ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”

MEDIDAS DE SEGURIDAD Y SU RELACIÓN CON EL CONTROL DE ACCESO A LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” - 2019

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES CON MENCIÓN EN INGENERÍA

PRESENTADO POR LOS BACHILLERES

SAMANIEGO ROMERO, YOSIMAR STEVIE

VERGARAY ROJAS, NATALY DEL MILAGRO

LIMA – PERÚ

2019

NOMBRE DEL TRABAJO

2019_SAMANIEGO - VERGARAY.pdf

RECUENTO DE PALABRAS

28862 Words

RECUENTO DE CARACTERES

155033 Characters

RECUENTO DE PÁGINAS

147 Pages

TAMAÑO DEL ARCHIVO

2.0MB

FECHA DE ENTREGA

Nov 30, 2023 11:19 AM GMT-5

FECHA DEL INFORME

Nov 30, 2023 11:20 AM GMT-5

21% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 21% Base de datos de Internet
- Base de datos de Crossref
- 11% Base de datos de trabajos entregados
- 3% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Bloques de texto excluidos manualmente

DEDICATORIA:

A nuestro Señor Todopoderoso por habernos iluminado en el desarrollo de la presente investigación

A nuestros amados progenitores por habernos brindado su permanente apoyo incondicional en nuestra educación.

AGRADECIMIENTO

A nuestra Alma Mater del Ejército del Perú, la gloriosa Escuela Militar de Chorrillos por su invalorable apoyo en formarnos profesionalmente.

A nuestros instructores militares y catedráticos por su permanente guía para desarrollar esta tesis.

PRESENTACIÓN

Señores Miembros del Jurado:

Dando cumplimiento a las normas establecidas en el Reglamento de Grados y títulos de la Escuela Militar de Chorrillos para optar título de Licenciado en Ciencias Militares, presentamos el Trabajo de Investigación titulado: MEDIDAS DE SEGURIDAD Y SU RELACIÓN CON EL CONTROL DE ACCESO A LAS INSTALACIONES DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI” - 2019

Las responsabilidades del trabajo son las siguientes:

- Aspecto metodológico: Bach. SAMANIEGO ROMERO, YOSIMAR STEVIE
- Aspecto temático: Bach. VERGARAY ROJAS, NATALY DEL MILAGRO

La investigación tiene por finalidad determinar la relación que existe entre las Medidas de Seguridad y el Control de Acceso a las Instalaciones de la Escuela Militar.

Por lo tanto señores miembros del jurado, ponemos a vuestra disposición el presente tema para ser debidamente evaluado por ustedes, esperando su aprobación.

Los Autores

ÍNDICE DE CONTENIDO

CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

CAPÍTULO II: MARCO TEÓRICO

CAPÍTULO III: MARCO METODOLÓGICO

CAPÍTULO IV: RESULTADOS

CONCLUSIONES

RECOMENDACIONES

ANEXOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo general del presente estudio se circunscribió en determinar la relación que existe entre Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” - 2019

Este estudio se realizó contando con una población conformada por doscientos veinticinco cadetes de cuarto año siendo la muestra de ciento cuarenta y tres personas, pertenecientes a la Escuela Militar.

Los datos fueron recogidos mediante una encuesta que contó con quince ítems, los cuales se construyeron en base a las variables de estudio, dimensiones e indicadores motivo del estudio.

Los datos fueron procesados con el paquete estadístico SPSS para obtener resultados consistentes en tablas y figuras resultantes de la encuesta aplicada a la muestra.

Como producto de este trabajo se obtuvo importantes conclusiones y recomendaciones respecto de la relación entre ambas variables.

Palabras clave: Medidas, Seguridad, Control, Acceso, Militar.

ABSTRACT

The general objective of this study was circumscribed in determining the relationship that exists between Security Measures and its relation with the Control of Access to the Facilities of the Military School of Chorrillos "Coronel Francisco Bolognesi" - 2019

This study was carried out with a population consisting of two hundred and twenty cadets of the fourth year, being the sample of two hundred people, belonging to the Military School.

The data were collected through a survey that included fifteen items, which were constructed based on the study variables, dimensions and indicators of the study.

The data were processed with the statistical package SPSS to obtain consistent results in tables and figures resulting from the survey applied to the sample.

