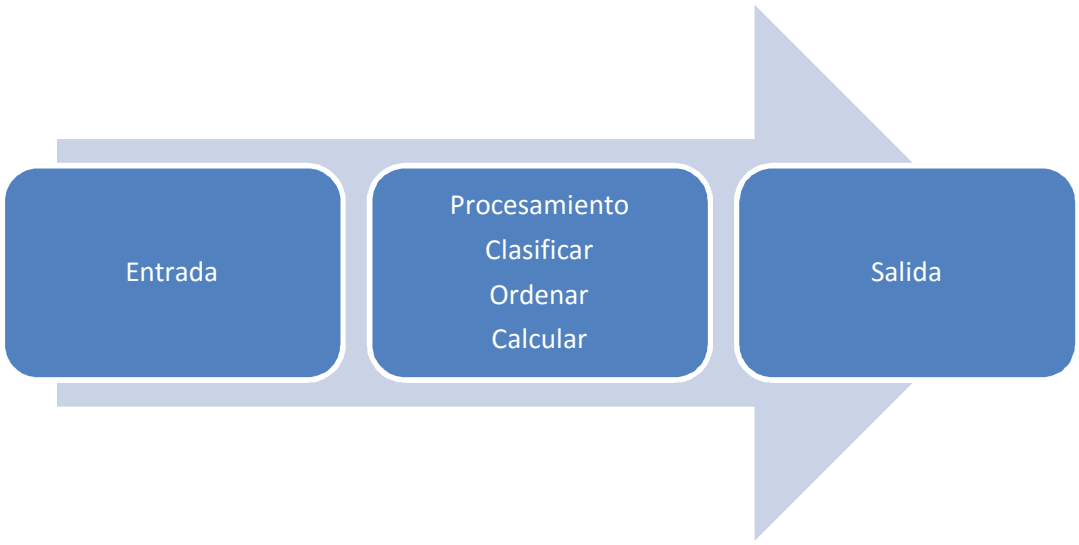
Entrada: capturan los datos desde su entorno interno o externo.

Procesamiento: organiza la información de una forma adecuada la cual permite ser recuperada o consultada.

Salida: transfiere la información al cliente que lo solicite.

[24] G. Levaggi. Teoría general de sistemas, UGERMAN editor, Buenas aires, 1999. Citado por FUENTES, Eddy. Sistemas de información gerencia. [En línea]. Co-autor Márquez José Luis. La Paz Bolivia, ANESAPA. Septiembre de 2003. p. 9. Disponible en Internet http://es.slideshare.net/nancy2805/sistemas-de-informacion-8872288?related=3.

Figura 4: Sistemas de Información



Fuente: Propiedad del Autor.

2.1.1.2 Entorno de un sistema de información

"Combinación organizada de personas, mecanismos físicos (Hardware), procedimientos e instrucciones de procesamiento de información (software), canales de comunicación (redes) y datos almacenados (recursos de datos) que reúnen, transforman y diseminan información en una organización[25]".

El entorno de la organización está formada por los clientes o usuarios, competidores, agencias regulatorias que interactúan con su sistema de información.

Por muy pequeña que se la organización esta debe interactuar con agentes externos.

Los sistemas de información crean un valor a la organización, creando una respuesta o solución a los retos que el entorno impone.

Enfocándonos en los sistemas de Circuitos Cerrados de Televisión, para la seguridad ciudadana operados por la Policía, este sistema crea valiosa

[25] James, A O Brien, sistemas de Información Gerencial. 4° Edición. McGraw-Hill. Bogotá, 2001. Citado por Ibíd., p. 17.

información, que puede ser utilizadas por diferentes entidades como pruebas de algún caso.

2.1.1.3 Dimensión de los sistemas de información

Un sistema de información, provee una solución a una organización en su conjunto para que esta pueda cumplir con el objetivo que se ha establecido.

Organización

"Cada organización tiene una cultura única, o conjunto fundamental de supuestos, valores y formas de hacer las cosas, que la mayoría de los miembros han aceptado[26]".

Son diferentes componentes que interactúan para que funcionen los procesos de negocio, hablando técnicamente de un negocio con fines de lucro, pero en el caso de la Policía, el negocio es la seguridad y en ellos intervienen diferentes componentes para cumplir su objetivo; como organización, está también tiene sus niveles de jerarquía que permite delegar funciones.

El sistema de CCTV, a la Policía, le permite como herramienta tecnológica cumplir con su objetivo de brindar seguridad y control a una población en específico, además de ofrecer información importante que le permita elaborar estrategias para su labor.

Administración

"El trabajo de la gerencia es dar sentido a las distintas situaciones a las que se enfrentan las organizaciones, tomas decisiones y formular planes de acción para resolver los problemas organizacionales[27]".

El sistema de CCTV, brinda información real del lugar, movimientos de gente y vehículos, que pueden ser tomadas por el comandante para hacer un plan de operatividad, sin poner en riesgo a su personal.

[26] LAUDON, Kenneth y LAUDON, Jane. Sistemas de información gerencial. 12° ed. México, Pearson, 2012. p. 20. ISBN 978-607-32-0949-6
[27] Ibíd.

La información obtenida de los operativos grabados, puede dar información al comandante del comportamiento y procedimientos ejecutados por su personal y hacer ajustes que permitan mejorar el servicio prestado.

Tecnología de la información

"Todas las tecnologías, junto con las personas requeridas para operarlas y administrarlas, representan recursos que se pueden compartir en toda la organización y constituye **la infraestructura de tecnología de la información (TI)** de la empresa[28]".

Este tipo de sistemas ha evolucionado, debido a los avances tecnológicos que se han desarrollado en el campo de la computación, software, almacenamiento y transmisión de los datos.

Estos avances permitieron que los sistemas de CCTV hoy en día sea más utilizados por empresas y particulares con el objetivo de vigilancia.

2.1.2 Sistema de gestión de seguridad de la información

"Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización"[29].

En la actualidad las empresas tienen sus sistemas de información en línea, ya sea internamente con una Intranet o externa con Internet, de cualquier forma la información está expuesta por alguna amenaza que pueda afectar su funcionamiento.

2.1.2.1 Norma ISO/IEC 27001:2013

La información es uno de los activos importantes de una organización, es por eso que se debe de gestionar de una forma segura, la cual permita su integridad,

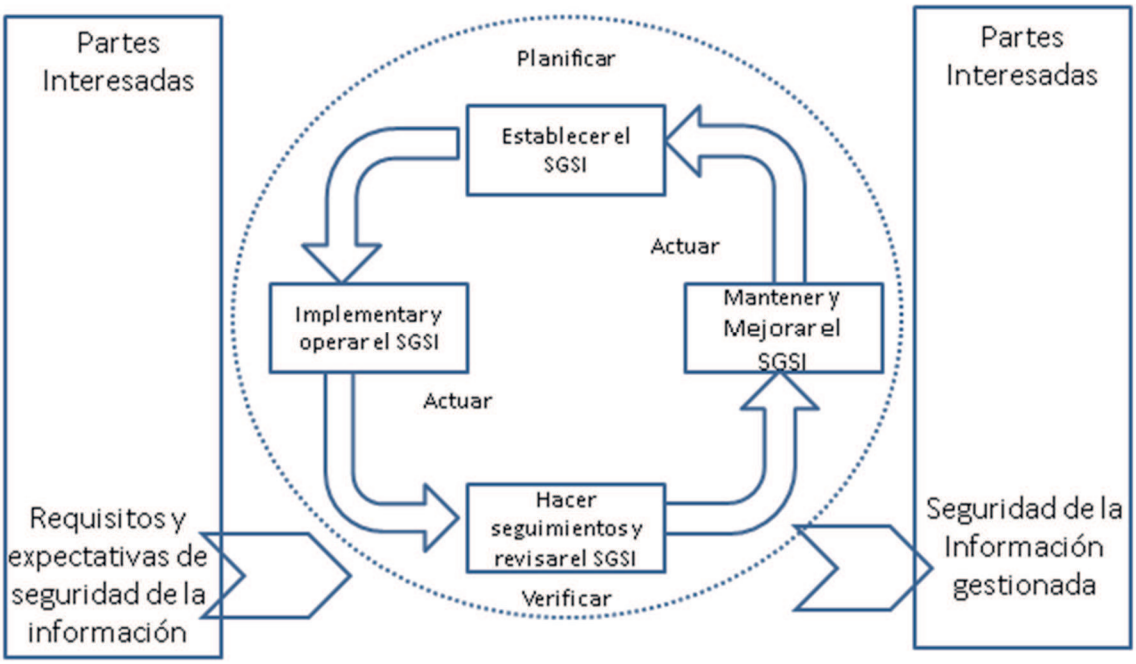
[28] Ibíd., p. 21.
[29] GOMEZ, Luis & FERNANDEZ, Pedro. Cómo Implantar Un SGSI Según UNE-ISO/IEC 27001:2014 Y Su Aplicación En El Esquema Nacional De Seguridad. [En línea]. España. AENOR. 2015. p 11. Disponible en Internet: http://www.aenor.es/aenor/descargafichero.asp?tipo= pub&registro=11248&archivo=1

confidencialidad y disponibilidad; para esto se ha creado un norma a nivel internacional para que las organizaciones puedan implementarla.

Una de las normas que más se han difundido es la ISO/IEC 27001:2013, "Esta norma específica los requisitos para establecer, implementar, mantener y mejorar de manera continua un SGSI, teniendo en cuenta los objetivos y riesgos de la organización"[30], ajustándose a las necesidades de la organización; como son sus objetivos y necesidades del negocio.

Para lograr que se cumpla este proceso, la norma se ajusta el modelo PHVA, esto permite al Sistema de Gestión de la Seguridad de la Información este en continuo cambio y mejora (figura 5).

Figura 5: Modelo PHVA Aplicado a los procesos de SGSI



Fuente: ICONTEC. Seguridad de la Información. Colombia, Legis, Marzo 2013. p, I.

[30] Ibíd., p. 14.

2.1.2.2 Implantación de un SGSI

"Este sistema consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad"[31], en el cual se compromete la dirección en apoyar y dirigir el sistema para que cada uno de las áreas o individuos que intervienen se involucren en su ejecución.

El diseño que se plantee debe estar orientado por los objetivos, necesidades y estructura de la organización, con esto se define el alcance que tendrá el SGSI; este sistema solo puede implantarse en las áreas que la dirección, crea que se necesite no es necesario que se deba involucrar a toda la organización.

Toda organización que implemente un SGSI, deberá ser consiente que el sistema debe estar en una continua evolución, que el modelo PHVA ofrece, para esto debe estar documentado y estos son:

Políticas: "documento de contenido genérico que establece el compromiso de la Alta Dirección y el enfoque de la organización en la gestión de la seguridad de la información"[32], las políticas deben responder a las necesidades de la organización en cuanto a la seguridad y deben ser conocidas por todos dentro de la organización.

Procedimientos, y guías que soportan el SGSI: aquellos documentos y mecanismos que regulan el propio funcionamiento del SGSI. Documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados -métricas.

Instrucciones: definido los procedimientos se debe hacer la descripción técnica, comandos para realizar un procedimiento, debe ser conocido solo para las personas técnicas.

Registros: son los documentos que se deben dejar como evidencia de los

[31] GOBIERNO EN LÍNEA. Entregables 3, 4, 5 Y 6: Informe Final – Modelo De Seguridad De La Información – Sistema Sansi - SGSI - Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea. [En línea]. Bogotá. Diciembre de 2008. p., 15. Disponible en Internet: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

[32] Ibíd., p. 18.

procedimientos, esto permitirá realizar una evaluación del cumplimiento de los objetivos.

1) **Planificar**. Se realiza un estudio de la situación de la organización, en cuanto a la seguridad; analizando los riesgos a los que están expuestos los activos, definido los riegos se deben gestionarlos para reducirlos; se establece la política, los objetivos, procesos y procedimientos de seguridad para mejorar la seguridad de la información; definiendo el alcance del SGSI.

2) **Hacer**: Es importante que en esta etapa se de una formación al personal, sobre el sistema, es importante el compromiso de los usuarios para su futuro funcionamiento.

Desarrollada la capacitación, se llevara a cabo la implantación de los controles seleccionados en la fase anterior, para esta fase es importante la documentación, la cual permitirá al sistema en el futuro ser evaluado, el registro de las actividades o controles por parte de los integrantes de las áreas que estén involucradas.

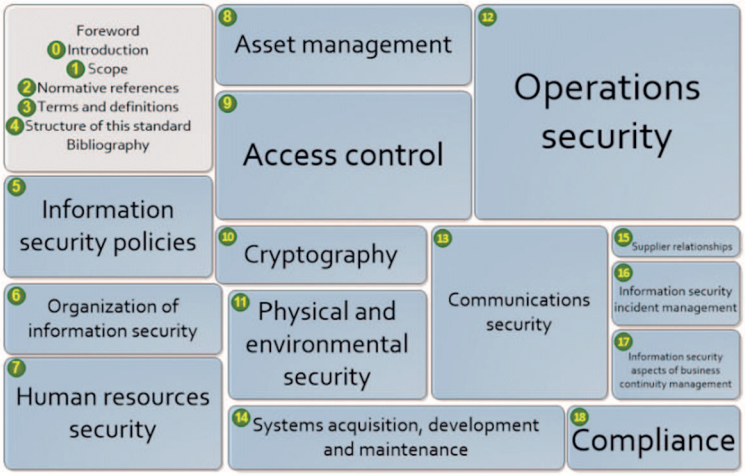
3) **Verificación**: Realizar seguimiento para medir los procesos y los controles en relación con las políticas, los objetivos y los requisitos, reportando los resultados alcanzados.

4) **Actuar**: Realizar actualizaciones en la información del inventario de activos. Adelantar las recomendaciones producto de las auditorías realizadas.

2.1.2.3 Norma ISO/IEC 27002

Esta se crea como una guía de buenas prácticas para la seguridad de la información en cualquier empresa, contiene 14 secciones; estas unas medidas que se debe tomar para asegurar los sistemas de información de una organización (ver figura 6).

Figura 6: Dominios de la norma



Fuente: ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. [En línea]. The second corrigendum was published in November 2015. Disponible en formato HTML en: http://www.iso27001security.com/html/27002.html#StructureAndFormatOfISO17799

2.1.2.4 Norma ISO/IEC 27005

Esta Norma internacional se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001:2013.

2.1.2.5 MAGERIT V3

El proceso de gestión de los riesgos a los cuales se ve expuesto un sistema, es un proceso complejo el cual se debe hacer minuciosamente sin dejar nada al azar, esto permite conocer a profundidad el sistema y como cumple su objetivo para la organización, MAGERIT "En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección. Al conjunto de estas

actividades se le denomina proceso de gestión de riesgos"[33].

El conocer los riesgos es importante para una organización, permite que se puedan tomar decisiones en cuanto a su operación y su costo, permitiendo un beneficio en cuanto a sus recursos económicos, es más barato prevenir que destinar recursos a arreglar lo que se ha dañado.

Las tareas que se deben realizar en el proceso de gestión de riesgo se gráfica en el siguiente cuadro (figura 7).

Figura 7: Gestión de riesgos

Fuente: Propiedad del Autor

El análisis de riesgos considera los siguientes elementos

1) Activos.

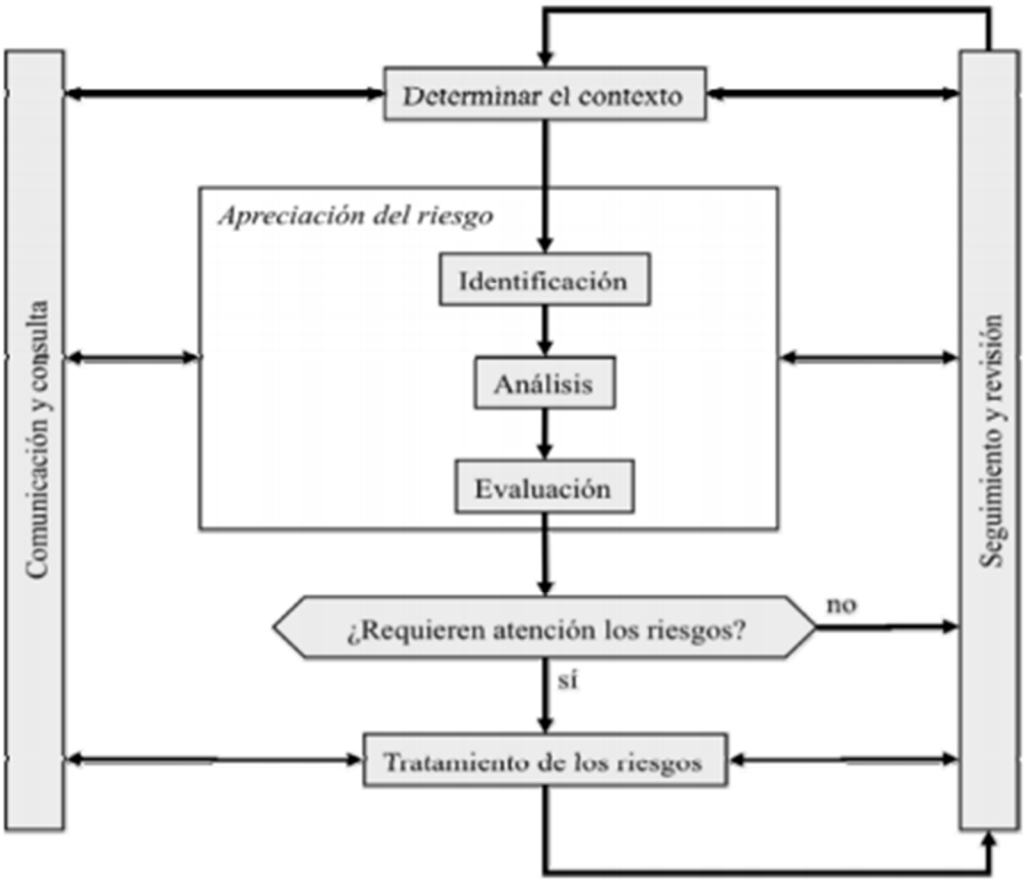
2) Amenazas

[33] Ministerio de Hacienda y Administraciones Públicas. MAGERIT. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. Madrid Octubre de 2012. Libro I – Método. p.; 10. Disponible en internet: http://administracionelectronica.gob.es /pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/ 2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9 todo_es_NIPO_630-12-171-8.pdf

3) Salvaguardas

El análisis de estos elementos, se hacen en forma metódica para establecer unas conclusiones con fundamento y proceder a su tratamiento, en el siguiente gráfico se puede ver la estructura de esa metodología (figura 8).

Figura 8: Gestión de riesgos



Fuente: Ministerio de Hacienda y Administraciones Públicas. MAGERIT. Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Online]. Madrid Octubre de 2012. Libro I – Método. p.; 20. Disponible en internet: http://administracionelectronica.gob.es /pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/ 2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9 todo_es_NIPO_630-12-171-8.pdf

2.1.2.6 Amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información a partir de la existencia de vulnerabilidades.

Una organización en la actualidad se puede ver expuesta a diferentes amenazas y es diferente para cada una y el grado de exposición.

Por eso es importante ayudarse de un método como lo es MAGERIT, que permita evaluar el grado de exposición del sistema, MAGERIT agrupa estas amenazas en las siguientes ítems.

1) **De origen Natural**: un sistema está expuesto a una amenaza de tipo natural cuando por razones o elementos del medio ambiente causan daños.

2) **Del entorno (origen Industrial):** son desastres industriales ajenos al sistema como pueden ser fallos eléctricos.

3) **Defectos de las aplicaciones**: este tipo de amenazas hace referencia a los equipos propios de su diseño o una mala implementación que causa consecuencias negativas.

4) **Causadas por las personas de forma accidental:** los usuarios del sistema en este caso operadores pueden causar daños al sistema por desinformación o por omisión; también pueden causados por persona externas en el caso del sistema de CCTV está expuesta la fibra por posibles accidentes.

5) **Causadas por las personas de forma deliberada:** esto se debe a que personas con acceso al sistema puedan dañar la información, en otros casos el sistema de CCTV puede estar expuesto en la calle a vandalismo.

La exposición de un activo ante las amenazas puede causar deterioro.

Valoración de la amenaza: el activo expuesto puede ser afectado no en su totalidad y se debe evaluar su influencia en el valor del activo, en dos sentidos:

1) **Degradación**: en cuanto se perjudico el activo

2) **Probabilidad**: que probable es que se materialicé la amenaza.

Tabla para determinar la degradación del valor de un activo, modelada cualitativamente (tabla 1).

Tabla 1: Riesgo Residual

MA	**Muy Alta**	**Casi seguro**	**Fácil**
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente difícil

Fuente: Ibíd.; p. 28

Tabla modelada numéricamente (tabla 2)

Tabla 2: Riesgo Residual - Numérica

MA	100	Muy Frecuente
A	10	Frecuente
M	1	Normal
B	1/10	Poco Frecuente
MB	1/100	Muy poco frecuente

Fuente: Ibíd.; p. 28

2.1.2.7 Salvaguardas

Es una contramedida o procedimiento que se implementa para reducir el riesgo al cual está expuesto un activo.

Existen diferentes tipos de salvaguardas dependiendo del objetivo que cumplan, entre esta se tiene:

1) **Prevención**: buscar reducir la oportunidad de que se produzca un incidente.

2) **Disuasión**: produce un efecto sobre un atacante para que lo piense antes de realizar alguna acción.

3) **Corrección**: se produce después de que se efectúa el daño para corregirla.

4) **Recuperación**: se produce después de un incidente y lo corrige regresándolo al estado inicial.

5) **Monitorización**: monitoriza lo que está ocurriendo en tiempo real.

6) **Concienciación**: son actividades de formación del personal.

2.2 MARCO LEGAL

El sistema de CCTV, implementado como instrumento para la convivencia de seguridad ciudadana, debe enmarcarse en un aspecto legal, para que los objetivos propuestos por la policía nacional se puedan alcanzar.

2.2.1 Decreto 4366 de 2006 por el cual se regula la operatividad de los sistemas integrados de emergencias y seguridad (SIES).

SIES sus siglas son sistema integrado de emergencias y seguridad, contempla varios subsistemas su implantación dependerá de la Alcaldía y los recursos que destine para su funcionamiento y el objeto para el cual se desarrolle, es el caso del sistema de llamadas 123, la cual se puede realizar, pero depende mucho de la disponibilidad de en rutar llamadas y de la cobertura que tenga el municipio, por lo general es instalado en las capitales de cada departamento.

En cada municipio, por la importancia que tiene se desarrollan los sistemas de vídeo vigilancia CCTV que es un subsistema del SIES.

En el artículo primero se establece la norma así:

"Artículo 1°. Los departamentos y municipios podrán solicitar la financiación o cofinanciación de proyectos de Sistemas Integrados de Emergencias y Seguridad (SIES), siempre y cuando garanticen su administración y sostenimiento, al Ministerio del Interior y de Justicia - Fondo Nacional de Seguridad y Convivencia Ciudadana (Fonsecon) bajo los parámetros señalados para el efecto, condición que deberá quedar consignada en los respectivos convenios interadministrativos que se celebran con cada una de las entidades solicitantes para la ejecución de los proyectos.

Parágrafo. Adicional al cumplimiento de las normas sobre presentación de proyectos, los proyectos de Sistemas Integrados de Emergencias y Seguridad (SIES) deben cumplir con los siguientes requisitos:

1. Establecer el objetivo fundamental para el uso e implementación del sistema, con el apoyo de la Fuerza Pública y los Organismos de Seguridad del Estado.

2. Justificación de la instalación del esquema tecnológico, puesta en marcha y su sostenibilidad en el tiempo, teniendo en cuenta que debe ser un sistema de carácter permanente para seguridad ciudadana y convivencia comunitaria.

En el artículo segundo se definen los subsistemas que lo pueden conformar, no es de obligatoriedad que se implementen todos, esto dependerá de la alcaldía y la Policía en cada municipio, de un estudio previo de seguridad y justificar su desarrollo.

Artículo 2°. El Sistema Integrado de Emergencias y Seguridad (SIES) estará conformado por los siguientes subsistemas:

1) Número Único Nacional de Seguridad y Emergencias (123).

2) Sistema de vídeo vigilancia mediante circuitos cerrados de televisión (CCTV).

3) Centros de Información Estratégica Policial (CIEPS).

4) Alarmas Comunitarias (A-C).

5) Sistemas de radio comunicaciones para redes de Cooperantes.

Artículo 3°. Las funciones de dirección del Sistema Integrado de Emergencias y Seguridad (SIES) serán ejercidas por la Policía Nacional[34]".

