ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y TRANSFERENCIA TECNOLÓGICA

UNIDAD DE POSGRADOS

MAESTRÍA EN GERENCIA DE LA SEGURIDAD Y RIESGOS

INFLUENCIA DE LA TECNOLOGÍA EN LA SEGURIDAD FÍSICA DEL FUERTE MILITAR. PROPUESTA ALTERNATIVA

AUTORES: ESPINOZA JARAMILLO CHRISTIAN GERMÁNICO
SALTOS VERDEZOTO VÍCTOR HUGO

DIRECTOR: CRNL. (S.P) VÁSQUEZ, RENÉ

SANGOLQUÍ

2016

ARTAMENTO DE SEGURIDAD Y DEFENSA

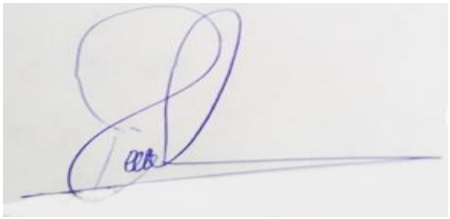
MAESTRIA EN GERENCIA DE LA SEGURIDAD Y RIESGOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "INFLUENCIA DE LA TECNOLOGÍA EN LA SEGURIDAD FÍSICA DEL FUERTE MILITAR. PROPUESTA ALTERNATIVA" realizado por los señores ESPINOZA JARAMILLO CHRISTIAN GERMÁNICO y SALTOS VERDEZOTO VÍCTOR HUGO, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar los señores ESPINOZA JARAMILLO CHRISTIAN GERMÁNICO y SALTOS VERDEZOTO VÍCTOR HUGO para que lo sustenten públicamente.

Sangolquí, diciembre de 2015

Atentamente



RENÉ VÁSQUEZ

Crnl. (S.P.)

DIRECTOR DE TESIS

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

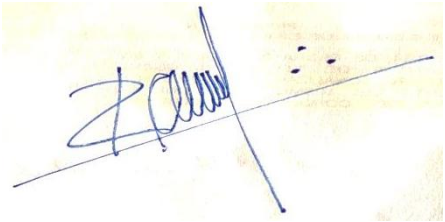
MAESTRIA EN GERENCIA DE LA SEGURIDAD Y RIESGOS

AUTORIZACIÓN

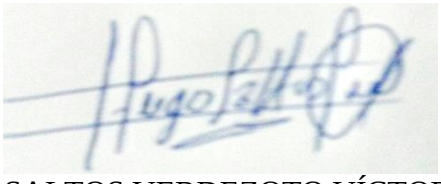
Nosotros, ESPINOZA JARAMILLO CHRISTIAN GERMÁNICO Y SALTOS VERDEZOTO VÍCTOR HUGO, Autorizamos a la Universidad de la Fuerzas Armadas ESPE, publicar en la biblioteca virtual de la institución, el presente trabajo de titulación: "INFLUENCIA DE LA TECNOLOGÍA EN LA SEGURIDAD FÍSICA DEL FUERTE MILITAR. PROPUESTA ALTERNATIVA", cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, diciembre de 2015

AUTORES:



ESPINOZA JARAMILLO CHRISTIAN GERMÁNICO



SALTOS VERDEZOTO VÍCTOR HUGO

AGRADECIMIENTO

Mi agradecimiento eterno a Dios, que me ha permitido concluir este trabajo a la ESPE y a sus docentes pues con los conocimientos adquiridos puedo ejercer la profesión, agradezco también al CRNL. (S.P) RENÉ VÁSQUEZ por el apoyo en la ejecución de este Proyecto.

VÍCTOR HUGO SALTOS VERDEZOTO

DEDICATORIA

Quiero dedicar el esfuerzo y enorme gusto en la elaboración de este proyecto a mis padres, mis Hermanos, seres magníficos que Dios puso en mi camino. Así También dedico con todo el amor a mi esposa Nancy y mis adorados hijos, fuente inagotable de motivación para todas las actividades de mi vida.

VÍCTOR HUGO SALTOS VERDEZOTO

AGRADECIMIENTO

Presento el testimonio de mi gratitud imperecedera al Gran Arquitecto del Universo por bendecirme a cada momento de mi vida.

Agradezco también a los docentes y a esta prestigiosa institución la ESPE, ya que durante toda mi carrera ha aportado significativamente a mi formación profesional, de manera especial a mi CRNL (S.P) René Vásquez, quien en calidad de Director, nos guió hasta la culminación de este trabajo.

.

CHRISTIAN GERMÁNICO ESPINOZA JARAMILLO

DEDICATORIA

Dedico el presente trabajo al Glorioso Ejército Vencedor, que ha depositado su entera confianza en mí, en cada reto que me ha impuesto en el arduo trajinar de la carrera de las armas, sin dudar de mis capacidades.

A Karla Christina y Kristelle Deianira, fuente eterna de inspiración y motivación.

CHRISTIAN GERMÁNICO ESPINOZA JARAMILLO

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Es necesario conocer que en la actualidad, son muy necesarios los sistemas de seguridad electrónica, para cubrir las áreas de monitoreo, supervisión y control. La seguridad que se pretende desarrollar a través de esta propuesta, está diseñada en base al estudio oportuno del FUERTE MILITAR, para disminuir el riesgo de pérdida de elementos importantes de esta institución, de esta manera se pueda implementar las medidas preventivas orientadas a la aplicación de un sistema de video vigilancia y control de acceso. Una de las razones fundamentales es disminuir los índices de pérdidas de bienes y eventos llevados a cabo tanto por personal interno como externo a la institución, garantizando la seguridad física de esta prestigiosa institución, de igual forma detectar el acceso a las áreas críticas e identificar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones correctivas para dar un ambiente de confianza y tranquilidad para quienes laboran en la institución. Después de realizado todo lo propuesto se llego a determinar que el empleo de la tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuirá a mejorar los niveles de seguridad física en el Fuerte Militar, teniendo en cuenta presupuestos y verificando su aceptabilidad.

PALABRAS CLAVES:

SISTEMAS DE VIDEO VIGILANCIA

SEGURIDAD FÍSICA

CONTROL DE RIESGOS

SISTEMAS TECNOLÓGICOS

ANÁLISIS FODA.

ABSTRACT

You need to know that currently , electronic security systems are necessary to cover the areas of monitoring , supervision and control.

Security to be developed through this proposal , is designed based on the timely study STRONG MILITARY , to decrease the risk of losing important elements of this institution , so it can implement preventive measures aimed at implementing a system of video surveillance and access control.

One of the main reasons is to decrease the rates of loss of assets and events held by both internal staff and external to the institution , guaranteeing the security of this prestigious institution , similarly detect access to critical areas and identify possible security breaches or violations and perform corrective actions to provide an environment of trust and tranquility for those who work in the institution.

After done everything proposed was reached to determine that the use of technology applied to video surveillance systems and access control, help to improve levels of physical security at the Military Fort , taking into account budgets and verifying their acceptability .

KEYWORDS: **VIDEO SURVEILLANCE**

PHYSICAL SECURITY

RISK MANAGEMENT

IT SYSTEMS

SWOT ANALYSIS SYSTEMS.

INFLUENCIA DE LA TECNOLOGÍA EN LA SEGURIDAD FÍSICA DEL FUERTE MILITAR. PROPUESTA ALTERNATIVA

En el siglo XXI, la seguridad está orientada a la prevención y por consiguiente los esfuerzos físicos y presupuestarios están encaminados a minimizar los riesgos y precautelar de esta manera los recursos humanos y materiales de las organizaciones.

Los sistemas de Seguridad física en el área tecnológica está relacionado con los sistemas electrónicos, diseñados para cubrir diferentes necesidades de monitoreo, control y/o supervisión, pero con capacidad de ser interconectados e integrados en un único macro sistema multifuncional. La utilización de cada uno de ellos depende de las necesidades particulares de cada instalación o edificación, así como de los procedimientos operativos contemplados.

Los abrumadores y, a veces, desconcertantes avances tecnológicos que nos obligan a ser muy cuidadosos en las inversiones proyectadas ante el inminente riesgo de prematura caducidad de los equipos “nuevos”, no escapan al sector seguridad; por lo que es particularmente necesario un serio análisis del factor costo-valor a la hora de decidir en qué clase de tecnología invertir.

La seguridad mediante la aplicación de un sistema de video vigilancia y control de acceso constituye la garantía, protección y prevención de situaciones adversas;

conllevando a garantizar la integridad física de instalaciones, bienes y personas que laboran para el Fuerte Militar; así como la protección del público en general que a ella acude.

CAPITULO I

1. GENERALIDADES

1.1 JUSTIFICACIÓN E IMPORTANCIA

La importancia de realizar esta investigación está relacionada con mejorar la seguridad física, a través de medios tecnológicos, identificando los riesgos más frecuentes de las áreas críticas para que de esta manera se pueda implementar las medidas preventivas orientadas a la aplicación de un sistema de video vigilancia y control de acceso.

En tal virtud es importante que el Fuerte Militar, disponga de un modelo de investigación, que permita determinar cómo el empleo de la tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuirá a mejorar los niveles de seguridad física.

Además el presente trabajo es importante para el Fuerte Militar porque permitirá:

- Disminuir, disuadir, impedir y detectar los índices de pérdidas de bienes y eventos llevados a cabo tanto por personal interno como externo a la institución.

- Actualizar y mejorar las medidas de seguridad establecidas en los planes, considerando los medios tecnológicos respectivos cuyas evidencias servirán como elementos probatorios de los actos ilícitos para determinar responsabilidades.
- Detectar el acceso a las áreas críticas e identificar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones correctivas con la mayor brevedad posible.
- Dar un ambiente de confianza y tranquilidad para quienes laboran en la institución.

1.2 PLANTEAMIENTO DEL PROBLEMA

Mientras a nivel mundial y nacional se ha evidenciado una creciente implementación de desarrollos tecnológicos aplicables a la seguridad, en el Fuerte Militar Patria, se mantienen sistemas de barreras humanas y artificiales carentes de tecnología que permitan la aplicación del principio de empleo de barreras mixtas (humana, tecnológicas, animales y artificiales) para proporcionar niveles de seguridad óptimos que incluyan una verdadera capacidad de respuesta.

Cuando se han presentado eventos de intrusión, perdidas y actos delictivos, ha sido casi imposible esclarecer los mismos así como determinar responsabilidades y grados de participación por la falta de elementos probatorios como videos o fotografías. La suma de estos elementos conlleva a

que los niveles actuales de seguridad física del Fuerte Militar sean bajos, generando niveles de riesgo intolerables para los activos y la áreas de misión crítica, debiendo tomarse acciones urgentes para el tratamiento de dichos riesgos, lo que frente a la realidad de otras entidades que poseen medios tecnológicos de seguridad, lleva a plantearse la siguiente interrogante:

¿Cómo la tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuiría a mejorar los niveles de seguridad física en el Fuerte Militar?

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo la tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuiría a mejorar los niveles de seguridad física en el Fuerte Militar?

Con la formulación del problema central se plantean las siguientes interrogantes que a continuación se enuncian y que serán contestadas con la propuesta planteada.

- ¿Qué medios tecnológicos existen en el sistema de seguridad física en el Fuerte Militar?
- ¿Existen políticas a nivel directivo y compromiso de este con la gestión de seguridad en el Fuerte Militar?

- ¿Qué metodologías, se emplea para la gestión de riesgos en el Fuerte Militar?
- ¿Qué grado de acceso, tiene el personal a las áreas críticas en el Fuerte Militar?
- ¿Es factible la implementación de sistemas tecnológicos de video vigilancia y control de accesos como alternativa de solución a los problemas de inseguridad del Fuerte Militar?

1.4 HIPÓTESIS

¿El empleo de tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuirá a mejorar los niveles de seguridad física en el Fuerte Militar?

1.5 OBJETIVO GENERAL

Determinar cómo el empleo de la tecnología aplicada a sistemas de video vigilancia y control de accesos, contribuirá a mejorar los niveles de seguridad física en el Fuerte Militar.

1.6 OBJETIVOS ESPECÍFICOS

- Diagnosticar los instrumentos de seguridad física existentes en el Fuerte Militar, con el fin de establecer los niveles de seguridad, riesgos y sus vulnerabilidades.

- Identificar el grado de acceso del personal a las áreas críticas en el Fuerte Militar, para establecer áreas que requieren mayor seguridad.

- Analizar las políticas establecidas a nivel directivo en materia de seguridad en el Fuerte Militar a fin de recomendar nuevas políticas considerando la aplicación de medios tecnológicos.

- Diseñar una propuesta de gestión de riesgos y su tratamiento mediante la aplicación de instrumentos tecnológicos que contribuyan a la seguridad física del Fuerte Militar.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1 ESTADO DEL ARTE

A nivel mundial, la dinámica de las técnicas, tácticas y procedimientos que usan las amenazas y factores de riesgo, han ocasionado un cambio permanente de medios y métodos de combate empleados por grupos y elementos desafectos a las instituciones del estado para emprender en actos que afectan a la seguridad e integridad de personas, bienes e instalaciones.

Basta un rápido vistazo para conocer como instalaciones de organismos de defensa han sido objeto de atentados violentos con graves consecuencias para las instalaciones, bienes y personas, ataques físicos y virtuales para sustraer información, armas y equipos; para atentar contra la integridad de personas o simplemente para dar demostraciones de fuerza ejecutando represalias contra los organismos de seguridad de un estado.

En el entorno inmediato, el vecino país de Colombia es uno de los claros ejemplos de la arremetida de las amenazas contra las instalaciones gubernamentales y militares, sufriendo graves pérdidas humanas y materiales que se pudieron haber evitado con inversión en seguridad, desarrollo e

implementación de sistemas con aplicaciones tecnológicas y que vinculen un compendio de elementos para minimizar las amenazas y sus posibilidades.

En nuestro país, si bien no se han suscitado aún eventos de ataques manifiestos, se evidencian sin embargo pérdidas de bienes, de información, de armamento, entre otras, que en suma diezman también la imagen institucional por la profundidad y extensión del daño lo cual resta el prestigio que constituye un valor imponderable y difícil de restaurar.

En las unidades militares de las Fuerzas Armadas se han presentado eventos de incendios, explosiones y demás accidentes que han conllevado daño a la comunidad local, con muertes de civiles y daños a la propiedad de éstos, eventos que se hubieran evitado o minimizado sus efectos con tan solo disponer de sistemas tecnológicos de alerta temprana, de control de accesos, de alarmas etc. que permitan la activación oportuna de los planes de contingencia y respuesta ante los sucesos.

Es de resaltar el último evento de pérdida ocurrido a inicios del año 2013 en el Destacamento Militar de “SANSAHUARI”, donde por la ausencia de consciencia y cultura de seguridad, no se realizaron inversiones en esta área y se dejó de lado el tratamiento de riesgos pese a ser un sector eminentemente conflictivo por su cercanía a la frontera: delincuencia común aprovechó la carencia de medidas de control de accesos y se sustrajo importante armamento, hecho que significó la pérdida del prestigio e imagen institucional del Ejército Ecuatoriano.

En torno a esto en el ámbito civil también existen eventos y varios estudiosos y tratadistas del tema manifiestan:

Suzanne Niles (2005), concluye que: “En la seguridad física, el control del personal que accede a las instalaciones, es esencial para alcanzar los objetivos relativos a la disponibilidad del centro de datos”. Donde además “el acceso a nuevas tecnologías, como la identificación biométrica y la administración remota de datos, los métodos de seguridad tradicionales basados en la lectura de tarjetas son reemplazados por sistemas de seguridad que permiten identificar sin lugar a dudas y rastrear la actividad humana dentro del centro de datos y en sus alrededores”.

Con lo enunciado anteriormente se puede establecer que las nuevas tecnologías en el ámbito de la seguridad física con sistemas de video vigilancia y control de acceso son esenciales para contribuir al mejoramiento de la seguridad en las instalaciones ya que proporcionan evidencia y rastrean las diferentes actividades que se desarrollaran en el Fuerte Militar.

Elvira Misfud (1998), en su publicación titulada Sistema Físico y Biométricos de Seguridad, concluye que: “la biometría es una serie de medidas de características específicas que permiten la identificación de personas utilizando dispositivos electrónicos que las almacena. Esta identificación consiste en comparar esas características físicas específicas de cada persona con un patrón conocido y almacenado en una base de datos”.

“Una de las ventajas de la utilización de la tecnología biométrica es que puede eliminar la necesidad de utilizar tarjetas de acceso, con todo lo que conlleva de gasto en su creación y sobre todo en su control y administración”.

Con lo mencionado por el autor anterior se puede determinar que la tecnología biométrica puede contribuir al control de acceso del personal, a través de elementos morfológicos únicos y propios de cada persona, poniéndose en manifiesto su aplicabilidad en la seguridad física y control de accesos del fuerte Militar, pues sería más personalizado el acceso y las autorizaciones de ingreso a ciertas áreas críticas, pudiendo además registrarse pruebas irrefutables y jurídicamente válidas de la presencia y/o acceso de personas a las áreas controladas tal y como ocurre en las investigaciones criminales donde las huellas digitales muchas veces nos llevan a identificar al responsable de un hecho.

Marcos Gómez Hidalgo (2003), en su publicación titulada, la seguridad hacia una sola dirección, concluye que: “la protección de los activos de una empresa involucra actual y necesariamente a las tecnologías de la información, pero también tiene que ver con la aplicación de las restricciones más clásicas desde el punto de vista físico, desde la denegación del acceso a determinadas áreas de las instalaciones, pasando por la ubicación de personal de control y seguridad en los accesos, hasta la grabación de los movimientos de nuestro personal o de las visitas en los distintos recintos y dependencias de nuestras oficinas”.

Esto aplicado a la seguridad del Fuerte Militar resalta el énfasis que se debe dar además de la tecnología para el control de acceso mediante monitoreo y grabaciones a las restricciones normales a determinadas áreas restringidas para contribuir a la seguridad física, con el empleo de personal, y demás medios con el afán de cumplir eficientemente el cometido de proteger los activos de la institución, considerando entre ellos a la información

Carlos Blanco Pasamontes (1999), indica que "existen mecanismos de gestión, incluso sistemas tecnológicos, que ayudan a integrar los procesos de seguridad en las organizaciones. La mayor barrera a la que se enfrenta la implantación de la Convergencia de la Seguridad en las organizaciones es que, actualmente, el estamento directivo de las mismas, con algunas excepciones, aún no concibe que un único equipo de personas dirijan y gestionen todos los procesos de seguridad de la organización"

Este autor resalta que los sistemas tecnológicos empleados para la seguridad deben integrar los procesos de seguridad, lo cual aplicado al Fuerte Militar va a generar mejores niveles de seguridad física, debiendo destacar la necesidad de que los mandos de los campamentos militares conciban la existencia de un equipo de seguridad que integre los procesos en esta área para optimizar los recursos y potenciar los resultados.

2.2 MARCO TEÓRICO

Al hablar de Seguridad Física en un Fuerte Militar, inevitablemente se debe pensar en un grupo de soldados fuertemente armados en misiones de custodia de las instalaciones del campamento militar, y es que tradicionalmente se concibe al servicio de guardia como el mejor y más efectivo método para dar protección y seguridad a una instalación militar. Esta manera de pensar se ha transmitido de generación en generación y se ha instituido en doctrina de las Fuerzas Militares, llegando a ser un paradigma muy difícil de superar. En este contexto, la sola idea de implementar desarrollos tecnológicos aplicables a la seguridad física de un Fuerte Militar presenta desde ya una actitud de resistencia al cambio, de oposición a la posibilidad de dejar de lado la histórica guardia humana, sin considerar que por principio fundamental de seguridad física la combinación de hombre y tecnología constituyen una unidad de eficiencia y eficacia en términos de seguridad.

Es necesario resaltar que los equipos tecnológicos por sí solos no son una solución de seguridad y que sin la operación adecuada y la interpretación derivada de un análisis de seres humanos capacitados en seguridad, no representan un aporte significativo.

De manera que esta investigación está orientada a determinar cómo contribuyen los desarrollos tecnológicos aplicados a la seguridad para mejorar el trabajo de los humanos que desarrollan esta tarea, con la finalidad de viabilizar un concepto de seguridad que integre humanos y equipos

tecnológicos para despersonalizar el trabajo, para economizar esfuerzos y mejorar resultados derivados de una fusión armónica que garantice óptimos niveles de seguridad con el empleo de menos personal, lo cual significa menos soldados por grupo de guardia y más grupos de guardia en un Fuerte Militar, más tiempo para descanso y recuperación, mayor productividad en las actividades diarias del militar así como empleo de las horas laborables en actividades de entrenamiento para sus misiones fundamentales.

2.2.1 Reseña Histórica de Seguridad

La seguridad es una necesidad básica, que se enfoca en la protección de la vida y las propiedades.

Los primeros datos acerca de la seguridad se evidencian a comienzos de la escritura con los sumerios (3000 AC) o Hamurabi (2000 AC). También se hace referencia en la Biblia, así como en las obras de Homero, Cicerón y César autores que hacen referencia a la seguridad.

Las más importantes pruebas se han obtenido con los descubrimientos arqueológicos. Las pirámides Egipcias, el palacio de Sargón y el templo de Karnak en el valle del Nilo, el dios Egipcio Anubi representado con una llave en la mano.