As a result of this work, important conclusions and recommendations were obtained regarding the relationship between both variables.

Key words: Measures, Security, Control, Access, Military.

INTRODUCCIÓN

La presente tesis está desarrollada de manera detallada habiéndose estructurado en cuatro capítulos que metodológicamente nos han llevado a formular conclusiones y recomendaciones importantes, tal es así que en el Capítulo I titulado Problema de Investigación, se desarrolló el Planteamiento del Problema, Formulación del problema, Objetivos, Justificación, Limitaciones y Viabilidad del estudio.

En lo que respecta al Capítulo II, denominado Marco Teórico, se ha recopilado valiosa información para sustentar la investigación respecto de las variables, así como otros temas relacionados con las dimensiones planteadas en la matriz de consistencia; entre los que podemos citar los Antecedentes, Bases Teóricas, Definición de Términos Básicos, Hipótesis y Variables

El Capítulo III lo conforma el Marco Metodológico, que comprende Enfoque, Tipo, Diseño, Método, Población, Muestra, Técnicas e Instrumentos para recolección de Datos, Validación, Confiabilidad del instrumento, Procedimientos para el Tratamiento de los datos y Aspectos Éticos.

En lo concerniente al Capítulo IV Resultados, se interpreta los resultados estadísticos de cada uno de los ítems considerados en los instrumentos, adjuntándose las tablas y figuras correspondientes; asimismo se dan a conocer las conclusiones y recomendaciones del tema investigado.

Los Autores

CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

Las medidas de seguridad desde épocas muy antiguas ha sido un tema de vital importancia para el control de acceso a las instalaciones cuya finalidad era impedir la entrada a personas extrañas o ajenas que podían realizar acciones de espionaje o de sabotaje en perjuicio del área de interés.

El caballo de troya es un claro ejemplo de falta de seguridad que permitió la incursión de tropas griegas enemigas en el reinado troyano, cuyo fin fue invadir y destruir la ciudad. Durante la noche, los guerreros salieron del caballo, mataron a los centinelas y abrieron las puertas de la ciudad para permitir la entrada del ejército griego, lo que provocó la caída definitiva de Troya.

Conforme ha ido avanzado el tiempo, los países del mundo han ido fortaleciendo las medidas de seguridad para proteger sus documentos clasificados, darle confianza a su personal, evitar sustracción de equipos y darle protección a las instalaciones ante posibles actos de sabotaje de terceros o delincuentes, lo que constituye un valor importante para la organización.

En la Escuela Militar de Chorrillos se cuenta con material muy valioso entre documentos reservados, material de comunicaciones, vehículos, municiones, armamento, equipos de proyección de multimedia, computadoras, salas de ayudas y los recursos humanos que en su mayoría conforman el Batallón de Cadetes, pasibles de ser atentados desde el exterior por actos delincuenciales, como sucedió en enero del 2019 en la

Escuela Superior de Policía de Bogotá - Colombia “General Santander”, que dejó 21 fallecidos y 68 cadetes heridos, atentado atribuido al Ejército de Liberación Nacional (ELN) que empleo la modalidad de coche bomba.

Por lo que se hace necesario darle la debida importancia a las medidas de seguridad que permita proteger sus recursos humanos, económicos y materiales, siendo necesario ejercer un estricto control tanto externo como interno de las instalaciones; esta investigación trata de establecer la relación que existe entre ambas variables.

1.2. Formulación del problema

1.2.1. Problema general

¿Qué relación existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.2.2. Problema específico 1

¿Qué relación existe entre las medidas de seguridad y el control de acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.2.3. Problema específico 2

¿Qué relación existe entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Determinar la relación que existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

1.3.2. Objetivos Específicos

1.3.2.1. Objetivo Específico 1

Determinar la relación que existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

1.3.2.2. Objetivo Específico 2

Determinar la relación que existe entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

1.4. Justificación

Martínez (2015) refiere que toda investigación debe justificarse, a efectos de conocer las razones que lleva a los tesistas a realizar el estudio. Esta investigación se justifica por lo siguiente:

1.2.1. Al punto de vista teórico, en vista que se va a contrastar las variables medidas de seguridad y el control de acceso para verificar que existe

una estrecha relación entre ellas, obteniéndose nuevos conocimientos teóricos sobre el tema.