Las Funciones operativas del Sistema Integrado de Emergencias y Seguridad (SIES) serán ejercidas por la Fuerza Pública, Organismos de seguridad del Estado y demás entidades públicas y privadas responsables de atender los eventos de seguridad, convivencia ciudadana y emergencias, de acuerdo con las áreas de su competencia.

2.2.2 Decreto 399 de 2011 por el cual se establece la organización y funcionamiento del fondo nacional de seguridad y convivencia ciudadana y los fondos de seguridad de las entidades territoriales y se dictan otras disposiciones.

"Objetivos del Fondo. FONSECON tendrá como objeto recaudar y canalizar recursos tendientes a propiciar la seguridad y convivencia ciudadana para garantizar la preservación del orden público y todas aquellas acciones tendientes a fortalecer la gobernabilidad local y el fortalecimiento territorial, en el marco de la Política y la Estrategia Nacional de Seguridad y Convivencia Ciudadana[35]".

"Fondos Territoriales de Seguridad y Convivencia Ciudadana - FONSET. De acuerdo con lo establecido en el artículo 119 de la Ley 418 de 1997, prorrogada, modificada y adicionada por las Leyes 548 de 1998, 782 de 2002, 1106 de 2006 y 1421 de 2010, artículo 6°, todo municipio y departamento deberá crear un fondo cuenta territorial de seguridad y convivencia ciudadana, con el fin de recaudar los aportes y efectuar las inversiones de que trata la mencionada ley[36]".

2.3 MARCO NORMATIVO

La Política Nacional frente a la seguridad y convivencia ciudadana, establece los alcances, que se debe hacer para que la sociedad tenga unos niveles de seguridad aceptables, no se puede afirmar que se pueda lograr el 100%, pero permitirá a las entidades territoriales y la Policía Nacional trabajar en proyectos

[34] DECRETO 4366 DE 2006. [En línea]. Colombia. Alcaldía de Bogotá. Diciembre 04 de 2006. [citado en 2016-03-10]. Disponible en Internet http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=22391.
[35] DECRETO 399 DE 2011. [En línea]. Colombia. Alcaldía de Bogotá. Febrero 14 de 2011. [Citado en 2016-03-10]. Disponible en Internet http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41658.
[36] Ibíd.

que permitan alcanzar ese objetivo.

"En tal sentido, para efectos de la política, se entiende por seguridad ciudadana la protección universal a los ciudadanos frente a aquellos delitos y contravenciones que afecten su dignidad, su seguridad personal y la de sus bienes, y frente al temor a la inseguridad. La convivencia, por su parte, comprende la promoción del apego y la adhesión de los ciudadanos a una cultura ciudadana basada en el respeto a la ley, a los demás y a unas normas básicas de comportamiento y de convivencia social[37]".

2.3.1 Primer eje: Prevención social y situacional

Prevención situacional: esto tiene que ver con las acciones que las instituciones realizan para mantener y prevenir los delitos en espacios públicos, también impulsan la recuperación de vías; en este punto las instituciones tienen que Promover, el marco del sistema integrado de emergencias y seguridad (SIES), el uso de CCTV sostenibles –con grabación, monitoreo y análisis– en lugares estratégicos de centros urbanos priorizados, con fines preventivos, disuasivos, de control y judicialización.

2.3.2 Segundo eje: Presencia y control policial

"La seguridad y convivencia ciudadana necesitan el fortalecimiento estratégico de la capacidad de la Policía Nacional para la disuasión y control del delito, especialmente el que opera en el marco de una criminalidad organizada. Para contrarrestarlo, se hace indispensable una presencia próxima y permanente de la policía en la comunidad[38]".

Esto se refiere al accionar de la fuerza pública, en combatir los delitos, en este punto los sistemas de vídeo vigilancia CCTV están ayudando a la Policía Nacional a combatir los sitios donde se presentan delitos.

[37] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política Nacional de Seguridad y Convivencia Ciudadana. Bogotá D.C., Colombia. DNP, Dirección de Justicia, Seguridad y Gobierno. 2011. p. 1-2. Disponible en Internet http://wsp.presidencia.gov.co/SeguridadCiudadana/consejeria/Documents/Pol%C3%ADtica%20Nacional%20de%20Seguridad%20y%20Convivencia%20Ciudadana-%20Espa%C3%B1ol.pdf.

[38] Ibíd., p. 18.

2.4 MARCO TECNOLÓGICO

2.4.1 Sistema CCTV

Es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades en forma remota, según portal Whatls.com "CCTV (circuito cerrado de televisión) es un sistema de televisión en el que las señales no se distribuyen públicamente, pero se controlan, principalmente con fines de vigilancia y seguridad"[39]

(Ver figura 9) Una cámara de seguridad, es el componente de un sistema de vídeo vigilancia que, colocado en el lugar y a la distancia necesaria, permite ver una escena más allá de la capacidad de observación natural del hombre. Para confeccionar una lista de los elementos básicos que componen un sistema de vídeo vigilancia, es importante identificar primero las funciones y los requisitos que debe cumplir la cámara:

1) Debe poder disponer de un elemento sensible a la luz.

2) La luz que llega al elemento sensible debe poder ser regulada en su intensidad para poder recibir tanto la imagen de una penumbra.

3) Elemento protector (por ejemplo, un acrílico).

4) La cámara deberá disponer de motores que le permita moverse vertical y horizontalmente para poder observar hacia arriba, hacia abajo y hacia los costados cuando sea necesario.

5) Las imágenes recibidas por el elemento sensible deben poder transmitirse y ofrecer la sensación de la visión que de ella se requiere.

[39] ROUSE, Margaret. CCTV (circuito cerrado de televisión). [En línea]. Abril 2012. [Citado en 2016-03-10]. (renglones 1-2). Disponible en Internet http://whatis.techtarget.com/definition/CCTV-closed-circuit-television.

Figura 9 Cámara de seguridad

Fuente: www.samsung-security.com

En la cámara de seguridad lo que se logra es, recibir imágenes, convertirlas en señales eléctricas y reconvertirlas para poder ver en el dispositivo llamado "monitor".

El sistema de circuito cerrado de televisión más simple consiste de un cámara de TV, un monitor y un cable coaxial (hoy también se usan pares trenzados) que los conecta.

2.4.1.1 Historia

Los sistemas de vigilancia con cámaras, no es algo nuevo, estos se han desarrollado conforme se han presentado las necesidades en la sociedad.

En el campo militar, es donde se inician los primeros usos, la primera aparición fue en el año de 1942, Alemania donde se instalaron cámaras para poder monitorear el lanzamiento de los misiles V2; en estos mismos años, el gobierno Americano, las utilizo para monitorear las armas atómicas desde un área segura.

La aparición de estos sistemas en el mercado fue en 1949, quien lo comercializo fue la empresa Vericon, estos no podían grabar por lo cual se debía hacer un monitoreo continuo; fue en el año de 1951 en el cual se incorporaron los sistemas

VHS y VTR para que se pudiera grabar. En este mismo tiempo se generalizo el uso de estos sistemas en las entidades como bancos, tráfico, empresas utilizándolas como una medida de seguridad.

"La vídeo vigilancia urbana se convirtió en tema de discusión por primera vez en 1997, cuando fue seleccionado como uno de los temas clave de la conferencia europea sobre "prevención del crimen: hacia un nivel europeo", estos eran los comienzos de la vídeo vigilancia. Tres años antes, en 1994, el departamento del interior de Gran Bretaña inició una verdadera "revolución de la cámara de vigilancia", financiando una serie de retos de la ciudad (city challenge competitions) con un primer tramo de 2 millones de libras"[40].

"Según un informe de la agencia del gobierno Británico "red de estudios sobre la vigilancia", existen en este país unas 4.2 millones de cámaras de circuito cerrado de televisión (CCTV), lo que equivale aproximadamente a una cámara por cada catorce personas"[41].

2.4.1.2 Evolución

La tecnología vídeo vigilancia (CCTV), desde sus orígenes comienza siendo básica y muy costosas, además de ser difíciles de instalar, los primeros sistemas de vídeo vigilancia fueron totalmente análogos.

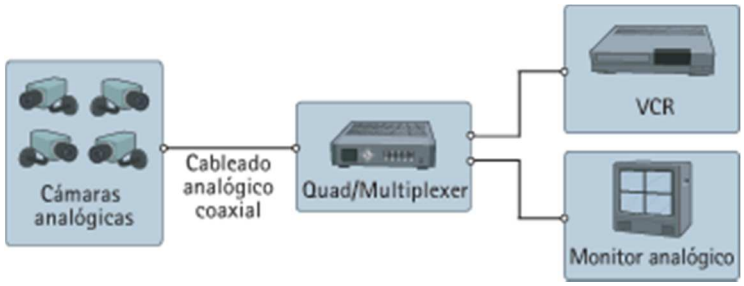
1) **Sistemas de circuito cerrado de TV analógicos usando VCR**: Estos sistemas se componían de cámaras análogas, que transmitían el vídeo a través de un cable coaxial[42], hasta el quad/multiplexer al cual está conectada una pantalla dividida, donde se observa las imágenes de cada cámara y de ahí hasta el VCR. Este utilizaba una cinta para grabar los vídeos, no ofrecía una calidad óptima. (Ver figura 10).

[40] Roxana C, Sperber S et alii. Ciudadanos, ciudades y vídeo vigilancia, Foro Europeo para la Seguridad Urbana. [En línea]. STIPA –Montreuil. Paris junio 2010. p.; 71,72. Disponible en Internet: http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_Publication_ES.pdf

[41] EL MUNDO INTERNACIONAL. Los británicos, Los Ciudadanos Más Vigilados. [En línea]. Actualizado jueves 02/11/2006 13:16. Disponible en internet: http://www.elmundo.es/elmundo/2006/11/02/internacional/1162469551.html

[42] CUAQUENTZI A, Vera et alii. Implementación de un Sistema de Seguridad vía Internet. [En línea]. México D.F 2008. p.; 11-12. Disponible en Internet: http://tesis.ipn.mx/jspui/bitstream/123456789/1986/1/IMPLEMENTACIONSISTVIA.pdf

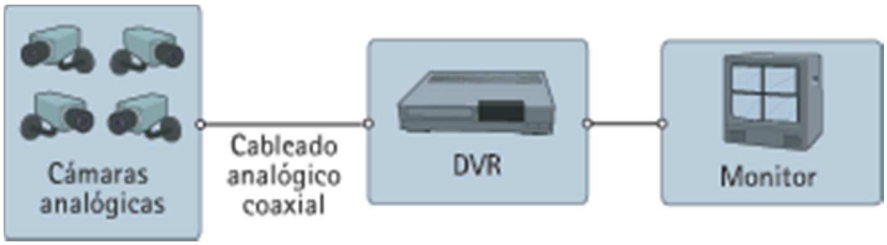
Figura 10: Sistema análogo



Fuente: GRUPO SOLUCIONES SIEMPRE. La evolución de los sistemas de CCTV. [Online]. México 4 de mayo de 2015. Disponible en Internet: http://www.solucionessiempre.mx/?p=699

2) **Sistemas de circuito cerrado de TV analógicos usando DVR**: Como evolución importante fue el cambio del quad/multiplexer y el VCR, por el DVR, esto constituye un gran avance, porque este dispositivo cambia el formato de una grabación análoga a una digital, utilizando como medio de almacenamiento el disco duro.; permitiendo que se guarden por más tiempo la grabaciones y acceder de forma inmediata a las grabaciones[43]. (Figura 11).

Figura 11: Sistema analógicos usando DVR

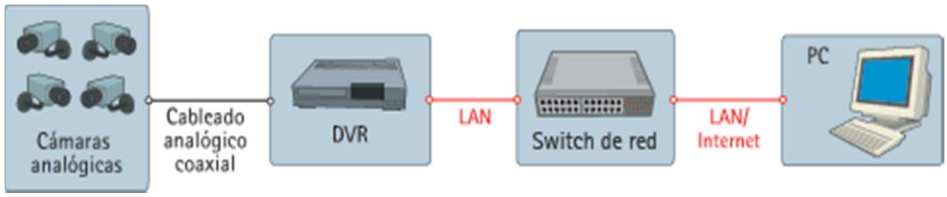


Fuente: Ibíd.

3) **Sistemas de circuito cerrado de TV analógicos usando DVR de red**: El DVR al incorporar un puerto de red Ethernet, esto permite que el sistema se pueda visualizar en forma remota, estas son las primeras apariciones de un sistema IP, el vídeo se puede transmitir a través de la red, porque el DVR comprime el vídeo y además tiene un formato digital (figura 12).

[43] CUAQUENTZI A, Op. cit.; p. 13

Figura 12: Sistema analógicos usando DVR de red

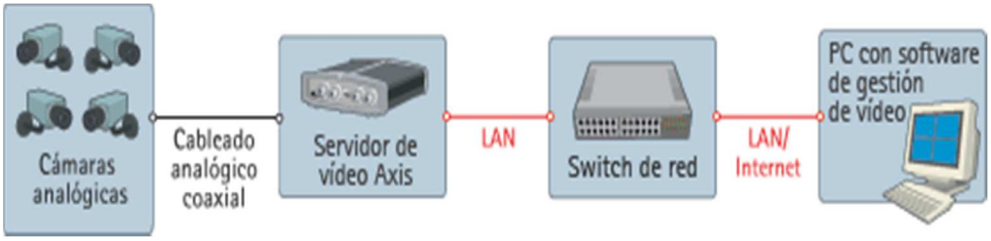


Fuente: Ibíd.

4) **Sistemas de vídeo IP que utilizan servidores de vídeo**: En este tipo de sistemas podemos destacar los siguientes elementos, como son: el servidor de vídeo, el cual comprime la imagen capturada y la digitaliza para ser enviado por un medio de red; siendo transmitida hasta un servidor, el cual tiene un software que gestiona los videos.

En este sistema, las cámaras son las únicas que vienen de los sistemas anteriores y como intermediario, está el servidor de vídeo, permitiendo que la imagen se digitalice y pueda ser administrada. (Figura 13).

Figura 13: Sistemas de vídeo IP utilizan servidores de vídeo



Fuente: Ibíd.

5) **Sistemas de vídeo IP que utilizan cámaras IP**: El vídeo IP es un sistema de vigilancia y monitorización remota, que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP.[44] (Figura 14)

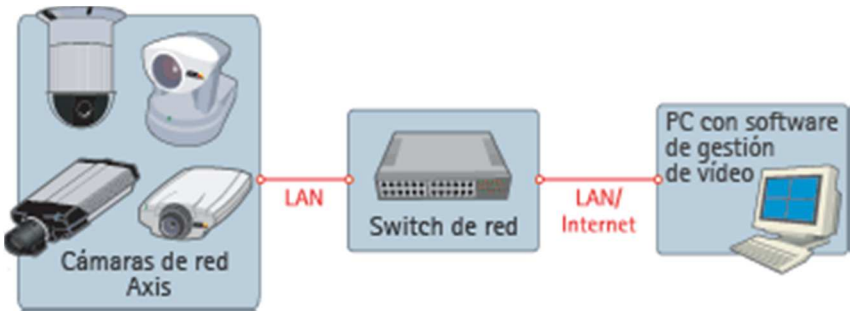
[44] G&M. Sistema de Video Vigilancia en Red. España. 2008. Disponible en Internet: http://www.gmingenieria.com/productos/nuevosProductos/camaraIP.html

“Los equipos electrónicos que manejan actualmente trafico IP se han vuelto parte integral de los sistemas de vigilancia”[45]; al ser una cámara IP esta puede ser operada a distancia utilizando los medios de transmisión para datos, adicionalmente este tipo de cámaras con la evolución que han tenido, se ha desarrollado nuevas aplicaciones.

Una cámara IP combina una cámara y un ordenador en una unidad. El vídeo se transmite a través de una red IP y se graba en un pc estándar con software de gestión de vídeo[46].

Otra de las ventajas es la distribución del almacenamiento, al ser un formato digital se puede hacer a través de las herramientas NAS, arreglos de discos utilizando los raid y sus ventajas, crear sistemas de respaldo o redundancia.

Figura 14: Sistemas de vídeo IP que utilizan cámaras IP



Fuente: Ibíd.

2.4.2 Componentes de un sistema de CCTV. Descripción

2.4.2.1 Cámara de seguridad

Una cámara de seguridad está compuesta fundamentalmente por un dispositivo captador de imágenes, un circuito electrónico asociado (DSP) y una lente, que de acuerdo a sus características permitirá visualizar una escena determinada.

[45] CUAQUENTZI A, Op. cit.; p. 14
[46] G&M Op. cit.

El dispositivo captador de imágenes, denominado comúnmente CCD[47] o CMOS, está compuesto por alrededor de 300.000 elementos sensibles denominados pixeles y su formato en las cámaras estándar es de 1/ 3" o 1/4".

A la hora de seleccionar una cámara, según el uso o instalación que quiera realizarse, las especificaciones más importantes a tener en cuenta son las siguientes:

1) Alimentación: 220 VCA, 24 VCA y/o 12 VCC.

2) Tipo de sensor: CCD o CMOS y su respuesta espectral (color, blanco y negro y/o infrarrojo).

3) Tamaño del sensor:1/4", 1/3", 1/2", 2/3", 1"

4) Resolución: Representa la definición de la imagen, expresada en líneas de TV (TV Líneas o TVL).

2.4.2.2 Medios de transmisión de la imagen

En la actualidad existen muchos medios de transmisión, desde el más sencillo que es un cable coaxial, la cual transmite las imágenes a una distancia corta y comúnmente aplicado en CCTV más pequeño, pero para aplicaciones más grande se utiliza la fibra óptica[48], la cual es un medio que permite transmitir una gran cantidad de streamings sin que se tenga retardo en la comunicación.

Para algunas aplicaciones en donde la topografía o la infraestructura no permitan llegar fibra, se contempla sistemas inalámbricos; hoy en día existen muchas marcas que ofrecen una gran variedad de antenas, las cuales soportan la transmisión de vídeo.

[47] ESPINOZA. Julio E. Desarrollo de un Circuito Cerrado de Televisión en un Local Comercial. [En línea]. Zacatecas, 11 de noviembre de 2011. p.; 14. Disponible en Internet: http://ice.uaz.edu.mx/c/document_library/get_file?uuid=72b44e91-3e32-4e14-b927-2df5114c9bc8&groupId=54327

[48] ESPINOZA. Ibíd.; p. 28

2.4.2.3 Medios de grabación

La aplicabilidad más común de un CCTV es que todo lo que se capte con las cámaras se pueda grabar para que posteriormente se puedan las imágenes utilizar en una investigación, en el caso de la policía, o en otro tipo de aplicaciones, como pueden ser para monitorear ríos, volcanes o vigilancia de infantes.

2.4.2.4 NVR para cámaras IP

La sigla NVR significa (Network Vídeo Recorder) o en español (Grabador de Vídeo de Red). Un NVR puede ser un dispositivo físico o un software que se instala en una computadora.

Un NVR es muy similar a un DVR, la diferencia es que el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas; en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.

Los NVR stand alone son equipo físico (electrónica con software embebido) en un gabinete cerrado. Los cuales están listos para ser utilizados.

Los NVR basados en computadoras, son simplemente un software que se instala en una computadora y administra nuestras cámaras IP.

2.4.2.5 Software para monitoreo

Es el software de administración, lo que permite controlar todos los equipos instalados para que pueda estar al mando del sistema, la interfaz de usuario plenamente integrada para la supervisión de imágenes de vídeo.

3. ANÁLISIS DEL ESTADO ACTUAL DE SEGURIDAD DE LA INFORMACIÓN EN EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV) DEL MUNICIPIO DE YACUANQUER

3.1 ESTACIÓN DE POLICÍA DEL MUNICIPIO DE YACUANQUER

La policía nacional como una entidad del estado, está formado con unos principios y valores con los cuales se han ido desarrollando y fortaleciendo en el tiempo.

3.1.1 Misión

"La policía nacional es un cuerpo armado permanente de naturaleza civil, a cargo de la nación, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz"[49].

3.1.2 Visión

"La policía nacional se considerará en el 2022 como institución fundamental para la constitución de un país equilibrado y en paz. Garante y respetuoso de los derechos humanos, afianzando la convivencia y seguridad a través del control del delito, la educación ciudadana, prevención, medición y articulación institucional e interinstitucional como ejes centrales del servicio"[50].

3.1.3 Ubicación

La estación de policía que está ubicada en la carrera 2 con calle 8 cerca de la alcaldía municipal de Yacuanquer, cuenta con una edificación de 2 pisos con un área aproximada de 240 mts^2.

Su zona de influencia el municipio de Yacuanquer, el cual se encuentra a 25 km de la capital San Juan de Pasto, ubicado en la zona andina al sur occidente del departamento de Nariño.

[49] Valores y Principios. [En línea]. 2015. Colombia, s.f. [Citado en 2016-03-03]. Disponible en Internet: http://oasportal.policia.gov.co/portal/page/portal/INSTITUCION/Direccionamiento_estrategico
[50] Ibíd.

Se caracteriza por ser eminentemente de actividad agropecuaria, con predominio de la economía campesina, en donde la gran mayoría de productores laboran en parcelas.

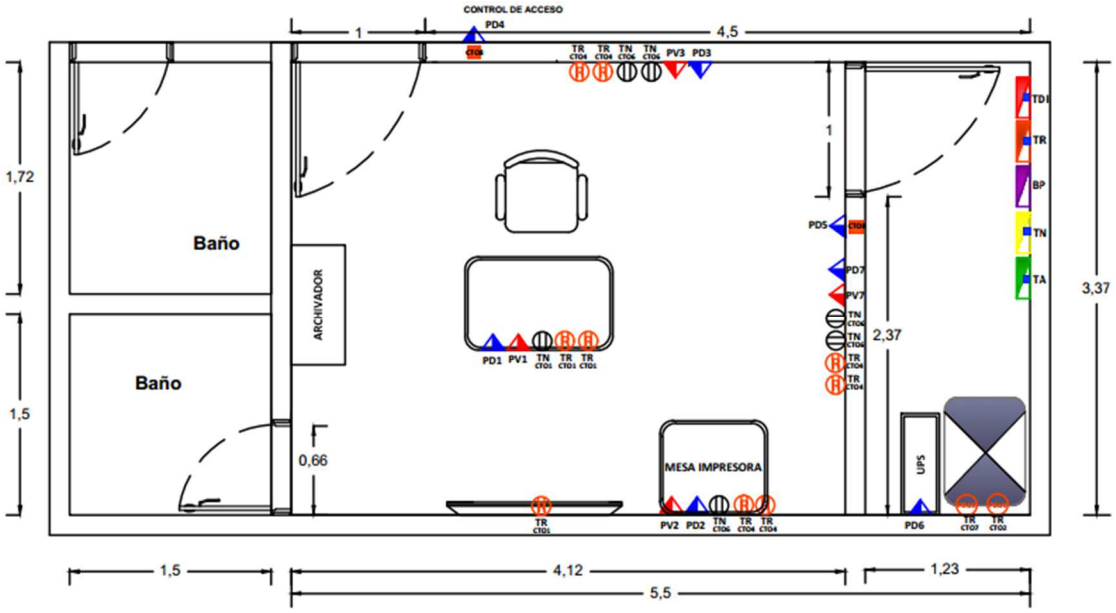
Datos Estadísticos (ceso general 2005 – DANE)[51]

Extensión área urbana: 1.5 Km^2

No. habitantes cabecera: 2700

3.2 CIRCUITO CERRADO DE VIGILANCIA CCTV

Figura 15: planos salidas normales, reguladas, voz y datos



Fuente: Documentación del sistema, estación de Policía de Yacuanquer

En la figura 15 podemos observar la distribución de la sala de monitoreo del circuito cerrado de televisión (CCTV) de la estación de policía del municipio de Yacuanquer, el cual cuenta con:

[51] Ibíd. Disponible en Internet: http://www.yacuanquer-narino.gov.co/informacion_general. shtml#geografia

3.2.1 Sala de monitoreo

Tiene un área de 13.88 mts^2 en donde se cuenta con los siguientes elementos: (figura 16)

1) computador de gama alta, con un procesador Xeon con 6GB de memoria RAM y un disco duro de 500GB, cuenta con una tarjeta gráfica con 2 Gb de RAM para vídeo, puertos HDMI, DVI, VGA para hacer las conexiones con los monitores.

2) Un monitor de 55", marca Samsung de leds.