Es de conocimiento, que los primitivos para evitar las amenazas reaccionaban con los métodos empleados por los animales para luchar o huir, o para conseguir eliminar o evitar. De esta manera la pelea por la vida se convertía en parte esencial y conceptos como evitar, alertar, detectar, alarmar y reaccionar ya eran manejados por ellos. En esos tiempos entonces lo que se conocía como seguridad era considerada como magia.

De esta forma la seguridad ha ido evolucionando dentro de las organizaciones sociales. Las cuales tienen su fundamento en las familias lo que constituye una limitante para huir.

La primera evidencia de una cultura y organización en seguridad se ubica en los documentos de la Resolución Pública de Roma Imperial y Republicana.

El siguiente paso de la seguridad fue la especialización, de donde nace la seguridad externa y la seguridad interna. De esta se pueden desprender la seguridad privada y pública, pues aparece el estado y deposita su confianza en unidades armadas.

En el siglo XVIII, los descubrimientos científicos han contribuido a la cultura de seguridad. Principios como la probabilidad, la predicción y reducción de fallos que generan pérdidas han traído nueva luz a los sistemas de seguridad.

La seguridad moderna nace con la revolución industrial combatiendo los delitos y movimientos laborales muy comunes en esa época.

Finalmente Henry Fayol teórico y pionero de la administración realiza una identificación de la seguridad como una de las funciones empresariales, luego de las técnicas comerciales, financiera, contable y directiva.

Fayol (1924) define a la seguridad como: "salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas, felonías y de forma amplia todos los disturbios sociales que pongan en peligro el proceso e incluso la vida del negocio".

Actualmente la seguridad está en manos de los políticos, quienes son los encargados de decidir, sobre su importancia, los delitos que pueden incurrir y su respectivo castigo.

Desde el punto de vista técnico la seguridad se encuentra en manos de la dirección de las organizaciones y en última instancia en la concientización.

En las épocas de la liberación de América se forman los primeros ejércitos o milicias de alguna manera "profesionales" en el territorio del actual Ecuador, sirviendo a causas e intereses locales americanos. Luego de la independencia y la formación de la Gran Colombia, el Perú invadió el

territorio del Distrito del Sur; con exigencias reivindicativas territoriales, la suerte del conflicto se decidió la mañana y tarde del 27 de febrero de 1829 en la batalla del Portete de Tarqui donde las tropas peruanas lideradas por el mariscal José de La Mar fueron derrotadas por las gran colombinas, lideradas por el mariscal Antonio José de Sucre. Éste fue el primer triunfo militar en el actual territorio del Ecuador en el que participaron tropas y comandantes locales y en el que no se encontraron como contraparte potencias coloniales.

La historia del Ejército Ecuatoriano va de la mano con la gesta imperecedera del 10 de Agosto de 1809, cuando al albor de la libertad, nace el Ejército Ecuatoriano, cuya labor en más de dos siglos ha contribuido indiscutiblemente a la edificación del Ecuador democrático y soberano.

Las campañas independentistas fueron el preámbulo de una organización y de una estructura militar más coherente y cercana a lo que debía ser un ejército. Las ideas progresistas del quiteño Javier Eugenio de Santa Cruz y Espejo, fiel representante de la Ilustración en América, del influjo del espíritu de la Revolución Francesa y de la independencia de los Estados Unidos, fue el ente motivador para que luego del 10 de Agosto de 1809, naciera no solo una nueva etapa para Quito y el continente, sino el inicio de lo que hoy conocemos como el Ejército ecuatoriano. Debiendo resaltar que desde sus inicios se ha considerado a la seguridad como uno de los aspectos más importantes para poder desarrollar las actividades de las unidades militares en

un marco de libertad de acción para poder emplear sus medios, tropas y recursos a voluntad.

La seguridad interna en el Ejército hoy en día se ha visto amenazada ya que por el alto índice delictivo actual, también se han suscitado una serie de eventos de pérdidas al interior de las unidades militares, por lo que se requiere de una modernización en los sistemas de seguridad integrando procesos, tecnología y capacitación al personal de manera que se lleve a cabo verdaderos procesos de gestión de riesgos con un tratamiento adecuado de los mismos, que conlleve a minimizarlos.

2.2.2 Seguridad Física

La seguridad física es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso. (Autoridad Nacional para la protección de la información clasificada, 2012)

Protección de las instalaciones físicas contra sabotaje o accidentes provocados por la presencia de personas no autorizadas o mal intencionadas. Los sistemas de seguridad física siempre incluyen dispositivos de control de acceso para la revisión automatizada en puntos de acceso, más un sistema de alarma con sensores. Entre los métodos de protección adicional, pueden encontrarse la vigilancia con cámaras y los guardias de seguridad. La

expresión seguridad física a veces se usa en un modo más amplio para referirse a protección de todo tipo de daño físico, incluidos factores climáticos, terremotos y bombardeos. (Suzanne Niles, 2004)

Las medidas de seguridad física aplicables a cada caso serán concebidas para:

- Impedir la entrada por parte de intrusos, tanto si emplean métodos subrepticios como si utilizan otros que impliquen el uso de la fuerza.

- Disuadir, impedir o detectar acciones llevadas a cabo por personal desleal.

- Permitir la limitación del personal en su acceso a información clasificada de acuerdo con el principio de la necesidad de conocer.

- Detectar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones de corrección sobre éstas con la mayor brevedad posible.

2.2.3 Medios Tecnológicos Aplicados a Sistemas de Video Vigilancia y Control de Acceso

Las nuevas tecnologías han supuesto un gran avance para los ciudadanos. Al igual que las nuevas tecnologías se han adaptado a los hogares o al mundo

laboral también se han ido incorporando a las instituciones y organismos que protegen la seguridad. (ACE Project, 2013)

El objetivo de las soluciones de Seguridad Física es resguardar la seguridad patrimonial de las personas, comunidades y organizaciones con tecnologías innovadoras de Video Vigilancia y Control de Acceso. (ACE Project, 2013)

Los métodos de identificación de personas se dividen en tres categorías generales de fiabilidad – y costo del equipo – en aumento:

- Qué tienes
- Qué sabes
- Quién eres

Qué tienes: Poco fiable (puede compartirse o robarse)

Qué tienes es algo que se puede llevar: una llave, una tarjeta o un pequeño objeto (un testigo) que puede llevarse puesto o en un llavero. Puede ser tan "tonto" como la típica llave metálica o tan "inteligente" como una tarjeta con un procesador integrado que intercambie información con un lector (una tarjeta inteligente). Puede tratarse de una tarjeta con una banda magnética con información personal (como la tarjeta del cajero automático); puede ser una tarjeta o un testigo con un transmisor y/o un receptor que puede comunicarse

con el lector a una distancia corta (una tarjeta o un testigo de proximidad, Mobil Speed pass®, por ejemplo).

Qué tienes es la forma de identificación menos fiable, ya que no hay garantía de que la esté utilizando la persona correcta: puede ser compartida, robada o perdida y encontrada por otra persona.

Qué sabes: Más fiable (no puede robarse, pero puede compartirse o escribirse)

Qué sabes es una contraseña, un código o un procedimiento para algo como la apertura de una cerradura con código, la verificación en un lector de tarjetas o el acceso por teclado a un ordenador. La contraseña/código presenta un dilema de seguridad: si es fácil de recordar, probablemente será fácil de adivinar; si es difícil de recordar, probablemente será difícil de adivinar, pero también es probable que se escriba, reduciendo así su seguridad.

Qué sabes es más fiable que Qué tienes, pero las contraseñas y los códigos pueden compartirse y, si se escriben, pueden descubrirse.

Quién eres: Lo más fiable (se basa en algo que físicamente es único en cada persona)

Quién eres hace referencia a la identificación por reconocimiento de características físicas únicas: es la forma natural en que nos identificamos unos a otros con certeza prácticamente total. Cuando se realiza (o se intenta) por medios tecnológicos, se llama biometría. Se han desarrollado técnicas de identificación biométrica de varias características humanas que se prestan por sí mismas al escrutinio y análisis cuantitativo. (Suzanne Niles, 2004)

2.2.3.1 Sistema de Video Vigilancia

- **Circuito Cerrado de Televisión (CCTV)**

Figura Nº 1: Circuito Cerrado de Televisión (CCTV)

Fuente (Google: cámaras- video)

Las cámaras de circuito cerrado de TV (CCTV) – visibles u ocultas – vigilan el interior o el exterior, sirven como medida disuasoria y permiten analizar la grabación después de un incidente. (Suzanne Niles, 2004)

Es una instalación de CCTV tradicional, con Latitude de DVTEL, se convierten en Centros Inteligentes de Operaciones de Seguridad. Los datos se transportan por redes IP, lo cual toma ventajas de la convergencia de datos. (ACE Project, 2013)

Ayuda a mejorar las condiciones de seguridad, a través del empleo de video grabadoras que aporta un respaldo operativo en eventos y situaciones de emergencias. Se emplea en el perímetro del establecimiento, en los accesos y otros puntos sensibles. (Sercuritybydefault.com, 2011)

Muy asociado a la defensa perimetral. Todos conocen y saben para qué sirven los circuitos cerrados de televisión. Efectivamente, permite observar lo que sucede alrededor. (Sercuritybydefault.com, 2011)

Las cámaras pueden ser a color (mayor realismo) o en blanco y negro (mayor definición), alta definición. Las hay adecuadas a la luz diurna, luz artificial, nocturnas, etc. Incluso con la luz de las estrellas pueden obtener imágenes de calidad. Las hay motorizadas o estáticas (las primeras tienen la ventaja de cubrir más amplitud pero a su vez es una desventaja). (Sercuritybydefault.com/2011)

Pueden detectar movimiento, mediante el software adecuado, de la imagen y alertar al operador o disparar alguna acción. Como cualquier sensor se ha de dimensionar correctamente para no obtener falsos positivos. Si se configura muy sensible puede que salte la alarma con cualquier animal pequeño (un gato, un ave, etc.) si, lo ponemos poco sensible, puede que no detecte un intruso (Sercuritybydefault, 2001)

Un fallo muy común son los ángulos muertos, zonas que las cámaras no cubren. Esto ocurre cuando dos cámaras puestas en un mismo punto apuntan a dos direcciones diferentes. Lo ideal, es que una cámara cubra el perímetro y a la vez a la siguiente cámara (en fila) de esta forma, se puede eliminar los puntos muertos así como cualquier manipulación directa sobre la cámara. Por supuesto, normalmente detrás de una cámara deberá haber un operador, si no como que la cosa no funciona igual (excepto las cámaras con sensor de movimiento). Por último comentar que puede llegar a ser interesante el ocultar las cámaras por cubiertas opacas, con objeto de no revelar información sobre qué puntos "vigilan" dichas cámaras (Sercuritybydefault, 2001)

Cámaras IP

Las cámaras IP de vigilancia se han vuelto muy populares en nuestros días, sus ventajas innegables y sus cada vez más bajos precios las han convertido en las favoritas de los usuarios en todo el mundo ya que lo único

que se necesita es una conexión a internet para poder vigilar las instalaciones desde cualquier parte del planeta.

Foscam FI8918W

Figura Nº 2: Cámaras Foscam FI8918W
Fuente: (google: img,nauticexpo)

Esta cámara viene liderando la lista con una serie de características que rápidamente la han convertido en la favorita de usuarios corporativos y domésticos, es utilizada para vigilar negocios, empresas, casas, habitaciones con niños pequeños, ancianos o personas enfermas y mascotas.

Tiene una resolución máxima estándar de 640 x 480 pixeles y una cobertura de 67 grados que es superior al promedio (50-60), esta cámara se puede manejar de forma remota haciéndola girar y hacer zoom, es posible visualizar múltiples cámaras instaladas en diferentes lugares desde un navegador web en la PC, laptop o smartphone y el acceso seguro se realiza mediante usuario y contraseña.

La Foscam FI8918W puede configurarse para que detecte movimiento y envíe una alerta a nuestro email cuando detecta un intruso o movimiento anormal en su campo de vigilancia, está alerta puede incluir una imagen capturada en ese momento crítico.

Podemos acceder a esta cámara desde cualquier lugar del mundo así tengamos la cámara conectada con un IP dinámico, para esto la cámara incluye su propio hostname DNS que resuelve el IP, se le puede programar para que comience a grabar en determinados horarios, donde graba? puede ser el disco duro de nuestra PC, en un servidor web a través del protocolo FTP o por email.

- **Cisco PVC 300**

Figura Nº 3: Cámara Cisco PVC 300
Fuente: (foscam)

La máxima resolución ofrecida por la cámara IP Cisco PVC 300 es de 640 x 480 pixeles, el promedio actual, mientras que su cobertura es de 73

grados, lo cual también está bastante por encima del promedio actual, esta cámara nos permite hacer pandeas horizontales, moverla verticalmente y hacer zoom, es posible visualizar más de una cámara a la vez desde el navegador, podemos usar IP dinámico ya que la misma cámara resuelve el IP mediante un hostname DNS, también podemos programar los horarios de grabación y activar el detector de movimiento que alerta sobre cualquier situación extraña mediante un email, con la foto anexada de la situación que ha disparado la alarma.

Para guardar los vídeos de vigilancia de la Cisco PVC 300 se puede apelar al método más usado que es de forma remota en el disco duro de una PC, o mediante FTP hacia un servidor web.

Para visualizar la vigilancia de la Cisco PVC 300 se puede acceder al navegador web favorito como Internet Explorer o Firefox, incluso acceder desde navegadores en smartphones usando la conexión 3G o 4G según la región.

Esta cámara de vigilancia IP no es compatible con tarjetas SD o sistema de DVR para almacenamiento de vídeos.

Panasonic BL-C210

Figura Nº 4: Cámara Panasonic BL-C210
Fuente: (foscam)

La cámara IP de seguridad Panasonic BL-C120 ofrece una resolución máxima de 640 x 480 pixeles lo cual es aceptable dentro de los estándares actuales de cámaras IP, mientras que el área de barrido que cubre esta cámara de vigilancia IP es de 58 grados lo cual también se encuentra dentro del promedio actual tecnológicamente aceptable, se puede visualizar todo desde cualquier navegador web e incluso desde los navegadores de los modernos smartphones, esta cámara funciona a la perfección con IP dinámico ya que el fabricante ha proveído con un hostname DNS que redirecciona al IP en uso.

Como resulta muy poco práctico, por no decir imposible, estar vigilando las 24 horas mediante una cámara, la Panasonic BL-C210 posee un práctico sistema que utiliza la detección de movimiento para lanzar una alerta vía email, la cual incluye la respectiva toma de imagen del momento en el que se

dispara la alarma, de tal forma que puede evaluar el grado de seriedad y decidir qué hacer.

La Panasonic BL-C210 permite guardar el vídeo de forma remota en el disco duro de un PC o laptop, sin embargo con esta cámara no es posible subir el vídeo a un servidor web vía FTP.

- **Panasonic BL-C1A**

Figura Nº 5: Cámara Panasonic BL-C1A
Fuente (foscam)

La cámara IP Panasonic BL-C1A ofrece una resolución estándar de 640 x 480 y un área de cobertura de 53 grados, esta cámara puede ser manejada desde cualquier navegador web como Internet Explorer o Mozilla Firefox pero también desde los navegadores web móviles en smartphones y tablets, se puede conectar varias cámaras en la red y visualizarlas en una sola interfaz, eso sí, hay que tener en cuenta que esta cámara no transmite sonido, solamente vídeo lo cual podría ser un inconveniente en algunos casos específicos.

Esta cámara de seguridad IP puede usar sin ningún problema IP dinámico ya que el fabricante provee su propio servidor de DNS que resuelve y direcciona al IP, si se desea guardar el vídeo hay que hacerlo de forma remota en el disco duro de la PC, esta cámara permite subir vídeo a servidores web mediante el protocolo FTP como otras cámaras.

2.2.3.2 Control de Acceso

Algunos dispositivos de control de acceso, lectores de tarjetas y escáneres biométricos, pueden capturar los datos de incidencias de acceso, como la identidad de las personas que pasan y la hora de entrada. Si están en red, estos dispositivos pueden enviarla información a un sistema de gestión remoto de supervisión y registro (quién entra y sale), control de dispositivos (configuración de un bloqueo para permitir el acceso a determinadas personas en determinados momentos), y alarma (notificación de repetidos intentos infructuosos o fallos del dispositivo). (Suzanne, 2004)

2.2.3.3 Combinación de métodos para aumentar la fiabilidad

Un esquema de seguridad típico utiliza métodos para aumentar la fiabilidad y los gastos progresivamente, de las áreas más exteriores (menos sensibles) a las más interiores (más sensibles). Por ejemplo, la entrada al edificio podría exigir una combinación de tarjeta magnética más código PIN; la entrada a la sala de ordenadores podría exigir teclear un código más una identificación biométrica.

La combinación de métodos en un punto de acceso aumenta la fiabilidad en ese punto; la utilización de distintos métodos en cada nivel aumenta significativamente la seguridad en los niveles interiores, ya que cada uno se asegura mediante sus propios métodos más los de los niveles exteriores a los que hay que entrar primero. (Saltos V. (2013). Elementos confiables en seguridad. Centro Científico de Datos Recuperado de: DCSC@Schneider-Electric.com)

2.2.3.4 Tarjetas y testigos: "qué tienes"

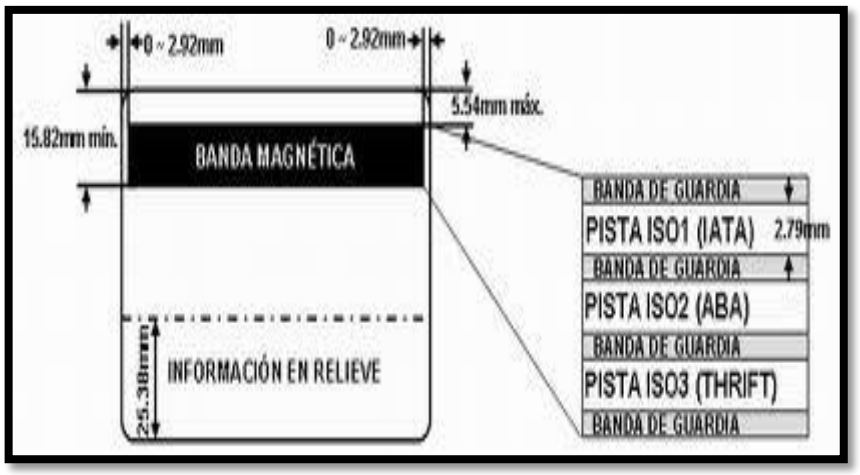


Figura Nº 6: Tarjeta banda magnética
Fuente: (foscam)

Actualmente se utilizan varios tipos de tarjetas y testigos de control de acceso, desde los más sencillos a los más sofisticados, que ofrecen toda una gama de prestaciones en varias dimensiones:

- Capacidad de reprogramación
- Resistencia a la falsificación
- Tipo de interacción con el lector de tarjetas: pasada, inserción, contacto, sin contacto (“proximidad”)
- Comodidad: forma física y cómo se lleva
- Cantidad de datos que incluye
- Capacidad computacional
- Coste de las tarjetas
- Coste del lector

Independientemente de lo seguras y fiables que puedan ser por su tecnología, la seguridad ofrecida por estas “cosas” físicas está limitada por el hecho de que no hay garantía de que las esté utilizando la persona adecuada. Por ello es normal combinarlas con uno o más métodos adicionales de confirmación de la identidad, como una contraseña o una identificación biométrica. (Saltos V. (2013). Elementos confiables en seguridad. Centro Científico de Datos Recuperado de: DCSC@Schneider-Electric.com)

La tarjeta de banda magnética es el tipo más normal de tarjeta, con una sencilla banda magnética de datos de identificación. Cuando la tarjeta se pasa por un lector, la información que contiene se lee y busca en una base de datos. El sistema es barato y cómodo; el inconveniente es que resulta relativamente fácil duplicar las tarjetas o leer la información que tienen almacenada.

La banda magnética en la tarjeta final puede ser codificada porque las partículas pueden ser magnetizadas en dirección sur o norte. Cambiando la dirección de codificación a lo largo de la banda permite escribir la información en la banda. Esta información puede ser leída y luego cambiada tan fácilmente como la primera codificación (Larconsia, 2013)

La tarjeta de ferrita de bario, también llamada "tarjeta de puntos magnéticos" es similar a la tarjeta de banda magnética pero ofrece más seguridad sin añadir un costo importante. Contiene una fina lámina de material magnético con puntos redondos dispuestos en un patrón. Más que leerse mediante pasada o escáner, la tarjeta se pone en contacto con el lector.

La tarjeta Weigand es una variante de la tarjeta de banda magnética. La tarjeta lleva incrustada una serie de hilos especialmente tratados con una firma magnética única. Cuando la tarjeta se pasa por el lector, hay una bobina de detección que detecta la firma y la convierte en una cadena de bits. La ventaja de este complejo diseño es que las tarjetas no pueden duplicarse; el inconveniente es que tampoco pueden reprogramarse. Con esta tecnología, la tarjeta no necesita estar en contacto directo con el lector; por ello, el cabezal del lector puede estar encapsulado: ideal para su instalación en exteriores. A diferencia de los lectores de tarjetas de proximidad y las tarjetas de banda magnética, a los lectores Weigand no les afectan las interferencias de radiofrecuencia (RFI) ni los campos electromagnéticos (EMF). La robustez

del lector combinada con la dificultad para duplicar la tarjeta hace que el sistema Weigand sea extremadamente seguro, dentro de los límites de un método “qué tienes”, pero también es más caro.