1.2.2. Al punto de vista práctico, porque al culminar la investigación se va a contar con nuevas formas de mejorar la medida de seguridad y el control de acceso, lo que se podría adaptar a investigaciones similares.

1.2.3. Al punto de vista de social, en vista que como resultado de este estudio se obtendrán resultados que irán en beneficio de la población en general tanto militar como civil.

1.2.4. Al punto de vista investigativo, en vista que este estudio tendrá como resultado la forma de mejorar la medidas de seguridad y el control de acceso las instalaciones

1.2.5. Al punto de vista normativo, en vista que del resultado de esta investigación se va a obtener nuevas reglas, normas, directivas órdenes y conclusiones respecto de medidas de seguridad y el control de acceso

12.6. Al punto de vista metodológico, porque en la presente investigación se emplearán instrumentos para medir las variables de estudio, así mismo se tendrá un procedimiento para el tratamiento de los datos.

.

1.5. Limitaciones

1.3.1. La biblioteca de la Escuela Militar tiene limitaciones en cuanto contar con libros actualizados respecto de temas relacionados con las medidas de seguridad y el control de acceso, limitación que puede ser superada asistiendo a otras bibliotecas del exterior, para lo cual se tendría que solicitar salidas extraordinarias.

1.3.2. Se cuenta con una economía que es limitada por cuanto los autores de la presente investigación son estudiantes que reciben propinas, obstáculo que se puede solucionar con apoyo de los familiares.

1.3.3. Por la modalidad de encontrarnos bajo un sistema de internamiento en la Escuela Militar, no se tiene libertad para salir al exterior a buscar información, obstáculo que se puede superar con la ayuda de los profesores e instructores militares.

1.3.4. No contamos con tiempo suficiente para realizar la investigación ya que tenemos que atender estudios de otras materias además de actividades que programa la Escuela Militar como guardias, servicio de cuartel, salidas al campo, desfiles, comisiones, deportes, ceremonias, etc.; lo que se puede superar realizando estas tareas en horas fuera del horario de estudio o en las salidas de paseo.

1.6. Viabilidad

El presente trabajo es viable por las razones siguientes:

1.4.1. Nuestra muestra está conformada por los cadetes de cuarto año quienes de manera voluntaria están dispuestos a colaborar con el desarrollo de la encuesta.

1.4.2. Los investigadores del presente tema tienen interés en desarrollar la tesis de manera incondicional así mismo contamos con el apoyo de asesores especialistas.

1.4.3. Los obstáculos de tiempo para realizar la investigación pueden superarse empleando horas de trabajo fuera del horario que programa la Escuela Militar.

CAPÍTULO II. MARCO TEORICO

2.1 Antecedentes

2.1.1 Antecedentes Internacionales

Vargas Z (2013) *"Sistema de Control de Acceso y Monitoreo con la Tecnología RFID para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil*" Tesis para optar el título de Ingeniería de Sistemas con mención de Telemática. Universidad Politécnica Salesiana Sede Guayaquil. Quito.

Resumen:

El proyecto nació de la necesidad de brindar seguridad a los equipos del laboratorio de Telemática de la Universidad Politécnica Salesiana. Este diseño consiste en un Sistema de Control de Acceso al Laboratorio, permitiendo un monitoreo constante de los equipos y el acceso controlado del personal autorizado. El sistema SCAL utiliza un módulo de identificación inalámbrica denominado RFID (Radio Frequency Identification) que tiene como fin identificar, gestionar y controlar al personal docente y de mantenimiento autorizado. El módulo de acceso que se realizó es un seguro método destinado a controlar el ingreso y egreso del personal al laboratorio. Fue elaborado en Netbeans mediante una conexión UDP. El software de control de acceso permite configurar el hardware desde la PC y elaborar cuadros estadísticos.

El Monitoreo se efectuó en LabVIEW empleando la tecnología RFID el cual permite identificar una etiqueta electrónica a distancia, que emite periódicamente una señal de radiofrecuencia hacia el módulo lector RFID.

El sistema SCAL y la tecnología RFID, ayudará en la reducción del costo por reposición de los equipos perdidos, tener precisión a la hora de necesitar los laboratorios y evitar la supervisión por parte del personal de mantenimiento.