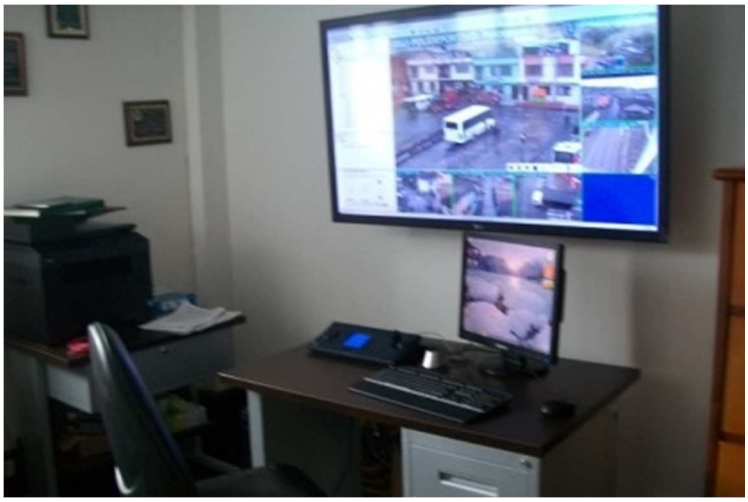
3) Monitor auxilias de 19", marca Samsung.

4) Joystick, marca IndigoVisión para la manipulación de las cámaras.

5) Escritorio de 0.7 x 1,0 mts, con dos cajones.

6) Una Impresora multifuncional marca DELL fotocopiadora, fax y escáner.

Figura 16: Sala de monitoreo



Fuente: Propiedad del autor

3.2.2 Cuarto de equipos

Con un área de 4,14 mts^2 en los cuales están instalados los elementos eléctricos

que conforman el sistema, los sistemas de datos y almacenamiento, distribuidos de la siguiente forma: (figura 17).

Figura 17: Cuarto de equipos

Fuente: Propiedad del autor

3.2.3 Sistema eléctrico

Los componentes eléctricos se encuentran en un área de 4,23 mt2 y está conformado por los siguientes elementos (ver figura 18):

1) Tablero normal de 24 circuitos.

2) Tablero regulado de 12 circuitos,

3) UPS de 3 KVA.

4) Transferencia automática.

5) Alarma contra incendios, un censor de humo ubicado en el cuarto de equipos y en el cuarto de monitoreo; cuanta con una palanca de pánico ubicada al lado de la salida principal y un extintor tipo solkaflam.

Figura: 18 Tableros eléctricos

Fuente: propiedad del autor

3.2.4 Control de acceso

Para el acceso a la sal de monitoreo se encuentra con dos biométricos ubicados uno en la puerta principal y otro en el acceso al cuarto de equipos (figura 19).

Figura 19: Biométrico

Fuente propiedad del autor

3.2.5 Sistema de almacenamiento

Se instaló dos NVRs para las grabaciones de los videos procedentes de las cámaras, de referencia NVR-AS 3000 con una capacidad de 6 TB cada uno, esto ofrece una línea de tiempo aproximado de 4 a 5 meses. Los NVRs esta configurados con raid5, esto permite que tenga un respaldo en caso de fallas en los discos, en la tabla 3 se puede observar las especificaciones técnicas del equipos. (Figura 20).

Figura 20: NVR-AS 3000

Fuente: Network Video Recorder. [En línea]. España. S.f. [Citado en 10/02/2016]. pp. 1 Disponible en Internet: http://www.cctvcentersl.es/upload/Catalogos/NVR-AS%203000%20RA_eng.pdf. Doc. ID:IV-NVRRA300 09.1.

Tabla 3 Especificaciones NVR-AS 3000

Specification

	RA Series					
	1500	3000	1000	2000	2000	4000
Network Redundancy	Y	Y	Y	Y	Y	Y
Redundant Power Supply	Y	Y	Y	Y	Y	Y
Removable Storage	Y*	Y*	Y*	Y*	Y*	Y*
Disk Space (GB)	1500	3000	1000	2000	2000	4000
Available Storage (GB)	1458	2943	963	1953	1953	3933
RAID	RAID5	RAID5	RAID1	RAID1	RAID0	RAID0
Max. Recording Streams	64	64	64	64	64	64
Max. Playback Streams	20	20	20	20	20	20
Max. Recording Bitrate	40	40	64	64	64	64
Max. Playback Bitrate	40	40	40	40	40	40
Licence Options	20 stream, 40 stream and 64 stream licenses are available					
Power consumption	53W max					
Physical Dimensions	483x272x87mm (2U)					
Electrical	Operating Voltage: Input 100-240V ~ 47-63Hz 1A. Connector for redundant external power supply					
Network Connections	Two redundant 100/1000 BaseT RJ-45 Connections					
Environmental	Operating temp: 50°C/122°F; Storage temp: -20 to+70°C/-4 to +158°F					
Onboard Diagnostics	Disk, CPU, Motherboard temperatures. Redundant power and network status. Cooling fan status					
Regulatory	EN55022 ITE Emission standard Class A; EN61000-3-2 Mains Harmonics Class A; EN61000-3-3 Voltage Fluctuation; En55024 ITE Immunity standard; CFR47: 2002 Part 15 Sub Part B (US federal code of regulations) UL 60950-01, Information Technology Equipment - Safety - Part 1: General Requirements					
Disks	SATA Seagate SV35.5 Series optimised for 24x7 video storage. 5-year warranty					

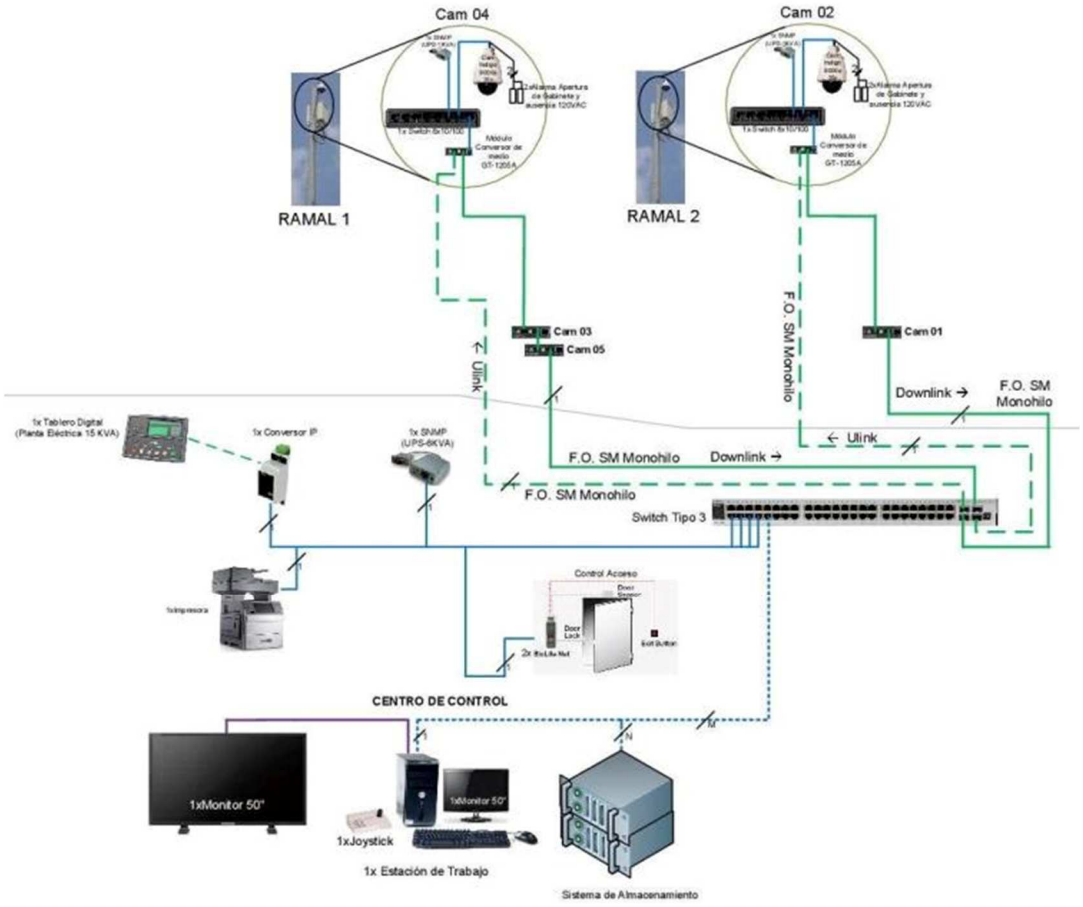
Fuente: Ibíd. p. 2.

3.2.6 Red de datos

El circuito cerrado de televisión CCTV, está conformado por 5 cámaras las cuales tienen un cubrimiento perimetral de 2,5 kms y que van conectada a una fibra óptica monomodo hacia el cuarto de equipos ubicado en la estación de policía.

En la parte interna se tiene instalado cable UTP categoría 6 para 10 puntos lógicos y distribuidos de la siguiente manera: 2 para área de trabajo, 1 impresora, 2 controles de acceso, 1 para planta eléctrica y 4 disponibles. (Figura 21)

Figura 21 Mapa de red



Fuente: Documentación del sistema, estación de Policía de Yacuanquer

3.2.7 Software

El computador cuanta con un software, que permite al operador realizar las actividades de vigilancia, por esta razón en este equipo no debe encontrarse ningún programa adicional, pero por la falta de control existen programas que no tiene nada que ver con la función.

El software implementado en el circuito cerrado de televisión CCTV – Yacuanquer, está conformado por:

3.2.7.1 Control center

Software fácil de instalar y utilizar, cuenta con una interfaz de usuario integrada para administrar los videos, la licencia sin restricciones le permite realizar instalaciones ilimitadas en el lugar.

Para su correcto funcionamiento necesita:

1) Que el operador conozca la clave de acceso.

2) Operar las diferentes funciones que tiene el programa para manejar las cámaras.

3) En caso de fallas, tener una copia actualizada de la base de datos de la configuración del sistema de vigilancia.

4) Para la reproducción de las grabaciones entregadas, cuanta con un software portable, llamado **Insident player** que debe ser copiado junto con la grabación**.**

3.2.7.2 Antivirus

La aplicación kaspersky security, que esta licenciada por un año. Pero no cuenta con una conexión a internet para realizar las actualizaciones que se necesitan, esto debe hacerse conectando una USB wiffi o en su defecto en forma manual, en cuyo caso recae la responsabilidad en el operador de las cámaras.

3.2.7.3 Software DES control de planta eléctrica

Software que permite gestionar, manejar a la planta desde el computador de monitoreo.

En el momento esta aplicación los operadores no la saben manejar, para lo cual se requiere realizar un manual donde se explique de forma básica el encendido y apagado de la planta y la verificación de combustible.

3.2.7.4 Sistema operativo Windows 7 profesional

El sistema operativo instalado en el computador de monitoreo es Windows 7 profesional y se encuentra debidamente licenciado.

3.2.7.5 SNMP View

Programa que monitorea el estado de las ups, a través del gestor Netagent mini, el programa permite emitir una alarma, en caso de que la energía en el punto de cámara se corte.

Se determina que los operadores no la pueden manejar y en algunos casos no saben que está instalada.

3.2.8 Zona de planta eléctrica

El sistema está respaldado por una planta eléctrica de 15 Kva, para suministrar energía al cuarto, cuando existan cortes y lo hace en forma automática ayudándose de la trasferencia. (Ver figura 22)

La policía debe garantizar que se suministre el combustible necesario para su operación, para lo cual debe realizar un control o revisión de los niveles, por lo tanto esta función se delega al operador de turno.

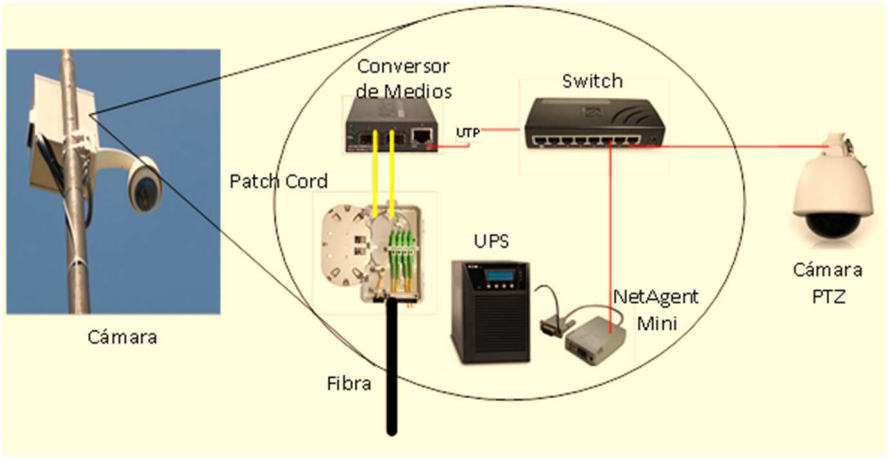
Figura 22: Planta eléctrica

Fuente: Propiedad del Autor

3.2.9 Puntos de cámara

Cada uno de los puntos de cámara está configurado de la misma forma, se tiene un poste de 14 mts para soportar la cámara y el gabinete, una cámara tipo exterior PTZ, con un brazo de 1,5 mts; el gabinete contiene los elementos que permiten a la cámara opere de forma adecuada. (Figura 23)

Figura 23: Organización Punto de Cámara



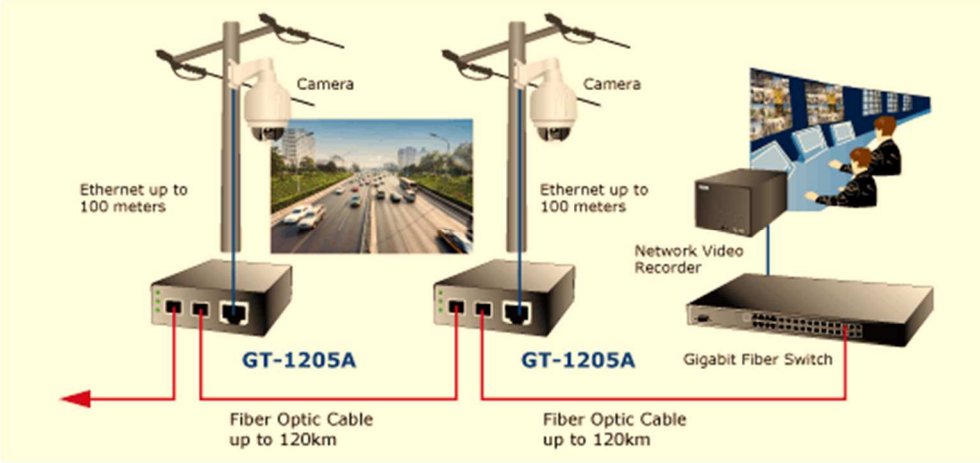
Fuente: propiedad del autor

Gabinete Permite proteger de agua y viento los equipos de conexión de red de la cámara como la parte eléctrica.

Los componentes internos en el gabinete son:

1) **Conversor de Medios**: de marca Planet 10/100/1000Base-t to dual, convierte directamente los medios de comunicación de la fibra gigabit ha interfaz de par trenzado. (Figura 24)

Figura 24: Extending Ethernet distance



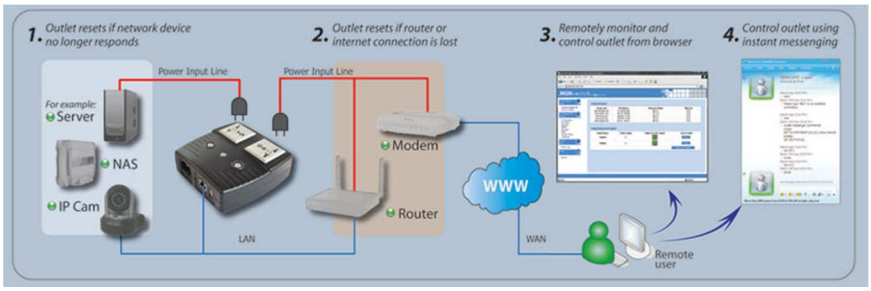
Fuente: Planet Network & Comunication. [En línea]. 2016. (sin Lugar). [Citado en 15/02/2016]. Disponible en Internet: http://www.planet.com.tw/en/product/product.php?id=48415#appl

2) **Switch 8 puertos:** Integrar el administrador de la ups, la cámara y el conversor de medios.

3) **UPS de 1Kva:** esta ups mantiene operando la cámara aproximadamente por una hora en caso de cortes de energía.

4) **NetAgent**: dispositivo que se conecta a la ups, para gestionar; permite hacer test de prueba para verificar su estado e informa si está operando con baterías. (Ver Figura 25)

Figura 25: NetAgent mini



Fuente: Megatec. [Online]. (Sin fecha). [Citado en 9/02/2016]. Disponible en Internet: http://www.megatec.com.tw/Products/NetAgent%20Mini/NetAgent%20Mini_eDM.p1.jpg

3.3 VIDEOS DE VIGILANCIA

"El vídeo se considera como un instrumento en dos estado, uno de prevención", al estar conectadas las cámaras con el centro de monitoreo y que una persona esté pendiente de ellas, permite visualizar en vivo las acciones que se están realizando en ese momento[52].

El otro de naturaleza delictiva que ayuda en una investigación criminal, donde las autoridades pertinentes como pueden ser la Fiscalía, CTI, DIJIN, acuden a verificar las imágenes, para encontrar pruebas o eventos que aclaren los hechos[53].

La contribución del sistema, es la posibilidad de almacenar los videos, con un tiempo de backup entre 4 y 5 meses, esto permite a las autoridades tener el tiempo suficiente, para poder hacer las solicitudes que se requieran.

Cuando los discos se llenan, el NVR realiza un borrando de los videos en forma automática empezando con los más antiguos.

La entregar de videos, por parte de la policía, debe hacerse siguiendo los parámetros exigido por la ley, teniendo en cuenta la cadena de custodia; "es un procedimiento destinado a garantizar la individualización, seguridad y preservación

[52] SUAREZ, Juan Carlos. Los Video-grabaciones Como Prueba en el Proceso Penal. [En línea]. Boletín núm. 2024. pp. 9. Disponible en Internet: http://www.mjusticia.gob.es/cs/Satellite/1292344081189?blobheader=application%2Fpdf&blobheadernam
[53] Ibíd. PP 10

de los elementos materiales y evidencias recolectados de acuerdo a su naturaleza o incorporados en toda investigación de un hecho punible destinados a garantizar su autenticidad"[54].

3.4 FACTORES INTERNOS

3.4.1 Comandante estación de policía

El manejo del sistema de vídeo vigilancia CCTV, responsabilidad y funcionamiento están bajo la directriz del comandante de la estación de policía de Yacuanquer, quien es él que designa a las personas que están a cargo del manejo de las cámaras, en el momento no existe un manual de funciones o documento, que determine cuál es la responsabilidad de esas personas, quedando bajo el criterio del comandante delegar su horario y función.

3.4.2 Operadores

Son patrulleros que están asignados a la estación de policía de Yacuanquer, que por sus conocimientos en sistemas y manejo del computador, son escogidos a la operación de las cámaras, por lo general sus funciones son administrativas, en algunas ocasiones el secretario de la estación, asume esta responsabilidad. Pero por disponibilidad de personal, él que se encuentra de turno, en la función de guardia en la estación, asume la responsabilidad de operador de cámaras, por estar la sala cerca al puesto de vigilancia.

Los operadores de las cámaras, no asumen funciones de reparación o mantenimiento de los equipos, esto se debe a su función policial, tiene que cumplir con lo designado por el comandante, en cuyo caso esa función queda a cargo del contratista la responsabilidad del mantenimiento preventivo y correctivo del sistema.

3.5 FACTORES EXTERNOS

Esto son los que influyen sobre el sistema o están directa o indirectamente involucrados en su funcionamiento.

[54] HENAO Juan F. La Cadena De Custodia En El Sistema Penal Acusatorio. [En línea]. Universidad De Medellín, 2012, pg. 9 Disponible en Internet: http://repository.udem.edu.co/bitstream/handle/11407/277/La%20cadena%20de%20custodia%20en%20el%20Sistema%20Penal%20Acusatorio.pdf?sequence=1

3.5.1 Secretaría de gobierno de Yacuanquer

La alcaldía es la dueña del sistema, pero deja el control y operación a la policía, por ser un sistema de seguridad ciudadana; asumiendo la secretaria de gobierno su sostenibilidad económica, esta debe suministrar combustible a la planta eléctrica, contratación de mantenimiento preventivo y correctivo, pago de energía por el consumo de las cámaras.

Esta responsabilidad está contemplada en un acto administrativo, entre la alcaldía de Yacuanquer y el Ministerio del Interior, que fue requisito para cofinanciar el 80% del costo del sistema.

3.5.2 Oficina de telemática MEPAS (Metropolitana de Pasto)

Esta oficina hace parte de la estructura organizativa de la Metropolitana de Pasto y se encarga de las comunicaciones y todo lo que tiene que ver con la parte tecnología, su influencia en el sistema de vídeo vigilancia CCTV de Yacuanquer es ayudar al comandante en asesorías en equipos y requerimientos.

3.5.3 Contratista mantenimiento de sistema de vídeo vigilancia CCTV de Yacuanquer

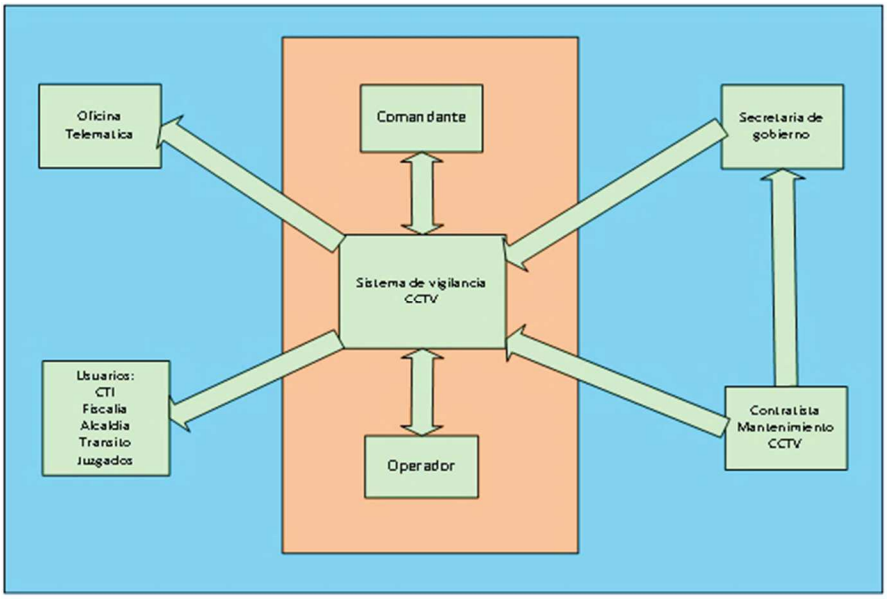
Es la persona o personas a cargo de mantener funcionando los equipos tecnológicos, las funciones son realizar mantenimiento preventivo o correctivo a las cámaras ubicadas en los postes, mantener funcionando la fibra óptica, realizar revisiones a los equipos de red, configurar el software control center.

3.5.4 Usuarios del sistema de vídeo vigilancia CCTV

Las entidades o personas que pueden solicitar los videos como pruebas son: las fiscalía, juzgados, CTI, MEPAS, Alcaldía, transito; las personas naturales que requieran un vídeo, deben hacerlo a través de cualquiera de las entidades mencionadas.

La relación del entorno del circuito de cerrado de televisión CCTV esta resumido en la figura siguiente. (Ver figura 26).

Figura 26: Entorno circuito de vigilancia CCTV



Fuente: propiedad del autor

3.6 PARTES INTERESADAS EN EL SGSI

Para el sistemas de gestión de la seguridad de la Información, las partes interesadas son: el comandante de la estación de policía de Yacuanquer, que es el encargado de la dirección y buen funcionamiento del sistema, la alcaldía de Yacuanquer, delega en la secretaria de gobierno su funcionamiento, esto permite cada año revisar las necesidades del sistema y en base al estudio se realiza un presupuesto y se efectúa la licitación para la contratación de la empresa o persona que se encargara del mantenimiento preventivo y correctivo del sistema.

3.6.1 Comandante de la estación policía de Yacuanquer

Los requisitos que planteo el comandante para el sistema son:

1) Que se defina las responsabilidades de cada integrante del sistema de vigilancia CCTV.

2) Definir los mecanismos de resolución de problemas.

3) Definir unas políticas que permitan realizar cambios de personal sin que el sistema de vigilancia CCTV se vea afectado.

4) Llevar un control de los equipos del sistema de vigilancia CCTV.

5) Manejo adecuado de la documentación e información que opera el sistema de vigilancia CCTV.

6) Definir las políticas que permitan al personal operar con los equipos del sistema de vigilancia CCTV.

7) Que las cámaras estén siempre operando, para brindar la vigilancia requerida y el sistema tenga efectividad en sus objetivos.