La tarjeta de código de barras lleva un código de barras que se lee al pasar la tarjeta por el lector. Este sistema es muy barato, pero muy fácil de engañar: una simple fotocopiadora puede duplicar lo suficientemente bien el código de barras como para engañar al lector.

Las tarjetas de códigos de barras son buenas para requisitos de seguridad mínimos, especialmente los que exigen un gran número de lectores en el emplazamiento o donde hay un tráfico intenso atravesando un punto de acceso determinado. No es tanto un sistema de seguridad como un método barato de control de acceso. Se dice que el acceso mediante código de barras solo sirve para “dejar fuera a las personas honestas”.

La tarjeta de sombra de infrarrojos mejora la escasa seguridad de la tarjeta de código de barras colocando el código de barras entre capas de plástico PVC. El lector pasa la luz infrarroja por la tarjeta y la sombra del código de barras es leída por los sensores del otro lado.

La tarjeta de proximidad (también llamada “tarjeta prox”) es un paso adelante en la comodidad comparada con las tarjetas que deben pasarse por el lector o tocarlo. Como su nombre indica, la tarjeta solo necesita

“aproximarse” al lector. Esto se consigue utilizando tecnología RFID (identificación por radiofrecuencia), que suministra energía a la tarjeta a través del campo electromagnético del lector de tarjetas. El diseño más conocido funciona a una distancia de unos 10 cm del lector; otro diseño – la llamada tarjeta de vecindad –funciona a una distancia de hasta un metro.

La tarjeta inteligente, el desarrollo más reciente de tarjetas de control de acceso, se está convirtiendo rápidamente en el método elegido para las nuevas instalaciones. Es una tarjeta con un chip de silicio incorporado para el almacenamiento y/o el cálculo de datos integrado.

Los datos se intercambian con el lector por contacto del chip con el lector (tarjeta inteligente de contacto) o por interacción con el lector a una distancia, utilizando la misma tecnología que las tarjetas de proximidad y vecindad (tarjeta inteligente sin contacto o de proximidad). (Suzanne, 2004)

2.2.3.5 Teclados y cerraduras con código: “qué sabes”

Los teclados y las cerraduras con código se utilizan ampliamente como método de control de acceso. Son fiables y fáciles de usar, pero su seguridad está limitada por la naturaleza de las contraseñas, que pueden compartirse o adivinarse. Tienen botones como los del teléfono, donde los usuarios marcan un código: si el código es exclusivo de cada usuario, se denomina código de acceso personal (PAC) o número de identificación personal (PIN). El teclado

generalmente implica la capacidad de aceptar múltiples códigos, uno por cada usuario; la cerradura con código normalmente hace referencia a un dispositivo que solo tiene un código que utilizan todos.

El nivel de seguridad de los teclados y cerraduras con código puede aumentarse cambiando periódicamente los códigos, lo que requiere un sistema para informar a los usuarios y comunicar los nuevos códigos. Las cerraduras que no cambian de código deben sustituirse periódicamente si el desgaste de las teclas permite detectar el código. Como con las tarjetas de acceso, la seguridad mediante teclado puede aumentarse añadiendo la identificación biométrica para confirmar la identidad del usuario. (Saltos V. (2013). Elementos confiables en seguridad. Centro Científico de Datos Recuperado de: DCSC@Schneider-Electric.com)

2.2.3.6 Biometría: "quién eres"

El término se deriva de las palabras griegas "bios" de vida y "metron" de medida. La biometría es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de una persona, para "verificar" identidades o para "identificar". (Biométrica, P. P. (11 de Septiembre de 2011). Wikipedia. Recuperado de:

Http://es.wikipedia.org/wiki/Biometr%C3%ADa

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas como es la huella digital.

Los sistemas Biométricos incluyen dispositivos de captación y un software biométrico que interpreta la muestra física y la transformada en una secuencia numérica, que en el reconocimiento de huella digital se deberá tomar en cuenta que en ningún caso se extrae la imagen de la huella, sino más bien una secuencia de números. **(**Biométrica, P. P. (Octubre, 2012). Sistema biométrico. (globalcard, 2000)

La verificación biométrica de elevada confianza, especialmente la del reconocimiento de huellas digitales, está entrando en el ámbito de las soluciones de seguridad. Muchos distribuidores suministran una amplia gama de dispositivos biométricos y, en combinación con los métodos tradicionales "qué tienes" y "qué sabes", la biometría puede completar las medidas de seguridad existentes para convertirse en el mejor control de acceso.

La identificación biométrica suele utilizarse no para reconocer la identidad buscando en una base de datos de usuario una coincidencia, sino más bien para verificar la identidad que primero se establece mediante un método "qué tienes" o "qué sabes": por ejemplo, primero se utiliza una tarjeta/PIN, y después la comprobación de la huella digital verifica el resultado. A medida que aumenta el rendimiento y la confianza en la tecnología biométrica,

finalmente puede convertirse en un método autónomo de reconocimiento de la identidad y eliminar la necesidad de llevar tarjetas o recordar contraseñas.

Figura Nº 7: Aparato biométrico dactilar
Fuente: (foscam)

Hay dos tipos de fallos en la identificación biométrica:

- Falso rechazo. Imposibilidad de reconocer a un usuario legítimo. Aunque puede alegarse que tiene el efecto de mantener el área protegida absolutamente segura, es una frustración intolerable para los usuarios legítimos a quienes se les deniega el acceso porque el escáner no los reconoce.

- Falsa aceptación. Reconocimiento erróneo, ya sea por confundir a un usuario con otro o por aceptar a un impostor como usuario legítimo.

Los índices de fallos pueden ajustarse cambiando el umbral (“qué grado de exactitud es suficiente”) para declarar una coincidencia, aunque la disminución de un índice de fallos aumentaría el otro.

Los criterios a la hora de elegir una función biométrica son el coste del equipo, los índices de fallos (tanto de falso rechazo como de falsa aceptación) y la aceptación del usuario, que significa qué grado de intrusión, incomodidad o incluso peligro percibe el usuario del procedimiento. Por ejemplo, se considera que los escáneres de retina tienen poca aceptación de los usuarios porque el ojo tiene que estar a una distancia de 2,5 a 5 cm del escáner con un LED dirigido al ojo

El diseño del sistema de seguridad se centra en dispositivos para identificar y filtrar personas en los puntos de entrada – “control de acceso” – que es todo lo que se necesitaría si la identificación tuviera una fiabilidad del 100% y se admitiera una confianza total en las intenciones de las personas admitidas y en la perfección física de paredes, puertas, ventanas, cierres y techos infranqueables. Para cubrir los inevitables fallos por errores o sabotaje, los sistemas de seguridad suelen incorporar métodos adicionales de protección, supervisión y recuperación.

2.2.3.7 Huella dactilar

Una huella dactilar o huella digital es la impresión visible o moldeada que produce el contacto de las crestas papilares. Depende de las condiciones en que se haga el dactilograma (impregnando o no de substancias de color distinto al soporte en que asiente), y de las características del soporte (materias plásticas o blandas, en debidas condiciones). Sin embargo, es una característica individual que se utiliza como medio de identificación de las personas. (Larconsia, 2013)

Figura Nº 8: Huella dactilar
Fuente: (foscam)

El sistema de identificación de las personas a través de las huellas fue inventado por Juan Vucetich, croata, nacionalizado argentino, y el invento se desarrolló y patentó en Argentina, donde también se usó por primera vez el sistema de identificación de huellas para esclarecer un crimen. La disciplina científica que estudia las huellas dactilares se llama dactiloscopia, y dentro de

ella existen dos grandes ramas con su propia clasificación de huellas. (Larconsia, 2013)

2.2.3.8 Dibujos papilares

Los dibujos papilares incluyen las papilas y los surcos interpapilares. Las crestas papilares son relieves epidérmicos situados en las palmas de las manos y en las plantas de los pies. Los surcos interpapilares se determinan por las depresiones que separan dichos relieves o crestas. La dermis es la capa interior y más gruesa de la piel, que contiene el dibujo papilar. La epidermis es la membrana que cubre la dermis. Los poros papilares son los diminutos orificios de forma y dimensiones variadas que en crecido número existen en las crestas papilares y por los cuales se expulsa el sudor. (Larconsia, 2013)

Está demostrado científicamente que los dibujos que aparecen visibles en la epidermis son perennes, inmutables, diversiformes y originales. (Larconsia, 2013)

- Son perennes porque, desde que se forman en el sexto mes de la vida intrauterina, permanecen indefectiblemente invariables en número, situación, forma y dirección hasta que la putrefacción del cadáver destruye la piel.

- Son inmutables, ya que las crestas papilares no pueden modificarse fisiológicamente; si hay un traumatismo poco profundo, se regeneran y si

es profundo, las crestas no reaparecen con forma distinta a la que tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.

- Son diversiformes, pues no se ha hallado todavía dos impresiones idénticas producidas por dedos diferentes.

Son originales, que todo contacto directo de los lofrogramas naturales producen impresiones originales con características microscópicas identificables del tejido epidérmico, para establecer si fue plasmada de manera directa por la persona o si trata de un lofograma artificial. (Larconsia, 2013).

2.2.3.9 Reconocimiento facial

Figura Nº 9: Reconocimiento Facial
Fuente: (foscam)

Es una aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una fuente de video, y comparándolas con una base de datos.

Se utiliza principalmente en sistemas de seguridad para el reconocimiento de usuarios. En estos sistemas se utiliza un lector que define las características del rostro, y cuando este solicita el acceso, se verifica comparando los datos obtenidos con la base de datos. Sin embargo, estos sistemas no son útiles a largo plazo ya que, a medida que pasan los años, los rasgos faciales varían y al solicitar el acceso ya no coinciden con la imagen en la base de datos. Para solucionar este problema se puede utilizar un algoritmo que interprete el paso de los años, aunque igualmente sigue sin ser del todo fiable), o bien, renovar frecuentemente la base de datos. (Sistema de reconocimiento facial. Wikipedia (Octubre, 2012). Recuperado de: http://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial)

2.2.4 Sistemas de sensores

Figura Nº 10: Sensores
Fuente: recuperado de: (foscam)

Los sensores electrónicos son dispositivos de reducido tamaño y alimentados por baterías, o fuente de alimentación a baja tensión (6v. a 12v.) que detectan con un campo de actuación variable, la presencia humana u otros elementos extraños.

Las variaciones eléctricas enviadas por los sensores son recogidas por la unidad de control, que una vez convenientemente tratadas dan lugar a la activación de los sistemas de señalización: ópticos, acústicos, entre otros. (Rincón del Vago. (Diciembre, 2012). (seguridad alarmas, 2012)

Todo el mundo está familiarizado con los sistemas de alarma tradicionales de casas y edificios: sensores de movimiento, sensores de calor, sensores de contacto (puerta cerrada), y similares.

Si los sensores están en red, pueden vigilarse y controlarse de forma remota mediante un sistema de gestión, que también podría incluir datos de movimiento del personal de los dispositivos de control de acceso

2.2.4.1 Clasificación de sensores

Sensores de intrusión

Los sensores de intrusión tiene por misión detectar la entrada de elementos extraños (personas), por los lugares en que estén colocados, entendiendo por lugares todos aquellos que sean factibles de intrusión o paso. Pueden ser Perimetrales, Volumétricos y lineales.

Perimetrales

- Sensores de vibración.
- Cinta conductora autoadhesiva.
- Sensor por contacto magnético.
- Sensor microfónico de rotura de vidrio.
- Sensor detector de doble tecnología.

Volumétricos

- Radar o microondas.
- Infrarrojos.

Lineales.

- Barreras infrarrojas.
- Barreras microondas.
- G.P.S.

Magnéticos: Sensores muy simples. Dos puntos están en contacto, pasa corriente eléctrica. Cuando se produce una intrusión (abertura de una ventana, por ejemplo), se produce una diferencia de potencial que activa la alarma.

Son sencillos de sabotear. (Clasificación de los sensores. (2011). Recuperado de: Sercuritybydefault.com)

Láser: Se suelen colocar en zonas de detección muy determinada, como pueden ser ventanas, puertas, cajas fuertes, pasillos, etc. A mayor número de sensores mayor cobertura de detección. Es común ocultar este tipo de sensores porque su inhabilitación es relativamente sencilla. Son utilizados tanto en interior como en exterior. Requieren de visibilidad entre el transmisor y receptor y por tanto no puede haber obstáculos entre ellos. Le afecta las condiciones climáticas que puedan dificultar la visión entre el transmisor y receptor, como hemos comentado anteriormente. (Clasificación de los sensores. (Sercurtybydefault, 2011)

Inducción: Este tipo de sensores mide la alteración de un campo de inducción (o magnético). Detectan el paso de un objeto metálico. El tamaño de dicho objeto irá en función de la calibración del sensor. Estos pueden presentarse en forma de arco de detección, como el que hay en los aeropuertos o pueden instalarse en el suelo, de tal forma que al pasar un vehículo o persona puedan detectar su presencia. Se han utilizado a modo de radar y cuenta la leyenda que los israelíes tiene todo el perímetro de sus fronteras (al menos las más "calientes") rodeado por este tipo de sensores. De tal forma que cualquier persona con un mínimo objeto metálico es detectado de inmediato (mínimo = clavos de los zapatos). Este tipo de sensores, muy a groso modo son dos cables que crean un campo magnético entre ellos. Como

se puede observar no sirve ante objetos no metálicos. No les afecta la climatología (exceptuando tormentas eléctricas). (Sercuritybydefault, 2001)

Microondas: Basados en el efecto doppler. Suelen cubrir un entorno en forma de óvalo. Se suelen instalar en el interior de zonas cerradas. Sensores muy efectivos pero que se han de calibrar correctamente porque puede llegar a traspasar paredes o muros y provocar falsos positivos al detectar "intrusiones" en zonas aledañas. En el exterior les puede afectar la climatología (niebla densa, lluvia intensa, etc.). (Sercuritybydefault, 2001)

2.2.5 Alarmas

Un sistema de alarma es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas.

Figura Nº 11: Alarma
Fuente: (foscam)

2.2.5.1 Funcionamiento

Una vez que la alarma comienza a funcionar, o se activa dependiendo del sistema instalado, este puede tomar acciones en forma automática. Por ejemplo: Si se detecta la intrusión de una persona a un área determinada, mandar un mensaje telefónico a uno o varios números, El uso de la telefonía para enviar mensajes, de señales o eventos se utilizó desde hace 60 años pero desde el año 2005 con la digitalización de las redes de telefonía, la comunicación deja de ser segura, actualmente la telefonía es solo un vínculo más y se deben enviar mensajes mediante GPRS a direcciones IP de servidores que ofician de receptores de las señales o eventos, también se utiliza la conectividad propia de las redes IP. Si se detecta la presencia de humo, calor o ambos, mandar un mensaje al "servicio de monitoreo" o accionar la apertura de rociadores en el techo, para que apaguen el fuego. Si se detecta la presencia de agentes tóxicos en un área, cerrar las puertas para que no se expanda el problema. (Funcionamiento de las alarmas. (Enero, 2013). Recuperado de: http://es.wikipedia.org/wiki/Sistema_de_alarma)

Para esto, la alarma tiene que tener conexiones de entrada, para los distintos tipos de detectores, y conexiones de salida, para activar otros dispositivos que son los que se ocupan de hacer sonar la sirena, abrir los rociadores o cerrar las puertas.

Uno de los usos más difundidos de un sistema de alarma es advertir el allanamiento en una vivienda o inmueble. Antiguamente los equipos de alarma podrían estar conectados con una Central Receptora, también llamada Central de Monitoreo, con el propietario mismo (a través de teléfono o

TCP/IP) o bien simplemente cumplir la función disuasoria, activando una sirena (la potencia de la sirena estará regulada por las distintas leyes de seguridad del Estado o región correspondiente). En la actualidad existen servicios de "monitoreo por Internet" que no utilizan una "central receptora" ni una "central de monitoreo" sino redes compartidas en Internet donde se derivan directamente las señales o eventos a teléfonos inteligentes (smartphones), tabletas y portátiles conectados a Internet utilizando un navegador de código abierto (Mozilla Firefox), envían la información directamente a quienes deben recibirla, usuarios o titulares de los servicios, personal técnico para la reparación de falsas alarmas, operadores de monitoreo quienes verifican las señales que requieren de procesamiento humano y la autoridad de aplicación (Policía, Bomberos, etc) para el caso de hechos reales donde el estado debe intervenir.

Para la comunicación con una vieja Central Receptora de Alarmas o un actual “servicio de monitoreo" en Internet, se necesita de un medio de comunicación, como podrían serlo: la antigua línea telefónica RTB o el canal GPRS de una línea GSM, un transmisor por radiofrecuencia o mediante transmisión TCP/IP que utiliza una conexión de banda ancha ADSL, enlaces TCP/IP inalámbricos y servicios de Internet por cable CableModem. (Funcionamiento de las alarmas. (Enero, 2013). Recuperado de: http://es.wikipedia.org/wiki/Sistema_de_alarma)

2.2.6 Gestión de Riesgos

A la hora de enfrentarse con el problema de decidir las medidas específicas de seguridad física y de otra índole, necesarias para asegurar la protección de una instalación en la que se va a manejar o almacenar información clasificada, existen dos aproximaciones posibles. Una es la aplicación de estándares fijos de protección que permitan dar una seguridad adecuada en cualquier condición y situación, lo que constituye una solución que va a exigir mayores recursos iníciales, pero es más estable y permite mantener la seguridad de forma más automática. (Autoridad Nacional para la protección de la información clasificada, 2012)

Otra opción es considerar los riesgos existentes, evaluando de la forma más aproximada posible las amenazas y vulnerabilidades que afectan o pueden afectar a dicha instalación en cada momento, mediante lo que se conoce como análisis de riesgos

Esta opción permite optimizar los recursos empleados, pero exige una mayor disciplina de seguridad, y mantener una gestión continua del riesgo existente, para adaptarse a las situaciones cambiantes sin merma de la protección en ningún momento.

El análisis de riesgos es, el proceso por el que se identifican las amenazas y vulnerabilidades contra la seguridad de una instalación, se determina su

magnitud y se descubren las áreas que necesitan medidas específicas de seguridad física o de otra índole.

El análisis de riesgos sirve para identificar el riesgo existente y evaluar la actual seguridad de una instalación en relación con el manejo de información clasificada, para a continuación reunir la información necesaria para seleccionar las medidas de seguridad más eficaces.

El análisis de riesgos no es una tarea que se haga una única vez. Debe realizarse periódicamente, con objeto de que se mantenga actualizado frente a los cambios. La gestión del riesgo supone planificación, organización, dirección y control de recursos para garantizar que el riesgo permanece dentro de unos límites y un costo aceptable (Autoridad Nacional para la protección de la información clasificada, 2012)

El proceso de análisis de riesgos es un ejercicio de recolección y valoración de datos que aborda dos cuestiones básicas: los activos que corren peligro, especialmente la información clasificada, y cuáles serían el impacto o las consecuencias si las vulnerabilidades identificadas fueran explotadas con éxito. (Autoridad Nacional para la protección de la información clasificada, 2012)

Una ventaja importante es que, a través del análisis de riesgos, se aumenta la concienciación en materia de seguridad, que debe estar presente en todos los niveles de la organización, desde el más alto nivel de gestión hasta el

personal auxiliar y de operaciones. Asimismo, el resultado del proceso de gestión del riesgo puede facilitar detalles importantes a incluir en la documentación de seguridad requerida, en concreto en el plan de protección.

2.2.7 Amenazas y Riesgos Existentes

La seguridad no es una ciencia exacta, pero si se combinan unos pocos elementos (de los muchos que participan en ella) el resultado será bueno.

La seguridad debe tener:

- Simplicidad
- Flexibilidad
- Coordinación

Simplicidad: Los planes de seguridad deben ser claros para todos los miembros de la institución u organización en estudio, desarrollados en términos de fácil interpretación y evitando malos entendidos. (Maciel, 2010)

Flexibilidad: Como es imposible prever todas las situaciones, estos planes deben ser desarrollados de tal forma en que puedan variar en función de entender situaciones no previstas para poder afrontar los hechos imponderables. (Maciel, 2010)

Coordinación: Debe estar bien claro quién será el coordinador o quien dirigirá en una situación de crisis o emergencia. Es por ello que deben

establecerse de tal forma, que no haya ninguna duda al respecto, quién asumirá la conducción según las características de la institución u organización en estudio y la oportunidad en que se presenta la necesidad para tal circunstancia. (Marcelo Maciel, 2010)

Hay que evaluar debidamente las amenazas, su probabilidad de ocurrencia lo que dará una idea del riesgo y por lo tanto del peligro que se ocurre. **(**Marcelo Maciel, 2010)

Tipos de riesgos

- Provocados
- Accidentales

Provocados: Son aquellos en los cuales intervienen la mano intencional del hombre con fines de hurto, robo, incendio, atentado, vandalismo, maltrato, violaciones, varias, venganzas, despechos, intencionales criminales de diferente tenor. (Marcelo Maciel, 2010)

Accidentales: Son en los que interviene la mano del hombre pero negligente o imprudencialmente, (Marcelo Maciel, 2010)

2.2.8 Métodos de Análisis y Evaluación de Riesgos

Es un proceso por el cual se realiza una valoración y ponderación, cualitativa y cuantitativa de los factores de riesgo que inciden en una determinada actividad, teniendo en cuenta los parámetros especificados.