Conclusiones:

El sistema SCAL, se recomienda para las empresas, los supermercados y en este caso en particular a los laboratorios de las Universidades, en donde existe la necesidad de salvaguardar los activos fijos, así también controlar el acceso de las personas autorizadas en horarios establecidos.

Cabe señalar que la tecnología RFID, tiene una amplia gama de aplicaciones que a futuro servirán para ir mejorando la idea.

Este sistema puede ser implementado no solamente en el laboratorio de Telemática sino también en las diferentes Facultades de la Universidad Politécnica Salesiana, aun cuando parecería que el proyecto no es escalable porque la tecnología está en constante innovación y por su costo.

La rentabilidad del proyecto se verá reflejada en el costo beneficio, que al invertir en la implementación del sistema, optimizaremos el tiempo, aumentaremos la seguridad en el acceso y el control de las personas mediante el continuo monitoreo, eliminando las pérdidas de los equipos.

Debo indicar que este sistema fue implementado con recursos propios, demostrando la efectividad en las hipótesis y los objetivos desarrollados.

Comentario:

El presente estudio nos señala que el sistema SCAL, es recomendable frente a la necesidad de salvaguardar los activos fijos, así también controlar el acceso de las personas autorizadas en horarios establecidos.

Enriquez A (2015) "*La seguridad electrónica en el fuerte militar Rumiñahui*" Tesis para optar el título de ingeniero en seguridad - mención seguridad pública y privada. Universidad de las fuerzas armadas "ESPE" Quito. Ecuador.

Resumen:

Frente a las amenazas y los riesgos actuales, se hace necesaria la implementación de sistemas de seguridad electrónicos que complementen a los sistemas de seguridad física tradicionales, esto con el objetivo de disminuir el riesgos y los daños a las personas, los bienes y la información; debido a que en el interior del Fuerte Militar Rumiñahui, se requiere proteger al personal militar y civil; los bienes tales como material bélico, material de intendencia, el material de comunicaciones que se encuentran en las bodegas, los laboratorios con todo su instrumental y herramientas y finalmente la información clasificada. Luego del estudio realizado, se ha podido determinar que se requiere de la instalación de un Circuito Cerrado de Televisión CCTV, enlazado a través una red mixta es decir alámbrica e inalámbrica con dispositivos IP; el mismo que estaría ubicado en puntos estratégicos del Fuerte Militar Rumiñahui, lo que permitirá desde un centro de control proteger a las personas, los bienes y la información.

Conclusiones:

a. El Fuerte Militar Rumiñahui, tiene en su interior cinco unidades relacionadas con el ámbito de comunicaciones del Ejército.
b. El AGRUCOMGE, es la unidad que establece las políticas para el funcionamiento de las comunicaciones del ejército.
c. El AGRUCOMGE dispone de bodegas de material bélico, en el cual se encuentra: fusiles, pistolas, munición, cascos, materia AC (contra disturbios y motines), chalecos antibalas, etc.
d. El AGRUCOMGE dispone de bodegas de material de intendencia, materiales de oficina, bodega de transportes.
e. Cada una de las instalaciones comunales están a cargo del AGRUCOMGE, cocinas, casinos, comedores en la cual constantemente hay un tráfico de personal.
f. El BC. 1 “RUMIÑAHUI”, es la unidad encargada de instalar explotar y mantener el sistema general de comunicaciones del ejército.
g. El BC. 1 dispone de una bodega de comunicaciones en donde se guarda todo el material orgánico, es decir material HF, VHF UHF, satelital, alámbricos ópticos y acústicos.
h. El BC. 1 dispone de documentación calificada, la cual es utilizada cuando la unidad se emplea en operaciones de defensa externa o defensa interna.
i. El Comando de Apoyo Logístico Electrónico, es la unidad encargada del mantenimiento y abastecimientos de los sistemas de comunicaciones e informática del ejército.
j. El CALE tiene 8 bodegas (Tádiran, Racal, Harris, Integradores, Repuestos y accesorios, Alámbricos, Troncalizado, Fotovoltaicos, Radio enlace, Tránsito, Instrumentación y herramienta.) y 6laboratorios (Estándar militar, Harris, Troncalizado, Radio enlace, Mantenimiento de Computadoras, fotovoltaico).