3.6.2 Secretaría de gobierno de Yacuanquer

Los requisitos que planteo la secretaria son:

1) Que se defina en un momento determinado las necesidades del sistema.

2) Que el sistema brinde la seguridad a la comunidad.

3) Que la policía y el sistema de vídeo vigilancia CCTV tengan una buena acogida en la comunidad.

4) La secretaria define sus obligaciones en el convenio firmado con el Ministerio del Interior para el sostenimiento, decreto 399 de 2011.

3.7 ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de la seguridad de la información, se enfocó en el sistema de circuito cerrado de televisión CCTV. “las ventajas del sistema incluyen la capacidad de observar las situaciones de peligro a distancia, la capacidad de proporcionar un ojo constante de las actividades rutinarias”[55] y a su vez estas son grabadas y resguardadas por cierto tiempo.

El circuito cerrado de vídeo vigilancia CCTV es eficaz en la medida que estén funcionando el 100% de las cámaras, pueden funcionar las 24 horas del día, durante los 365 días del año; las grabaciones serán resguardarlas durante el

[55] RODRÍGUEZ Inaki, Planificación Y Desarrollo De Sistemas De Video Vigilancia Digital Vía WIMAX - Universidad Politécnica de Catalunya. [En línea]. [España]. 24 de Mayo de 2012. pp. 14. Disponible en Internet: http://upcommons.upc.edu/bitstream/handle/2099.1/15255/memoria.pdf?sequence=1&isAllowed=y.

tiempo que permanezcan en el sistema de almacenamiento, para que posteriormente sean utilizadas en caso de algún delito.

Las partes importantes que se deben proteger son:

1) Vídeo en vivo, para el monitoreo de los eventos.

2) Grabaciones, protegerlas de su manipulación o barrado por daños en los equipos.

3) Manejo de equipos y software.

4) Personal autorizado.

Roles y responsabilidades

El sistema para su buen funcionamiento y gestión de la seguridad, necesita que el personal de la estación establezca responsabilidades, para ello se debe definir los roles de cada uno de los integrantes, en la tabla 4 están clasificados estos roles y responsabilidades para el sistema de CCTV.

Tabla 4: Clasificación de los roles

Roles	Responsabilidades
Comandante de estación	1. Responsable de control y dirección del sistema CCTV. 2. Designa el personal que operara las Cámaras del CCTV. 3. Determinará las necesidades del sistema y elaborara el presupuesto para ser entregado a la Alcaldía. 4. Es el responsable de guardar las claves del sistema.
Secretario de Gobierno	1. Gestionar los recursos para el funcionamiento del sistema CCTV. 2. Gestión de ampliación de sistema en conjunto con el comandante de la estación.
Responsable del sistema CCTV	3. Patrullero designado por el Comandante por sus conocimientos en sistemas. 4. Gestionar que se lleven los registros del sistema CCTV. 5. Controlar a los operadores que cumplan con sus responsabilidades. 6. Acceso y exportación de las grabaciones para la entrega a las entidades solicitantes. 7. Configurar y gestionar los usuarios designados para

Roles	Responsabilidades
	ingresar al sistema. 8. Acceso al cuarto de equipos. 9. Solicitud de soporte y mantenimiento al sistema. 10. Registro y control de los soportes y mantenimientos realizados al sistema. 11. Elaborar informe de las necesidades que tiene el sistema al comandante.
Operadores de cámaras	1. Designados por el comandante de la estación de policía de Yacuanquer. 2. Operar y monitorear las cámaras del sistema. 3. Verificar estado de la planta eléctrica y niveles de combustible. 4. Manejo de escritorio limpio en el puesto de monitoreo. 5. Informar a las patrullas de algún evento de importancia para ser verificado en sitio. 6. Registrar en el libro de anotaciones. 7. Recibir y registrar solicitudes de grabaciones realizadas por las entidades correspondientes. 8. Informar de las fallas que presenta el sistema al responsable del CCTV.
Contratista	1. Responsable de realizar los soportes y mantenimientos necesarios según contrato realizado con la alcaldía. 2. Debe diligenciar formato de mantenimiento donde se describa en detalle lo que se ha realizado. 3. Obligado a firmar documento de confidencialidad de la información.

Fuente: propiedad del Autor

Además el sistema cuenta con unos equipos para su funcionamiento, los cuales están instalados en los puntos de cámara y en el cuarto de monitoreo, a continuación en la tabla 5 se listan estos activos.

Tabla 5: Listado de activos del sistema

Ítem	Activo	Marca	Cantidad
1	Tablero regulado		1
2	Tablero normal		1
3	Caja DPS		1
4	Tablero de incendios, luz estroboscópica, 2 sensores de humo, palanca de pánico	BOSH	1
5	Tablero de control de Acceso		1
6	Llave selectora		1

Ítem	Activo	Marca	Cantidad
7	Rack negro para equipos con dos regletas de corriente		1
8	Planta eléctrica	POWERLINK	1
9	Computador operador	Dell	1
10	Teclado	Dell	1
11	Mouse	Dell	1
12	Monitor de 19"	HP	1
13	Monitor de 55"	LG	1
14	Teclado IndigoVisión	IndigoVisión	1
15	Mueble 1 puesto	Metálicas GIP	1
16	Una silla ergonómica	Metálicas GIP	1
17	Mesa de impresora	Metálicas GIP	1
18	Impresora Dell 2335 láser	DELL	1
19	Archivador	Metálicas GIP	1
20	Cámara PTZ	IndigoVisión	5
21	Switch 8 puertos	D-link	5
22	Conversor de medio	Planet	5
23	Transiver R	D-link	5
24	Transiver T	D-link	5
25	Ups	FENTON	5
26	Netagent	DP592	5

Fuente: Inventario CCTV Yacuanquer

3.8 PROCESOS DE SOLICITUD Y REVISIÓN DE VIDEOS

En el sistema de vídeo vigilancia es común encontrar, solicitudes de los ciudadanos para revisar los videos, también solicitudes de las entidades que llevan investigaciones y necesitan encontrar algún elemento probatorio con los videos.

3.8.1 Solicitud por parte de los ciudadanos

Los habitantes de Yacuanquer pueden hacer una solicitud formal al comandante de la estación, para ver algún vídeo, al ser aprobado, el operador primero buscara el vídeo solicitado, con los parámetros que el ciudadano entrega, como son fecha y hora de inicio; si es encontrado se le permitirá observarlo y determinara si lo necesita, para lo cual se procede a guardarlo en el disco duro o en un CD para que a través de una entidad autorizada pueda retirarlo (ver figura 27).

En el caso que no esté el vídeo, se debe hacer la aclaración de los motivos por el cual no está grabado, esto lo puede hacer el operador en forma escrita o verbal.

Motivos por el cual no esté el vídeo:

1) Existió un mantenimiento en esa fecha.

2) La cámara estuvo fuera de servicio.

3) Un corte de energía largo.

3.8.2 Solicitud de vídeo entidades autorizadas

Las entidades autorizadas son: DIJIN, transito, alcaldía, juzgados y CTI las cuales deben diligenciar un oficio al comandante y radicarlo en la secretaria de la estación, solicitando el vídeo donde definan:

1) cámara o cámaras de donde necesita la grabación.

2) Fecha y hora inicio; fecha y hora final.

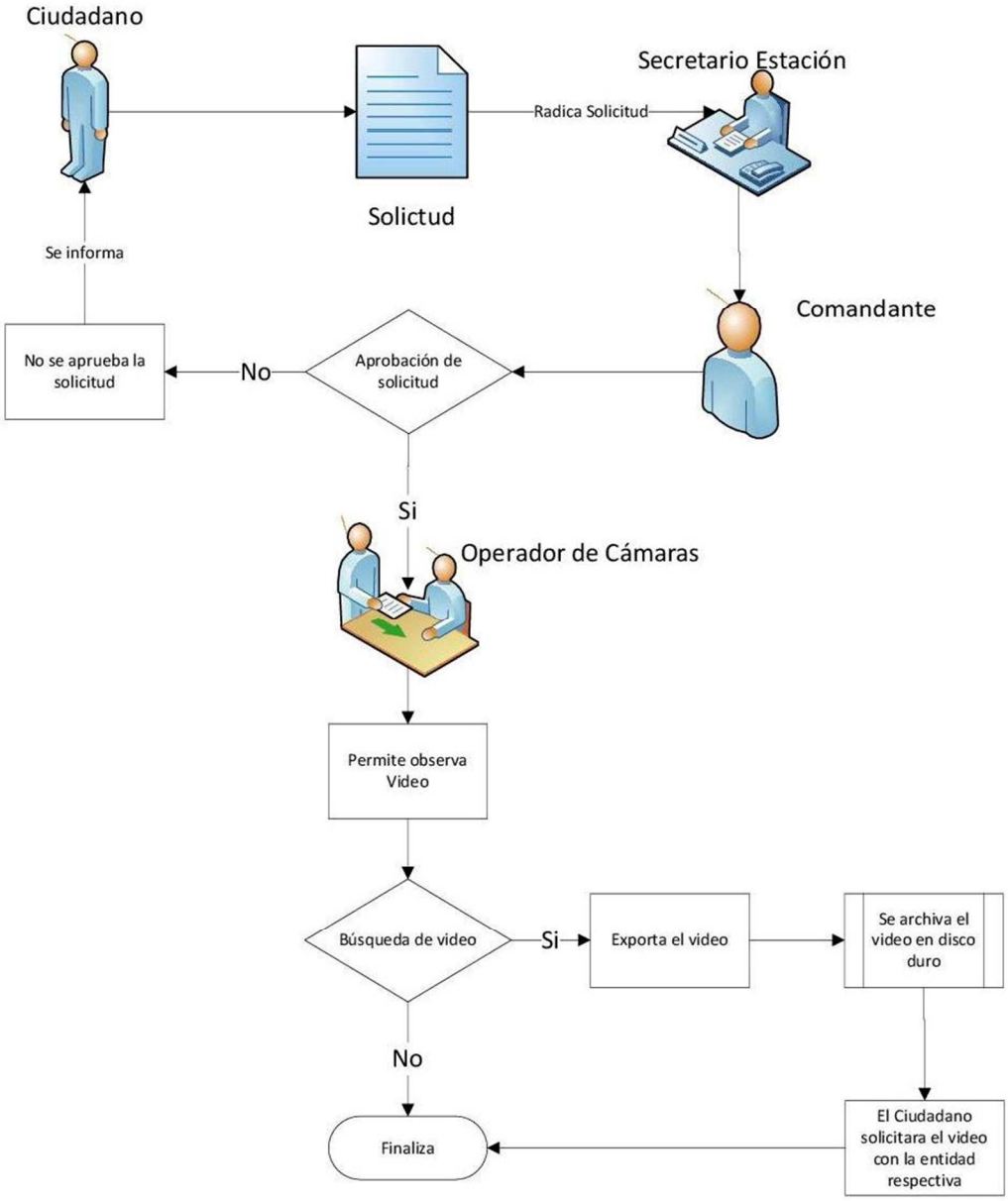
El comandante entrega el oficio al operador, el cual buscara el vídeo con los datos suministrado, en caso de encontrarlo procede a realizar la copia en un DVD, en el cual debe grabar, la carpeta donde está el vídeo y el programa portable que lo reproduce (**Insident player**), a esto debe adjuntar el oficio de entrega del vídeo, para registrar su entrega. (Ver figura 28)

En caso que no se encuentre, debe realizar un oficio de respuesta donde se informe el motivo por el cual no está grabado.

Motivos por el cual no esté el vídeo:

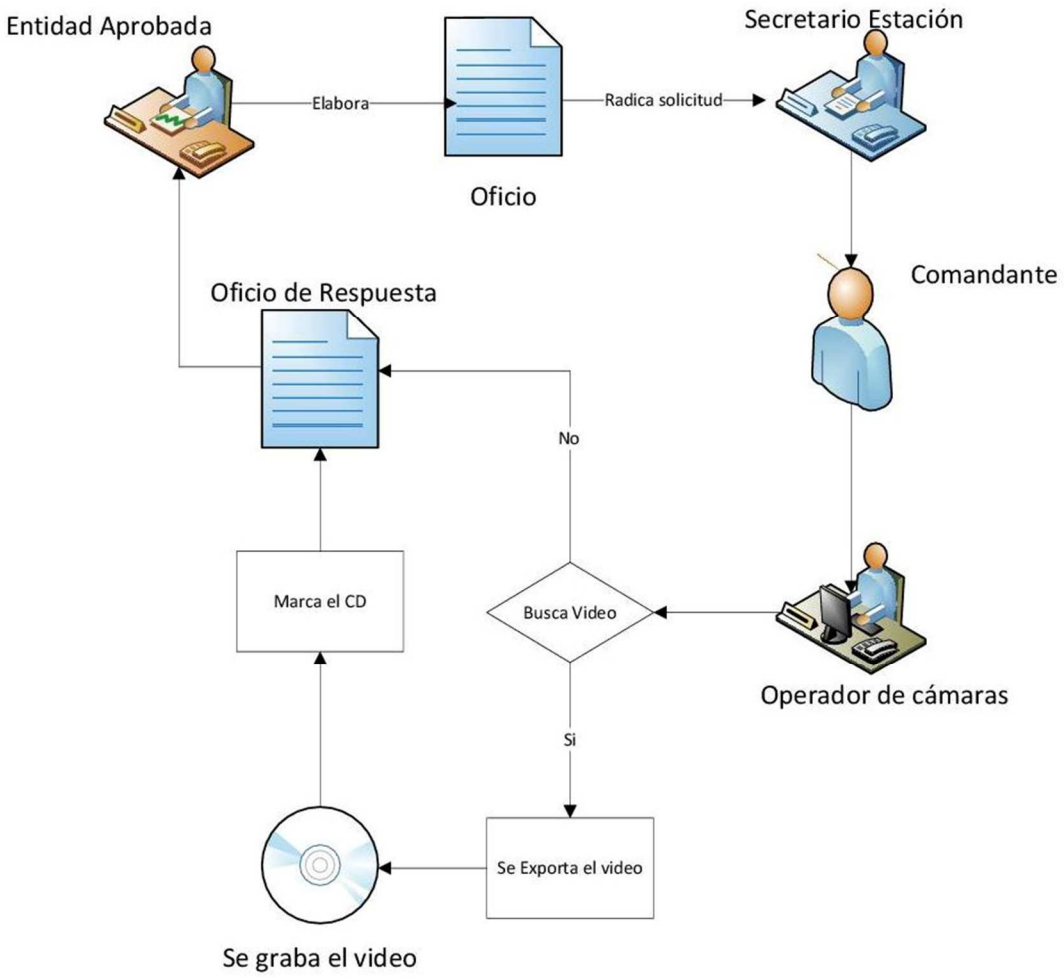
1) Existió un mantenimiento en esa fecha.
2) La cámara estuvo fuera de servicio.
3) Un corte de energía largo.
4) La fecha del vídeo excede los meses que se pueden almacenar.

Figura 27: solicitud de revisión de vídeos por parte de los ciudadanos.



Fuente: Propiedad del autor

Figura 28: Diagrama de solicitud de videos.



Fuente: Propiedad del autor

4. DEFINICIÓN DE POLÍTICAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, PARA EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

Para alcanzar la aceptación de la dirección, se realizó un análisis del sistema actual, esto permitió dar a conocer cuáles son los procedimientos que se están realizando, conocer el personal, la tecnología que está funcionando.

4.1 INTRODUCCIÓN

Un aspecto fundamental en la seguridad ciudadana, permitiendo al sistema recolecta información importante para la prevención y posterior prueba para los delitos, es mantener los procesos definidos y que cada integrante conozca sus funciones y así la dirección, en cabeza del comandante, pueda gestionar su seguridad, integridad y continuidad.

Un punto vital del sistema es tener funcionando las cámaras de seguridad, es la fuente que permite registrar las imágenes, para que el operador pueda hacer su labor de monitoreo y coordinar los llamados a las patrullas en el sitio, además el sistemas de vídeo vigilancia guardara en medio físico las imágenes por un tiempo determinado.

4.2 CONTENIDO

Reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con el sistema de vídeo vigilancia, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información (SGSI).

4.3 OBJETIVO

Presentar en forma clara y coherente los elementos que conforman la política de seguridad, que deben conocer y cumplir todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el sistema circuito cerrado de televisión CCTV.

4.4 TÉRMINOS Y DEFINICIONES

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una inconformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales inconformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: Cualquier cosa que tiene valor para la estación de policía. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la estación.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos. Se pueden clasificar de la siguiente manera:

1) **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen.

2) **Aplicaciones**: Es todo el software que se utiliza para la gestión de la información.

3) **Personal**: Es todo el personal de la estación de Policía, el personal subcontratado, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información.

4) **Servicios**: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a usuarios.

5) **Tecnología**: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

6) **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información.

7) **Equipamiento auxiliar**: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente

definidos. Ejemplo: Aire acondicionado, planta eléctrica.

Alcance: Ámbito de la organización que queda sometido al SGSI. Sobre todo si sólo incluye una parte de la organización.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista.

Confidencialidad: Acceso a la información únicamente de quienes estén autorizados, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información, por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4.5 POLÍTICAS DEL SISTEMA DE VÍDEO VIGILANCIA (CCTV)

4.5.1 Políticas de seguridad de la información

Los videos son información importante del sistema que deben estar almacenados, resguardados y está conformada por los videos y documentos que se elaboren y archiven en relación al sistema.

4.5.1.1 Introducción

Los videos almacenados son los datos importantes en el sistema de vídeo vigilancia, estos son recolectados desde las cámaras, que estas ubicadas en los lugares definidos por la policía para prestar seguridad, estos pueden contener información importante para un proceso de investigación o seguimiento de algún delito que posteriormente pueden ser solicitados.

4.5.1.2 Alcance

Esta política sustenta la importancia y continuidad del sistema de vídeo vigilancia.

Se aplica a: Comandante, Responsable de la sala y operador.

Objetivos de la seguridad de la información

1) La confidencialidad de las imágenes contenidas en los videos.

2) El sistema sea una herramienta tecnológica para la seguridad de la ciudadanía.

3) Mantener un espacio de almacenamiento prudencial para guardar las imágenes.

4) Mantener un acceso restringido para los videos.

Principios de la seguridad de la información

1) Promover la contratación de personal para el mantenimiento preventivo de los

equipos del sistema.

2) Delegar las funciones de exportación de vídeo a una sola persona, la cual se responsabilice de su buen uso.

3) No permitir el ingreso de unidades de almacenamiento que no estén autorizados, dentro del cuarto de monitoreo.

4) La utilización del sistema de control de acceso para proteger el ingreso de personal no autorizado.

5) Conocer las restricciones a la información y deberán comunicar a cualquier persona que no esté autorizada.

Responsabilidades

1) La dirección se compromete a elegir a un patrullero, que por su perfil pueda quedar como responsable de la sala de monitoreo, para llevar los controles y cumplimientos de las obligaciones de la seguridad.

2) Los operadores son responsables de garantizar la seguridad en el turno que esté prestando, impidiendo el ingreso de unidades de almacenamiento externas.

3) El comandante autorizara la exportación y salida de videos y quedara registrado en el libro de anotaciones y una copia de recibido en el archivo.

4) El responsable del circuito cerrado de televisión (CCTV) es el único que podrá exportar los videos desde el sistema de almacenamiento, para ser entregados a la entidad solicitante.

5) El responsable del circuito cerrado de televisión (CCTV) ingresara al sistema de control de acceso, los usuarios autorizados por el comandante.

Resultados Claves

1) Existencia de un responsable de la sala de monitoreo.

2) Archivo de la documentación del sistema de vigilancia.

3) Los videos estarán disponibles para su solicitud.

4) El cuarto de equipos y rack donde están las unidades de almacenamiento de los videos siempre están restringidos.

Políticas Relacionadas

1) Política de mantenimiento.

2) Política de seguridad sala de monitoreo.

4.5.2 Política de seguridad sala de monitoreo

Se debe mantener la seguridad de acceso y protección de los elementos que están instalados para poder realizar los seguimientos a las cámaras de seguridad.

4.5.2.1 Introducción

Es la ubicación estratégica para que los operadores puedan hacer los seguimientos y revisiones a las cámaras de seguridad instaladas, en esta área están instalados todos los equipos de red y computacionales que permiten al sistema funcionar correctamente.

Se encuentra dividida en dos zonas una monitoreo y la otra de equipos, el cuarto de equipos está conformado por el rack donde están el switch y las unidades de almacenamiento (NVR), los tableros eléctricos, el control de acceso y de incendios; en la zona de monitoreo esta la impresora, computador y los monitores, es donde el operador puede hacer los seguimientos y vigilancia de cada punto de cámara.

4.5.2.2 Alcance

La protección y buena practicas dentro de la sala de monitoreo por parte del personal que labora en la estación de policía de Yacuanquer.

Se aplica a: Responsable sala de monitoreo, operador.

Objetivos de seguridad sala de monitoreo

1) Promover el cuidado de los elementos que están instalados.

2) Controlar el acceso a la sala de monitoreo y de equipos.

Principios De Seguridad Sala de Monitoreo

1) Se prohíbe el acceso de personal no autorizado.

2) Se prohíbe el consumir alimentos, cigarrillos y bebidas, para lo cual se colocaran los avisos respectivos.

3) se debe realizar el aseo de las sala con supervisión del operador.

4) Se debe mantener la puerta principal y de cuarto de equipos cerrada.

5) Se debe llevar el registro en libro de anotaciones, de los eventos que sucedan con las cámaras y durante el turno del operador.

6) Se deben mantener seguro los sistemas de almacenamiento bajo llave y activo el control de acceso.

Responsabilidades

1) El operador es responsable de hacer cumplir las normas en el turno en el cual está laborando.

2) El encargado de la sala de monitoreo, velara por lo manifestado en esta política para su cumpliendo, verificando los registros.

3) El operador debe hacer una inspección del nivel de combustible en la planta eléctrica y registrarlo.

4) El operador es el responsable de informar sobre la falta de combustible en la planta eléctrica durante su turno.

5) El comandante será la única persona que determina la autorización de ingreso en caso necesario.

6) El comandante es la persona que designa a los operadores y responsable de la sala.

7) Para el retiro de algún elemento del sistema que está instalado en la sala de monitoreo, el comandante de la estación es el único que dará la autorización y se debe hacer por escrito.

8) El responsable del sistema de vídeo vigilancia debe inspeccionar los niveles y fecha de caducidad del extintor solkaflam y de ser necesario remitirlo a la oficina pertinente en la alcaldía para el proceso de recarga o mantenimiento.

Resultados Claves

1) Utilización del control de acceso a la sala de monitoreo.

2) Control de los registros en el libro de anotación y formatos.

3) Delegar funciones para los operadores.

Políticas Relacionadas

1) Política de seguridad para software implementado en el sistema de vídeo vigilancia CCTV.

4.5.3 Política de seguridad para software implementado en el sistema de vídeo vigilancia CCTV

El software implementado como sistema operativo, control center, antivirus, control planta eléctrica y control de acceso, se deben gestionar su seguridad con acceso restringido, copias de seguridad y manejo adecuado de sus funciones y configuraciones.

4.5.3.1 Introducción

En el sistema de vídeo vigilancia se incorporan aplicaciones que permitirán el manejo adecuado de la sala de monitoreo, como son el sistema operativo en el Workstation, el sistema de control de acceso para el registro de los usuarios, control de la planta eléctrica para poder manipularla remotamente, el SMNP viewer para observar el estado de las UPS y el control center que permite el monitoreo de las cámaras.

Para el comandante es importante conocer cuál es el software instalado dentro del sistema, esto permitirá que se pueda controlar software innecesario y que puedan afectar el buen funcionamiento.

4.5.3.2 Alcance

Está dado por el acceso a los programas y el control de instalaciones de software innecesario que afecten el sistema.

Se aplica a: Responsable de la sala de monitoreo y operador de cámaras.

Objetivos de seguridad para software implementado en el sistema de vídeo vigilancia CCTV

1) Restringir la instalación de software que no tenga que ver con el sistema de vídeo vigilancia.

2) Controlar el acceso a las aplicaciones con usuarios y contraseñas.

3) Designar la responsabilidad de la custodia de contraseñas de administrador al responsable de la Sala de monitoreo.

4) Archivar copia de las aplicaciones utilizadas en el sistema y sus respectivas licencias.

5) Realizar copias de seguridad de control center y su base de datos.

6) Capacitar al personal que caso de traslados.

Principios de seguridad para software implementado en el sistema de vídeo vigilancia CCTV

1) Realizar copia de seguridad de la base de datos del control center.

2) Archivar los instaladores de los aplicativos utilizados en el sistema.