Figura Nº 12: Método de análisis y evaluación de riesgos
Fuente: (Duque, 2001)

A continuación citaré algunos ejemplos de métodos que permiten analizar y evaluar los riesgos.

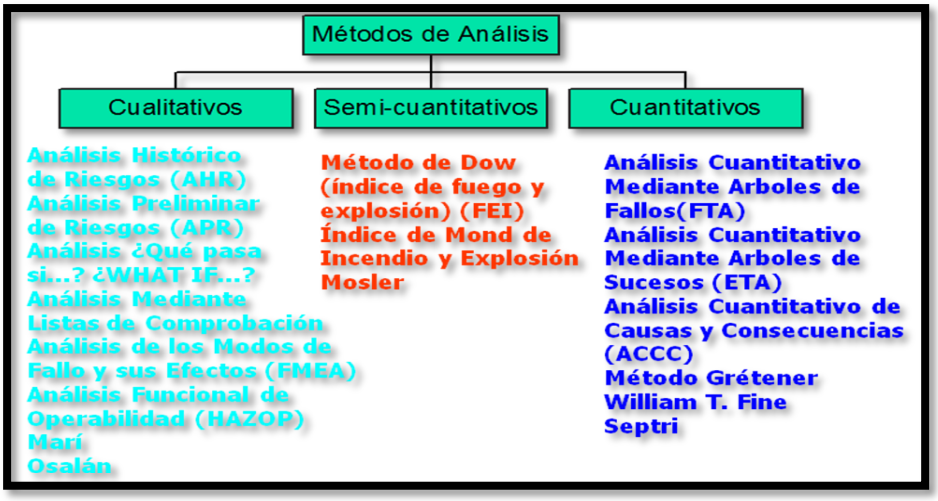


Figura Nº 13: Método de análisis del riesgo
Fuente: (Duque, 2001)

Para el presente estudio, emplearé como herramienta de análisis el método FODA y MOSLER.

2.2.8.1 Método FODA

Para la elaboración de las estrategias y planes se requiere de un diagnóstico y análisis previo de todos los factores que de alguna forma influyen en la Organización.

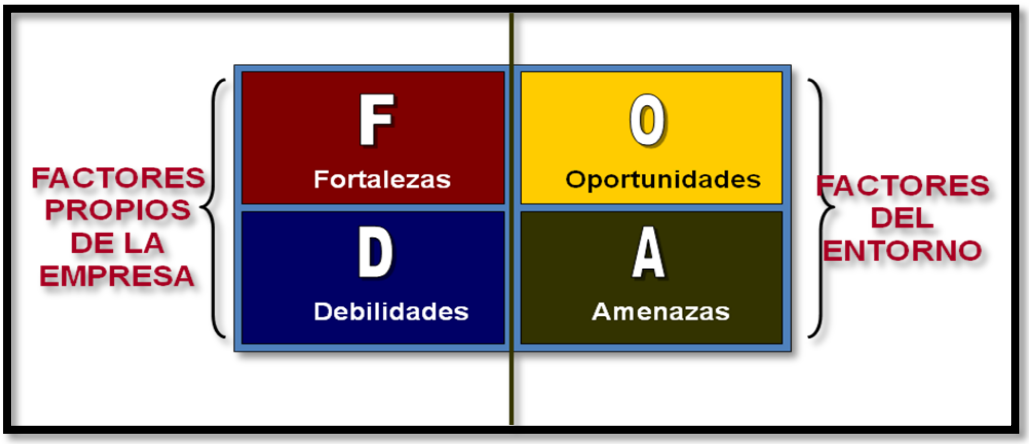


Figura Nº 14: Método FODA del riesgo
Fuente: (Duque, 2001)

Oportunidades:

Las Oportunidades se dan en el medio en el que se desenvuelve de forma constante.

Determinar qué Oportunidades son de interés estratégico para la institución puede permitir superar las expectativas propuestas.

Puede ser un catalizador de las Fortalezas y las Debilidades

Amenazas:

Las Amenazas presentes en el entorno de la institución son aquellas que pueden alterar las expectativas corporativas.

Su origen exógeno hace de las Amenazas un factor determinante de las estrategias preventivas.

Fortalezas:

Las fortalezas, como factor intrínseco de la corporación, establecen estrategias operativas para compensar a las debilidades.

Deben ser manejadas de forma integral y coordinada para multiplicar sus efectos. La evaluación continuada de éstas, evidenciará si las fortalezas son reales o aparentes.

Debilidades:

Las debilidades, nacen de la propia corporación y deben ser ampliamente conocidas y comprendidas por las gerencias. Una cadena es tan fuerte como el más débil de sus eslabones.

La evaluación continuada de las debilidades de las áreas críticas es el único camino a la superación.

Consideraciones básicas:

El método FODA o DOFA, se desarrolla, para facilitar la toma de medidas preventivas y reactivas que ayuden a disminuir el nivel de RIESGO latente de una instalación o persona.

Se desarrolla un análisis de los factores externos y un diagnóstico de los factores internos.

Los factores tanto externos como internos son considerados como facilitadores o no del riesgo analizado.

Luego se formulan dos Tablas, uno para los factores externos y otro para los factores internos.

Los dos Tablas tienen cinco secciones: Factores; Peso; Calificación; Ponderación y Observaciones.

Los factores, están relacionados con aspectos tanto internos como externos a evaluar y que tengan relación con el riesgo evidente o encubierto.

El peso está expresado en % y no debe exceder del 100% en la suma de todos los factores.

Las calificación se determina en base a una tabla del 1 al 4; donde el 1 determina mayor debilidad; el 2 determina menor debilidad; el 3 determina menor fortaleza y el 4 mayor fortaleza.

La ponderación es el resultado de la multiplicación del peso por la calificación, convertido al sistema decimal.

En las observaciones, se consigna los parámetros de mayor relevancia que ha tenido en cuenta el analista.

La matriz formulada, nos determinará una ponderación, que si es menor a 2.5 representará DEBILIDAD y si es mayor a 2.5 representará FORTALEZA.

Terminado las dos matrices o Tablas de evaluación se formulan las recomendaciones que en muchas oportunidades determina un replanteamiento de la seguridad integral.

MATRIZ DE FACTORES INTERNOS DE RIESGO				
Factores	Peso 100%	Calificación 1 a 4	Ponderación	Observaciones

Figura Nº 15: Matriz de factores internos del riesgo
Fuente: (Duque, 2001)

Total ponderado: el resultado de la matriz coloca en una posición de Fortaleza o de Debilidad

Factores	Peso 100%	Calificación 1 a 4	Ponderación	Observaciones

Figura Nº 16: **Matriz de factores externos del riesgo**

(Duque, 2001)

El resultado de la matriz coloca en una posición de Oportunidad o Amenaza

2.2.8.2 Método MOSLER

El método Mosler tiene como finalidad servir de base para la identificación, análisis y evaluación de los factores que pueden influir en la manifestación y materialización de un riesgo.

El objetivo del método Mosler, es de calcular la clase y dimensión del riesgo para: cuantificarlo, contrarrestarlo y asumirlo.

- Fases del método MOSLER:

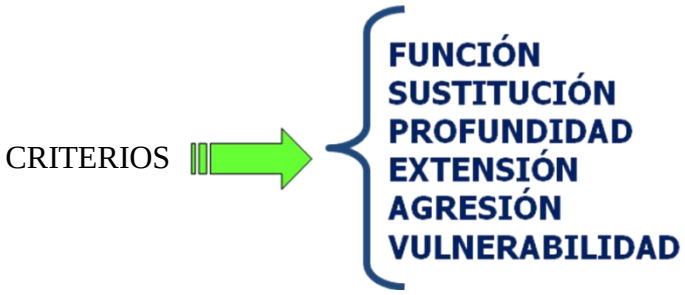
El método es de tipo secuencial y el desarrollo de las diferentes fases con las que cuenta se fundamenta en los datos y resultados obtenidos en las fases precedentes.

a) Definición del riesgo

Tiene por objeto la identificación del riesgo delimitando su contenido y alcance para diferenciarlo de otros riesgos. Se basa en la identificación específica de sus elementos característicos como son: EL BIEN y EL DAÑO

b) Análisis del riesgo

Tiene por objeto la determinación y cálculo de los criterios que, con posterioridad, facilitarán la evaluación del riesgo.



Criterio de función (F)

Se refiere a las consecuencias negativas o daños que puedan alterar o afectar a la propia actividad de la institución u organización. Se consideran cinco graduaciones:

Muy gravemente (5)

Gravemente (4)

Medianamente (3)

Levemente (2)

Muy levemente (1)

Criterio de sustitución (S)

Está referido a las dificultades que pueden tenerse para sustituir los productos o los bienes:

Muy difícilmente (5)

Difícilmente (4)

Sin mucha dificultad (3)

Fácilmente (2)

Muy fácilmente (1)

Criterio de profundidad (P)

Está referido a la perturbación y efectos psicológicos que se podrían producir como consecuencia en la propia imagen de la institución u organización:

Muy graves (5)

Graves (4)

Limitados (3)

Leves (2)

Muy leves (1)

Criterio de extensión (E)

Está referido al alcance que los daños o pérdidas pueden causar:

Internacional 5)

Nacional (4)

Regional (3)

Local (2)

Individual (1)

Criterio de agresión (A)

Muy elevada (5)

Elevada (4)

Normal (3)

Reducida (2)

Muy reducida (1)

Criterio de vulnerabilidad (V)

Está referido a la posibilidad o probabilidad de que realmente se produzcan daños o pérdidas:

Muy elevada (5)

Elevada (4)

Normal (3)

Reducida (2)

Muy reducida (1)

c) Evaluación del riesgo

Esta fase tiene por objeto cuantificar el riesgo previamente definido y analizado. Para esta evaluación se consideran tres aspectos, con sus correspondientes cálculos:

- Cálculo del carácter del riesgo (C)

Está referido al resultado obtenido de sumar la importancia del suceso (I), más los daños ocasionados (D).

$$C = I + D \quad \text{Donde} \quad I = F \times S \qquad D = P \times E$$

- Cálculo de la probabilidad (Pb)

Está referido al resultado obtenido de multiplicar el criterio de agresión (A) por el criterio de vulnerabilidad (V).

$$Pb = A \times V$$

- Cuantificación del riesgo considerado (ER)

Está referido al resultado obtenido de multiplicar los datos resultantes en el cálculo del carácter del riesgo (C) por los datos resultantes en el cálculo de la probabilidad (Pb).

$$ER = C \times Pb$$

Para un mejor entendimiento la evaluación del riesgo la resumo en el siguiente Tabla:

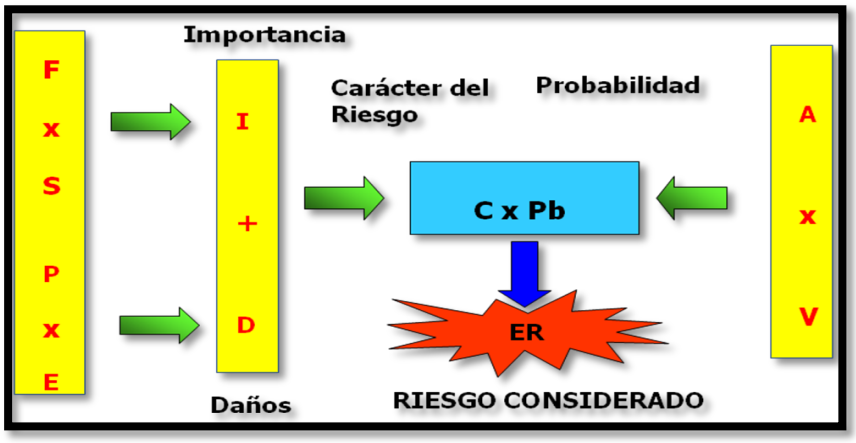


Figura Nº 17: Evaluación del riesgo
Fuente: (Duque, 2001)

d) Calculo de la clase de riesgo

Esta fase tiene por objeto clasificar el riesgo en función del valor obtenido en la evaluación del mismo. Su valor se tabulará dentro de una escala de graduación comprendida entre 2 y 1250, quedando clasificado finalmente de la manera siguiente

Tabla Nº 1:
Escala de Riesgo

VALOR ENTRE	CLASE DE RIESGO
2 y 250	Muy reducido
251 y 500	Reducido
501 y 750	Normal
751 y 1000	Elevado
1001 y 1250	Muy elevado

Fuente: Duque Arbeláez, C. (2001).

Para el análisis y evaluación del riesgo, emplearé la siguiente matriz MOSLER, en la cual me permitiré indicar la forma de cómo llenar la mencionada matriz:

Tabla Nº 2:
Escenarios de Riesgo

Nº	ESCENARIOS / RIESGOS	ESCENARIO 1							ESCENARIO 2							ESCENARIO n						
		F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR
01	Incendios																					
02	Inundaciones																					
03	Terremotos																					
04	Asaltos																					
05	Secuestros																					
06	Extorsiones																					
07	Accidentes de trabajo																					
08	Rotura de maquinaria																					
09	Grupos hostiles																					
10	Terrorismo																					
n	Otros riesgos																					

Fuente: (Montero Martínez, 1997)

- Identificado el riesgo colocarlo en la columna de la izquierda de la matriz y los escenarios en la parte superior, en forma horizontal.

- Debajo de cada escenario se colocan 7 columnas, en las 6 primeras van los criterios (F, S, P, E, A y V) y en la última la cuantificación del riesgo (CR).

2.3 MARCO CONCEPTUAL

2.3.1 Seguridad

Etimológicamente SEGURIDAD proviene del latín SECURITAS que significa calidad de seguro. Sin embargo, en el sentido semántico de la palabra, el término SEGURIDAD ampliado en su interpretación se refiere a un ambiente estable donde se presume la inexistencia de peligros, temores y daños hacia las personas y sus pertenencias. (Juan Haroldo Zamora, 2012)

Es una actividad encaminada a conseguir la protección de personas, bienes e información, ante cualquier amenaza. Para conseguir esta protección es preciso contar con medios humanos y materiales; de cuyo funcionamiento, organización y despliegue dependerá en mayor o menor grado la consecución del fin perseguido. (Juan Haroldo Zamora, 2012)

2.3.2 Seguridad física

Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Protección de instalaciones en base a barreras que permiten disuadir, detectar, denegar y defenderse de ataques, a fin de evitar o minimizar daños. Seguridad mediante barreras físicas y controles, para proteger instalaciones y lo que contengan. (Julio Díaz Estica, 2012)

2.3.3 Amenaza

Cualquier evento que de suceder afectaría a la seguridad de una persona o un bien, provocando pérdidas.

Uso sistemático de la información de la información disponible, para determinar la frecuencia con la cual pueden ocurrir eventos especificados y la magnitud de sus consecuencias. (Díaz Estica, 2012)

2.3.4 Evaluación del riesgo

Proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación del nivel de riesgo contra normas predeterminadas, niveles de riesgo objeto y otros criterios (Díaz Estica, 2012)

Proceso de evaluar el riesgo o riesgos que surgen de uno o varios peligros teniendo en cuenta la adecuación de los controles existentes, y decidir si el riesgo o riesgos son o no aceptables.

2.3.5 Factores externos

Son las fuerzas que se generan fuera de la organización, que inciden en los asuntos de control y seguridad y que deben tenerse en cuenta de manera apropiada. (Díaz Estica, 2012)

2.3.6 Factores internos

Son los aspectos de la organización que inciden en su capacidad para cumplir con la gestión de control y seguridad; incluye aspectos tales como: reorganización interna, cambio en la tecnología, cultura en materia de prevención de riesgos y modificaciones a procesos. (Díaz Estica, 2012)

2.3.7 Gestión del riesgo

Cultura, proceso y estructuras que se dirigen hacia la gestión eficaz de las oportunidades potenciales y los efectos adversos.

En materia de protección física de instalaciones, el riesgo es una condición o acto que al materializarse puede causar un daño parcial o total a una instalación o área protegida. Este daño involucra pérdida de materiales, equipos y mercancías, pérdidas de documentos importantes, fuga de información, daños a los edificios y otras áreas, daños a la integridad física de las personas que se encuentran en la instalación, daños a los sistemas de energía eléctrica y suministro de agua, fractura o rotura en las tuberías de gases, alteraciones en los sistemas de alarmas y otros dispositivos de protección. **(**Juan Haroldo Zamora, 2012).

2.3.8 Objetivos de control y seguridad

Conjunto de resultados que la organización se propone alcanzar en cuanto a su actuación en materia de control y seguridad, programados cronológicamente y cuantificados en la medida de lo posible. Organización, compañía, firma, empresa, institución o asociación, o parte o combinación de ellas, ya sea incorporada o no, pública o privada, que tiene sus propias funciones y administración. (Zamora, 2012)

2.3.9 Peligro

Es una fuente o situación con potencial de pérdidas en términos de lesiones, daño a la propiedad y/o procesos, al ambiente o una combinación de estos. (Díaz Estica, 2012)

2.3.10 Pérdida

Es la consecuencia de que suceda un riesgo (Julio Díaz Estica, 2012)

2.3.11 Proceso de Gestión del riesgo

Aplicación sistema de políticas de gestión, procedimientos y prácticas, a las tareas de establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo. (Juan Haroldo Zamora, 2012)

2.3.12 Riesgo

Posibilidad de que suceda algo que tendrá impacto en los objetivos. Se mide en términos de consecuencias y posibilidad de ocurrencia. (Juan Haroldo Zamora, 2012)

Combinación de la probabilidad de que ocurra un suceso o exposición peligrosa y la severidad del dato o deterioro de la salud que puede causar el suceso o exposición

2.3.13 Tecnología

Es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad. (Iván Escalona, 2012)

2.3.14 Control de acceso

Conjunto de actos que se realizan en la entrada de un edificio o recinto cerrado, para evitar la entrada de delincuentes, terroristas o personas indeseables, u objetos peligrosos, armas, drogas, etc., con el fin de evitar posibles ataques o situaciones de peligro, para las personas o los bienes que se encuentran en el interior. (Iván Escalona, 2012)

El control de acceso discrecional se define generalmente en oposición al control de acceso mandatorio (MAC) (algunas veces llamado control de acceso no-discrecional). A veces, un sistema en su conjunto dice tener control de acceso discrecional o puramente discrecional como una forma de indicar que carece de control mandatorio. Por otro lado, sistemas que indican implementaciones de MAC o DAC en forma simultánea, tienen DAC como una categoría de control de acceso donde los usuarios pueden pasar de uno a otro y MAC como una segunda categoría de control de acceso que impone restricciones a la primera. (Smalley, 1998)

2.3.15 Biometría

Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos (Iván Escalona, 2012)

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital. (Mapfre, 2007)

2.3.16 Circuito cerrado de televisión o CCTV

Es una tecnología de video vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. (Iván Escalona, 2012)

2.3.17 Video vigilancia IP

Es una tecnología de vigilancia visual que combina los beneficios analógicos de los tradicionales CCTV (Circuito Cerrado de Televisión) con las ventajas digitales de las redes de comunicación IP (Internet Protocol), permitiendo la supervisión local y/o remota de imágenes y audio así como el tratamiento digital de las imágenes, para aplicaciones como el reconocimiento de matrículas o reconocimiento facial entre otras. (Iván Escalona, 2012)

2.4 MARCO LEGAL

2.4.1 CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

Art. 66.- "Se reconoce y garantizará a las personas:

3. El derecho a la integridad personal, que incluye:

a) La integridad física, psíquica, moral y sexual.

b) Una vida libre de violencia en el ámbito público y privado. El Estado adoptará las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia, en especial la ejercida contra las mujeres, niñas, niños y

adolescentes, personas adultas mayores, personas con discapacidad y contra toda persona en situación de desventaja o vulnerabilidad; idénticas medidas se tomarán contra la violencia, la esclavitud y la explotación sexual." (Constitución de la República del Ecuador, 2008)

Art. 83.-"Son deberes y responsabilidades de las ecuatorianas y los ecuatorianos, sin perjuicio de otros previstos en la Constitución y la ley:

4. Colaborar en el mantenimiento de la paz y de la seguridad.

Art. 393.-"El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos". (Constitución de la República del Ecuador, 2008)

La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno.

2.4.2 LEY DE SEGURIDAD PÚBLICA Y DEL ESTADO

La creación y aprobación de esta ley que actualmente está en plena vigencia, proporciona la base legal y el contexto jurídico como plataforma que posibilita el empleo de los medios y métodos para las tareas de seguridad,

toda vez que las unidades militares al ser parte de Fuerzas Armadas tienen una institucionalidad fundamentada en el cumplimiento y respeto de la ley.

De lo anterior se desprende que es necesario considerar algunos artículos de la Ley de Seguridad Pública y del Estado que sustentan el desarrollo e implementación de proyectos, estudios e investigaciones en esta materia que hoy por hoy es uno de los temas fundamentales de los ejes de gobernabilidad de nuestro país y constituye también uno de los Objetivos Nacionales Permanentes del Estado Ecuatoriano.

Art. 1.- Del objeto de la ley.- "La presente ley tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado.

El Estado protegerá a las ecuatorianas y a los ecuatorianos que residan o estén domiciliados en el exterior, conforme lo previsto en la Constitución de la República, los tratados internacionales y la ley.