k. El Centro de Metrología del Ejército, es la unidad encargada de realizar la calibración de equipos en las diferentes magnitudes tales como presión, temperatura, voltaje y tiempo.
l. En las instalaciones del Centro de Metrología del Ejército existe equipamiento de precisión y costosos.
m. En las diferentes unidades existen activos fijos que son propiedad del ejército.
n. En las diferentes oficinas existe información y documentación de tipo calificado, es decir: planes de defensa interna, planes de defensa externa, ordenes de operaciones, documentos de carácter administrativos y otros de carácter secreto, secretísimo y reservados.
o. Está previsto que el comando de ciber defensa, pase a ocupar un área del Fuerte Militar Rumiñahui.
p. El sector perimetral es vulnerable debido a que la seguridad física es realizada por la guardia y es susceptible que éstos no lo realicen en una forma eficiente.
q. La seguridad física es realizada diariamente por un jefe de control, un jefe de cuartel, oficial de guardia/suboficial de guardia y seis grupos de guardia.
r. Existen personal civil y militar, ajeno o de planta que ingresan o salen del FMR, por diferentes motivos.
s. La seguridad perimetral y en la prevención, lo realiza el personal de guardia / Policía Militar.
t. La seguridad en las oficinas e instalaciones lo realizan el personal de guardia.
u. El fuerte militar se encuentra al norte de la ciudad de Quito y colinda con varios barrios tales como: (Comité del pueblo, la Kennedy, la Rumiñahui).
v. Se ha podido determinar que las principales amenazas son elementos delincuenciales y vandálicos, que podrán afectar al personal, los bienes e información.
w. Los principales riesgos determinados son: Robo/hurto de

material bélico, equipos de comunicaciones e informática; Robo / hurto; Robo / hurto de información y el ingreso al campamento de personas ajenas al Fuerte Militar.

x. La seguridad física es insuficiente y requiere de un sistema de seguridad electrónico que puede ser el CCTV.

Comentario:

La presente tesis realiza su estudio en las instalaciones del Fuerte militar “Rumiñahui”, en Quito, donde están las tres principales unidades de comunicaciones del Ejército ecuatoriano que las hacen vulnerables a amenazas de carácter táctico operacional y estratégico motivo por el cual es necesario desarrollar medidas de seguridad para el material bélico como alarmas de movimiento, sensores en puestas y ventanas; lo que se requiere es establecer la conectividad simultanea de todos los sistemas para que converjan en un solo centro de control, que permita actuar centralizadamente en la seguridad de todo el campamento.

2.1.2 Antecedentes Nacionales:

Salvador C. (2017) Propuesta del Sistema de Video Vigilancia en la Seguridad Ciudadana distrito de Pueblo Libre 2016-2020. Tesis para optar el grado de Maestro en Gestión Pública. Universidad Cesar Vallejo. Lima Perú.

Resumen:

La presente investigación tuvo como objetivo general es implementar y articular el sistema de video vigilancia para solucionar una parte importante del problema de la seguridad ciudadana en el distrito de Pueblo Libre entre el 2016 y 2020, la que tiene a cargo la Gerencia de Seguridad Ciudadana de la Municipalidad, que cuenta con un aproximado de 200 trabajadores, y una cantidad aproximada

de 189 equipos de video vigilancia, habiendo concluido y recomendado la cantidad y tipos de equipos de video vigilancia que faltan, los puntos sensibles donde se requieren las cámaras, la descentralización del centro de control y la articulación con la Policía Nacional, Serenazgo y los Comités de Juntas vecinales del distrito de Pueblo Libre.

El método utilizado en la investigación es el deductivo, de enfoque cualitativo, el diseño es de estudio de casos, hermenéutico Interpretativo, cuya información es de un período específico, que se desarrolló al aplicar las preguntas de acuerdo al problema del tema en investigación y el cuestionario de entrevista no estructurada, que brindaron información sobre cámaras de video, del incremento, la descentralización, los puntos sensibles y la articulación con la Policía, serenazgo y la juntas vecinales, que realizado el diagnostico se pudo determinar que puesta en práctica este estudio de investigación, se puede obtener la respuesta oportuna para la emergencia en el distrito.