3) Mantener actualizados los manuales de proceso que se llevan a cabo en la sala de monitoreo en el manejo de los programas.

4) Crear un ambiente de trabajo seguro en la sala de monitoreo.

5) Realizar una buena operación de los aplicativos.

Responsabilidades

1) El comandante deberá hacer un proceso de empalme cuando existan traslados de los operadores o responsable de la sala de monitoreo.

2) El responsable de la sala de monitoreo, deberá hacer una copia de seguridad de la base de datos del control center y archivarla en un lugar seguro y etiquetarla con la fecha de creación.

3) El responsable de la sala de monitoreo mantendrá y actualizara los manuales de procedimientos para las operadores, en el manejo de los diferentes aplicativos utilizados en el sistemas para casos de consulta o capacitación.

4) El responsable de la sala de monitoreo realizara la actualización del antivirus del Workstation cada 8 días como mínimo.

5) El responsable de la sala de monitoreo administrara las contraseñas y usuarios asignados a cada programa instalado y será responsabilidad de su seguridad.

6) El responsable de la sala de monitoreo debe archivar los instaladores de los programas que se están utilizando en el sistema con su respectiva información (claves, seriales).

7) El responsable de la sala, es el encargado de exportar videos en el Control Center.

8) Los operadores de cámaras tendrán asignado una cuenta común o individual, para ingresar al sistema operativo, pero con restricciones para evitar cambios en el software o hardware.

9) Los operadores de las cámaras se le asignara una cuenta en el Control Center común o individual, con acceso restringido solo visualización de vídeo en vivo y grabaciones.

Resultados claves

1) Archivar copias de seguridad.

2) Archivar claves de acceso.

3) Fomentar la seguridad en los operadores.

4) Mantener actualizado el antivirus.

Políticas relacionadas

1) Política De Seguridad Sala De Monitoreo

4.5.4 Política de seguridad para los equipos de red, switch, netagent, nvr, cámaras

Los equipos que tienen un sistema administrable, se deben configurar las opciones de seguridad, como contraseña y restricción de IPs si el equipo lo permite.

4.5.4.1 Introducción

En el sistema de vídeo vigilancia se instalaron equipos que permiten ser administrados, esta propiedad es un valor agregado que consiente en restringir aún más la transmisión de la información, dentro de la red.

Es el caso del switch, que es administrable, restringir su acceso y configuración, esto protege para que no sean manipulados y presenten problemas en su funcionamiento.

4.5.4.2 Alcance

Equipos instalados en la red para el funcionamiento del sistema de vídeo vigilancia.

Se aplica a: Responsable de la sala de monitoreo.

Objetivos

1) Crear restricciones con contraseña a los equipos.

2) Gestionar las contraseñas para que no se extravíen o confundan.

3) Configurar los equipos para mejorar su seguridad.

Principios

1) Almacenar las claves de cada equipo en un lugar seguro.

2) Realizar un procedimiento de cambio de claves y registrar el proceso.

3) Mantener en un lugar seguro las claves de los equipos.

4) Configurar las cámaras con la seguridad suministrada por el equipo como es contraseña y filtro de IPs

Responsabilidades

1) El comandante tendrá conocimiento de las claves y en qué lugar se almacenan.

2) El comandante será el que autorice a realizar el cambio de claves de los equipos.

3) Los archivos en donde se mantienen guardadas las claves no deben ser de acceso a los operadores, se deben mantener en custodia del responsable de la sala de monitoreo.

4) El proceso de cambio de las claves deben quedar registrado ante un acta o formato de cambio, en el cual el comandante lo diligenciara y se registrará el motivo del cambio y posteriormente se archivara. El responsable de la sala de monitoreo realizara el cambio según lo autorizado por el comandante.

5) En caso de traslado del comandante o responsable de la sala de monitoreo, deberá hacer el empalme y entrega de los registros al nuevo personal.

6) El responsable de la sala de monitoreo realizara la configuración de contraseñas y configuración de filtro de IPs para las cámaras., proceso que se debe registrar en un documento y se archivara en un lugar seguro.

7) El responsable de la sala de monitoreo realizara copia de seguridad de la configuración de los equipos, siempre y cuando el equipo lo admita.

Resultados Claves

1) Los equipos quedaran asegurado con su respectiva configuración.

2) Registros de cambio de claves en un lugar seguro.

3) Las claves solo de conocimiento del comandante y responsable de la sala de monitoreo.

Políticas Relacionadas

1) Política de seguridad sala de monitoreo.

4.5.5 Política de seguridad para sitios de puntos de cámaras.

Se debe gestionar la seguridad de los puntos de cámara para que estos estén funcionales y permitan realizar la vigilancia para lo cual fueron destinados.

4.5.5.1 Introducción

La ubicación de las cámaras se efectuó, previo a un estudio de seguridad entre la alcaldía y la estación de policía, estas permite la visualización de los movimientos en la zona, permitiendo monitorear y guardar en el NVR para su posterior uso, el funcionamiento se debe garantizar durante las 24 horas del día y durante los 365 días del año, para que brinde la seguridad para lo cual fue instalada.

4.5.5.2 Alcance

Las instalaciones eléctricas, equipos de gabinete, fibra óptica y cajas de paso que son parte de la acometida, desde el poste de energía hasta el poste de la cámara.

Se aplica a: Comandante, responsable sala de monitoreo, operador y contratista.

Objetivos

1) Asegurar los equipos instalados en gabinete.

2) Asegurar su mantenimiento para el buen funcionamiento.

3) Estar pendiente de las alarmas instaladas para su protección.

4) Estar pendientes de vandalismo o accidentes en la zona que perjudique el funcionamiento de los equipos.

Principios

1) Velar por la seguridad de la zona donde opera la cámara, de accidentes o vandalismo.

2) Gestionar ante la alcaldía la contratación del personal para los mantenimientos del sistema.

3) Mantener registro de los mantenimientos y cambios realizados a los equipos.

4) El medio de transmisión (fibra óptica) en caso de daño deberá ser reparada en menos de 24 horas para que el sistema no quede sin funcionamiento.

5) El suministro de energía para el funcionamiento de las cámaras.

Responsabilidades

1) El comandante realizara el proyecto para solicitar a la alcaldía la contratación para el mantenimiento del sistema.

2) El operador informara al comandante de forma inmediata de alguna anomalía que esté sucediendo en el sitio y que afecte el funcionamiento de la cámara, esto debe quedar registrado en el libro de anotaciones.

3) El operador de cámaras no permitirá que se realicen el mantenimiento, si el trabajador no presenta su carnet de riesgos profesionales y su equipo o dotación respectiva para ese trabajo.

4) El contratista se responsabiliza del mantenimiento de los equipos en sitio, teniendo en cuanta las normas para trabajos en alturas. Se debe realizar acta de trabajo en donde detalle las actividades realizadas.

5) Los equipos que necesiten ser retirado por cuestiones de mantenimiento más técnicos y que no se puedan desarrollar en sitio, deben ser autorizados por el comandante y se dejara constancia del retiro del equipo detallando la información del equipo.

6) Los equipos de transmisión como conversor de medios, switch, cámara deberán ser remplazados de forma inmediata en caso de daño, para evitar que la zona quede sin monitoreo.

7) La alcaldía será la responsable de suministrar los equipos que se necesiten remplazar.

8) La alcaldía es responsable de los pagos del consumo de energía para las cámaras.

Resultados Claves

1) Operación de las cámaras en un 100%.

2) Tiempos de mantenimiento adecuados para que los equipos funcionen correctamente.

3) Registro de los mantenimientos realizados.

Políticas Relacionadas

1) Política de seguridad mantenimiento del sistema por parte del contratista

4.5.6 Política de seguridad mantenimiento del sistema por parte del contratista

El contratista deberá realizar los mantenimientos solicitados, manteniendo la reserva de información y seguridad del sistema.

4.5.6.1 Introducción

El sistema de vídeo vigilancia para su buen funcionamiento requiere de personal capacitado en áreas como sistemas eléctricos, comunicaciones, operación de equipos, además de personal idóneo en trabajos en alturas, esto porque las cámaras están instaladas a una altura de 10 mts, para brindar una mejor cobertura y por seguridad de vandalismo.

4.5.6.2 Alcance

El mantenimiento realizado por el contratista dentro de la sala de monitoreo y en los puntos de cámara.

Se aplica a: El contratista.

Objetivos

1) Gestionar la seguridad en el proceso de mantenimiento.

2) Garantizar el funcionamiento del sistema.

Principios

1) Personal capacitado para realizar labores de mantenimiento.

2) Garantizar la reserva de la información del sistema.

3) Que el sistema este soportado por el mantenimiento por un tiempo prudencial.

Responsabilidades

1) El comandante es responsable de gestionar ante la alcaldía, que se contrate el personal para el mantenimiento.

2) El comandante junto con el responsable del sistema, determinaran las necesidades del sistema para su buen funcionamiento.

3) El contratista pone a disposición personal capacitado y con sus respectivos documentos para realizar las labores de mantenimiento.

4) El contratista deberá firmar formato de confidencialidad o reserva de la información que se le suministre para que pueda hacer su labor.

5) El contratista deberá responde a un llamado de mantenimiento en menos de 24 horas.

6) El contratista deberá diligenciar formato de mantenimiento donde detalle las labores realizadas y dejara copia en el comando para el archivo.

7) El contratista junto con el responsable de la sala de monitoreo deberán actualizar el inventario.

Resultados Claves

1) Contratación de personal para mantenimiento.

2) Respuesta de mantenimiento efectiva.

3) Registro de mantenimiento realizados.

4) Que este actualizada la base de datos del inventario.

Políticas Relacionadas

1) Políticas de seguridad de la información.

2) Política de seguridad sala de monitoreo.

3) Política De Seguridad Para Software Implementado En El Sistema De Vídeo Vigilancia CCTV.

4) Política De Seguridad Para Los Equipos De Red, Switch, Netagent, Nvr, Cámaras

5) Política de seguridad para sitios de puntos de cámaras.

5. ACTIVOS DE INFORMACIÓN MEDIANTE LA METODOLOGÍA MAGERIT EN EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

5.1 MAGERIT V.3

"Un análisis de riesgos TIC es recomendable en cualquier organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión[56]"

Para determinar los riesgos del sistema, en primer lugar se identificó los activos relevantes que permiten cumplir con el objetivo de la organización, definiendo su valor.

Estos activos están expuestos a unas amenazas, las cuales se identificaron para determinar, cuál es el grado de impacto posible.

5.2 ACTIVOS

"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos[57]".

Para el análisis del sistema de CCTV se determinaron los activos relacionados a continuación (tabla 6)

Tabla 6: Listado de activos

Ámbito	Activo
Esenciales: información	Videos grabados
Activos esenciales: servicio	Entrega de evidencias

[56] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. Versión 3. Madrid. octubre de 2012. [2016-03-13]. p. 16. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m %C3%A9todo_es_NIPO_630-12-171-8.pdf. NIPO: 630-12-171-8.

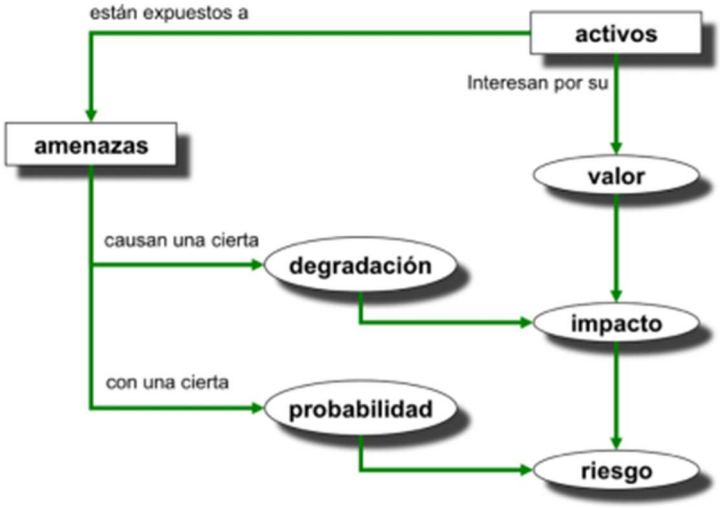
[57] Ibíd., p. 22.

Ámbito	Activo
Datos / información	Base de datos configuración de cámaras
	Base de datos inventario de equipos
	Carpeta información de proyecto
[SW] aplicaciones (software)	Control center
	Sistema operativo
[HW] equipamiento informático (hardware)	Workstation
	Impresora
	Monitor de 55”
	Switch de 24 puertos
	Conversores de fibra
	Switch de 8 puertos
	Teclado joystick
	Cámara ptz
[Media] soportes de información	Network vídeo recorders
	Manuales de equipos
[Media] soportes de información	Ups
	Fibra óptica
	Escritorio
	Rack de equipos
[L] instalaciones	Salón de monitoreo
	Canalizaciones eléctricas
[P] personal	Comandante
	Responsable sala de monitoreo
	Operadores

Fuente: Propiedad del autor

Los elementos para el análisis del riesgo potencial están resumidos en la siguiente (ver figura 29).

Figura 29: Elementos del análisis de riesgos potenciales



Fuente: MAGERIT – versión 3.0, Libro I Método

A los anteriores activos se los define por importancia dentro del sistema, para el caso de estudio se tomarla siguiente valoración como se puede observar en la tabla 7.

Tabla 7: Tabla de valoración de los activos

tabla de valor		
MB	1	Irrelevante para el proyecto
B	2	Importancia menor para el proyecto
M	3	Importancia para el proyecto
A	4	Altamente importante para el proyecto
MA	5	De vital importancia para los objetivos del proyecto

Fuente: MAGERIT – versión 3.0, Libro I Método

5.2.1 Clasificación de los activos

La clasificación para los activos del sistema se tomó como base a MagerIT V.3 libro II, presenta un catálogo de elementos que facilita al proyecto el análisis y gestión de riesgos.

Este método clasifica los activos creando unas tablas que van desde la 8 hasta la 33, donde cada tabla describe el activo y se determina un valor dentro del sistema de vigilancia.

5.2.1.1 Esenciales Información

Se considera importante para el sistema de vídeo vigilancia y marca la seguridad para los demás activos, en la tabla 8 se describe el activo información como son videos grabados.

Tabla 8: [Info] esenciales: información

[Essential] Activos esenciales		
Código:	**Nombre**: Videos Grabados	
Descripción: Es la información guardada en los NVR, estas imágenes son capturadas por las cámaras.		
Propietario: Alcaldía		
Responsable: Comandante de Estación		
Tipo: [classified] [R]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Tiene el valor alto porque la razón de ser del sistema es entregar evidencias para casos o delitos
[I]	**5**	La información guardada no puede ser modificada
[C]	**3**	Se debe resguardar pero puede estar sujeto a revisiones por parte de las personas con autorización
Dependencia de Activos Inferiores (hijos)		
Activo: Switch de 24 puertos, Conversores de fibra, Switchs de 8 puertos, Fibra Óptica,		**Grado**: Alto
¿Por qué?: Permite la transmisión de los datos		
Activo: Cámara PTZ		Grado: Alto
¿Por qué? Que la cámara esté funcionando		
Activo: NVR		Grado: Alto
¿Por qué? Que la información se esté grabando		

Fuente: Propiedad del autor

5.2.1.2 Esenciales servicios

La información manejada en este sistema de vigilancia, genera un servicio que presta la policía a las entidades que necesiten las imágenes guardadas. (Tabla 9)

Tabla 9: [Service] activos esenciales: servicio

[service] Servicio		
Código:	**Nombre**: entrega de evidencias	
Descripción: El sistema de vídeo vigilancia permite grabar las situaciones monitoreadas durante las 24 horas del día, las cuales pueden ser solicitadas como evidencias para casos o delitos		
Propietario: Alcaldía		
Responsable: Comandante de estación		
Tipo: [classified] [R]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Debe suministrar la información solicitada
[A]	**4**	Solo debe acceder con password para evitar que se sustraiga información que pueda perjudicar la reputación de la estación
[T]	**5**	Se debe registrar quien solicita y quien recibe la información, se contempla la cadena de custodia para la evidencia.
Dependencia de Activos Inferiores (hijos)		
Activo: Videos grabados		**Grado**: Alto
¿Por qué?: si existen videos grabados se entrega de lo contrario se informa que no existe las grabaciones.		

Fuente: Propiedad del autor

5.2.1.3 Datos / Información

Estos datos son importantes para que el sistema opere con normalidad, en la tabla 10 tenemos el activo base de datos, que configura la cámaras, también tenemos el inventario, información esencial para cualquier organización saber cuáles elementos tiene (ver tabla 11).

Adicionalmente, en la estación tienen la carpeta con la información del proyecto de ejecución, planos CDs, manuales de equipos que permiten dar información del sistema instalado (ver tabla 12).

Tabla 10: [D] datos / información – Base de datos configuración de cámaras

[info] Información		
Código:	**Nombre**: Base de datos configuración de Cámaras	
Descripción: Es la base de datos que contiene la configuración de las cámaras, usuarios, alarmas del sistema de vigilancia CCTV de Yacuanquer, también permite la visualización de las cámaras en vídeo en vivo.		
Propietario: Alcaldía		
Responsable: Responsable de sala de monitoreo		
Tipo: [conf]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	La base de datos de configuración es la que permite que el sistema funcione, la perdida puede dejar inutilizado el sistema
[I]	**3**	Se restringe solo para el personal autorizado a la sala
[C]	**3**	No implica perdida de datos ya que se puede reconstruir
Dependencia de Activos Inferiores (hijos)		
Activo:		**Grado**:
¿Por qué?:		

Fuente: Propiedad del autor

Tabla 11: [D] datos / información base de datos inventario de equipos

[info] Información		
Código:	**Nombre**: base de datos Inventario de equipos	
Descripción: archivo de Access que tiene el inventario de los equipos instalados en el sistema, nombre ubicación y serial.		
Propietario: Alcaldía		
Responsable: Responsable de sala de Monitoreo		
Tipo: [int], [source]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Se debe tener actualizado los datos de los equipos instalados
[I]	**5**	Permita conocer los elementos instalados
[C]	**3**	Disponible para la consulta
Dependencia de Activos Inferiores (hijos)		

Activo: Responsable sala de monitoreo	**Grado**: Alto
¿Por qué?: él debe velar por que este actualizado	

Fuente: Propiedad del autor

Tabla 12: [D] datos / información carpeta información del proyecto

[info] Información		
Código:	**Nombre**: Carpeta información de proyecto	
Descripción: Se encuentra toda la información del proyecto las cantidades, diagramas de datos, eléctricos, arquitectónicos del sitio.		
Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [files]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	La información es indispensable para la ampliación y mantenimientos del sistema
[I]	**3**	Solo para el personal autorizado
[C]	**2**	Debe ser consultada por las personas involucradas en el funcionamiento
Dependencia de Activos Inferiores (hijos)		
Activo: Responsable sala de monitoreo		**Grado**: Medió
¿Por qué?: es la persona que debe velar por que este archivado		

Fuente: Propiedad del autor

5.2.1.4 [SW] Aplicaciones (Software)

En esta clasificación está el software importante que permite el funcionamiento del sistema y se describen en las tablas 13 y 14

Tabla 13: [SW] Aplicaciones (Software) Control center

[SW] Aplicaciones (software)	
Código:	**Nombre**: Control Center
Descripción: Programa que permite monitorear y configurar las cámaras para que puedan ser utilizadas, además permite la gestión de los usuarios para restringir las acciones.	
Propietario: Alcaldía	
Responsable: Responsable de sala de monitoreo	

Tipo: [std]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Debe estar funcionando para que se puedan operar las cámaras
[I]	**3**	De debe mantener la configuración para que funcionen correctamente las cámaras
[C]	**2**	El programa tiene una licencia gratuita y solo funciona con estas cámaras
Dependencia de Activos Inferiores (hijos)		
Activo: Base de datos configuración de Cámaras		**Grado**: Alto
¿Por qué?: si la base de datos permite funcionar correctamente al programa de monitoreo de las cámaras		
Activo: Workstation, Sistema operativo		**Grado**: Alto
¿Por qué?: El computador es el equipo donde se ejecuta el programa		

Fuente: Propiedad del autor

Tabla 14: [SW] Aplicaciones (Software) Sistema operativo

[SW] Aplicaciones (software)		
Código:	**Nombre**: sistema operativo	
Descripción: La computadora de monitoreo cuenta con Windows 7 profesional		
Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [std] - [os]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Plataforma donde se instalan los aplicativos
[I]	**4**	Debe estar libre de virus y errores
[C]	**3**	Solo para personal autorizado
Dependencia de Activos Inferiores (hijos)		
Activo:		**Grado**:
¿Por qué?:		

Fuente: Propiedad del autor

5.2.1.5 [Hw] Equipamiento informático (hardware)

Es el equipo (hardware) necesario para que el sistema esté operando y esta descrito en las tablas 15, 16, 17, 18, 19, 20, 21, 22.

Tabla 15: [Hw] equipamiento informático (hardware) Workstation

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Workstation	
Descripción: Equipo de cómputo con características avanzadas para la visualización de las cámaras		
Propietario: Alcaldía		
Responsable: Operador		
Tipo: [mid]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Permite la visualización de las cámaras, donde se instala los programas para monitoreo
[I]	**4**	No debe ser accesible a toda persona por cuanto cumple la función de monitoreo, cualquier otra función debe descartarse.
[C]	**1**	Será utilizado por los operadores
Dependencia de Activos Inferiores (hijos)		
Activo: Sistema operativo		**Grado**: Alto
¿Por qué?: su funcionamiento depende del sistema operativo instalado		

Fuente: Propiedad del autor

Tabla 16: [Hw] equipamiento informático (hardware) impresora

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Impresora	
Descripción: Impresora láser multifuncional para realizar la documentación solicitada.		
Propietario: Alcaldía		
Responsable: Operador		
Tipo:		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**3**	Para informes y repuestas a oficios
[I]	**2**	Por costo
[C]	**1**	No aplica
Dependencia de Activos Inferiores (hijos)		
Activo: Workstation		**Grado**: Medio
¿Por qué?: la impresora se conecta al computador, pero tiene funciones individuales.		

Fuente: Propiedad del autor

Tabla 17: [Hw] equipamiento informático (hardware) monitor de 55”

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Monitor de 55”	
Descripción: Monitor con gran dimensión para poder observar las imágenes de las cámaras.		
Propietario: Alcaldía		
Responsable: Operador		
Tipo: [peripheral]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Debe estar funcional para observar las imágenes
[I]	**2**	Por el costo
[C]	**1**	No aplica
Dependencia de Activos Inferiores (hijos)		
Activo: Workstation		**Grado**: Medio
¿Por qué?: Está conectado a la computadora para mostrar las imágenes		

Fuente: Propiedad del autor

Tabla 18: [Hw] equipamiento informático (hardware) Switch de 24 puesto

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Switch de 24 puertos	
Descripción: switch de 24 puertos administrable y gama alta para poder administrar el tráfico de las cámaras.		
Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [switch]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Para todo el tráfico de la red
[I]	**4**	Debe estar funcional todo el tiempo, además permite incorporar seguridad a la red
[C]	**3**	La configuración y protegido con password
Dependencia de Activos Inferiores (hijos)		
Activo:		**Grado**:
¿Por qué?:		

Fuente: Propiedad del autor

Tabla 19: [Hw] equipamiento informático (hardware) Conversores de fibra

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Conversores de fibra	
Descripción: equipos para conectar la fibra óptica con el cableado UTP		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [network]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Sin ellos las cámaras no se conectan
[I]	**4**	Por el costo y su función
[C]	**2**	No es importante
Dependencia de Activos Inferiores (hijos)		
Activo: Fibra Óptica		**Grado**: Alto
¿Por qué?: el medio de comunicación es la fibra óptica		

Fuente: Propiedad del autor

Tabla 20: [Hw] equipamiento informático (hardware) Switch de 8 puertos

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Switchs de 8 puertos	
Descripción: permite conectar los dispositivos en cada punto de cámara		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [switch]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**3**	Su función es conectar equipos en gabinete
[I]	**2**	Bajo valor del equipo
[C]	**1**	No se aplica
Dependencia de Activos Inferiores (hijos)		
Activo: Fibra Óptica, Conversor de fibra		**Grado**: Alto
¿Por qué?: el medio de comunicación es la fibra óptica		

Fuente: Propiedad del autor

Tabla 21: [Hw] equipamiento informático (hardware) teclado joystick

[HW] Equipamiento informático (hardware)	
Código:	**Nombre**: Teclado Joystick
Descripción: permite manipular las cámaras los movimientos, zoom	
Propietario: Alcaldía	
Responsable: Operador	

Tipo: [peripheral]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**3**	Para manipular los movimientos de las cámaras
[I]	**2**	Se debe cuidar para su mejor operación
[C]	**1**	No aplica
Dependencia de Activos Inferiores (hijos)		
Activo: Workstation		**Grado**: Alto
¿Por qué?: está conectado al puerto serial del computador		

Fuente: Propiedad del autor

Tabla 22: [Hw] equipamiento informático (hardware) cámaras PTZ

[HW] Equipamiento informático (hardware)		
Código:	**Nombre**: Cámara PTZ	
Descripción: Cámara de seguridad transmite las imágenes desde el punto donde se instaló para brindar seguridad		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [network]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Debe estar funcionando 24 horas del día
[I]	**4**	Restringir el ingreso a la configuración de la cámara
[C]	**3**	Reserva de la información
Dependencia de Activos Inferiores (hijos)		
Activo: Fibra Óptica, Conversor de fibra		**Grado**: Alto
¿Por qué?: el medio de transmisión es la fibra óptica		

Fuente: Propiedad del autor

5.2.1.6 [Media] soportes de información

Medios de almacenamiento de forma permanente o por algún tiempo, en esta clasificación tenemos los NVRs y manuales de los equipos (ver tablas 23 y 24)

Tabla 23: [Media] soportes de información Network Vídeo Recorder

[Media] Soportes de información	
Código:	**Nombre**: Network Vídeo Recorders
Descripción: Equipos en los cuales se graban los videos transmitidos desde las cámaras.	

Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [san]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Es el medio en el cual se graban las imágenes
[I]	**5**	Debe estar en buen funcionamiento
[C]	**5**	Se debe proteger de acceso no autorizado
Dependencia de Activos Inferiores (hijos)		
Activo: Fibra Óptica, Switch de 24 pts		**Grado**: Alto
¿Por qué?: el medio de transmisión es la fibra óptica		

Fuente: Propiedad del autor

Tabla 24: [Media] soportes de información manuales de equipos

[Media] Soportes de información		
Código:	**Nombre**: Manuales de equipos	
Descripción: se almacena los manuales de los diferentes equipos que se instalaron en el sistema de vídeo vigilancia.		
Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [printed]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**3**	Para consulta de las configuraciones de los equipos
[I]	**1**	No aplica
[C]	**1**	No aplica
Dependencia de Activos Inferiores (hijos)		
Activo: Responsable sala de monitoreo		**Grado**: Medio
¿Por qué?: es el que debe resguardar lo que este archivado		

Fuente: Propiedad del autor

5.2.1.7 [AUX] Equipamiento auxiliar

Equipos para soporte a los sistemas informáticos, que están definidos en las tablas 25, 26, 27 y 28.

Tabla 25: [Media] Soportes De Información UPS

[Media] Soportes de información		
Código:	**Nombre**: UPS	
Descripción: ups instaladas en los puntos de cámara y en el rack como soporte para evitar caídas de energía		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [ups]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Deben estar funcionales y protegiendo los equipos
[I]	**3**	Que permita su monitorización para saber el estado
[C]	**3**	Solo personal autorizado

Fuente: Propiedad del autor

Tabla 26: [Media] Soportes De Información fibra óptica

[Media] Soportes de información		
Código:	**Nombre**: Fibra Óptica	
Descripción: Red de fibra para conectar las cámaras ubicadas en el casco urbano del municipio.		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [fiber]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**5**	Permite la trasmisión del vídeo desde el punto de calle hasta el centro de monitoreo
[I]	**5**	Debe estar sin cortes
[C]	**5**	La ruta de fibras solo para personal autorizado

Fuente: Propiedad del autor

Tabla 27: [Media] Soportes De Información escritorio

[Media] Soportes de información	
Código:	**Nombre**: Escritorio
Descripción: Escritorio donde se instaló los equipos de monitoreo	
Propietario: Alcaldía	
Responsable: Responsable sala de monitoreo	
Tipo: [furniture]	
Valoración	

Dimensión	Valor	Justificación
[D]	**3**	Permite crear un espacio de monitoreo donde el operador pueda hacer su trabajo
[I]	**2**	Se debe mantener en las mejores condiciones
[C]	**1**	No aplica

Fuente: Propiedad del autor

Tabla 28: [Media] Soportes De Información Rack de equipos

[Media] Soportes de información		
Código:	**Nombre**: Rack de equipos	
Descripción: Permite organizar los NVR, switch, organizador de fibra, cableado estructurado y mantenerlo bajo llave		
Propietario: Alcaldía		
Responsable: Responsable sala de monitoreo		
Tipo: [furniture]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**3**	Para organizar los equipo en un solo sitio
[I]	**2**	Es de material duradero
[C]	**1**	No aplica

Fuente: Propiedad del autor

5.2.1.8 [L] Instalaciones

Lugar donde se opera el sistema de vigilancia y las tablas 29 y 30 describen estos lugares.

Tabla 29: [L] Instalaciones Salón de monitoreo

[L] Instalaciones		
Código:	**Nombre**: salón de monitoreo	
Descripción: espacio designado por la estación de policía para implementar el sistema de vídeo vigilancia.		
Propietario: Alcaldía		
Responsable: Comandante estación		
Tipo: [local]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Es mejor para el proyecto por cuanto se asegura los

		equipo y tableros eléctricos
[I]	**2**	Mantener en orden
[C]	**3**	Asegurar que no ingrese personal no autorizado

Fuente: Propiedad del autor

Tabla 30: [L] Instalaciones canalizaciones eléctricas

[L] Instalaciones		
Código:	**Nombre**: canalizaciones eléctricas	
Descripción: cada punto de cámara se realizó una canalización subterránea para instalar cableado.		
Propietario: Alcaldía		
Responsable: Alcaldía		
Tipo: [channel]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Se debe adecuar una canalización para la conexión de la cámara
[I]	**4**	Que la canalización deba estar en buen estado
[C]	**4**	No debe suministrase información del recorrido

Fuente: Propiedad del autor

5.2.1.9 [P] Personal

Persona que se relacionan con el sistema de vigilancia descritos en las tablas 31, 32 y 33

Tabla 31: [P] Personal Comandante

[P] Personal		
Código:	**Nombre**: Comandante	
Descripción: Persona jefe de la estación de policía		
Responsable::		
Ubicación:: Estación de policía Yacuanquer		
Numero: 1		
Tipo: [ui]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Importante para el funcionamiento

Fuente: Propiedad del autor

Tabla 32: [P] Personal responsable sala de monitoreo

[P] Personal		
Código:	**Nombre**: Responsable sala de monitoreo	
Descripción: Persona que el comandante a designado para velar por el buen funcionamiento de la sala de monitoreo		
Responsable: Comandante de policía.		
Ubicación:: Estación de policía Yacuanquer		
Numero: 1		
Tipo: [adm], [ui]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Importante para el funcionamiento

Fuente: Propiedad del autor

Tabla 33: [P] Personal operadores

[P] Personal		
Código:	**Nombre**: Operadores	
Descripción: Persona que el comandante a designado para monitorear las cámaras		
Responsable: Comandante de policía.		
Ubicación:: Estación de policía Yacuanquer		
Numero: 1		
Tipo: [op]		
Valoración		
Dimensión	**Valor**	**Justificación**
[D]	**4**	Importante para el funcionamiento

Fuente: Propiedad del autor

5.3 VALOR DEL RIESGO

De acuerdo a la información obtenida en la clasificación de los activos, a continuación se hace la valoración de los activos identificados en el sistema de CCTV. (Ver tabla 35)

A cada activo se le asigna un valor de acuerdo a lo expuesto en la tabla 7, teniendo en cuenta los siguientes atributos. (Ver tabla 34)

Tabla 34: Nomenclatura

D	Disponibilidad
I	Integridad
C	Confidencialidad
A	Autenticidad
T	Trazabilidad

Fuente: Realizado por el autor

Tabla 35: Valor del riesgo

		Valor					
Ámbito	Activo	D	I	C	A	T	Valor
ESENCIALES: INFORMACIÓN	Videos grabados	5	5	3	3	1	MA
Activos esenciales: Servicio	Entrega de evidencias	5	5	3	4	5	MA
Datos / información	Base de datos configuración de cámaras	5	3	3	2	1	MA
	Base de datos inventario de equipos	5	4	2	2	3	M
	Carpeta información de proyecto	4	3	2	2	1	A
[SW] APLICACIONES (SOFTWARE)	Control center	5	3	2	1	1	A
	Sistema operativo	5	4	3	3	1	A
[HW] Equipamiento informático (hardware)	Workstation	5	4	1	1	1	A
	Impresora	3	2	1	1	1	B
	Monitor de 55”	4	2	1	1	1	M
	Switch de 24 puertos	5	4	3	3	1	A
	Conversores de fibra	5	4	2	1	1	A
	Switchs de 8 puertos	3	2	1	1	1	B
	Teclado joystick	3	2	1	1	1	M
	Cámara ptz	5	4	3	3	3	MA
[Media] Soportes de información	Network vídeo recorders	5	5	5	5	2	MA
	Manuales de equipos	3	1	1	1	1	B
[Media] Soportes de información	UPS	5	3	3	1	2	A
	Fibra óptica	5	5	5	1	3	A
	Escritorio	3	2	1	1	1	M
	Rack de equipos	3	2	1	1	1	M
[L] Instalaciones	Salón de monitoreo	4	2	3	1	1	M

Ámbito	Activo	Valor					
		D	I	C	A	T	Valor
[P] Personal	Canalizaciones eléctricas	4	4	4	1	1	A
	Comandante	5	1	1	1	1	M
	Responsable sala de monitoreo	5	1	1	1	1	M
	Operadores	5	1	1	1	1	M

Fuente: Propiedad del autor

5.4 AMENAZAS

"Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización[58]".

Valores para el cálculo de riesgo (tabla 36)

Tabla 36: Valores de impacto

	Impacto	
Muy alta	MA	5
Alta	A	4
Media	M	3
Baja	B	2
Muy baja	MB	1

Fuente: Propiedad del autor

[58] Ibíd., p. 27.

Tabla 37: Valores probabilidad

Probabilidad		
MA	5	MUY FRECUENTE
A	4	FRECUENTE
M	3	NORMAL
B	2	POCO FRECUENTE
MB	1	MUY POCO FRECUENTE

Fuente: propiedad del autor

Formula: Riesgo

R= P*I Con esta fórmula se estable la tabla 38

Tabla 38: El riesgo en función del impacto y la probabilidad

Riesgo		probabilidad				
		MB (1)	B (2)	M (3)	A (4)	MA (5)
impacto	MA (5)	5	10	15	20	25
	A (4)	4	8	12	16	20
	M (3)	3	6	9	12	15
	B (2)	2	4	6	8	10
	MB (1)	1	2	3	4	5

Fuente: Realizado por el autor

Código de Colores

	Riesgos muy probables y de muy alto impacto
	Riesgos Altos se deben tratar porque existen una probabilidad de que sucedan
	Riesgo moderado que se deben de tratar que son poco probables
	Riesgo bajo y poco probable
	Riesgo muy bajo y muy baja probabilidad

Se determina el siguiente listado de amenazas (tabla 39), basándose en el libro 2, catálogo de elementos MAGERIT – versión 3.0, se estima el valor de amenaza en relación a impacto (ver tabla 36), probabilidad (ver tabla 37) y riesgo (ver tabla 38).

Tabla 39: Listado de Amenazas

Amenazas						
sigla	**Grupo**	**Sigla**	**Detalle**	**I**	**P**	**R**
N	Desastres naturales	N1	Fuego	5	1	5
I	De origen industrial	I1	Fuego	5	1	5
		I5	Avería de origen físico o lógico	4	3	12
		I6	Corte del suministro eléctrico	4	4	16
		I7	Condiciones inadecuadas de temperatura o humedad	3	3	9
		I9	Interrupción de otros servicios y suministros esenciales	3	3	9
		I10	Degradación de los soportes de almacenamiento de la información	5	3	15
E	Errores y fallos no intencionados	E1	Errores de los usuarios	3	4	12
		E2	Errores del administrador	2	2	4
		E4	Errores de configuración	3	3	9
		E7	Deficiencias en la organización	3	4	12
		E8	Difusión de software dañino	3	5	15
		E15	Alteración accidental de la información	3	3	9
		E19	Fugas de información	3	2	6
		E24	Caída del sistema por agotamiento de recursos	5	3	15
		E25	Pérdida de equipos	4	1	4
A	Ataques intencionados	A4	Manipulación de la configuración	3	2	6
		A6	Abuso de privilegios de acceso	3	1	3
		A7	Uso no previsto	3	3	9
		A11	Acceso no autorizado	4	1	4
		A12	Análisis de tráfico	3	1	3
		A19	Divulgación de información	3	1	3
		A22	Manipulación de programas	3	1	3
		A26	Ataque destructivo	5	3	15
		A28	Indisponibilidad del personal	4	3	12

Fuente: Propienda del autor

5.5 ESTIMACIÓN DEL RIESGO POTENCIAL DE LOS ACTIVOS

Para la estimación del riesgo potencial (R) utilizamos la formula R = I x P y se obtiene la tabla 40.

Tabla 40: Riesgo potencial de los Activos

Ámbito	Activo	Sigla	Amenaza	VR A	D	I	P	R
ESENCIALES: INFORMACIÓN	Videos grabados	N1	Fuego	5	1,0	5	1	5
		I1	Fuego	5	1,0	5	1	5
		I5	Avería de origen físico o lógico	5	0,5	3	3	9
		I6	Corte del suministro eléctrico	5	0,8	4	4	16
		I10	Degradación de los soportes de almacenamiento de la información	5	1,0	5	4	20
		E4	Errores de configuración	5	0,5	3	3	9
Activos esenciales: Servicio	Entrega de evidencias	N1	Fuego	5	1,0	5	1	5
		I1	Fuego	5	1,0	5	1	5
		I5	Avería de origen físico o lógico	5	0,5	3	3	9
		I10	Degradación de los soportes de almacenamiento de la información	5	1,0	5	4	20
		E24	Caída del sistema por agotamiento de recursos	5	0,5	3	3	9
Datos / información	Base de datos configuración de cámaras	E8	Difusión de software dañino	5	0,8	4	5	20
		A4	Manipulación de la configuración	5	0,5	3	2	6
	Base de datos inventario de equipos	E2	Errores del administrador	5	0,5	3	2	6
		E7	Deficiencias en la organización	5	0,5	3	4	12
		E15	Alteración accidental de la información	5	0,6	3	3	9

Ámbito	Activo	Sigla	Amenaza	VRA	D	I	P	R
	Carpeta información de proyecto	I10	Degradación de los soportes de almacenamiento de la información	4	0,8	3	3	9
[SW] APLICACIONES (SOFTWARE)	Control center	E1	Errores de los usuarios	5	0,8	4	4	16
		E2	Errores del administrador	5	0,7	4	2	8
		E4	Errores de configuración	5	0,7	4	3	12
	Sistema operativo	I5	Avería de origen físico o lógico	5	0,8	4	3	12
		E1	Errores de los usuarios	5	0,5	3	4	12
		E2	Errores del administrador	5	0,5	3	2	6
		E4	Errores de configuración	5	0,5	3	3	9
		E8	Difusión de software dañino	5	0,8	4	5	20
		E15	Alteración accidental de la información	5	0,5	3	3	9
		A4	Manipulación de la configuración	5	0,5	3	2	6
		A6	Abuso de privilegios de acceso	5	0,5	3	1	3
[HW] Equipamiento informático (hardware)	Workstation	N1	Fuego	5	1,0	5	1	5
		I1	Fuego	5	1,0	5	1	5
		I10	Degradación de los soportes de almacenamiento de la información	5	0,5	3	3	9
		I5	Avería de origen físico o lógico	5	0,5	3	3	9
	Impresora	N1	Fuego	3	1,0	3	1	3
		I1	Fuego	3	1,0	3	1	3
		I5	Avería de origen físico o lógico	3	0,5	2	3	6
		I9	Interrupción de otros servicios y suministros esenciales	3	0,8	2	3	6
	Monitor de 55”	N1	Fuego	4	1,0	4	1	4
		I1	Fuego	4	1,0	4	1	4
		I5	Avería de origen físico o lógico	4	0,5	2	3	6

Ámbito	Activo	Sigla	Amenaza	VR A	D	I	P	R
	Switch de 24 puertos	N1	Fuego	5	1,0	5	1	5
		I1	Fuego	5	1,0	5	1	5
		I5	Avería de origen físico o lógico	5	0,8	4	3	12
	Conversores de fibra	I5	Avería de origen físico o lógico	5	0,8	4	3	12
	Switchs de 8 puertos	I5	Avería de origen físico o lógico	3	0,8	2	3	6
	Teclado joystick	N1	Fuego	3	1,0	3	1	3
		I1	Fuego	3	1,0	3	1	3
		I5	Avería de origen físico o lógico	3	0,8	2	3	6
	Cámara ptz	I5	Avería de origen físico o lógico	5	1,0	5	4	20
		I7	Condiciones inadecuadas de temperatura o humedad	5	0,8	4	3	12
[Media] Soportes de información	Network vídeo recorders	N1	Fuego	5	1,0	5	1	5
		I1	Fuego	5	1,0	5	1	5
		I5	Avería de origen físico o lógico	5	0,8	4	4	16
		I6	Corte del suministro eléctrico	5	0,8	4	4	16
		I7	Condiciones inadecuadas de temperatura o humedad	5	0,5	3	3	9
		I10	Degradación de los soportes de almacenamiento de la información	5	0,8	4	3	12
		E4	Errores de configuración	5	0,5	3	3	9
	Manuales de equipos	N1	Fuego	3	1,0	3	1	3
		I1	Fuego	3	1,0	3	1	3
		E7	Deficiencias en la organización	3	0,5	2	4	8
[Media] Soportes de información	Ups	I5	Avería de origen físico o lógico	5	0,5	3	3	9
		I6	Corte del suministro eléctrico	5	0,5	3	4	12

Ámbito	Activo	Sigla	Amenaza	VRA	D	I	P	R
		I7	Condiciones inadecuadas de temperatura o humedad	5	0,5	3	3	9
		I10	Degradación de los soportes de almacenamiento de la información	5	0,5	3	3	9
	Fibra óptica	I5	Avería de origen físico o lógico	5	0,8	4	3	12
	Escritorio	I5	Avería de origen físico o lógico	3	0,3	1	3	3
	Rack de equipos	N1	Fuego	3	1,0	3	1	3
		I1	Fuego	3	1,0	3	1	3
		E7	Deficiencias en la organización	3	0,3	1	4	4
		A11	Acceso no autorizado	3	0,5	2	1	2
[L] Instalaciones	Salón de monitoreo	N1	Fuego	4	1,0	4	1	4
		I1	Fuego	4	1,0	4	1	4
		A11	Acceso no autorizado	4	0,5	2	1	2
	Canalizaciones eléctricas	E19	Fugas de información	4	0,5	2	2	4
		A11	Acceso no autorizado	4	0,5	2	1	2
		A19	Divulgación de información	4	0,8	3	1	3
		A26	Ataque destructivo	4	0,8	3	3	9
[P] Personal	Comandante	E7	Deficiencias en la organización	5	0,5	3	4	12
	Responsable sala de monitoreo	A28	Indisponibilidad del personal	5	0,8	4	5	20
	Operadores	A28	Indisponibilidad del personal	5	0,8	4	5	20

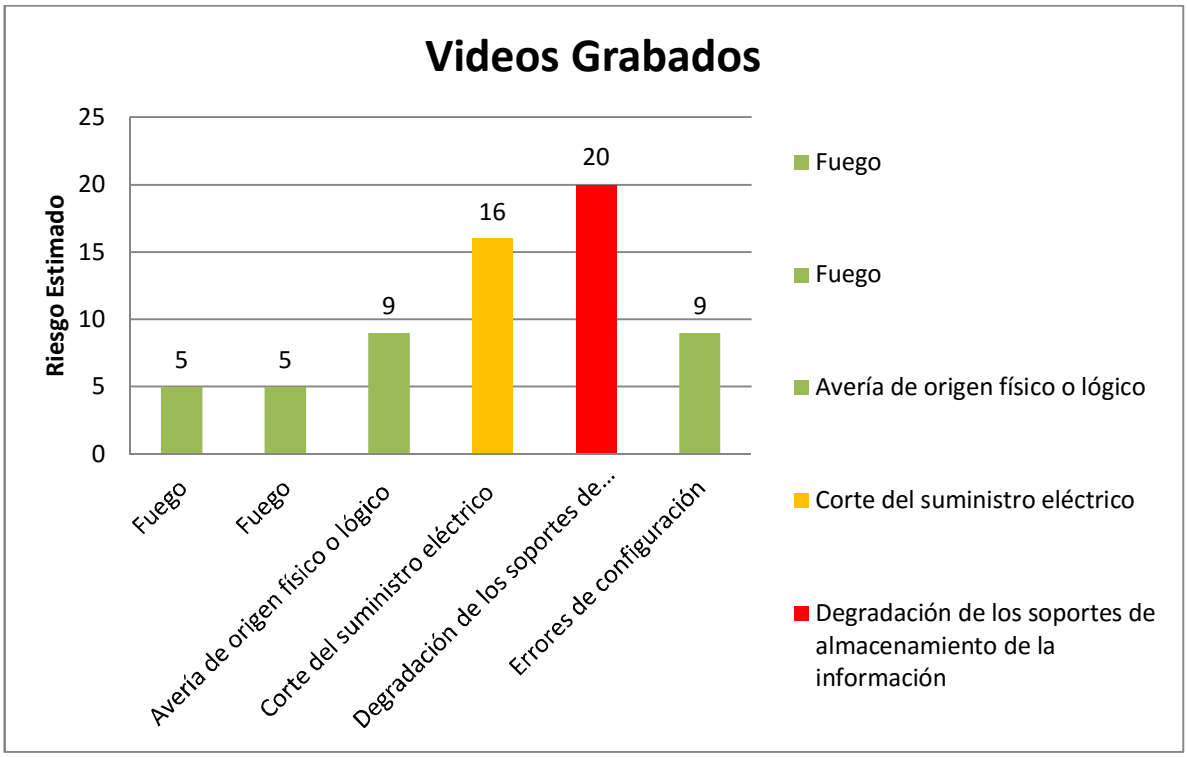
Fuente: Propiedad del autor.

5.6 ANÁLISIS GRÁFICO DE ACTIVOS IMPORTANTES PARA EL SISTEMA

Para mejor entendimiento de los riesgos del sistema, se tomó los activos esenciales, que permiten cumplir al sistema el objetivo por el cual fue implementado, se realiza una representación gráfica del activo.

1) Videos Grabados

Gráfico 1: Activo Videos Grabados



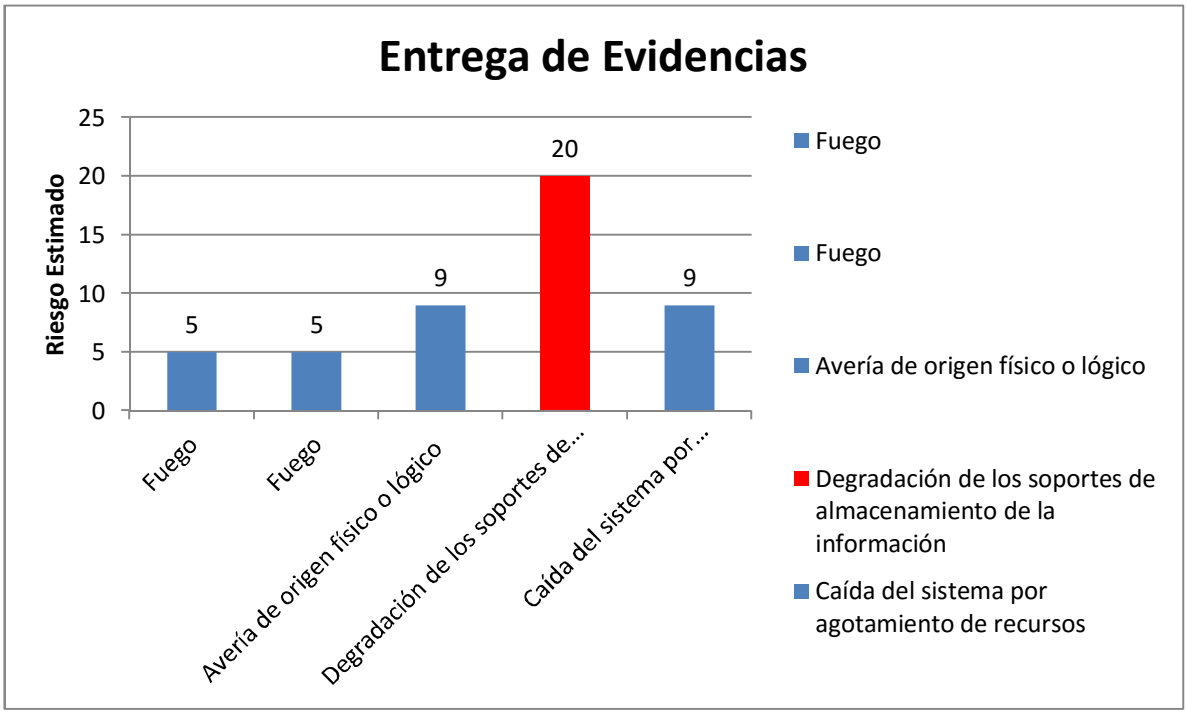
Fuente: Propiedad del autor

En el gráfico 1, se puede analizar, que la información guardada en el sistema de almacenamiento, tiene una amenaza en cuanto a la degradación de los soportes de almacenamiento, esto se debe a que son equipos que están prendidos durante las 24 horas del día, si no se realiza una adecuada gestión, la información puede quedar expuesta a una perdida.