Art. 3.- "De la garantía de seguridad pública.- Es deber del Estado promover y garantizar la seguridad de todos los habitantes, comunidades,

pueblos, nacionalidades y colectivos del Ecuador, y de la estructura del Estado, a través del Sistema de Seguridad Pública y del Estado, responsable de la seguridad pública y del Estado con el fin de coadyuvar al bienestar colectivo, al desarrollo integral, al ejercicio pleno de los derechos humanos y de los derechos y garantías constitucionales."

Art. 9.- "Del Ministerio de Coordinación de Seguridad o quien haga sus veces.- El Ministerio de Coordinación de Seguridad o quien haga sus veces, es el responsable de la elaboración de las políticas públicas, la planificación integral y la coordinación de los organismos que conforman el Sistema de Seguridad Pública y del Estado, así como también el seguimiento y evaluación de las acciones aprobadas en materia de seguridad

Art. 23.- "De la seguridad ciudadana.- La seguridad ciudadana es una política de Estado, destinada a fortalecer y modernizar los mecanismos necesarios para garantizar los derechos humanos, en especial el derecho a una vida libre de violencia y criminalidad, la disminución de los niveles de delincuencia, la protección de víctimas y el mejoramiento de la calidad de vida de todos los habitantes del Ecuador.

Con el fin de lograr la solidaridad y la reconstitución del tejido social, se orientará a la creación de adecuadas condiciones de prevención y control de la delincuencia; del crimen organizado; del secuestro, de la trata de personas; del contrabando; del coyoterismo; del narcotráfico, tráfico de armas, tráfico

de órganos y de cualquier otro tipo de delito; de la violencia social; y, de la violación a los derechos humanos.

Se privilegiarán medidas preventivas y de servicio a la ciudadanía, registro y acceso a información, la ejecución de programas ciudadanos de prevención del delito y de erradicación de violencia de cualquier tipo, mejora de la relación entre la policía y la comunidad, la provisión y medición de la calidad en cada uno de los servicios, mecanismos de vigilancia, auxilio y respuesta, equipamiento tecnológico que permita a las instituciones vigilar, controlar, auxiliar e investigar los eventos que se producen y que amenazan la ciudadanía.

Art. 45.- "De la Participación ciudadana.- La ciudadanía podrá ejercer su derecho de participación en el Sistema de Seguridad Pública, de conformidad con lo prescrito en la Constitución, las normas legales de participación ciudadana y control social, de modo individual u organizado, en los procesos de definición de las políticas públicas y acciones de planificación, evaluación y control para los fines de la presente ley...

Son deberes y responsabilidades de las ecuatorianas y ecuatorianos colaborar con el mantenimiento de la paz y la seguridad

2.4.3 PLAN NACIONAL DE SEGURIDAD INTEGRAL, AÑO 2011

El Gobierno de la Revolución Ciudadana, inscrito en el proceso de consolidación de la Unión de Naciones Suramericanas (UNASUR) y ratificando su postura radical al cambio estructural de la política regional de seguridad, asume la responsabilidad de construir una Seguridad con Enfoque Integral, que responda a un diagnóstico propio de la problemática del país.

El enfoque integral hace referencia al sentido de un Sistema Integrado de Seguridad, que abarca todos los ámbitos del ser humano y del Estado, sin dejar nada al azar. Tiene que ver con la integración de todas las esferas de la seguridad, las mismas que complementan y se integran en un solo sistema, el Sistema de Seguridad Pública y del Estado.

Allí encontramos la seguridad internacional, la seguridad interna, la Defensa Nacional, la seguridad económica, la soberanía alimentaria, la seguridad ambiental, entre otras

La seguridad con Enfoque Integral, es la condición que tiene por finalidad garantizar y proteger los derechos humanos y las libertades de ecuatorianas y ecuatorianos, la gobernabilidad, la aplicación de la justicia, el ejercicio de la democracia a solidaridad, la reducción de vulnerabilidades, la prevención, protección, respuesta y remediación ante riesgos y amenazas.

A diferencia de los conceptos tradicionales de seguridad cuya razón de ser era el Estado, este nuevo enfoque sitúa al ser humano como eje principal y

transversal, incorporando a la ciudadanía como actor protagónico de los procesos de seguridad individual y colectiva

Este alcance integral, recoge la visión multidimensional de la seguridad que incluye a las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos de la seguridad. Además incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social; y se basa en valores democráticos: el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y la soberanía nacional

Este nuevo enfoque que el Ecuador inicia, también está en concordancia con los conceptos de Seguridad Humana, los mismos que desde hace más de una década han venido debatiéndose y desarrollándose en este nuevo paradigma de la seguridad centrada en el Ser Humano. La Seguridad Humana, es la condición necesaria para la subsistencia y calidad de vida de las personas y sociedades y sus componentes abarcan la seguridad económica, la seguridad alimentaria, la seguridad sanitaria, la seguridad ambiental, la seguridad política, la seguridad comunitaria y la seguridad personal, dándole justamente al ser humano atención a todas sus necesidades para su bienestar.

La seguridad es un derecho fundamental de los ecuatorianos y el Estado es responsable de su pleno ejercicio. La seguridad no es un fin en sí mismo, sino un medio para conseguir un fin.

En cuanto a la seguridad estatal, el Ecuador promueve el modelo de Seguridad Cooperativa en lugar del modelo de Seguridad Colectiva que prevaleció durante la Guerra Fría y que fue impulsado por los Estados Unidos mediante el Tratado Interamericano de Asistencia Recíproca TIAR, así como los postulados de la Doctrina Monroe que señalaba "América para los Americanos", doctrina que se orientaba a proteger a los Estados del Nuevo Mundo contra la intervención europea, y se constituía en una forma de intervención de los EE.UU en América Latina y el Caribe.

La Seguridad Cooperativa, es un nuevo modelo de seguridad que tiene sus orígenes en la permanente búsqueda del hombre por lograr concebir un sistema internacional que garantice la seguridad de los Estados Naciones en sus relaciones con el resto de los actores internacionales.

La Seguridad Cooperativa busca alcanzar la seguridad por medio del consentimiento institucionalizado entre los actores internacionales involucrados en el sistema, en lugar de que entre ellos se utilice la amenaza o uso de la fuerza coercitiva para subsanar sus diferencias. Supone que los objetivos de seguridad de los socios han sido identificados como comunes y compatibles, pudiéndose establecer relaciones de cooperación entre ellos para alcanzarlos.

La Seguridad Cooperativa emplea varios mecanismos, estrategias y procedimientos para cumplir sus propósitos de prevenir conflictos como: la cooperación en diferentes ámbitos, las Medidas de Confianza Mutua, la Diplomacia Preventiva, la limitación y transparencia en los gastos militares, el compromiso de no utilizar la fuerza para resolver los conflictos, es decir, tiene una naturaleza preactiva y preventiva, buscando en todo momento que la escalada del conflicto dentro de su espectro no llegue a la crisis, diferenciándose de esta manera de la forma reactiva.

Figura Nº 18: Ámbitos de la seguridad con enfoque integral
Fuente: (Plan Nacional de Seguirdad Integral)

2.4.4 REGLAMENTO GENERAL DE INSPECCIONES DEL EJERCITO, AÑO 1981

Fue creado con la finalidad de contar con un Instrumento Normativo que respalde en el cumplimiento de la misión de la Inspectoría General del

Ejército, en el cual oriente sus diversas funciones y actividades. Así como también que permita dar disposiciones generales para canalizar adecuadamente el sistema de inspecciones a fin de que, a través de ellas, el Comandante General del Ejército obtenga la información y los elementos de juicio que son imprescindibles cuando deban tomarse las decisiones a solucionar los problemas y satisfacer las necesidades existentes.

Art. 2. Son objetivos de las inspecciones:

1. Observar y verificar el cumplimiento de las leyes, decretos, resoluciones, reglamentos, directivas, disposiciones, órdenes y normas vigentes, en las unidades y repartos del Ejército;
2. Propender a que las unidades y repartos del ejército alcancen y mantengan el máximo grado de preparación y alistamiento para cumplir exitosamente las misiones impuestas;
3. Corregir oportunamente las fallas, errores y omisiones que se hubiera detectado;
4. Atender y resolver los problemas detectados;
5. Otorgar estímulos o imponer sanciones, de acuerdo con el desempeño de las funciones y la obtención de las calificaciones correspondientes; y,
6. Contribuir al mantenimiento y perfeccionamiento de la unidad de doctrina.

2.4.5 MANUAL DE NORMAS DE SEGURIDAD TERRESTRE, AÉREA, FLUVIAL E INDUSTRIAL DE LA F.T.

El presente Manual tiene el propósito de establecer normas y procedimientos de seguridad para todo el personal de la Fuerza Terrestre, tendientes a la eliminación de riesgos innecesarios y como consecuencia, evitar que los accidentes se produzcan.

El objetivo es el de establecer normas y procedimientos específicos de seguridad a seguirse en todas y cada una de las funciones y actividades cotidianas, operacionales, de instrucción o de trabajo para prevenir riesgos innecesarios y/o accidentes o minimizar sus efectos cuando estos se produzcan, a fin de concientizar a todo el personal de la F.T. creando en ellos un estado mental en el cual el desempeño de sus actividades se base en el empleo y utilización de las normas, procedimientos y medidas de prevención expuestas en el presente manual.

CAPÍTULO III

3.1 METODOLOGÍA DE INVESTIGACIÓN

En el presente trabajo investigativo es necesario realizar un análisis de datos, en base a encuestas que permitirá obtener un Tabla de frecuencias, el cual ayudará a observar las tendencias con relación a los porcentajes obtenidos, y determinar las respectivas conclusiones y recomendaciones, además se obtendrá los criterios de los Directivos del Fuerte Militar a través de las entrevistas realizadas, datos que contribuirán al desarrollo del tema.

3.1.1 Ubicación Geográfica del Proyecto de Investigación

El Fuerte Militar donde se desarrollará el estudio de investigación, se encuentra ubicado en la Provincia Cotopaxi, ciudad de Latacunga, al sur de la parroquia Guaytacama, Av. Panamericana, Km 12 1/2. Vía a Quito.

3.1.2 Identificación de variables/categorías a Utilizar en el Proceso Investigativo

VARIABLE INDEPENDIENTE: Tecnología aplicada a sistemas de video vigilancia y control de accesos

VARIABLE DEPENDIENTE: Seguridad física

3.1.3 Tipo de Investigación

En este proyecto se aplicaran los siguientes tipos de investigación que a continuación se mencionan:

Investigación de campo.- "Es la que se realiza con la presencia del investigador o científico en el lugar de concurrencia del fenómeno". (Tamayo, M, 1990)

Esta se aplicó al momento en que la investigación se realizó para la obtención de la información mediante instrumentos de investigación aplicados al personal en el lugar de los hechos.

Investigación documental.- "Es la actividad humana realizada para descubrir el conocimiento o solucionar un problema, al utilizar los documentos escritos o representativos como medio para lograr tal fin". (Tena, R, 1995)

Esta investigación se utilizó al momento de emplear documentación referente al tema para contribuir a la investigación.

3.1.4 Métodos de Investigación

Para lograr el cumplimiento de los objetivos en el estudio se determinó la vía adecuada, para lo cual se consideró los siguientes métodos:

Método Deductivo:

"La deducción, tanto si es axiomática como matemática, puede emplearse de manera que facilite el análisis estadístico y el contraste. Sin embargo, el deductivismo implica que la estadística y el conocimiento empírico es tan transitorio que no vale la pena y que un primer análisis deductivo puede proporcionar una mejor comprensión de un determinado fenómeno" (Pheby, 1988).

Este método se aplicó en el análisis de la información obtenida en forma general para llegar a un criterio más particular que contribuyo al desarrollo de este estudio.

Método científico:

"El método científico es "el estudio sistemático, controlado, empírico y crítico de proposiciones hipotéticas acerca de presuntas relaciones entre varios fenómenos" (Kerlinger, 1990).

Este método se empleó para el fundamento de las bases teóricas, empleando los conocimientos científicos biblioFiguras necesarios para el estudio de investigación.

3.1.5 Técnicas de Investigación

Entrevistas

"Son medios directos de investigación cara a cara, entrevistador – entrevistado, con el mismo objeto, determinar aquellas exigencias de capacitación sentidas y manifestadas por las personas objeto de estudio. En cierto momento se pueden constituir como un sistema de prueba del instrumento anterior, cuando éste resultó incompleto o hay que confirmar una serie de detalles" (Kerlinger, 1990)

En este caso se empleó una entrevista estructurada mediante un cuestionario escrito donde se recopilo toda la información requerida.

La entrevista se aplicara a los Comandantes, Jefes de Estado Mayor y Jefes Departamentales

Encuestas:

"Técnica de investigación que permitirá la recolección de información, a través de cuestionarios que serán elaborados de acuerdo a los requerimientos del estudio" (Kerlinger, 1990)

Estas se aplicaran a los oficiales, voluntarios y servidores públicos del

Fuerte Militar Patria, con el fin de obtener información real y confiable

3.1.6 Población y Muestra

Población: "La población es un conjunto de individuos de la misma clase, limitada por el estudio". Según Tamayo y Tamayo, (1997)

En el presente estudio de investigación, la población referencial (Brigada Patria y Grupo), según su ubicación y en coherencia con los objetos la constituyen: Directivos (14), Oficiales (70) voluntarios operativos (1050) y otros (23).

La población se estableció considerando al personal que está vinculado con el tema del proyecto.

Muestra: "La muestra es la que puede determinar la problemática porque es capaz de generar los datos con los cuales se identifican las fallas dentro del proceso". (Tamayo, T. Y Tamayo, 1997)

En este caso como la población supera las 30 personas investigadas, se requiere aplicar la fórmula para obtener la muestra.

$$n = \frac{m}{e^2(m-1)+1}$$

n = x (tamaño de la muestra)

m = tamaño de la población

e = 0.05 (error admisible)

Tabla Nº 3:
Población y Muestra

SUJETOS A ESTUDIO	POBLACIÓN	MUESTRA	PORCENTAJES
Directivos	14	14	**3,25%**
Oficiales	70	59	**16,94%**
Voluntarios operativos	1050	289	**72,16%**
Otros	23	23	**7,66%**
TOTAL	**1157**	**385**	**100,00%**

3.2 Evaluación de resultados y discusión

3.2.1 Encuesta Aplicada al Personal de Oficiales, Voluntarios y Otros del Fuerte Militar

Tabla Nº 4:
Estadísticos Evaluación de Preguntas

		TIPO	EDAD	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
N	Válidos	371	371	371	371	371	371	371	371	371	371
	Perdidos	0	0	0	0	0	0	0	0	0	0
Media		1,9030	1,7062	2,4771	2,2749	1,0512	1,0162	3,2803	10,2722	8,6954	1,0323
Mediana		2,0000	2,0000	2,0000	2,0000	1,0000	1,0000	2,0000	10,0000	7,0000	1,0000

Moda	2,00	2,00	2,00	1,00	1,00	1,00	1,00	10,00	7,00	1,00
Desv. típ.	,46063	,71466	2,64910	1,70370	,22073	,14615	2,29149	6,66891	6,53816	,17715
Varianza	,212	,511	7,018	2,903	,049	,021	5,251	44,474	42,748	,031
Rango	2,00	3,00	32,00	10,00	1,00	2,00	7,00	27,00	26,00	1,00
Suma	706,00	633,00	919,00	844,00	390,00	377,00	1217,00	3811,00	3226,00	383,00

3.2.2 Distribución del Personal Fuerte Militar

Tabla Nº 5:
Personal del Fuerte Militar

TIPO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	OFICIALES	59	15,9	15,9	15,9
	VOLUNTARIOS	289	77,9	77,9	93,8
	OTROS	23	6,2	6,2	100,0
	Total	371	100,0	100,0	

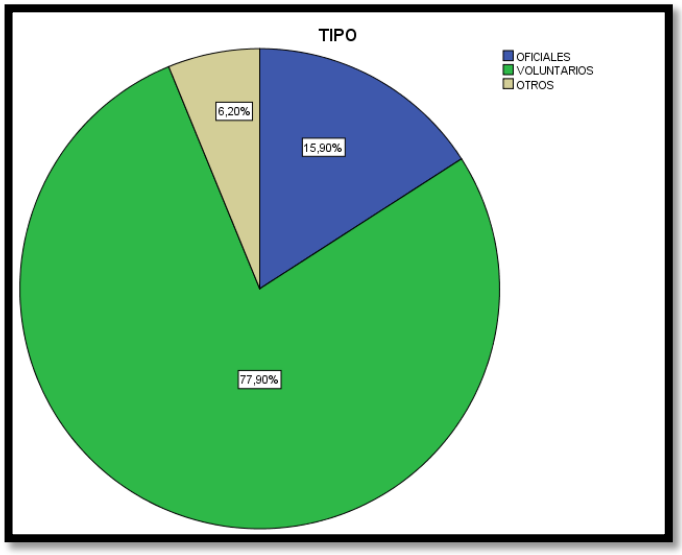


Figura Nº 19: Personal del Fuerte Militar

Análisis e Interpretación

En el Tabla Nº 5 y Figura Nº 20 se evidencia que, el 77,9% de los encuestados corresponden a los voluntarios, el 15,9% a los oficiales y el 6,2% corresponden a otro personal que labora en el fuerte militar, lo que determina que el criterio de la población más extensa determina las tendencias.

3.2.3 Edad

Tabla Nº 6:
Edad

EDAD

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	20-30	161	43,4	43,4	43,4
	31-40	162	43,7	43,7	87,1
	41-50	44	11,9	11,9	98,9
	51 - +	4	1,1	1,1	100,0
	Total	371	100,0	100,0	

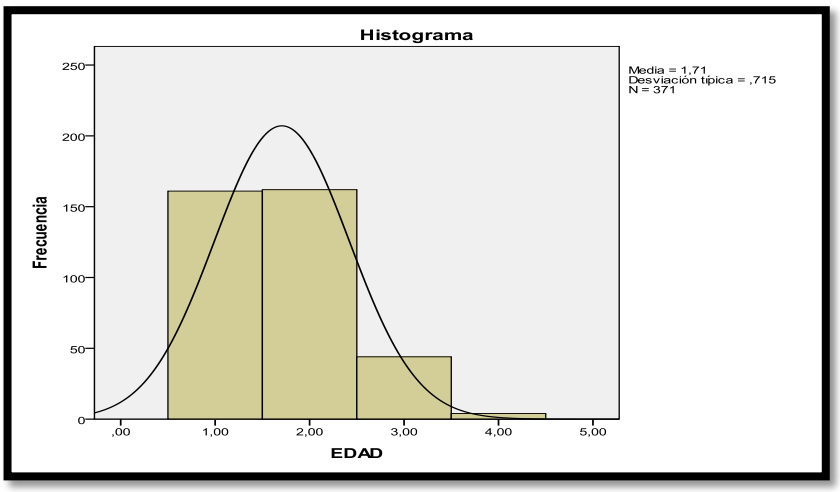


Figura Nº 20: Edad

Análisis e Interpretación

En el Tabla Nº 6 y Figura Nº 21 se puede identificar que, el 43,4% el rango de edades de los encuestados es de 20-30 años, el 43,1% el rango de edades de los encuestados es de 31-40 años, el 11,9% el rango de edades de los encuestados es de 41-50 y el 1,1% de rango de edades de los encuestados es de 51 años y más, lo que determina que en el Fuerte Militar el personal que se encuentra vinculado de forma directa a la seguridad, está entre los grados de oficiales de subtenientes a capitanes y en el personal de voluntarios de soldados a cabos primeros.

3.2.4 Análisis por Pregunta

1. Considera Ud. que el nivel de seguridad física en el Fuerte Militar es

Tabla Nº 7:
Pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	ALTO	27	7,3	7,3	7,3
	MEDIO	250	67,4	67,4	74,7
	BAJO	94	25,3	25,3	100,0
	Total	371	100,0	100,0	

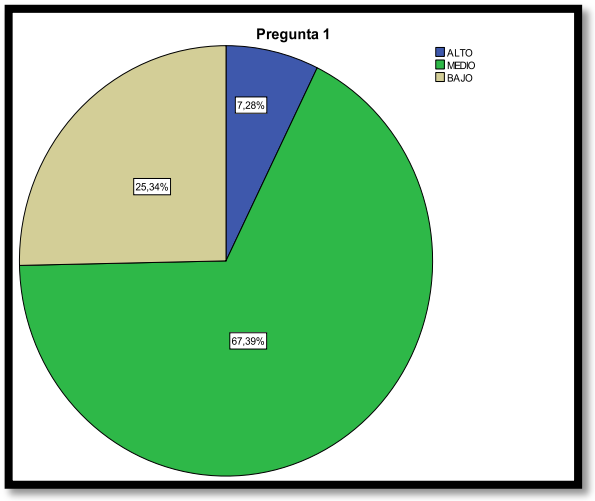


Figura Nº 21: Pregunta 1

Análisis e Interpretación

Se puede establecer que el nivel de seguridad física en el Fuerte Militar es medio con un 67,4% y bajo con un 25,3% lo que determina que existen debilidades a donde se debe orientar medidas correctivas que permitan mejorar el sistema de seguridad empleado.