La investigación recomienda que para proponer una buena seguridad en el distrito de Pueblo Libre, se requiere de seis (06) centrales de control de Video Vigilancia descentralizados, aparte del centro de control principal, la instalación de sesenta (60) Equipos de cámaras de video vigilancia, en los lugares recomendados y la coordinación con Serenazgo, PNP y Juntas Vecinales .

Conclusiones:

Se concluye que faltan cámaras de video, para mejorar el sistema de control electrónico de video vigilancia, falta determinar los lugares que requieren cámaras para mejorar el control de las acciones anómalas, de igual modo falta descentralizar los Centros de Control para la mejor administración de las cámaras de video vigilancia, y determinar sus ubicaciones, así mismo falta mejorar la articulación en la comunicación entre Seguridad Ciudadana de la Municipalidad con Serenazgo, la Policía Nacional y los Comités de Juntas Vecinales,

para que sea fluida y oportuna, para una capacidad de respuesta eficiente.

La necesidad de una buena coordinación entre los elementos de la Seguridad Ciudadana es de mucha importancia, en vista que soluciona a la respuesta que debe existir cuando suceda una emergencia.

Los resultados alcanzados con el incremento de los equipos (cámaras) de video vigilancia y sistemas de alerta, con la determinación de los puntos críticos que requieren de cámaras de video, así como la descentralización de los Centros de Control, para la buena administración del sistema y la eficiente articulación en la comunicación con Serenazgo, la Policía Nacional y los Comités de Juntas Vecinales, incrementará el potencial de la seguridad para todos los cuadrantes y barrios en el distrito, creando la fortaleza de trabajar juntos como un equipo para la lucha contra la inseguridad ciudadana, y con la ayuda de cámaras de video vigilancia serán de mucho impacto para la solución de los problemas delincuenciales y de acciones de personas que están al margen de la ley, y otros siniestros que se puedan presentar.

Comentario:

El presente estudio destaca la importancia del empleo de cámaras de video vigilancia como alternativa de seguridad, así como también el uso de alarmas para una adecuada administración de los ambientes y que estén interconectados con la policía nacional, serenazgo y juntas vecinales.

Ccama (2014) “Diseño e implementación de un sistema de video vigilancia y control de asistencia Biométrico de la empresa auto accesorios los gemelos S.A.C. de la ciudad de Juliaca” Tesis para optar el título de ingeniero electrónico. Universidad Nacional del Altiplano Puno.

Resumen:

La investigación de este proyecto tiene como objetivo la instalación de las cámaras de seguridad y el control de asistencia biométrico y así disminuir las pérdidas de los materiales, mercadería, herramientas, etc. también se optimizará la productividad al instalar el registrador de asistencia biométrico para el personal; el impacto en la empresa de la instalación de las cámaras de seguridad, el control de asistencia biométrico y el cableado estructurado, para la mayor eficiencia en el control del personal, de los almacenes y todo movimiento de material que debe ser registrado, esto incrementará y contribuirá a la eficiencia de la seguridad y el control, toda vez que para su instalación se colocarán materiales modernos con un costo accesible para la empresa; es importe resaltar la disposición que tiene el investigador en considerar la capacitación para el personal de seguridad en el manejo y control de estos sistemas.

Conclusiones:

El diseño del sistema de video vigilancia y del control biométrico se desarrolló teniendo en cuenta los diferentes criterios de ingeniería ajustándose a las normas que son necesarios para su posterior implementación; asimismo se plantea los diferentes equipos y medios de transmisión que han de formar parte del proyecto para su correcto funcionamiento. Todo esto teniendo en cuenta las condiciones físicas del establecimiento donde funciona la empresa “Autoaccesorios Los Gemelos SAC”.

La Implementación del sistema de video vigilancia y del control biométrico se realizó teniendo en cuenta el diseño planteado y teniendo en cuenta las normas de seguridad que son necesarios para este tipo de proyectos y en coordinación con los dueños de la empresa y demás personal que labora en dicho establecimiento.

Considerando que en dicha empresa no se contaba con un sistema de video vigilancia y un sistema de control de personal adecuado, por lo tanto, con el diseño e implementación de un sistema de video vigilancia y un sistema de control biométrico de asistencia, permitirá mejorar tanto la seguridad en y un mejor control de asistencia del personal que labora en dicha empresa.