En un segundo nivel está el suministro de energía, esta amenaza influye sobre la información, por cuanto los cortes de energía abruptos sobre los equipos de almacenamiento pueden causar daños y deterioro de los discos.

2) El servicio de Entrega de Evidencia

Gráfico 2: Entrega de evidencia

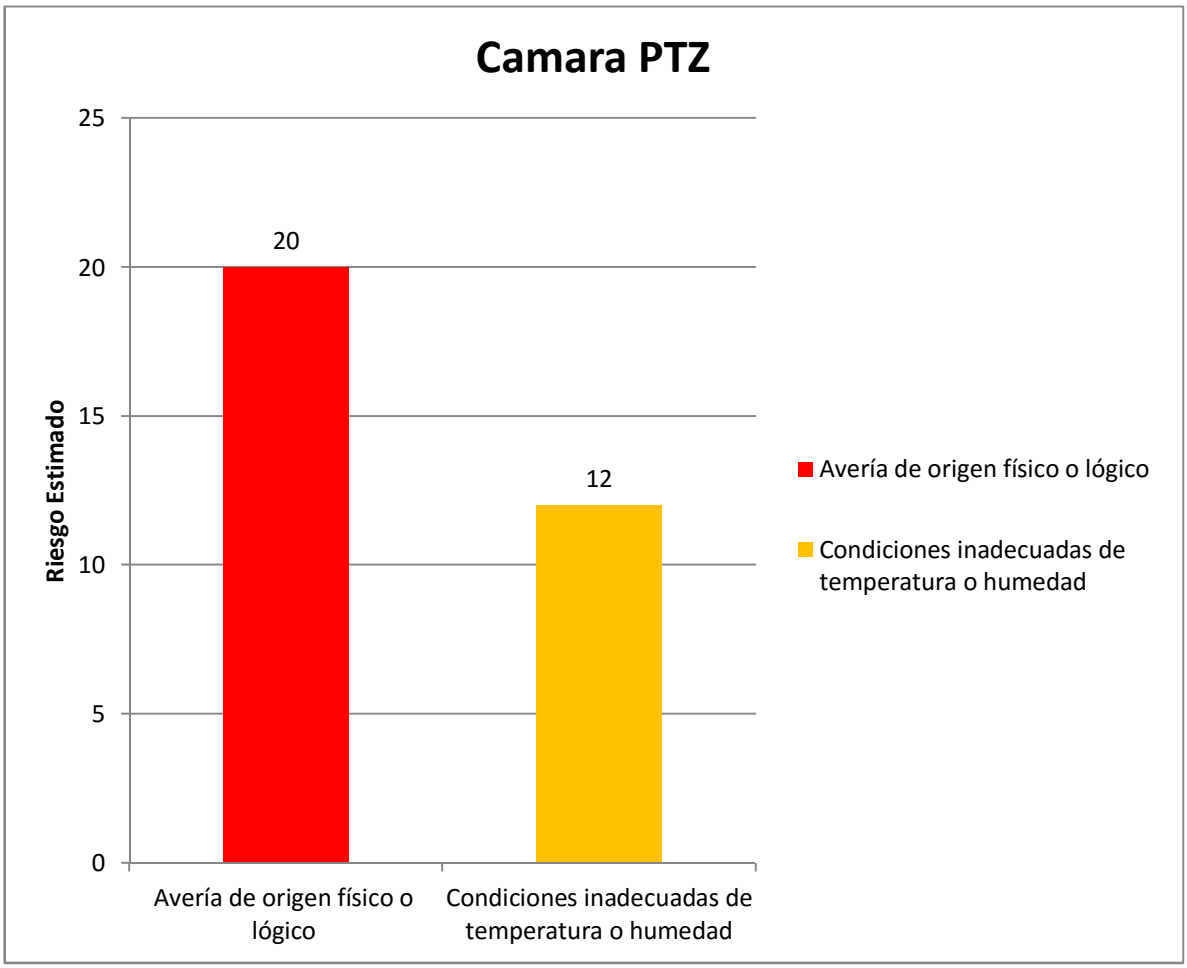


Fuente: Propiedad del autor

El sistema de vídeo vigilancia, permite entregar a las autoridades competentes, evidencias entorno a un caso, esto puede verse afectado cuando no se encuentra el vídeo, como se observa en el gráfico 2, se debe a una amenaza que afecta al sistema de almacenamiento.

3) Cámaras PTZ

Gráfico 3: Riesgo Cámaras PTZ



Fuente: Propiedad del autor

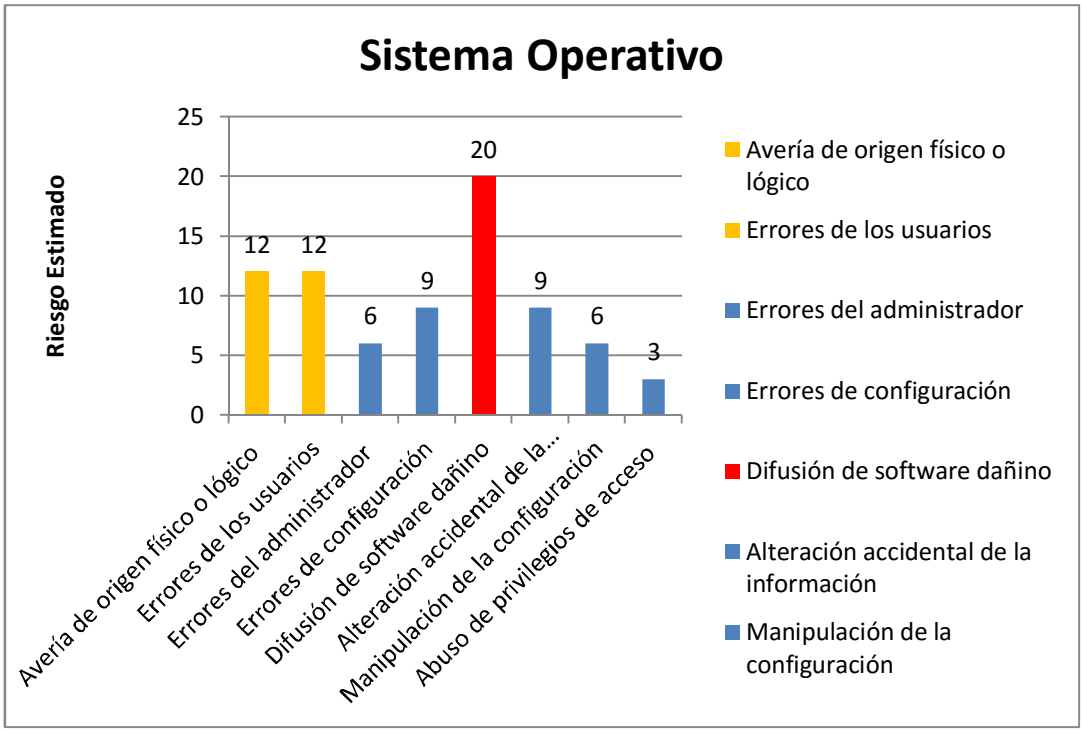
La cámara es un equipo electrónico, que está instalado en el exterior y funciona las 24 horas, cumple la función de capturar las imágenes y las envía al centro de monitoreo, para que puedan ser monitoreadas y grabadas.

En el gráfico 3, se muestra un riesgo alto, en cuanto a las averías que pueda presentar por el desgaste normal de la utilización del equipo y de sus funciones de movimiento.

El valor del activo es importante, no por el valor comercial, sino por la función del equipo; permite monitorear y capturar las imágenes que posteriormente puedan ser solicitadas.

4) Activo Sistema Operativo

Gráfico 4: Riesgo del Sistema Operativo



Fuente: Propiedad del autor

Este activo es importante por la plataforma, el software Control Center está diseñado para este sistema operativo, permitiendo visualizar y manipular las cámaras en forma remota.

El recurso de monitoreo, se puede ver afectado, si el sistema operativo no funciona correctamente o es afectado por virus o mala manipulación del operador.

Un alto riesgo se observa en la difusión de virus esto se debe a la utilización de celulares y memorias que se conectan al computador. (Ver gráfico 4),

6. DEFINICIÓN DE SALVAGUARDAS Y PLAN DE SEGURIDAD MEDIANTE MAGERIT PARA EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

6.1 SALVAGUARDAS

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Definido los riesgos a los que están expuestos los activos, se debe definir las salvaguardas para protegerlos, se listan las posibles salvaguardas seleccionadas de libro 2 Catalogo de elementos MAGERIT – versión 3.0.

Tabla 41: Listado de Salvaguardas

PROTECCIONES GENERALE U HORIZONTALES	H	H Protecciones Generales
	H.IA	H.IA Identificación y autenticación
	H.AC	H.AC Control de acceso lógico
	H.ST	H.ST Segregación de tareas
	H.IR	H.IR Gestión de incidencias
	H.tools	H.tools Herramientas de seguridad
	H.tools.AV	H.tools.AV Herramienta contra código dañino
	H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
	H.tools.CC	Herramienta de chequeo de configuración
	H.tools.VA	Herramienta de análisis de vulnerabilidades
	H.tools.TM	Herramienta de monitorización de tráfico
	H.tools.DLP	DLP: Herramienta de monitorización de contenidos
	H.tools.LA	Herramienta para análisis de logs
	H.tools.HP	Honey net / honey pot
	H.tools.SFV	Verificación de las funciones de seguridad
	H.VM	Gestión de vulnerabilidades
	H.AU	Registro y auditoría
Protección de los datos / información	D	Protección de la Información
	D.A	Copias de seguridad de los datos (backup)
	D.I	Aseguramiento de la integridad
	D.C	Cifrado de la información
	D.DS	Uso de firmas electrónicas
	D.TS	Uso de servicios de fechado electrónico (time stamping)

Protección de los equipos (hardware)	HW	Protección de los Equipos Informáticos
	HW.start	Puesta en producción
	HW.SC	Se aplican perfiles de seguridad
	HW.A	Aseguramiento de la disponibilidad
	HW.op	Operación
	HW.CM	Cambios (actualizaciones y mantenimiento)
	HW.end	terminación
	HW.PCD	Informática móvil
	HW.print	Reproducción de documentos
	HW.pabx	Protección de la centralita telefónica (PABX)
Protección de los elementos auxiliares	AUX	Elementos Auxiliares
	AUX.A	Aseguramiento de la disponibilidad
	AUX.start	Instalación
	AUX.power	Suministro eléctrico
	AUX.AC	Climatización
	AUX.wires	Protección del cableado
Seguridad física – Protección de las instalaciones	L	Protección de las Instalaciones
	L.design	Diseño
	L.depth	Defensa en profundidad
	L.AC	Control de los accesos físicos
	L.A	Aseguramiento de la disponibilidad
	L.end	Terminación
Salvaguardas relativas al personal	PS	Gestión del Personal
	PS.AT	Formación y concienciación
	PS.A	Aseguramiento de la disponibilidad
Salvaguardas de tipo organizativo	G	Organización
	G.RM	Gestión de riesgos
	G.plan	Planificación de la seguridad
	G.exam	Inspecciones de seguridad

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. Versión 3. Madrid, octubre de 2012. [2016-03-14]. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VubA-pzhDIU. NIPO: 630-12-171-8.

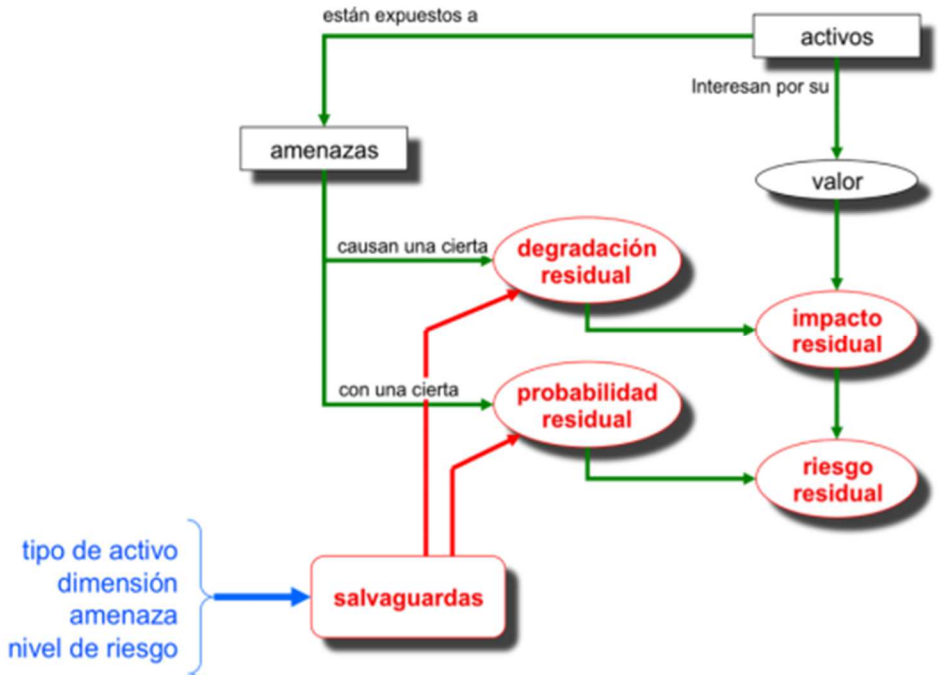
Impacto Residual

Es el valor que se puede aceptar después de aplicar una salva guarda a un activo.

Riesgo Residual

Los activos a pesar de aplicar salvaguardas para protegerlos de las amenazas y potenciales riesgos, siempre existe un riesgo mínimo. (Figura 30)

Figura 30: Elementos de análisis del riesgo residual



Fuente: Libro I - Método, MAGERIT – versión 3.0

Nomenclaturas para el análisis. Para realizar el cálculo de la tabla 45 tendremos en cuenta los valores de las tablas 42, 43 y 44

Tabla 42: Riesgo Residual

0	MB
1	MB
2	B
3	M
4	A
5	MA

Fuente: Propiedad del autor

Tabla 43: Valor Columnas

R	Riesgo Potencial
S	Salvaguarda
D	Degradación
V	Valor Activo
E	Eficiencia de la salvaguarda
DR	Degradación Residual
IR	Impacto Residual
P	Probabilidad
RR	Riesgo Residual

Fuente: Realizado por el autor

Tabla 44: Cuadro valores de eficiencia

0	L0	Inexistente
0,2	L1	Inicial / ad hoc
0,4	L2	Reproducible pero intuitivo
0,6	L3	Proceso definido
0,8	L4	Gestionado y Medible
1	L5	Optimizado

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Op. cit., p. 34

Formulas:

DR = D – (E*D)

IR = V * DR

RR = P * IR

Procedemos a realizar el cuadro de cálculo residual (ver tabla 45) teniendo en cuenta las formulas anteriores.

Tabla 45: Calculo de Riesgo Residual

Ámbito	Activo	Sigla	Amenaza	R	S	D	V	E	DR	IR	IR	P	RR
ESENCIALES: INFORMACIÓN	Videos Grabados	N1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I6	Corte del suministro eléctrico	16	AUX.power	0,8	5	0,8	0,2	1	MB	4	4
		I10	Degradación de los soportes de almacenamiento de la información	20	HW.CM	1	5	0,6	0,4	2	B	4	8
		E4	Errores de configuración	9	HW.print	0,5	5	0,2	0,4	2	B	3	6
Activos esenciales: Servicio	entrega de evidencias	N1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I10	Degradación de los soportes de almacenamiento de la información	20	HW.CM	1	5	0,6	0,4	2	B	4	8
		E24	Caída del sistema por agotamiento de recursos	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
Datos / información	Base de datos configuración de Cámaras	E8	Difusión de software dañino	20	H.tools.AV	0,8	5	0,8	0,2	1	MB	5	5
		A4	Manipulación de la configuración	6	D.A	0,5	5	0,4	0,3	2	B	2	4
	base de datos Inventario de equipos	E2	Errores del administrador	6	HW.print	0,5	5	0,2	0,4	2	B	2	4
		E7	Deficiencias en la organización	12	G.RM	0,5	5	0,4	0,3	2	B	4	8
		E15	Alteración accidental de la información	9	HW.print	0,6	5	0,2	0,5	2	B	3	6
	Carpeta información de proyecto	I10	Degradación de los soportes de almacenamiento de la información	9	HW.CM	0,8	4	0,6	0,3	1	MB	3	3
[SW] APLICACIONES (SOFTWARE)	Control Center	E1	Errores de los usuarios	16	PS.AT	0,8	5	0,4	0,5	2	B	4	8
		E2	Errores del administrador	8	HW.print	0,7	5	0,2	0,6	3	M	2	6
		E4	Errores de configuración	12	HW.print	0,7	5	0,2	0,6	3	M	3	9
	sistema operativo	I5	Avería de origen físico o lógico	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
		E1	Errores de los usuarios	12	PS.AT	0,5	5	0,4	0,3	2	B	4	8
		E2	Errores del administrador	6	HW.print	0,5	5	0,2	0,4	2	B	2	4
		E4	Errores de configuración	9	HW.print	0,5	5	0,2	0,4	2	B	3	6
		E8	Difusión de software dañino	20	H.tools.AV	0,8	5	0,8	0,2	1	MB	5	5

Ámbito	Activo	Sigla	Amenaza	R	S	D	V	E	DR	IR	IR	P	RR
		E15	Alteración accidental de la información	9	HW.print	0,5	5	0,2	0,4	2	B	3	6
		A4	Manipulación de la configuración	6	D.A	0,5	5	0,4	0,3	2	B	2	4
		A6	Abuso de privilegios de acceso	3	L.AC	0,5	5	0,8	0,1	1	MB	1	1
[HW] Equipamiento informático (hardware)	Workstation	N1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I10	Degradación de los soportes de almacenamiento de la información	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I5	Avería de origen físico o lógico	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
	Impresora	N1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	6	HW.CM	0,5	3	0,6	0,2	1	MB	3	3
		I9	Interrupción de otros servicios y suministros esenciales	6	AUX.A	0,8	3	0,2	0,6	2	B	3	6
	Monitor de 55”	N1	Fuego	4	L	1	4	0,8	0,2	1	MB	1	1
		I1	Fuego	4	L	1	4	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	6	HW.CM	0,5	4	0,6	0,2	1	MB	3	3
	Switch de 24 puertos	N1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
	Conversores de fibra	I5	Avería de origen físico o lógico	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
	Switchs de 8 puertos	I5	Avería de origen físico o lógico	6	HW.CM	0,8	3	0,6	0,3	1	MB	3	3
	Teclado Joystick	N1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	6	HW.CM	0,8	3	0,6	0,3	1	MB	3	3
	Cámara PTZ	I5	Avería de origen físico o lógico	20	HW.CM	1	5	0,6	0,4	2	B	4	8
		I7	Condiciones inadecuadas de temperatura o humedad	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
[Media] Soportes de información	Network Vídeo Recorders	N1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I1	Fuego	5	L	1	5	0,8	0,2	1	MB	1	1
		I5	Avería de origen físico o lógico	16	HW.CM	0,8	5	0,6	0,3	2	B	4	8

Ámbito	Activo	Sigla	Amenaza	R	S	D	V	E	DR	IR	IR	P	RR
		I6	Corte del suministro eléctrico	16	AUX.power	0,8	5	0,8	0,2	1	MB	4	4
		I7	Condiciones inadecuadas de temperatura o humedad	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I10	Degradación de los soportes de almacenamiento de la información	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
		E4	Errores de configuración	9	HW.print	0,5	5	0,2	0,4	2	B	3	6
	Manuales de equipos	N1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		E7	Deficiencias en la organización	8	G.RM	0,5	3	0,4	0,3	1	MB	4	4
[Media] Soportes de información	: UPS	I5	Avería de origen físico o lógico	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I6	Corte del suministro eléctrico	12	AUX.power	0,5	5	0,8	0,1	1	MB	4	4
		I7	Condiciones inadecuadas de temperatura o humedad	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
		I10	Degradación de los soportes de almacenamiento de la información	9	HW.CM	0,5	5	0,6	0,2	1	MB	3	3
	Fibra Óptica	I5	Avería de origen físico o lógico	12	HW.CM	0,8	5	0,6	0,3	2	B	3	6
	Escritorio	I5	Avería de origen físico o lógico	3	HW.CM	0,3	3	0,6	0,1	0	MB	3	0
	Rack de equipos	N1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		I1	Fuego	3	L	1	3	0,8	0,2	1	MB	1	1
		E7	Deficiencias en la organización	4	G.RM	0,3	3	0,4	0,2	1	MB	4	4
		A11	Acceso no autorizado	2	L.AC	0,5	3	0,8	0,1	0	MB	1	0
[L] Instalaciones	salón de monitoreo	N1	Fuego	4	L	1	4	0,8	0,2	1	MB	1	1
		I1	Fuego	4	L	1	4	0,8	0,2	1	MB	1	1
		A11	Acceso no autorizado	2	L.AC	0,5	4	0,8	0,1	0	MB	1	0
	canalizaciones eléctricas	E19	Fugas de información	4	L.AC	0,5	4	0,8	0,1	0	MB	2	0
		A11	Acceso no autorizado	2	L.AC	0,5	4	0,8	0,1	0	MB	1	0
		A19	Divulgación de información	3	Se acepta el riesgo	0,8	4	0,6	0,3	1	MB	1	1
		A26	Ataque destructivo	9	se Transfiere	0,8	4	0,6	0,3	1	MB	3	3
[P] Personal	Comandante	E7	Deficiencias en la organización	12	G.RM	0,5	5	0,4	0,3	2	B	4	8
	Responsable sala de monitoreo	A28	Indisponibilidad del personal	20	PS	0,8	5	0,4	0,5	2	B	5	10
	Operadores	A28	Indisponibilidad del personal	20	PS	0,8	5	0,4	0,5	2	B	5	10

6.2 PROGRAMA DE SEGURIDAD

Tabla 46: Programa de Seguridad

S	Detalle	Tipo	Medida de Salvaguarda	Observaciones	Eficiencia
AUX.A	Aseguramiento de la disponibilidad	[PR]	Suministro de tóner de tinta por parte de la Alcaldía	El comandante debe hacer un convenio con la alcaldía.	0,2
AUX.power	Suministro eléctrico	[PR]	Planta Eléctrica con su respectiva transferencia	Se debe monitorear el combustible para mejorar su operación, mantenimiento periódico de la planta eléctrica	0,8
		[PR]	UPS para el cambio de suministro de energía	Se debe monitorear su estado con el gestor NetAgent software instalado en el computador de monitoreo de cámaras	
D.A	Copias de seguridad de los datos (backup)	[RC]	Realizar copias de seguridad de la base de datos	se indica los pasos en instructivo para la copia de seguridad	0,4
		[RC]	se realiza disco de rescate para evitar problemas en el sistema operativo		

S	Detalle	Tipo	Medida de Salvaguarda	Observaciones	Eficiencia
		[RC]	Se realiza copia de seguridad de la información contenida en la Workstation		
G.RM	Gestión de riesgos	[AD]	Aplicar las políticas de seguridad de la información para el CCTV de Yacuanquer	Documento Políticas de Seguridad	0,4
		[AD]	Delegar las funciones y responsabilidades de los integrantes de los sistemas	Documento Políticas de Seguridad	
H.tools.AV	Herramienta contra código dañino	[PR]	Software antivirus kasspersky actualizado y con licencia	Actualizar la base de datos. Actualmente está licenciado por un año	0,8
HW	Protección de los Equipos Informáticos	[MN]	Alarmas de apertura en gabinetes. Corona antiescalatoria en poste		0,8
HW.CM	Cambios (actualizaciones y mantenimiento)	[MN]	Instalar un software para monitorear el estado de las ups	viene software con la UPS	0,6
		[AD]	La alcaldía contratara a personal externo para cumplir las funciones de mantenimiento y comprara los repuestos necesarios	en casos excepcionales se debe dejar un Stock de elementos para ser remplazados de forma inmediata que no tenga que hacer un plan de	

S	Detalle	Tipo	Medida de Salvaguarda	Observaciones	Eficiencia
				compras	
HW.print	Reproducción de documentos	[PR]	Se documentara todo cambio de elementos en un acta para dejar registro y posteriormente se actualiza la base de datos	Programa realizado en Access para llevar el inventario del sistema de CCTV	0,2
		[PR]	Documentos donde estén consignados los procesos del sistema para el operador de las cámaras	los documentos deben ser de carácter público entre los funcionarios para consultas	
		[PR]	Documento de manejo del control center las funciones básicas de operación	los documentos deben ser de carácter público entre los funcionarios para consultas	
L	Protección de las Instalaciones	[PR]	Extintor solkaflam	se debe monitorear los mantenimientos y fechas de vencimiento	0,8
		[PR]	Sistema de incendios	verificar su funcionamiento	
L.AC	Control de los accesos físicos	[PR]	Control de acceso biométrico	documento de operatividad básica ingreso de usuario y/o Eliminación	0,8
PS	Gestión del Personal	[AD]	Se debe hacer la definición de las funciones	Documento de Políticas de	0,4

S	Detalle	Tipo	Medida de Salvaguarda	Observaciones	Eficiencia
				Seguridad	
PS.AT	Formación y concienciación	[AW]	Documentos de procesos básico de la operatividad del centro de monitoreo	Se debe hacer una entrega del puesto, Documento de Políticas de Seguridad	0,4

Fuente: Propiedad del autor

CONCLUSIONES

La importancia de implantar unas políticas en el sistema CCTV, permite al comandante dentro de su cargo, definir las responsabilidades y procesos que se deben llevar en la sala de monitoreo.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), permitirá al comandante con la gestión de los riesgos y salvaguardas definidas en el proyecto, saber cuáles son las necesidades que debe gestionar ante la alcaldía.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), permite obtener una visión global del estado de los sistemas de información, sin caer en detalles técnicos, además de poder observa las medida de seguridad aplicadas y los resultados obtenidos para poder con todos estos elementos tomar mejores decisiones estratégicas.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), debe ser dado a conocer a los distintos niveles por el personal que conforma el equipo en la estación de policía del municipio de Yacuanquer, lo que le permitirá la mejora continua de todos sus procesos.