2. Cuál cree Ud. que es el mayor problema de seguridad física en el Fuerte Militar

Tabla Nº 8:
Pregunta 2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A	162	43,7	43,7	43,7
	B	104	28,0	28,0	71,7

	C	25	6,7	6,7	78,4
	D	46	12,4	12,4	90,8
	a,b	14	3,8	3,8	94,6
	a,c	11	3,0	3,0	97,6
	b,d	2	,5	,5	98,1
	Otros	2	,5	,5	98,7
	a,d	2	,5	,5	99,2
	b,c	2	,5	,5	99,7
	a,b,c,d	1	,3	,3	100,0
	Total	371	100,0	100,0	

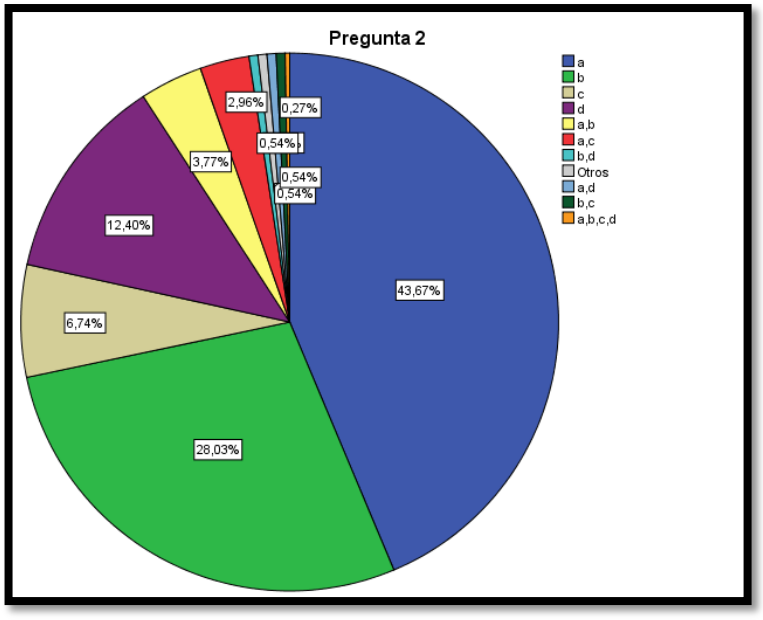


Figura Nº 22: Pregunta 2

Análisis e Interpretación

En el Tabla Nº 8 y Figura Nº 23 se evidencia que el 43,7% responden el literal a) control de acceso, 28,0% el literal b) perdida de bienes, 12,4% el literal d) falta de elementos probatorios, 3,8% el literal a) y b) (control de acceso y perdida de bienes), 3% el literal a) y c) (control de acceso y fuga de información), 5% el literal a), b), c), otros y d) (control de acceso , perdida de bienes, fuga de información y falta de elementos probatorios) y el 3% el literal(control de acceso , perdida de bienes, fuga de información y falta de elementos probatorios).

Se puede establecer que el mayor problema de seguridad es el control de acceso con un 43,7%, seguido por la pérdida de bienes con un 28,0%, falta de elementos probatorios con un 12,4% y con el 3% la fuga de información, lo que determina que en el Fuerte Militar no se dispone de un excelente control de acceso a las áreas críticas, efecto por el cual se han producido perdidas de bienes y fuga de información, sin disponer de elementos probatorios.

3. Considera Ud. que las herramientas y equipos tecnológicos mejorarán la seguridad física en el Fuerte Militar

Tabla Nº 9:
Pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	352	94,9	94,9	94,9
	NO	19	5,1	5,1	100,0
	Total	371	100,0	100,0	

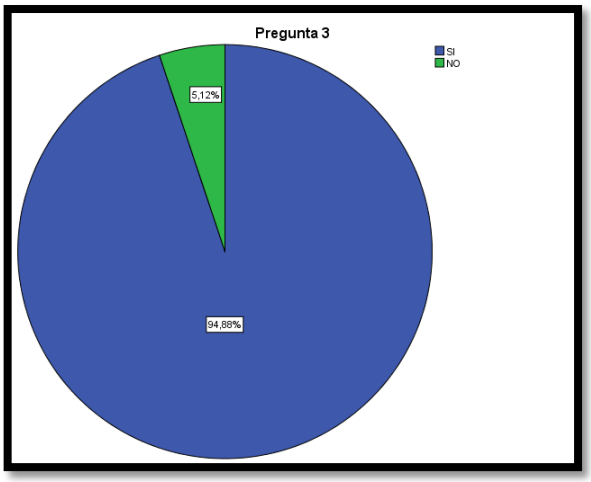


Figura Nº 23: Pregunta 3

Análisis e Interpretación

En el Tabla Nº 9 y Figura Nº 24 se evidencia que el 94,9% responden en forma afirmativa y el 5,1% responden en forma negativa.

Se puede establecer que las herramientas y equipos tecnológicos de seguridad mejorarán la seguridad física del Fuerte Militar

4. **Qué efecto considera Ud. que tendría la implementación de sistemas tecnológicos en la seguridad del Fuerte Militar**

Tabla Nº 10:
Pregunta 4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	POSITIVO	366	98,7	98,7	98,7
	NEGATIVO	4	1,1	1,1	99,7
	SIN EFECTO	1	,3	,3	100,0
	Total	371	100,0	100,0	

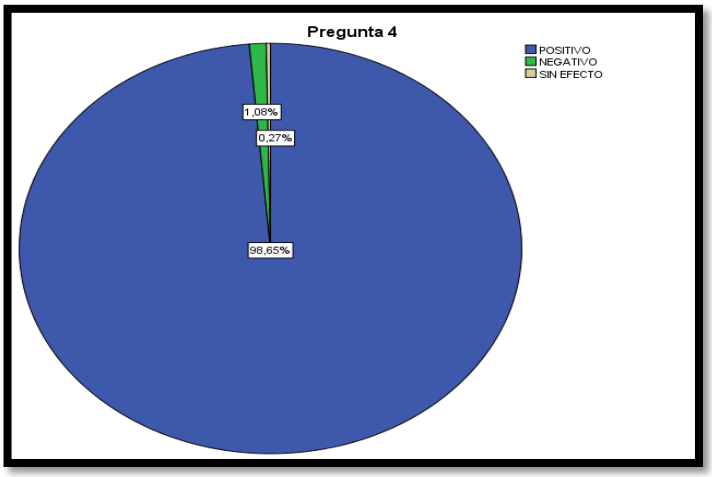


Figura Nº 24: Pregunta 4

Análisis e Interpretación

El Tabla Nº 10 y Figura Nº 25 se evidencia que el 98,7% responden en forma positiva, el 1,1% responden en forma negativa y el 0,3% responden sin efecto.

Se puede establecer que la implementación de sistemas tecnológicos tendrá un efecto positivo en la seguridad física del Fuerte Militar, porque mejorara el nivel de seguridad.

5. **Señale dentro de los sistemas de seguridad abajo propuesto, cuales pueden mejorar la seguridad física del Fuerte Militar, de acuerdo a la prioridad**

Tabla Nº 11:
Pregunta 5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A	133	35,8	35,8	35,8
	B	68	18,3	18,3	54,2
	C	15	4,0	4,0	58,2
	D	6	1,6	1,6	59,8
	a,b	59	15,9	15,9	75,7
	a,c	52	14,0	14,0	89,8
	a,b,c	32	8,6	8,6	98,4
	b,c	6	1,6	1,6	100,0
	Total	371	100,0	100,0	

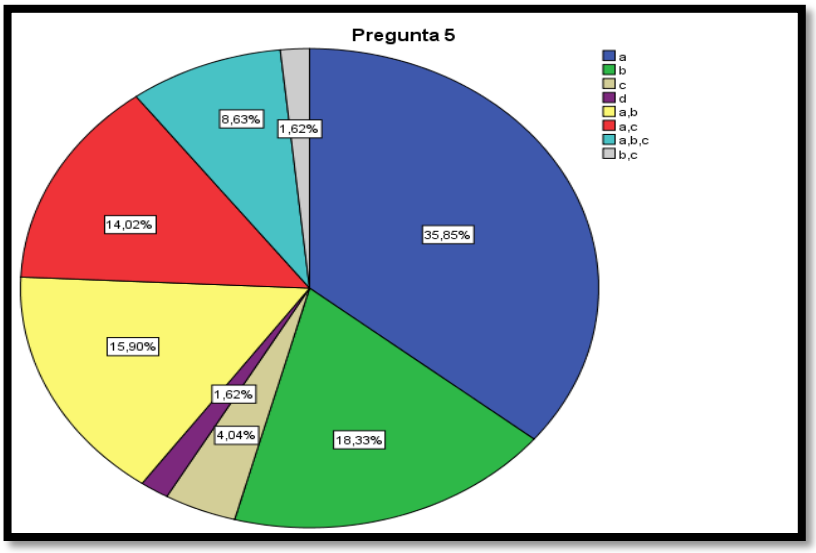


Figura Nº 25: Pregunta 5

Análisis e Interpretación

El Tabla Nº 9 y Figura Nº 6 se evidencia que el 35,8% responden el literal a) video vigilancia, el 18,3% el literal b) control de acceso, el 15,9% el literal a) y b) (video vigilancia y control de acceso), el 14% el literal a) y c) (video vigilancia y alarma), 8,6% el literal a), b) y c) (video vigilancia, control de acceso y alarmas) y el 1,6% b), c) y d) (control de acceso , alarmas y otros.

Se puede establecer que los sistemas con mayores frecuencias que mejoran la seguridad física son la video vigilancia, el control de acceso y alarmas; lo que evidencia que es necesario que el Fuerte Militar disponga de un sistema integrado de seguridad compuesto por los sistemas antes señalados.

6. Cuales considera que son las áreas críticas del Fuerte Militar

Tabla Nº 12:
Pregunta 6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A	51	13,7	13,7	13,7
	B	4	1,1	1,1	14,8
	C	26	7,0	7,0	21,8
	D	22	5,9	5,9	27,8
	E	7	1,9	1,9	29,6
	F	1	,3	,3	29,9
	G	14	3,8	3,8	33,7
	H	4	1,1	1,1	34,8
	a,d	16	4,3	4,3	39,1
	a,c,d	68	18,3	18,3	57,4
	a,c	18	4,9	4,9	62,3
	a,b,c,d	33	8,9	8,9	71,2
	c,e	2	,5	,5	71,7
	b,c	11	3,0	3,0	74,7
	a,g	8	2,2	2,2	76,8
	a,d,g	13	3,5	3,5	80,3
	c,d	24	6,5	6,5	86,8
	b,e,g	3	,8	,8	87,6
	c,g	6	1,6	1,6	89,2
	c,d,e,g	10	2,7	2,7	91,9
	b,d	5	1,3	1,3	93,3
	a,b	6	1,6	1,6	94,9
	d,g	2	,5	,5	95,4
	a,b,c	7	1,9	1,9	97,3
	b,c,d	4	1,1	1,1	98,4
	Todas las anteriores	1	,3	,3	98,7
	a,c,d,g	4	1,1	1,1	99,7
	a,e	1	,3	,3	100,0

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A	51	13,7	13,7	13,7
	B	4	1,1	1,1	14,8
	C	26	7,0	7,0	21,8
	D	22	5,9	5,9	27,8
	E	7	1,9	1,9	29,6
	F	1	,3	,3	29,9
	G	14	3,8	3,8	33,7
	H	4	1,1	1,1	34,8
	a,d	16	4,3	4,3	39,1
	a,c,d	68	18,3	18,3	57,4
	a,c	18	4,9	4,9	62,3
	a,b,c,d	33	8,9	8,9	71,2
	c,e	2	,5	,5	71,7
	b,c	11	3,0	3,0	74,7
	a,g	8	2,2	2,2	76,8
	a,d,g	13	3,5	3,5	80,3
	c,d	24	6,5	6,5	86,8
	b,e,g	3	,8	,8	87,6
	c,g	6	1,6	1,6	89,2
	c,d,e,g	10	2,7	2,7	91,9
	b,d	5	1,3	1,3	93,3
	a,b	6	1,6	1,6	94,9
	d,g	2	,5	,5	95,4
	a,b,c	7	1,9	1,9	97,3
	b,c,d	4	1,1	1,1	98,4
	Todas las anteriores	1	,3	,3	98,7
	a,c,d,g	4	1,1	1,1	99,7
	a,e	1	,3	,3	100,0
	Total	371	100,0	100,0	

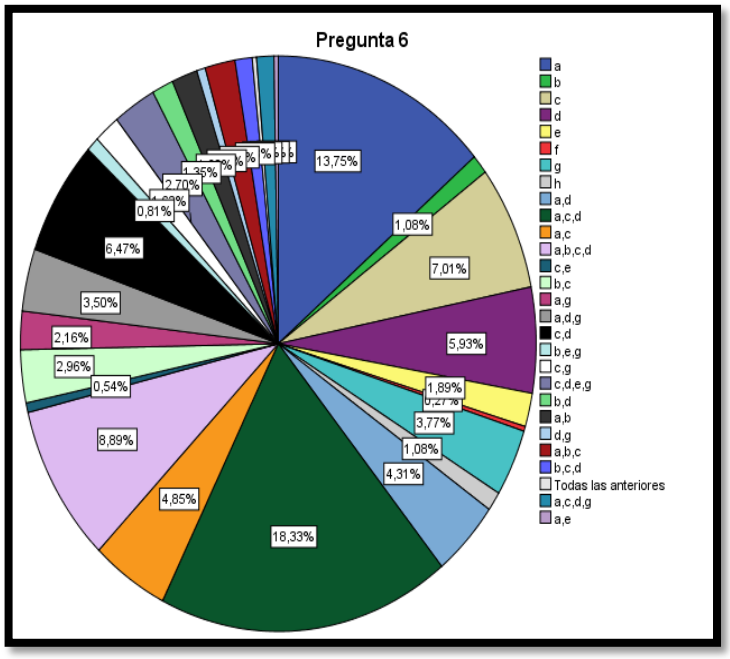


Figura Nº 26: Pregunta 6

Análisis e Interpretación

En el Tabla Nº 12 y Figura Nº 27 se evidencia que el 18,3% responden el literal a), c) y d) (oficinas, refugio de explosivos y complejo de bodegas del CAL), el 13,7% el literal a) oficinas, el 8,9% el literal a), b), c) y d) (oficinas, gasolinera, refugio de explosivos y complejo de Bodegas de CAL), el 7% el literal c) refugio de explosivos, el 6,5% el literal c) y d), el 5,9% el literal d) complejo de bodegas del CAL, el 4,9% del literal a) y c) (oficinas y refugio de explosivos) , el 4,3% del literal a) y d) (oficinas y complejo de bodegas del CAL), el 3,8% del literal g) dormitorios, el 3,5% del literal a), d) y g) (oficinas, complejo de bodegas del Cal y dormitorios), el 2,7 % literales c), d), e) y g) (refugio de explosivos, complejo de bodegas del Cal y dormitorios), el 2,2% literal a) y g) (oficinas y dormitorios), el 1,9% del

literal a), b) y c) (oficinas, gasolinera y refugio de explosivos), el 1,6% del literal c) y g) (refugio de explosivos y dormitorios), el 1,1% del literal b), c), d) y h) (gasolinera, refugio de explosivos, complejo de bodegas del CAL y dormitorios), el 0,5% del literal c), d) e) y g) (refugio de explosivos, complejo de bodegas del CAL, cocinas y comedor y dormitorios) y el 0,3% todas las opciones.

Se puede establecer que las principales áreas críticas del Fuerte Militar son oficinas, refugio de explosivos, complejo de bodega del CAL, gasolinera y dormitorios, por lo que es necesario mayor atención en el desarrollo de la propuesta, a fin de mejorar el nivel de seguridad física.

Tabla Nº 13:
Pregunta 7

Desde su conocimiento, en cuál de las siguientes áreas , existen mayores incidentes contra la seguridad en el Fuerte Militar

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	a	60	16,2	16,2	16,2
	b	8	2,2	2,2	18,3
	c	22	5,9	5,9	24,3
	d	36	9,7	9,7	34,0
	e	16	4,3	4,3	38,3
	f	3	,8	,8	39,1
	g	64	17,3	17,3	56,3
	h	20	5,4	5,4	61,7
	a,d	19	5,1	5,1	66,8
	a,e	7	1,9	1,9	68,7
	a,b,c,d	12	3,2	3,2	72,0
	b,e	3	,8	,8	72,8
	b,g	2	,5	,5	73,3

	b,c	3	,8	,8	74,1
	a,g	9	2,4	2,4	76,5
	c,d	14	3,8	3,8	80,3
	d,g	35	9,4	9,4	89,8
	a,c	8	2,2	2,2	91,9
	a,c,d	7	1,9	1,9	93,8
	a,d,,f,g	6	1,6	1,6	95,4
	a,b	5	1,3	1,3	96,8
	c,g	1	,3	,3	97,0
	b,d	1	,3	,3	97,3
	a,d,g	3	,8	,8	98,1
	g,h	1	,3	,3	98,4
	c.g	3	,8	,8	99,2
	c,d,g	3	,8	,8	100,0
	Total	371	100,0	100,0	

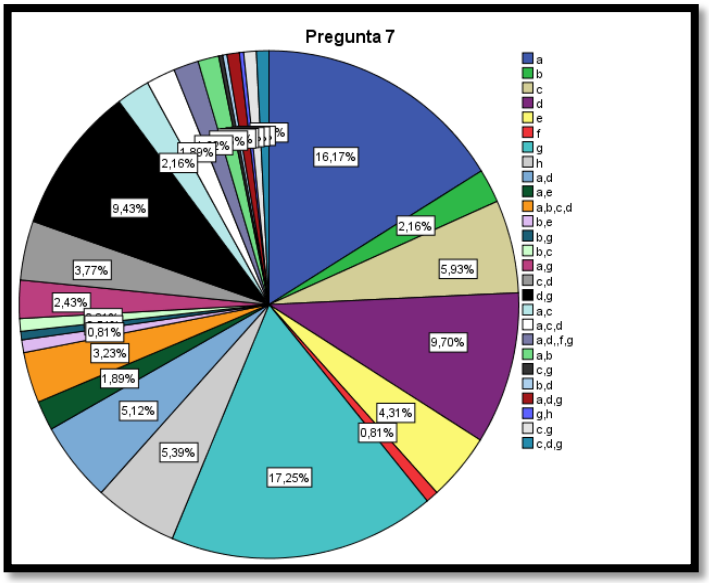


Figura Nº 27: Pregunta 7

Análisis e Interpretación

El Tabla Nº 11 y Figura Nº 8se evidencia que el 17,3% responden el literal g) dormitorios, el 16,2% el literal a) oficinas, el 9,7% el literal d) complejo de bodegas del CAL, el 5,9% el literal c) refugio de explosivos, el 5,4% el literal h) otras, el 5,1% del literal a) y d) (oficinas y complejo de bodegas del Cal, 4,3% del literal e) cocina y comedor, el 3,8% del literal c) y d) (refugio de explosivos y complejo de bodegas del CAL, el 3,2% del literal a), b), c) y d) (oficinas, gasolinera, refugio de explosivos y complejo de bodegas del Cal), el 2,4% del literal a) y g) (oficinas y dormitorios), el 2,2% del literal a), b) y c) (oficinas, gasolinera y refugio de explosivos), el 1,9% del literal a), c), d) y e) (oficinas, refugio de explosivos, complejo de bodega del Cal y cocinas y comedor), el 1,6% del literal a), d) f) y g) (oficina, complejo de bodega de Cal, casino y áreas de esparcimiento y dormitorios), el 1,3% del literal a) y b) (oficinas y gasolinera),el 0,8% del literal a), b), c), d), e), g) y f) (oficinas, gasolinera, refugio de explosivos, complejo de bodegas del Cal, cocinas y comedor; y casino y áreas de esparcimiento), el 0,5% del literal b) y g) (gasolinera y dormitorios) y el 0,3% del literal b), c), d) g), h) (gasolinera, refugio de explosivos, complejo de bodega del Cal, dormitorios y otras).

Se puede establecer que las áreas donde existen mayor índice de incidentes es: dormitorios, oficinas, complejo de bodegas del CAL, refugio de explosivos y cocina; lo cual determina que el Fuerte Militar debe mejorar la seguridad en estas áreas para reducir los niveles de inseguridad.

7. **Considera Ud. que la implementación de un centro de control integrado de seguridad tecnológica para monitoreo respuesta ante amenazas, permitirá una seguridad integral en el Fuerte Militar**

Tabla Nº 14:
Pregunta 8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	359	96,8	96,8	96,8
	NO	12	3,2	3,2	100,0
	Total	371	100,0	100,0	

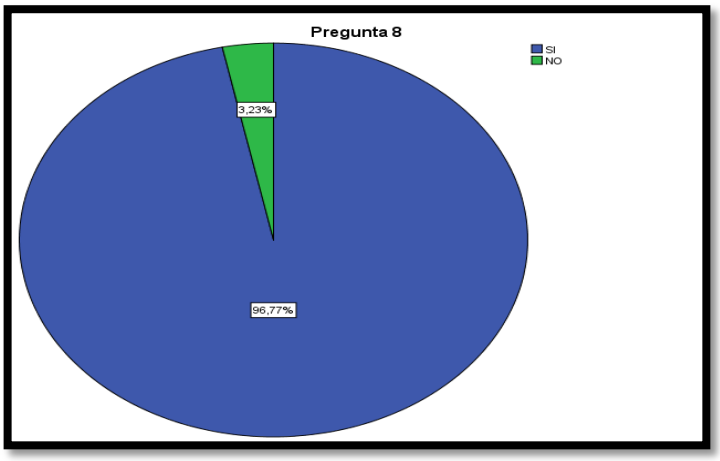


Figura Nº 28: Pregunta 8

Análisis e Interpretación

El Tabla Nº 12 y Figura Nº 9 se evidencia que el 96,8% responden en forma afirmativa y el 3,3% manifiesta su criterio de una forma negativa.