Se demostró que la instalación de cámaras de seguridad y el control de asistencia biométrico para el control de asistencia de personal en una empresa es muy importante y necesario cuando se tiene un alto crecimiento económico ya que se tiene mayor afluencia de clientes y más personal para atender la demanda, con eso podemos observar tanto a los clientes como al personal, así como también tener estrictamente la asistencia del personal.

Comentario:

La presente investigación destaca el empleo de cámaras de seguridad, así como uso del sistema biométrico beneficia a los clientes y al personal a fin de poder facilitar una mejor atención de calidad.

Situación Actual de la seguridad para el control de acceso de la Escuela Militar CFB

En la actualidad la Escuela Militar de Chorrillos CFB cuenta con varios dispositivos de seguridad para el control de acceso a las instalaciones entre ella tenemos

1. Control con tarjetas magnéticas
2. Circuito cerrado de cámaras
3. Esquema de radio
4. Control con brazo mecánico
5. Control con tarjeta vehicular
6. Cámaras en todas las cuadras

El acceso de la Escuela militar en la actualidad llena ciertos requisitos para poder tener acceso se consta con la guardia que esta bajo mando del cadete comandante de la guardia y los cadetes de guardia los cuales se dividen en tres turnos facción, reten, y reserva los cuales brinda seguridad y controlan el acceso en los distintas puntos de ingreso a la Escuela Militar de Chorrillos los cuales están divididos por puertas y PVS, la puerta principal que esta vigilada por cámaras que controlan desde la oficina de inteligencia encargada de la seguridad de acceso en esta oficina se centralidad los radios y pantallas en donde ser visualiza todos los puntos y áreas sensibles de la Escuela Militar de chorrillos.

El sistema de iluminación en todos puntos de acceso hace de que facilite el control del todo personal o vehículo que quiera ingresar a las instalaciones con los reflectores de LED que tiene gran capacidad de iluminación se cumple la función de control de acceso en horas de la noche.

Tenemos que tomar varios puntos muy importantes que es el estado de operatividad de las cámaras, de los brazos mecánicos y de las cámaras que se

encuentran en las zonas de instrucción ya que están muy deterioradas por la inclemencia del tiempo, debido a esto han bajado la resolución y no muestra una buena calidad de imagen.

Los principales puntos de acceso a la Escuela Militar de Chorrillos en la actualidad no existen mejoras tales como la infraestructura que ayuden a contener o controlar el acceso ya que hay muros y rejas muy deteriorados

2.2. Bases teóricas

ME 38 – 10 Seguridad Militar (2015)

Principales riesgos de seguridad

Los riesgos que atentan contra la Seguridad son múltiples y variados, siendo difícil hacer una enumeración de todos los existentes, por lo que la clasificación que se presenta a continuación, solo debe tenerse como simple guía:

a. Riesgos producidos por fenómenos naturales:

1) Es importante tener en cuenta los riesgos producidos por fenómenos naturales, porque pueden afectar a las instalaciones que protegen al personal, a la información y material de valor para la Seguridad Nacional.

2) Entre estos fenómenos tenemos:

a) Inundaciones

b) Marejadas

c) Incendios

d) Tempestades eléctricas

e) Terremotos

f) Huracanes

g) Ciclones

h) Lluvias torrenciales

i) Derrumbes

b. Riesgos producidos por acción de individuos o grupos enemigos:

1) Riesgos evidentes. - Se llama así a las acciones realizadas por las personas en forma ostensible y manifiesta; siendo los principales:

a) Ataques enemigos

b) Acciones de guerrillas

c) Disturbios civiles

d) Robos

e) Captura e interrogatorio de personal amigo

f) Secuestro de personalidades

g) Rapto de personalidades.

2) Riesgos encubiertos. - Se llama así a las acciones que se ejecutan sin que nos demos cuenta. Entre los principales riesgos encubiertos tenemos:

a) El espionaje

b) El sabotaje

c) La subversión

d) Observación y fotografía

e) Interceptación de todo tipo de comunicaciones

f) Radiogoniometría

g) Criptoanálisis.

c. Riesgos internos del propio personal:

1) Son los riesgos que se originan en nuestro mismo personal y que resultan de su propia naturaleza, de su manera de ser, de su manera de pensar y de su carácter. La mayoría de las veces estos riesgos no son ni calculados ni voluntarios, pero constituyen un peligro constante, porque no pueden ser controlados desde fuera, ya que son inherentes al individuo.