RECOMENDACIONES

Que por parte de la dirección deba poner en funcionamiento las políticas y salvaguardas definidas en el presente proyecto.

Gestionar a nivel central por el alto volumen de rotación de los patrulleros, para que se mantenga el personal capacitado en el manejo del sistema.

Capacitar al personal nuevo en el manejo del sistema y manipulación de la información que se procesa.

Gestionar mecanismos de almacenamiento masivo para salvaguardar la información.

Difundir constantemente las políticas de seguridad para el manejo del sistema a los usuarios nuevos.

Para que el sistema de vídeo vigilancia, obtenga los resultados esperados se debe hacer la definición de funciones de cada cargo.

BIBLIOGRAFÍA

ANGARITA, Alexis y TABARES, Cesar. Análisis De Riesgos Para El Proceso Administrativo: Departamento De Informática En La Empresa De Acueducto Y Alcantarillado De Pereira S.A E.S.P, Basados En La Norma ISO 27005. [En línea]. Pereira, Diciembre de 2012. Disponible en Internet http://repositorio.utp.edu.co/dspace/bitstream/11059/3914/1/T0058A581.pdf.

BAYONA, Leidy; MEJIA, Katherine y SARMIENTO, Beatriz. Creación De Un Manual De Políticas De Seguridad De La Información Para La Dependencia Secretaria De La Institución Educativa Nuestra Señora De Belén De Cúcuta. [En línea]. Ocaña, 10-04-2012. Disponible en Internet http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/328/1/25097.pdf.

CARLI, Vivien, Valoración del CCTV como una Herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes. [En línea]. Montreal, diciembre 2008. Disponible en Internet http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/Valoracion_del_CCTV_como_una_Herramienta_efectiva_de_manejo_y_seguridad_ESP.pdf.

DNP, Dirección de Justicia, Seguridad y Gobierno. Política Nacional de Seguridad y Convivencia Ciudadana. [En línea]. Bogotá D.C., Colombia, 2011. Disponible en Internet http://wsp.presidencia.gov.co/Seguridad-Ciudadana/consejeria/Documents/Pol%C3%ADtica%20Nacional%20de%20Seguridad%20y%20Convivencia%20Ciudadana-%20Espa%C3%B1ol.pdf. ISBN: 978-958-8340-68-5.

FERNANDEZ, Carlos y VELTHUIS, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. [En línea]. España, 2012. Disponible en Internet http://www.aenor.es/aenor/descargafichero.asp?tipo=pub&registro=9918&archivo=3. ISBN: 978-84-8143-764-5.

Formato e Implementación De Políticas De Seguridad Y Privacidad De La Información. [En línea]. Colombia. [Citado en 2016-02-25]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf.

Gestión De Riesgo Una Guía De Aproximación Para El Empresario. [En Línea]. [España]. [Citado en 2016-02-25]. Disponible en Internet https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf.

ICONTEC. Compendio seguridad de la información. Bogotá, Marzo de 2011. 96 p. Norma Técnica Colombiana. ISBN 978-958-8585-37-6.

ICONTEC. Normas técnicas Colombianas NTC-ISO-IEC 27001. Primera actualización. Bogotá, 2013-12-20. 26 p. I.C.S 35.040.

LAUDON, Kenneth y LAUDON, Jane. Sistemas de información gerencial. 12° ed. México, Pearson, 2012. ISBN 978-607-32-0949-6

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo I. [En línea]. Versión 3. Madrid. Octubre de 2012.Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO _630-12-171-8.pdf. NIPO: 630-12-171-8.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo II. [En línea]. Versión 3. Madrid. Octubre de 2012. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_cat%C3%A1logo%20de%20elementos_es_NIPO_630-12-171-8.pdf

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo III. [En línea]. Versión 3. Madrid. Octubre de 2012. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8/2012_Magerit_v3_libro3_gu%C3%ADa%20de%20t%C3%A9cnicas_es_NIPO_630-12-171-8.pdf

NORMAS TECNICAS COLOMBIANAS TNC 1496. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización. Bogotá. Editada por ICONTEC. 2008. 36 p.

NORMAS TECNICAS COLOMBIANAS TNC 4490. Referencias documentales para fuentes de información electrónica. Bogotá. Editada por ICONTEC. 1998. 23 p.

NORMAS TECNICAS COLOMBIANAS TNC 5613. Referencias bibliográficas forma y estructura. Bogotá. Editada por ICONTEC. 2008. 33 p.

ANEXOS

ENCUESTA DE SEGURIDAD APLICADA AL COMANDANTE

Objetivo: Evaluar la seguridad en el sistema de CCTV (Circuito Cerrado de Televisión) desde el punto de vista de los operadores.

1. ¿Existe una Política de seguridad aplicable al sistema de cámaras?

☐ Si ☐ No

2. ¿Existe un manual de funciones para los operadores de las cámaras?

☐ Si ☐ No

3. ¿Tiene Registrado su huella en el control de acceso?

☐ Si ☐ No

4. ¿Existe un manual donde se explique el manejo y operación de las cámaras?

☐ Si ☐ No

5. ¿Qué área del sistema de cámaras tiene acceso?

☐ Cuarto de Monitoreo ☐ Cuarto de Equipos ☐ Las dos anteriores

6. ¿El programa de monitoreo (Control Center) le permite visualizar videos grabados?

☐ Si ☐ No

7. ¿El programa de monitoreo (Control Center) le permite Exportar videos grabados?

☐ Si ☐ No

8. ¿Ha recibido capacitación en el manejo del programa de monitoreo (Control Center)?

☐ Si ☐ No

9. ¿Tiene conocimiento como operar las cámaras en el Control Center?

☐ Si ☐ No

10. ¿Prohíbe la instalación de software que no tiene que ver con el monitoreo en el computador?

☐ Si ☐ No

11. ¿prohíbe Insertar unidades extraíbles como USB, discos externos, celulares al computador de monitoreo?

	Si		No

12. ¿Se ha establecido un programa de concientización para mantener seguro la información del sistema de cámaras?

	Si		No

13. ¿Califique de 1 a 5 el nivel de seguridad del cuarto de monitoreo?

	1		2		3		4		5

14. ¿Cree que es importante que exista un documento donde se especifique las funciones del operador de cámaras?

	Si		No

15. ¿Cree que es importante que se implemente una política de seguridad al sistema de CCTV?

	Si		No

16. ¿Cree que es importante que se restrinja la visualización y exportación de vídeo para los operadores?

	Si		No

17. ¿Cómo comandante usted delega a una persona como responsable del sistema de CCTV?

	Si		No

18. ¿Cuándo hay traslado del personal que opera las cámaras existe un procedimiento de capacitación para el nuevo personal?

	Si		No

19. ¿Cree importante que exista una documentación que permita capacitar al personal nuevo que cumplirá las funciones de operador?

	Si		No

ENCUESTA DE SEGURIDAD APLICADA OPERADORES

Objetivo: Evaluar la seguridad en el sistema de CCTV (Circuito Cerrado de Televisión) desde el punto de vista de los operadores.

1. ¿Existe una Política de seguridad aplicable al sistema de cámaras?

☐ Si ☐ No

2. ¿Existe un manual de funciones para los operadores de las cámaras?

☐ Si ☐ No

3. ¿Tiene Registrado su huella en el control de acceso?

☐ Si ☐ No

4. ¿Existe un manual donde se explique el manejo y operación de las cámaras?

☐ Si ☐ No

5. ¿Qué área del sistema de cámaras tiene acceso?

☐ Cuarto de Monitoreo ☐ Cuarto de Equipos ☐ Las dos anteriores

6. ¿Usted como operador del sistema de cámaras realiza revisiones al nivel de combustible de la planta eléctrica?

☐ Si ☐ No

7. ¿El programa de monitoreo (Control Center) le permite visualizar videos grabados?

☐ Si ☐ No

8. ¿El programa de monitoreo (Control Center) le permite Exportar videos grabados?

☐ Si ☐ No

9. ¿Ha recibido capacitación en el manejo del programa de monitoreo (Control Center)?

☐ Si ☐ No

10. ¿Tiene conocimiento como operar las cámaras en el Control Center?

☐ Si ☐ No

11. ¿El computador tiene antivirus actualizado?

☐ Si ☐ No

12. ¿Inserta unidades extraíbles como USB, discos externos, celulares al computador de monitoreo?

☐ Si ☐ No

13. ¿Tiene conocimientos básicos en el manejo del computador?

☐ Si ☐ No

14. ¿Existe restricciones para instalar software en el computador?

☐ Si ☐ No

15. ¿El usuario para el ingreso al sistema operativo Windows del computador de monitoreo es?

☐ Usuario restringido ☐ Administrador ☐ No sabe

16. ¿Califique de 1 a 5 el nivel de seguridad del cuarto de monitoreo?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

17. ¿Cree que es importante que exista un documento donde se especifique las funciones del operador de cámaras?

☐ Si ☐ No

18. ¿Cuándo se cambia de turno de operador de cámaras, se hace el proceso de entrega del turno?

☐ Si ☐ No

FORMATO RECOLECCION DE DATOS

Ubicación	
Fecha	

Cuarto de equipos

Biométrico	Instalado No( ) Si( )____Funcionando Si( ) No( )			
Puerta de acceso	Existe No( ) Si( ) ____Abierta( )___Cerrada( )			
Tablero Regulado	Cantidad ( )	Circuitos ( )		
Tablero Normal	Cantidad ( )	Circuitos ( )		
Rack Equipos	Cantidad ( )	Sistema de tierra Si( ) No( )	Llave Si( ) No( )	
Switch	Cantidad ( )	Puertos ( ) Transivers ( )		
	Seguridad	Password Si( ) No( )	Llave Si( ) No( )	
NVR	Cantidad ( )	Capacidad total ( )TB	Llave Si( ) No( )	
ODF	Cantidad ( )	Patch Panel Si( ) No( ) Can Puertos ( )		
UPS	Cantidad ( )	Capacidad ( )kva	Gestor UPS Si( ) No( )	
Puntos de Red	Cantidad ( )	Voz ( ) Datos ( )		
Control de Acceso	Baterías ( )	Llave Si( ) No( )	Biométricos ( )	
Tablero de incendios	Baterías ( )	Llave Si( ) No( )	Sensores ( ) Funcionado Si( ) No( )	
Observaciones:				

Cuarto de Monitoreo

Biométrico	Instalado No( ) Si( )____Funcionando Si( ) No( )	
Puerta de acceso	Existe No( ) Si( ) ____Abierta( )___Cerrada( )	
Puntos de Red	Cantidad ( )	Voz ( ) Datos ( )
Computador	Cantidad( ) Monitor: 19"( ) funcionando( ) 55"( ) Funcionando( ) Mouse: Funcionando Si( ) No( ) Teclado: Funcionando Si( ) No( ) **Software**: (marcar se está licenciado) Ofimático No( ) Si( ) Cual: _____( )Lic **Antivirus** No( ) Si( ) Cual_____( )Lic Actualizado Si( ) No( ) Juegos No( ) Si( ) Programas de descargas No( ) Si( ) Otros programas No( ) Si( ) **Sistema Operativo Windows:** Usuario Operador Contraseña Si( ) No( ) Usuario Administrador Contraseña Si( ) No( )	

	Puestos USB Habilitados Si( ) No( ) Discos de Rescate No( ) Si( ) DVD del sistema operativo No( ) Si( )
Impresora	Instalada No( ) Si( ) Funcionando Si( ) No( )
Sensor de Humo	Instalado No( ) Si( )_ Cantidad ( ) Funcionando Si( ) No( )
Observaciones:	

Panta Eléctrica

Capacidad ( )KVA Funcionando Si( ) No( ) Combustible No( ) Si( )__Porc%( )
Seguridad: Cerramiento Si( ) No( ) Asegurada con Llave Si( ) No( )
Cableado Estado Bueno( ) Regular( )

Software Control Center

Existe un Administrador No( ) Si( )
Usuario Operador: Visualiza vídeo Grabado Si( ) No( ) Exporta Vídeo Grabado Si( ) No( )
Copia de seguridad de la base de datos No( ) Si( )__almacenamiento DVD( ) HD( )
DVD del programa control center No( ) Si( ) _Almacenamiento DVD( ) HD( )

Almacenamiento NVR

Funcionamiento: No( ) Si( )	
Capacidad ( )TB	Disco_0 Funciona SI( ) No( )
	Disco_1 Funciona SI( ) No( )
	Disco_2 Funciona SI( ) No( )
	Disco_3 Funciona SI( ) No( )
Seguridad: Filtro IP Activado( ) Desactivado( )	
Contraseña: Activado( ) Desactivado( )	
Filtro de IP: Activado( ) Desactivado( )	

Diligenciado Por:
Firma
Nombre:

FORMATO RECOLECCIÓN DE DATOS PUNTO DE CÁMARA

Ubicación:		**Fecha**:	
Cámara Funcionando Si( ) No( )			
Tapa de 60x60 Estado Bueno( ) Regular( ) Sin tapa( )			
Tapa de 30x30 Estado Bueno( ) Regular( ) Sin tapa( )			
Conexión Eléctrica Estado Buena( ) Regular( ) Desconectada( )			
Gabinete Estado Buena( ) Regular( )			
Seguridad:	Llave Si( ) No( )		
	Corona antiescalatoria Si( ) No( )		
Equipos:	UPS: No( ) Si( )	Gestor No( ) Si( )	Funciona Si( ) No( )
	Switch No( ) Si( )	Funciona Si( ) No( )	
	Conversor FO No( ) Si( )	Funciona Si( ) No( )	
Cámara de Seguridad PTZ			
Funcionamiento: Pan Si( ) No( ) / Tilt Si( ) No( ) / Zoom Si( ) No( )			
Seguridad: Filtro IP Activado( ) Desactivado( )			
Contraseña: Activado( ) Desactivado( )			
Filtro de IP: Activado( ) Desactivado( )			

Diligenciado Por:
Firma
Nombre:

FORMATO CONTROL PLANTA ELECTRICA
Versión 01

Fecha de Inicio: D M A

Fecha			Hora		Nombre	% comb	Tanqueo	C. tan	Firma
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					
D	M	A	H	M					

Aprobado por:

Nombre Comandante

ACTA DE TRABAJO	
Fecha de Inicio(d/m/a):	**Hora:**
Fecha de Finalización(d/m/a):	**Hora:**
MUNICIPIO: YACUANQUER	**TELÉFONO:**
NOVEDAD REPORTADA:	
TIPO DE MANTENIMIENTO: PREVENTIVO ( ) CORRECTIVO ( )	
REPORTADO O SOLICITADO POR:	
ACTIVIDAD REALIZADA:	
OBSERVACIONES:	
USUARIO DEL SISTEMA	**Realizado Por:**
NOMBRE: **CARGO:** **CC:**	**NOMBRE:** **CARGO:** **CC:**
FIRMA	**FIRMA:**

RESUMEN ANALITICO EDUCATIVO

RAE

Título del texto	**APLICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV) SISTEMA INTEGRADO DE EMERGENCIAS Y SEGURIDAD (SIES) DEL MUNICIPIO DE YACUANQUER**
Nombres y Apellidos del Autor	**JOSE HERNAN CORTES ROSERO**
Año de la publicación	**2016**

Resumen del texto:

El desarrollo de las tecnologías ha permitido en algunos casos la aparición de nuevos productos, en otros la evolución, como es el caso de las cámaras de vídeo vigilancia, que pasaron de enviar simples imágenes sin procesar por un cable coaxial, a ser enviadas y procesadas por otros mecanismos más eficientes en las redes de datos.

Las cámaras se han incorporado o son parte de las redes computacionales, permitiendo ejecutar diferentes procesos. La información capturada puede ser guarda en sistemas de almacenamiento, además de ser monitoreadas a distancia, estas funcionalidades son las que permiten utilizarlas en diferentes aplicaciones, como son el control de tráfico, seguridad y es esta última, donde se enfoca la presente monografía, para orientar a los usuarios que tienen a cargo un sistema de vigilancia urbana, para que sean conscientes que la información manejada es importante y se debe proteger de una forma eficiente.

La aplicación de estas cámaras en sistemas de vídeo vigilancia puede involucrar muchos dispositivos tecnológicos en redes como: switch, computadores, servidores, sistemas de

almacenamiento, medios de transmisión, sistemas eléctricos, controles de acceso, sistemas de refrigeración. Es en este punto, donde un sistema de gestión de seguridad de la información entra a jugar un papel importante; la mala manipulación de estos recursos puede dejar completamente fuera de servicio los sistemas de vídeo vigilancia, colocando en riesgo la seguridad de la comunidad y la Información.	
Palabras Claves	Seguridad, CCTV, MAGERIT, ISO 27001
Problema que aborda el texto: La aplicación de un sistema de gestión de seguridad en un sistema de circuito cerrado de televisión bajo la norma ISO 27001.	
Objetivos del texto: Implementar un sistema de gestión de seguridad de la información en el circuito cerrado de televisión (CCTV) subsistemas SIES del municipio de Yacuanquer. Bajo la norma ISO 27001:2013	
Hipótesis planteada por el autor:	
Tesis principal del autor:	
Argumentos expuestos por el autor:	

Conclusiones del texto:

La importancia de implantar unas políticas en el sistema CCTV, permite al comandante dentro de su cargo, definir las responsabilidades y procesos que se deben llevar en la sala de monitoreo.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), permitirá al comandante con la gestión de los riesgos y salvaguardas definidas en el proyecto, saber cuáles son las necesidades que debe gestionar ante la alcaldía.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), permite obtener una visión global del estado de los sistemas de información, sin caer en detalles técnicos, además de poder observa las medida de seguridad aplicadas y los resultados obtenidos para poder con todos estos elementos tomar mejores decisiones estratégicas.

El sistema de gestión de seguridad de la información (SGSI) para el circuito cerrado de televisión (CCTV), debe ser dado a conocer a los distintos niveles por el personal que conforma el equipo en la estación de policía del municipio de Yacuanquer, lo que le permitirá la mejora continua de todos sus procesos.

Bibliografía citada por el autor:

ANGARITA, Alexis y TABARES, Cesar. Análisis De Riesgos Para El Proceso Administrativo: Departamento De Informática En La Empresa De Acueducto Y Alcantarillado De Pereira S.A E.S.P, Basados En La Norma ISO 27005. [En línea]. Pereira, Diciembre de 2012. Disponible en Internet http://repositorio.utp.edu.co/ dspace/bitstream/11059/3914/1/T0058A581.pdf.

BAYONA, Leidy; MEJIA, Katherine y SARMIENTO, Beatriz. Creación De Un Manual De Políticas De Seguridad De La Información Para La Dependencia Secretaria De La Institución Educativa Nuestra Señora De Belén De Cúcuta. [En línea]. Ocaña, 10-04-2012. Disponible en Internet http://repositorio.ufpso.edu.co: 8080/dspaceufpso/bitstream/123456789/328/1/25097.pdf.

CARLI, Vivien, Valoración del CCTV como una Herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes. [En línea]. Montreal, diciembre 2008. Disponible en Internet http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/Valoracion_del_CCTV_como_una_Herramienta_efectiva_de_manejo_y_seguridad_ESP.pdf.

DNP, Dirección de Justicia, Seguridad y Gobierno. Política Nacional de Seguridad y Convivencia Ciudadana. [En línea]. Bogotá D.C., Colombia, 2011. Disponible en Internet

http://wsp.presidencia.gov.co/Seguridad-Ciudadana/consejeria/Documents/Pol%C3%ADtica%20Nacional%20de%20Seguridad%20y%20Convivencia%20Ciudadana-%20Espa%C3%B1ol.pdf. ISBN: 978-958-8340-68-5.

FERNANDEZ, Carlos y VELTHUIS, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. [En línea]. España, 2012. Disponible en Internet http://www.aenor.es/aenor/descargafichero.asp?tipo=pub&registro=9918&archivo=3. ISBN: 978-84-8143-764-5.

Formato e Implementación De Políticas De Seguridad Y Privacidad De La Información. [En línea]. Colombia. [Citado en 2016-02-25]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf.

Gestión De Riesgo Una Guía De Aproximación Para El Empresario. [En Línea]. [España]. [Citado en 2016-02-25]. Disponible en Internet https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf.

ICONTEC. Compendio seguridad de la información. Bogotá, Marzo de 2011. 96 p. Norma Técnica Colombiana. ISBN 978-958-8585-37-6.

ICONTEC. Normas técnicas Colombianas NTC-ISO-IEC 27001. Primera actualización. Bogotá, 2013-12-20. 26 p. I.C.S 35.040.

LAUDON, Kenneth y LAUDON, Jane. Sistemas de información gerencial. 12° ed. México, Pearson, 2012. ISBN 978-607-32-0949-6

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo I. [En línea]. Versión 3. Madrid. Octubre de 2012.Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO _630-12-171-8.pdf. NIPO: 630-12-171-8.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo II. [En línea]. Versión 3. Madrid. Octubre de 2012. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_cat%C3%A1logo%20de%20elementos_es_NIPO_630-12-171-8.pdf

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Tomo III. [En línea]. Versión 3. Madrid. Octubre de 2012. Disponible en Internet http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8/2012_Magerit_v3_libro3

<table>
<tr><td colspan="2">_gu%C3%ADa%20de%20t%C3%A9cnicas_es_NIPO_630-12-171-8.pdf

NORMAS TECNICAS COLOMBIANAS TNC 1496. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización. Bogotá. Editada por ICONTEC. 2008. 36 p.

NORMAS TECNICAS COLOMBIANAS TNC 4490. Referencias documentales para fuentes de información electrónica. Bogotá. Editada por ICONTEC. 1998. 23 p.

NORMAS TECNICAS COLOMBIANAS TNC 5613. Referencias bibliográficas forma y estructura. Bogotá. Editada por ICONTEC. 2008. 33 p.</td></tr>
<tr><td>Nombre y apellidos de quien elaboró este RAE</td><td>JOSE HERNAN CORTES ROSERO</td></tr>
<tr><td>Fecha en que se elaboró este RAE</td><td>16 de abril de 2016</td></tr>
<tr><td colspan="2">Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:</td></tr>
<tr><td colspan="2">Comentarios finales:</td></tr>
</table>