Se puede establecer que la implementación de un centro de control integrado de seguridad tecnológica para monitoreo y respuesta de amenazas, es fundamental para mejorar el nivel de seguridad física del Fuerte Militar, lo cual permitirá disminuir la cantidad de personal en los puestos de guardia y contribuir al bienestar del personal de tal formar de que se encuentren en condiciones óptimas para el cumplimiento de las misiones fundamentales y subsidiarias.

8. Según su criterio que tipo de repercusiones conllevaría la implementación de un sistema de video vigilancia y control de acceso para las áreas corticas del Fuerte Militar

El tipo de repercusiones que mencionan los encuestados es:

- Minimizar los índices de inseguridad
- Incrementar la confianza del personal
- Disminuir los índices de perdidas
- Identifica las personas que se sustraen los bienes
- Mantener una reacción rápida en una emergencia
- Mayor control del personal del Fuerte Militar
- Control de las áreas sensibles
- Mayor control de las instalaciones
- Mayor bienestar para el personal que labora en el Fuerte Militar

3.3 Comprobación de Hipótesis

3.3.1 Interrelación en las Encuestas Aplicadas

Tablas de contingencia

Tabla Nº 15:
Tabla de Contingencia Pregunta 5

Tabla de contingencia TIPO * Pregunta 5

Recuento

		Pregunta 5								
		a	B	c	d	a,b	a,c	a,b,c	b,c	Total
TIPO	OFICIALES	20	5	1	2	3	8	18	2	59
	VOLUNTARIOS	109	47	14	4	54	43	14	4	289
	OTROS	4	16	0	0	2	1	0	0	23
Total		133	68	15	6	59	52	32	6	371

Tabla Nº 16:
Prueba Chi cuadrado pregunta 5

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	92,421[a]	14	,000
Razón de verosimilitudes	73,270	14	,000
Asociación lineal por lineal	13,978	1	,000
N de casos válidos	371		

a. 12 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,37.

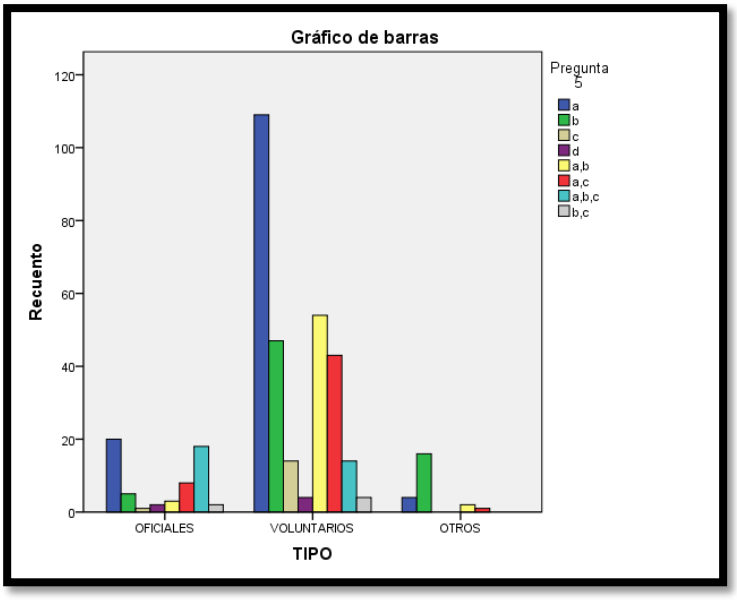


Figura Nº 29: Interrelación entre pregunta 5

Análisis e Interpretación

La tabla de chi- cuadrado de la relación entre el tipo y la pregunta 5, donde se determinó que el grado de asociación de las variables Sig astigmática es 0,00 comprobándose las hipótesis Ho y Hi, por lo tanto se estableció que existe asociación entre variables.

Tablas de contingencia

Tabla Nº 17:
Tabla de Contingencia Pregunta 6

Tabla de contingencia TIPO * Pregunta 6

		Pregunta 6																																Total
		a	b	c	d	e	f	g	h	a, d	a, c, d	a, c	a, b, c, d	c, e	b, c	a, g	a, d, g	c, d	b, e, g	c, g	c, d, e, g	b, d	a, b	d, g	a, b, c	b, c, d	Todas las anteriores	a, c, d, g	a, e					
TIPO	OFICIALES	1	2	1	2	0	0	5	0	3	30	1	0	0	0	2	4	1	0	0	2	0	0	0	0	1	0	4	0					59
	VOLUNTARIOS	33	2	25	20	4	1	9	4	13	36	17	33	2	11	6	9	23	3	6	8	5	6	2	7	3	1	0	0					289
	OTROS	17	0	0	0	3	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1					23
Total		51	4	26	22	7	1	14	4	16	68	18	33	2	11	8	13	24	3	6	10	5	6	2	7	4	1	4	1					371

Tabla Nº 18:
Prueba Chi cuadrado pregunta 6

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	213,798[a]	54	,000
Razón de verosimilitudes	180,033	54	,000
Asociación lineal por lineal	14,268	1	,000
N de casos válidos	371		

a. 66 casillas (78,6%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,06.

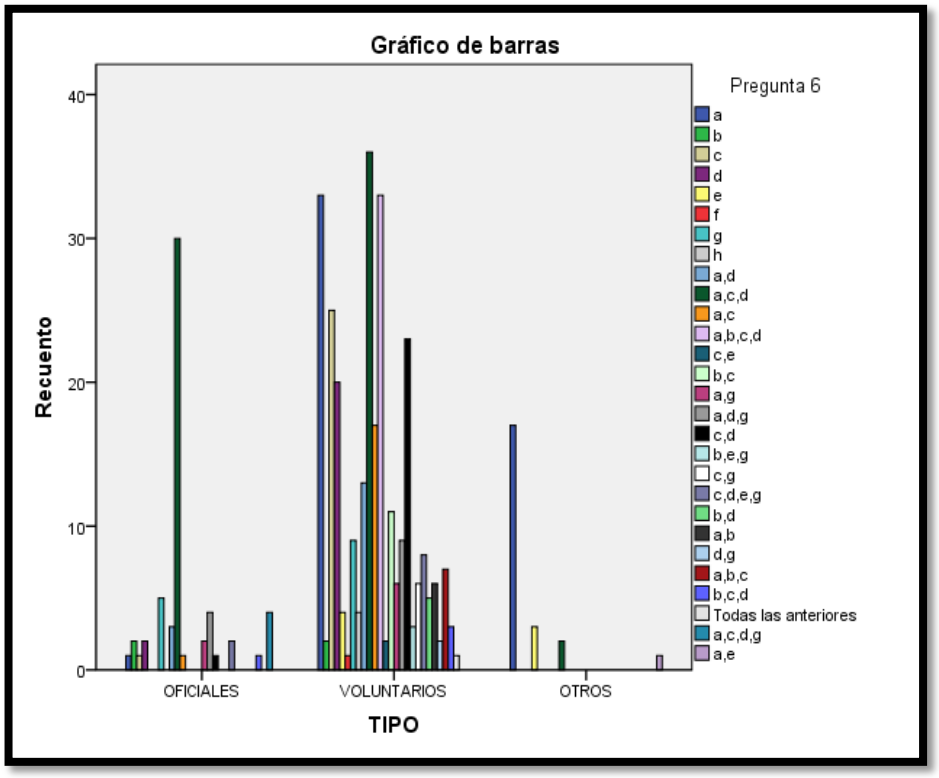


Figura Nº 30: Interrelación entre pregunta 6

Análisis e Interpretación

La tabla de chi- cuadrado de la relación entre el tipo y la pregunta 6, donde se determinó que el grado de asociación de las variables Sig astigmática es 0,00 comprobándose las hipótesis Ho y Hi, por lo tanto se estableció que existe asociación entre variables.

Tablas de contingencia

Tabla Nº 19:

Tabla de contingencia Pregunta 1

Tabla de contingencia TIPO * Pregunta 1

Recuento

		Pregunta 1			
		ALTO	MEDIO	BAJO	Total
TIPO	OFICIALES	1	51	7	59
	VOLUNTARIOS	26	196	67	289
	OTROS	0	3	20	23
Total		27	250	94	371

Pruebas de chi-cuadrado
Tabla Nº 20:
Prueba Chi cuadrado pregunta 1

	Valor	Gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	57,864[a]	4	,000
Razón de verosimilitudes	52,981	4	,000
Asociación lineal por lineal	18,190	1	,000
N de casos válidos	371		

Tabla de contingencia TIPO * Pregunta 1

Recuento

		Pregunta 1			
		ALTO	MEDIO	BAJO	Total
TIPO	OFICIALES	1	51	7	59
	VOLUNTARIOS	26	196	67	289
	OTROS	0	3	20	23

a. 2 casillas (22,2%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,67.

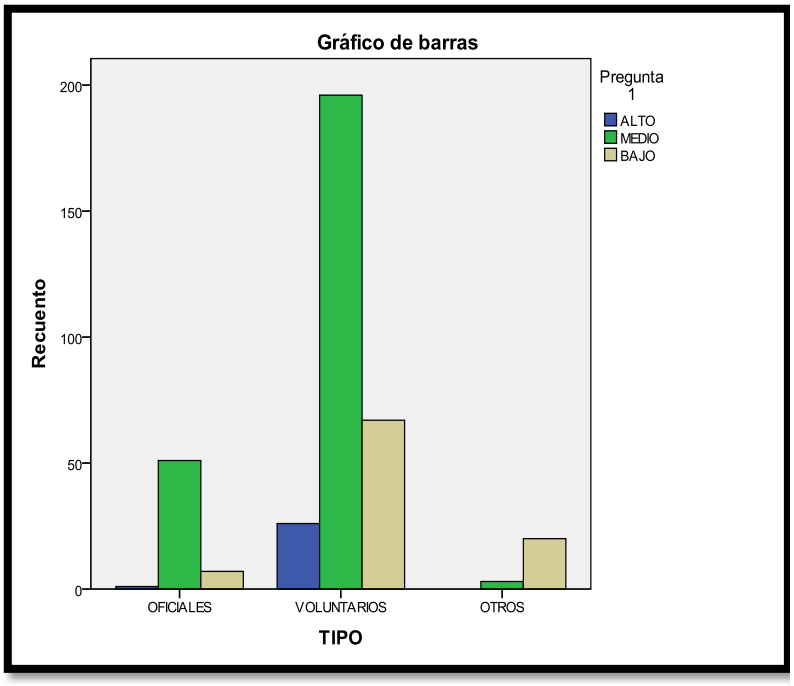


Figura Nº 31: Interrelación entre pregunta 1

Análisis e Interpretación

La tabla de chi- cuadrado de la relación entre el tipo y la pregunta 1, donde se determinó que el grado de asociación de las variables Sig astigmática es 0,00 comprobándose las hipótesis Ho y Hi, por lo tanto se estableció que existe asociación entre variables.

3.4 Operacionalización de las variables

3.4.1 Variable Independiente

Tabla Nº 21:
Variable Independiente

Variables	Definición	Categorización	Indicadores	Técnicas Instrumentos
Tecnología aplicada a sistemas de video vigilancia y control de accesos	Es la instalación, adecuación y funcionamiento de equipo tecnológico de video vigilancia, sistemas de control de accesos por reconocimiento facial, biométrico, reconocimiento de placas vehiculares, sensores y demás instrumentos que tiendan a evitar la ocurrencia de eventos de inseguridad, eventos de pérdidas, acceso no autorizado.	Tecnología aplicada a la seguridad física	▪ Equipamiento y sistema de seguridad física ▪ Sistema de control de accesos ▪ Sistemas de video vigilancia	▪ Encuesta ▪ Entrevista

3.4.2 Variable Dependiente

Tabla Nº 22:
Prueba Chi cuadrado pregunta 1

Variables	Definición	Categorización	Indicadores	Técnicas Instrumentos
Seguridad física	Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información calificada.	Seguridad física	▪ Identificación de peligros y riesgos ▪ Procedimientos ▪ Identificación de áreas críticas o sensibles ▪ Estructura del Sistema Integrado de Seguridad ▪ Normativas y leyes	▪ Entrevista ▪ Encuestas

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- De los encuestados en el Fuerte Militar el 43,4% que se encuentra en el rango de 20 – 30 años de edad; el 43,1% se encuentra en el rango de edades de los 31 a 40 años, lo que establece que en el Fuerte Militar el personal que se encuentra vinculado de forma directa a la seguridad, está entre los grados en oficiales de subtenientes a capitanes y en el personal de voluntarios de soldados a sargentos primeros.

- Se establece que el nivel de seguridad en el Fuerte Militar es medio de acuerdo a los resultados obtenidos de un 67,4% y el 25,3% bajo, lo que determina que existen debilidades a donde se deben orientar medidas correctivas que permitan mejorar el sistema de seguridad empleado.

- El mayor problema de seguridad física en el Fuerte Militar, se encuentra en el control de acceso con el 43, 7%, seguida de la pérdida de bienes con un porcentaje de 28,0% y la falta de elementos probatorios con el 12,4%, lo que determina que en el Fuerte Militar no se dispone de un excelente control de acceso a las áreas críticas, efecto por el cual se han producido perdidas de bienes y fuga de información, sin disponer de elementos probatorios.

- Los encuestados manifiestan que las herramientas y equipos tecnológicos mejorarán la seguridad física con un porcentaje de opinión del 94,9%.

- La implementación de sistemas tecnológicos de seguridad es positiva dado un porcentaje que es de 98,7%.

- Los sistemas que mejoraran la seguridad física son la video vigilancia, el control de acceso y alarmas; lo que evidencia que es necesario que el Fuerte Militar disponga de un sistema integrado de seguridad.

- Las áreas más críticas de seguridad física según los encuestados son con un 18,3% las oficinas, refugio de explosivos y complejo de bodegas del CAL, con un 13,7% son las oficinas, con 8,9% mencionan que son las oficinas, gasolineras, refugio de explosivos y complejo de bodegas del CAL y el 3,8% los dormitorios. por lo que es necesario una mayor atención de estas áreas en el desarrollo de la propuesta, a fin de mejorar el nivel de seguridad física.

- Las áreas que poseen mayor número de incidentes son: con un 17,3% dormitorios, el 16,2% las oficinas, el 9,7% el complejo de bodegas del CAL, el 4,3% cocina y comedor, con el 3,8% refugio de explosivos y complejo de bodegas del CAL.

- La implementación de un centro de control integrado de seguridad tecnológica para monitoreo y respuesta ante una amenaza es positiva, ya que contribuirá a una seguridad integral de acuerdo al criterio emitido por los encuestados en un porcentaje del 96,8% y permitirá utilizar el talento humano en sus actividades específicas.

- La implementación de un sistema de video vigilancia y control de acceso, según el criterio de los encuestados apoyara en forma positiva en:

    - Minimizar los índices de inseguridad
    - Incrementar la confianza del personal
    - Disminuir los índices de perdidas
    - Identifica las personas que se sustraen los bienes
    - Mantener una reacción rápida en una emergencia
    - Mayor control del personal del Fuerte Militar
    - Control de las áreas sensibles
    - Mayor control de las instalaciones
    - Mayor bienestar para el personal que labora en el Fuerte Militar

4.3 Recomendaciones

- La seguridad física en el Fuerte Militar es medio, sin embargo existe un porcentaje significativo de inseguridad, por lo que es necesario adoptar medidas de seguridad física empleando los medios tecnológicos.

- Que se analice el trabajo de investigación realizado y su propuesta, a fin de que con el mejor criterio esto sea puesto en ejecución, como una prueba piloto que luego de ser analizado su utilidad pueda ser aplicado a los demás Fuertes Militares.

- Que se capacite al personal del departamento del SIS (Sistema Integrado de Seguridad), acerca del uso de los medios tecnológicos, cuando se inicie la implementación de este proyecto, a fin de que se obtengan los resultados deseados.

- Que las autoridades del Fuerte Militar contribuyan en la ejecución de la propuesta, determinando lineamientos y políticas relacionadas con el ámbito de seguridad física.

- Que se incluya en el presupuesto anual los recursos necesarios para la implementación de este proyecto considerando principalmente la adquisición de los medios tecnológicos requeridos.

CAPITULO V

5. PROPUESTA

5.1 Tema

“Propuesta de gestión de riesgos y su tratamiento mediante la aplicación de instrumentos tecnológicos que contribuyan a la seguridad física del Fuerte Militar.”

5.2 Introducción

Uno de los importantes conceptos de seguridad en este siglo, es la prevención y por consiguiente deberían realizarse los esfuerzos físicos y presupuestarios para desplegar en forma racional toda medida encaminada a minimizar los riesgos y precautelar de esta manera los recursos humanos y materiales de las organizaciones, teniendo como guía el proceso de gestión de riesgos, lo que permitirá que la organización y/o empresa realice su trabajo cotidiano de una forma normal, permitiendo que su productividad sea más elevada y con resultados positivos para la misma, tanto en el nivel administrativo como en el operativo que forman parte activa de una institución

Eventos adversos que ocasionan consecuencias negativas a una empresa da resultados y consecuencias negativas por lo que se tiene que:

- Implementar procedimientos y recursos especiales.

- Garantizar una respuesta oportuna y eficaz.
- diseñar la aplicación efectiva de medios tecnológicos aplicados a la seguridad física, como apoyo a la gestión de riesgos tendiente a:

  - Prevenir
  - Minimizar
  - Evitar

  } Pérdidas

Tener una cultura del Riesgo establecida en todos los niveles de la Organización es una cuestión básica, en la que deben estar involucrados todos los miembros de una empresa pública y/o privada, desde el primer empleado hasta el último, y por supuesto, dentro de la Alta Dirección que tiene que impulsar este reto como uno de los objetivos alcanzables y medibles.

Todo esto lo podemos lograr teniendo como base un sistema de seguridad que integre la parte humana y la tecnología aplicada en medios de video vigilancia y control de accesos que permitan optimizar el empleo del recurso humano en las tareas esenciales de la organización.

Sin la cooperación y el compromiso de los usuarios, las medidas de seguridad son un ejercicio inútil, además de un gasto innecesario de dinero.

Es necesario resaltar que los equipos tecnológicos por sí solos no son una solución de seguridad y que sin la operación adecuada y la interpretación

derivada de un análisis de seres humanos capacitados en seguridad, no representan un aporte significativo.

El Fuerte Militar al momento cuenta con una seguridad totalmente humana, ligeramente ayudada por alarmas en determinados puntos sensibles específicos, lo cual ha demostrado ser ineficaz, pues en el contexto general se han seguido suscitando incidentes de perdidas, accesos no autorizados y lo que es más la inexistencia de elementos probatorios que permitan esclarecer los incidentes y determinar responsabilidades reales o presuntas. Además al no estar integrados adecuadamente los sistemas de alarma y respuesta no permiten una reacción oportuna ante los eventos que se susciten.

Los hechos noticiosos que suceden diariamente a nuestro alrededor involucran directa o indirectamente al tema de la seguridad. Actualmente existe la necesidad de contar con esquemas seguros a todo nivel para poder mantener una vida tranquila, sana, alegre, es decir sin problemas.

En este contexto, la presente propuesta constituye una alternativa de solución para minimizar los riesgos a través de un sistema integrado de video vigilancia y control de accesos para el Fuerte Militar, con características tecnológicas actuales que adecuadamente instaladas permitirán desde un centro de mando y control vigilar y grabar mediante video en forma permanente lo que ocurra o deje de ocurrir en las áreas sensibles, a la vez que hace posible disparar las alarmas a fin de que la fuerza de reacción (equipo de respuesta), acuda a tomar procedimiento en tiempo real.

5.3 Justificación e Importancia

La importancia de realizar esta propuesta alternativa está relacionada con mejorar la seguridad física, identificando los riesgos más frecuentes de las áreas críticas para que de esta manera se pueda implementar las medidas preventivas orientadas a la aplicación de un sistema de video vigilancia y control de acceso.

En tal virtud es importante que el Fuerte Militar, disponga de un sistema de video vigilancia y control de accesos, que contribuya a mejorar los niveles de seguridad física.

Además el presente propuesta alternativa es importante para el Fuerte Militar porque permitirá:

- Disminuir, disuadir, impedir y detectar los índices de pérdidas de bienes y eventos llevados a cabo tanto por personal interno como externo a la institución.
- Actualizar y mejorar las medidas de seguridad establecidas en los planes, considerando los medios tecnológicos respectivos cuyas evidencias servirán como elementos probatorios de los actos ilícitos para determinar responsabilidades.

- Detectar el acceso a las áreas críticas e identificar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones correctivas con la mayor brevedad posible.
- Dar un ambiente de confianza y tranquilidad para quienes laboran en la institución.

5.4 Objetivos

5.4.1 Objetivo General

Gestionar los riesgos del Fuerte Militar y su tratamiento mediante la aplicación de instrumentos tecnológicos que contribuyan a la seguridad física.

5.4.2 Objetivos Específicos

- Establecer el contexto, mediante la determinación de la estructura organizacional, misión, diagnostico de seguridad y la determinación de las fortalezas, debilidades, amenazas y oportunidades de la seguridad física del Fuerte Militar.

- Identificar los riesgos principales que puedan afectar la seguridad de las personas, instalaciones, bienes, documentos e información del fuerte Militar.

- Analizar y evaluar los riesgos identificados mediante la utilización del Método Mosler.

- Diseño de un sistema integrado de video vigilancia y control de accesos para el Fuerte Militar.

5.5 Ámbito de Aplicación

La presente propuesta alternativa será aplicada en el ámbito de la seguridad Física del Fuerte Militar, con especial atención a las áreas críticas determinadas en el proceso de investigación.

CAPITULO VI

6. ESTABLECIMIENTO DEL CONTEXTO

6.1 Organización

El Fuerte Militar, tiene la siguiente estructura organizacional:

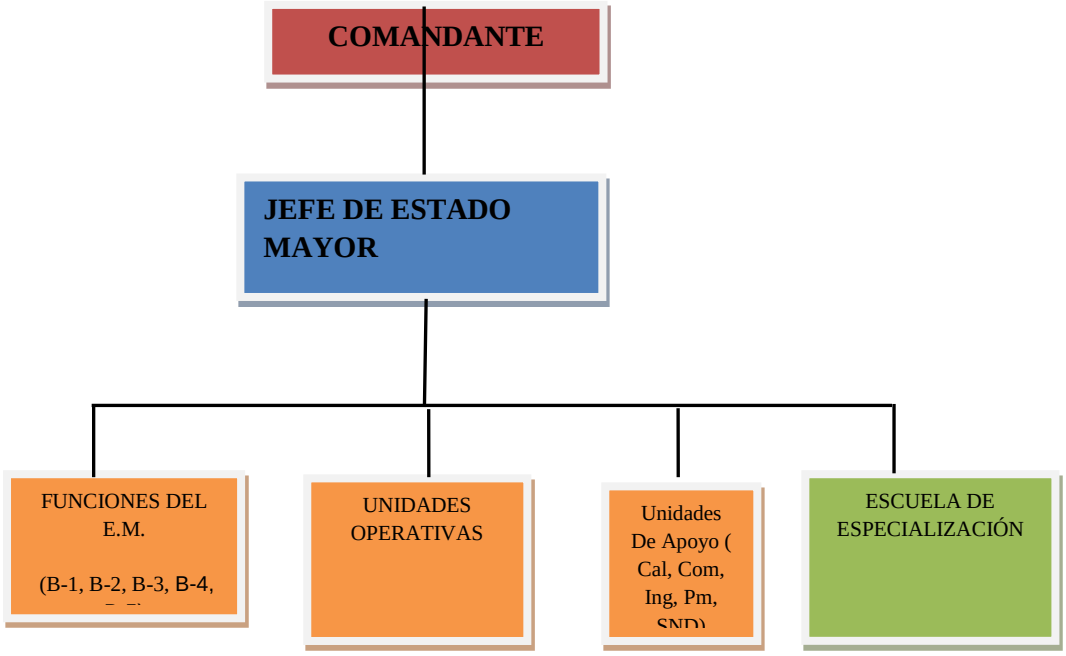


Figura Nº 32: Organigrama organizacional

6.2 Misión del Fuerte

Por tratarse de una unidad militar se recomienda no expresar la misión para fines de seguridad.

6.3 Diagnóstico de seguridad

Con parte del proceso investigativo se llegó a las siguientes conclusiones en cuanto a seguridad:

- Que el nivel de seguridad en el Fuerte Militar es medio de acuerdo a los resultados obtenidos de un 67,4% y el 25,3% bajo, lo que determina que existen debilidades a donde se deben orientar medidas correctivas que permitan mejorar el sistema de seguridad empleado.

- El mayor problema de seguridad física en el Fuerte Militar, se encuentra en el control de acceso con el 43, 7%, seguida de la pérdida de bienes con un porcentaje de 28,0% y la falta de elementos probatorios con el 12,4%, lo que determina que en el Fuerte Militar no se dispone de un excelente control de acceso a las áreas críticas, efecto por el cual se han producido perdidas de bienes y fuga de información, sin disponer de elementos probatorios

- Las áreas más críticas de seguridad física según los encuestados son con un 18,3% las oficinas, refugio de explosivos y complejo de bodegas del CAL, con un 13,7% son las oficinas, con 8,9% mencionan que son las oficinas, gasolineras, refugio de explosivos y complejo de bodegas del CAL y el 3,8% los dormitorios. por lo que es necesario una mayor

atención de estas áreas en el desarrollo de la propuesta, a fin de mejorar el nivel de seguridad física.

- Las áreas que poseen mayor número de incidentes son: con un 17,3% dormitorios, el 16,2% las oficinas, el 9,7% el complejo de bodegas del CAL, el 4,3% cocina y comedor, con el 3,8% refugio de explosivos y complejo de bodegas del CAL.

- La implementación de sistemas tecnológicos de seguridad es positiva dado un porcentaje que es de 98,7%.

- Los sistemas que mejoraran la seguridad física son la video vigilancia, el control de acceso y alarmas; lo que evidencia que es necesario que el Fuerte Militar disponga de un sistema integrado de seguridad.

- La implementación de un centro de control integrado de seguridad tecnológica para monitoreo y respuesta ante una amenaza es positiva, ya que contribuirá a una seguridad integral de acuerdo al criterio emitido por los encuestados en un porcentaje del 96,8% y permitirá utilizar el talento humano en sus actividades específicas.

- La implementación de un sistema de video vigilancia y control de acceso, según el criterio de los encuestados apoyara en forma positiva en:
  - Minimizar los índices de inseguridad
  - Incrementar la confianza del personal

- Disminuir los índices de perdidas
- Identifica las personas que se sustraen los bienes
- Mantener una reacción rápida en una emergencia
- Mayor control del personal del Fuerte Militar
- Control de las áreas sensibles
- Mayor control de las instalaciones
- Mayor bienestar para el personal que labora en el Fuerte Militar

6.4 Análisis FODA

Tabla Nº 23:
Matriz de Factores Internos

METODO FODA					
MATRIZ DE FACTORES INTERNOS					
FACTORES	FORTALEZA / DEBILIDAD	PESO 100%	CALIFICACIÓN 1 a 4	PONDERACIÓN	OBSERVACIÓN
APOYO DE LA DIRECCIÓN	F	15	3	0,45	
CAPACITACIÓN EN SEGURIDAD	F	10	3	0,30	
SEGURIDAD FISICA (VIGILANCIA ARM	F	10	2	0,20	
PLANES DE DEFENSA, CONTRAINCENDIOS Y EVACUACIÓN	F	10	3	0,30	
PLAN DE PREVENCIÓN DE RIESGOS	D	15	1	0,15	
PROCEDIMIENTOS EN SEGURIDAD	D	10	2	0,20	
POLÍTICAS	D	10	2	0,20	
COMUNICACIÓN Y DIFUSIÓN	D	12	2	0,24	
SEGURIDAD ELECTRÓNICA	D	8	2	0,16	
				2,20	DEBILIDAD
TOTAL		100			
TOTAL DE PONDERACIÓN =	PONDERACION > 2,50 FORTALEZA				
	PONDERACION < 2,50 DEBILIDAD				

Tabla Nº 24:
Matriz de Factores Externos

METODO FODA					
MATRIZ DE FACTORES EXTERNOS					
FACTORES	OPORTUNIDADES/ AMENAZAS	PESO 100%	CALIFICACIÓN 1 a 4	PONDERACIÓN	OBSERVACIÓN
SITUACION DE INSEGURIDAD	A	20	1	0,20	
DELINCUENCIA	A	30	1	0,30	
IMPUNIDAD	A	10	2	0,20	
LEGISLACIÓN EN SEGURIDAD	O	9	4	0,36	
PROFESIONALIZACIÓN DE LA SEGURIDAD	O	6	3	0,18	
ACCESO A TECNOLOGÍA	O	8	3	0,24	
RECURSOS PARA PROYECTO	O	9	4	0,36	
REALACIÓN CON AUTORIDADES LOCALES	O	8	3	0,24	
				2,08	AMENAZA
TOTAL		100			

Del análisis realizado podemos determinar que existe en el Fuerte Militar, debilidades y amenazas, hacia las cuales se debería orientar el mayor esfuerzo por parte del mando, para mantener poder influir sobre los factores antes mencionados.

6.5 Escenarios

De la investigación realizada se puede determinar que las áreas críticas, donde se realizará la intervención como parte de la presente propuesta alternativa son:

- Oficinas
- Complejo de Bodegas
- Refugio de explosivos
- Dormitorios

6.6 Identificación de los Peligros

Sabotaje

El sabotaje es una acción deliberada dirigida a debilitar a un enemigo mediante la subversión, la obstrucción, la interrupción o la destrucción de material.

Destruir, inutilizar, desaparecer de cualquier modo, dañar herramientas, bases de datos, soportes lógicos, instalaciones, comités o materias primas, con el fin de suspender o paralizar el trabajo.

Incendio

Son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad.

Pérdida de bienes

Es un delito contra el patrimonio, personal e institucional, consistente en el apoderamiento de bienes ajenos, con intención de lucrarse, empleando para ello la fuerza, violencia o intimidación en el caso de un robo; o el aprovechamiento de un descuido del propietario o custodio del bien en el caso de un hurto. Son precisamente estas dos modalidades de ejecución las que

diferencian los dos tipos de delito, quedando a la sana critica del juez competente la discriminación en base a los elementos probatorios.

Pérdida de información

La pérdida de información sin una correcta planificación e implementación de medidas de seguridad, podría requerir de una alta inversión en tiempo e incluso dinero para su recuperación, y eso siempre y cuando sea posible ya que no siempre lo es, o por lo menos no totalmente. La disponibilidad de la información es fundamental para el correcto desarrollo de su actividad diaria.

Intrusión

Introducción en una propiedad, lugar, asunto o actividad sin tener derecho o autorización para ello. Pudiendo ser ejecutada por intrusos de la misma organización y externos.

Asalto

Un delito caracterizado por violencia contra las personas, generalmente con fines de apoderamiento ilegítimo (por ejemplo, asalto a mano armada).

6.7 Análisis Y Evaluación

Se efectuó un análisis de riesgos dentro del cual se busca establecer los diferentes niveles a que puede estar expuesto el Fuerte Militar; éste fue realizado con un método matricial (*MOSSLER*) basado en criterios de medición definidos lo cual es un proceso matemático y objetivo.

La fórmula con la que se evalúa los riesgos arroja un puntaje de 2 a 1250 puntos. El siguiente Tabla muestra los rangos y porcentajes empleados para asignar la clasificación de riesgo:

Tabla Nº 25:
Clasificación de riesgo

RIESGO	RANGO
BAJO	**2 – 200**
MEDIO	**201 – 600**
ALTO	**601 -1250**

Tabla Nº 26:
Clasificación de riesgo por áreas

	Escenario	OFICINAS							CONPLEJO DE BODEGAS							REFUGIO DE EXPLOSIVOS							DORMITORIOS							MAYOR RIESGO
No	Riesgo	F	S	P	E	A	V	CR1	F	S	P	E	A	V	CR2	F	S	P	E	A	V	CR3	F	S	P	E	A	V	CR3	
1	Sabotaje	4	4	4	5	4	4	576	5	5	4	5	4	4	720	5	5	4	5	3	5	675	4	4	4	5	4	5	720	2691,00
2	Incendio	4	4	4	4	4	4	512	5	5	4	5	4	4	720	5	5	4	5	3	5	675	4	4	4	5	4	5	720	2627,00
3	Perdida de Bienes	3	3	4	2	5	5	425	4	5	4	4	5	5	900	4	5	4	4	5	5	900	4	5	4	4	5	5	900	3125,00
4	Perdida de Información	4	4	4	4	5	4	640	3	3	3	2	4	5	300	3	3	3	2	4	5	300	2	3	3	2	4	5	240	1480,00
5	Intrusión	4	3	4	2	5	5	500	4	3	4	2	5	5	500	4	3	4	2	5	5	500	4	3	4	2	5	5	500	2000,00
6	Asalto	3	3	4	2	3	4	204	4	5	4	4	5	5	900	4	5	4	4	5	5	900	3	3	4	2	3	4	204	2208,00
	ÁREA MÁS CRÍTICA							2857,0							4040,0							3950,0							3284,0	

Del análisis y la evaluación realizada a las áreas críticas, podemos indicar que el área **COMPLEJO DE BODEGAS**, presenta el nivel más elevado de riesgo con un valor acumulado de 4040, seguido por REFUGIO DE EXPLOSIVOS con un valor acumulado de 3950, en tercer lugar el área de DORMITORIO con un valor acumulado de 3284, y por último el área de OFICINAS con un valor acumulado de 2857.

Del análisis y la evaluación realizada a los riesgos, se establece que el mayor riesgo en el Fuerte Militar es la **PERDIDA DE BIENES,** con un valor acumulado de 3125.

En cada una de las áreas críticas determinadas en el trabajo de investigación se ponen de manifiesto los riesgos considerados con un criterio que alcanza el nivel medio y alto, lo cual implica que se debe dar tratamiento a cada uno de los riesgos en todas las área críticas del Fuerte Militar, mediante un sistemas de video vigilancia y control de acceso

6.8 Diseño de un Sistema de Video Vigilancia y Control de Acceso para el Fuerte Militar

6.8.1 Áreas de Intervención

- Prevención (entrada)
- Complejo de bodegas
- Refugios de explosivos
- Dormitorios
- Oficinas

6.8.2 Equipos Tecnológicos a Implementarse

ESCÁNER CON RAYOS X

Figura Nº 33: Escáner con rayos X

CLARIDAD DE IMAGEN (TRI-MART), diferencia entre materiales orgánicos, no-orgánicos y metálicos

FLEXIBILIDAD DE OPERACIÓN: Cinta transportadora ajustable – Chequeo bidireccional

SIMPLICIDAD INTUITIVA – Ergonómica y fácil de manejar (disminuye la fatiga del operador)

TODO EN UNO – Conexión total a redes

SISTEMA TIP – envío de imágenes ficticias al operador para mantener alerta

ALTO ALMACENAMIENTO (mínimo 20.000 imágenes).

ARCO DE DETECCIÓN DE METALES

Figura Nº 34: Arco de detección de metales

TOTAL SEGURIDAD DE DETECCIÓN

DOBLE DISPLAY de elevada visibilidad para localización simple o múltiple de armas en tránsito.

ALTA VELOCIDAD DE INTERCEPCIÓN

Elevada inmunidad a las INTERFERENCIAS EXTERNAS

SELECCIÓN DIRECTA – de estándares internacionales de seguridad

ELEVADA FIABILIDAD

CONEXIÓN TOTAL A RED

CÁMARA TIPO 1

Figura Nº 35: Cámara Tipo 1

EXTERIOR - DOBLE LENTE DE 90 GRADOS

UN LENTE DE DÍA Y OTRO DE NOCHE

IP 65

SENSOR DE MOVIMIENTO INFRARROJO

AUDIO DE DOS VÍAS

CÁMARA TIPO 2 TELEOBJETIVO

Figura Nº 36: Cámara Tipo 2

EXTERIOR - DOBLE LENTE DE 135 mm 15 GRADOS

UN LENTE DE DÍA Y OTRO DE NOCHE

IP 65

SENSOR DE MOVIMIENTO INFRARROJO

AUDIO DE DOS VÍAS

CÁMARA TIPO 3

Figura Nº 37: Cámara Tipo 3

INTERIOR – LENTE DE 90 GRADOS

UN LENTE DE DÍA

IP 65

SENSOR DE MOVIMIENTO INFRARROJO

AUDIO DE DOS VÍAS

CÁMARA TIPO 4

Figura Nº 38: Cámara Tipo 4

INTERIOR – LENTE DE 180 GRADOS

UN LENTE DE DÍA

IP 65

SENSOR DE MOVIMIENTO INFRARROJO

AUDIO DE DOS VÍAS

CAM – IO INTEGRADOR (CENTRO DE CONTROL)

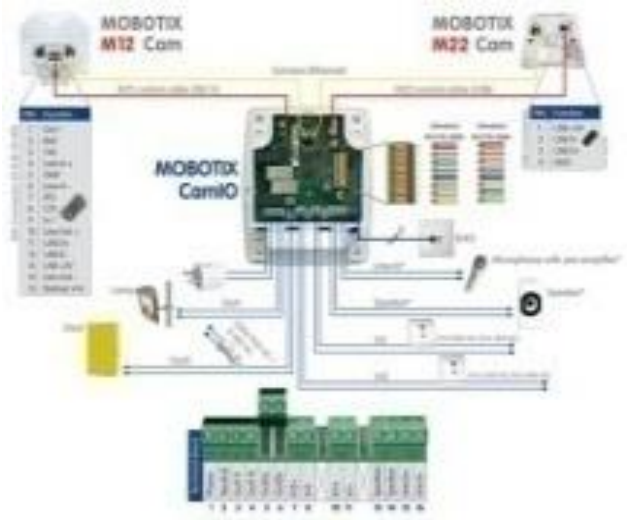


Figura Nº 39: CAM – IO Integrador

INTEGRACIÓN CON CANDADOS MAGNÉTICOS

INTEGRACIÓN CON SISTEMAS DE AUDIO

INTEGRACIÓN CON LUCES Y ALARMAS

BATERÍA DE EMERGENCIA

AMPLIFICADOR

Figura Nº 40: Amplificador

15 CM X 7 CM

USOS INTERIORES

REFLECTORES EXTERIORES

Figura Nº 41: Reflectores Exteriores

REFLECTORES DE EXTERIORES PARA ACTIVACIÓN AUTOMÁTICA.

CANDADOS MAGNÉTICOS

Figura Nº 41: Candados Magnéticos

CANDADOS MAGNÉTICOS DE ACTIVACIÓN AUTOMÁTICA

MONITORES LCD

Figura Nº 42: Monitores

PANTALLA DE LCD 32

ALMACENAMIENTO DIGITAL

Figura Nº 43: Almacenamiento Digital

SERVIDORES DE ALTO RENDIMIENTO

SISTEMA DE ALMACENAMIENTO DE HASTA 5 TB. PROCESADOR QUAD CORE INTEL XEON 2.33 GHZ, RAM 2GB, CONTROLADORA DE ALMACENAMIENTO, 7 DISCOS DE 750 GB.

6.9 Contexto General del Sistema

SISTEMA ÚNICO INTEGRADO CON UN SOLO CEREBRO CENTRAL

VIDEO VIGILANCIA DIGITAL DE ALTA RESOLUCIÓN

SISTEMAS DE EMERGENCIA INTEGRADOS CON INTELIGENCIA ARTIFICIAL

CONTROL DE ACCESOS Y DE VISITA CON RECONOCIMIENTO FACIAL Y DE PLACAS DE AUTO

REGISTRO DE HORAS DE TRABAJO PARA ROLES DE PAGO

6.10 Ubicación del Equipo Tecnológico en las Áreas del Fuerte Militar

Figura Nº 44: Ubicación del equipo tecnológico
Elaborado por: Espinoza Christian y Saltos Víctor

6.11 Presupuesto Referencial

ORD.	ESPECIFICACIÓN	CANTIDAD	V/ UNITARIO	V / TOTAL
1	CAMARA EXTERIOR 90 GRADOS D / N	27	3690	99630
2	CAMARA INTERIOR 90 GRADOS D	8	2181	17448
3	CAMARA INTERIOR 180 GRADOS D	19	2715	51585
4	CAMARA EXTERIOR TELEOBJETIVO 45 GRADOS	8	3235	25880
5	CANDADO ELECTROMAGNÉTICO	11	110	1210
6	REFLECTOR	12	315	3780
7	AMPLIFICADOR	1	105	105
8	ARCO DETECTOR DE METALES	1	6750	6750
9	ESCANER DE RAYOS X	1	12320	12320
10	SERVIDOR	2	5700	11400
11	MONITOR LCD	12	550	6600
12	INTEGRADOR DE SISTEMAS	12	1361	16332
13	SOFTWARE (INTEGRACION, FACIAL, ETC.)	1	35000	35000
14	CABLEADO Y CALIBRACIONES	1	8000	8000
15	CAPACITACIÓN	1	5000	5000
	TOTAL GENERAL			**301040**

Tabla Nº 27: Presupuesto Referencial

BIBLIOGRAFÍA

Constitución de la República del Ecuador. (2008). Quito.

Díaz Estica, j. (2012).

Duque, A. C. (2001). *Metodología para la gestión de riesgos.*

foscam. (s.f.). Obtenido de www.foscam.es

globalcard. (2000). Obtenido de www.golbalcard.com

Google: cámaras- video. (s.f.). Obtenido de www.google.com.ec/images

google: img,nauticexpo. (s.f.). Obtenido de www.google.com.ec/imgres

Larconsia. (2013).

Maciel, M. (2010).

Montero Martínez, R. (1997). *Reflexiones sobre la gestión de la Seguridad Industrial .*

Plan Nacional de Seguirdad Integral. (s.f.). Quito.

seguridad alarmas. (diciembre de 2012). Obtenido de html.rincondelvago.com

Sercuritybydefault. (2001). Obtenido de www.Sercuritybydefault.com

Sercurtybydefault. (2011). Obtenido de www.Sercurtybydefault.com

Suzanne, N. (2004).

Zamora, H. (2012).