2) Estos riegos son muchos y variados, dependiendo del carácter de cada persona, pero los más comunes:

   a) La Fe.- Es considerada generalmente como una virtud; sin embargo, desde el punto de vista Seguridad, puede no serlo. La experiencia demuestra que el personal no adoctrinado, tiene fe y confianza en sus familiares y amigos íntimos, y por consiguiente los puede hacer participes de informaciones clasificadas que por razones de trabajo o de función han pasado a su conocimiento.

   b) El Amor Propio.- Es el sentimiento de auto estimación que toda persona tiene en mayor o menor grado y que hábilmente explotado por el enemigo o sus intermediarios, pueden permitir la obtención de informaciones de valor. A nadie le gusta ser considerado menos de lo que es. Muchas veces tratamos de comunicar a las personas que nos rodean que “somos importantes” o que "estamos “cumpliendo funciones importantes, que son normalmente clasificadas, para satisfacer nuestro amor propio.

   c) El Entusiasmo .- Es la peculiaridad de algunas personas de tipo extrovertido, que al preguntárseles sobre cualquier asunto, se entusiasman y hablan más de lo necesario, pudiendo, sin quererlo, proporcionar información clasificada y de valor, tan solo por haberse dejado llevar por su entusiasmo.

   d) El Orgullo.- Este término puede ser tomado en dos sentidos, ambos indicando actitud peligrosa para la seguridad. El primero que identifica con el sentimiento elevado que cada uno tiene por él puesto que ocupa, la función que desempeña o el trabajo que

realiza en la dependencia donde uno presta servicios. En este caso, por hacer resaltar el elevado concepto que se tiene sobre estos aspectos, puede proporcionar información clasificada. El segundo, se identifica con la vanidad u ostentación, cayendo así en el amor propio ya visto.

e) La Ignorancia.- Se refiere a la falta de "conciencia de Seguridad" y al desconocimiento de las medidas de Seguridad existentes en el lugar donde se presta servicios, que pueden dar lugar a proporcionar información, en forma inocente, sin darse cuenta del daño que se está ocasionando. Este es uno de los mayores riesgos.

f) El Rencor .- Los individuos rencorosos, por hacer daño a terceras personas, pueden llegar al extremo de revelar información de valor, que si bien les puede permitir cumplir con su cometido de agraviar a la persona a quien tiene rencor, en cambio ocasiona un grave daño a la Seguridad, por el solo hecho de alimentar dicha vigencia negativa.

g) La Desafección.- Es el hecho de perder la fe y la lealtad hacia una persona, causa o institución y volverlas hacia otras, muchas veces antagónicas, como sería el caso de un desafecto a la Fuerza Armada que comienza a realizar actividades en favor de las guerrillas comunistas. Este es de por sí peligroso y exige la adopción de medidas que permitan detectarlo a tiempo, antes de que pueda causar grave daño a la Seguridad.

h) El Apetito Sexual.- Es otro de los móviles que frecuentemente utiliza una organización interesada en obtener informaciones de otra. Este riesgo está íntimamente relacionado con el amor provocado por agentes especialmente entrenados. En estos casos, los mejores frutos se obtienen mediante el chantaje.

i) La Extroversión .- Las personas extrovertidas son factibles de ser fácilmente conducidas a dar informaciones en forma involuntaria ya

que el entusiasmo puesto en sus conversaciones, no le permiten controlar sus ideas o pensamiento que personas interesadas pueden captar o conducir a obtener una información determinada.

3) Los riegos internos del personal, hábilmente aprovechados por el enemigo o elementos interesados, pueden dar origen a otros riesgos como:

   a) Delito de infidencia

   b) Descuido e indisciplina del personal

   c) Pérdida punible

   d) Subversión

   e) Traición

   f) Rebelión, etc.

Normas básicas de seguridad

Son las disposiciones estables destinadas a contrarrestar los riesgos que se presentan en forma permanente. Estas normas permitirán alcanzar la Seguridad mínima y son las siguientes:

a. Responsabilidad. La seguridad es una responsabilidad del Comando. Sin embargo, toda persona integrante de una unidad, dependencia o instalación es responsable del cumplimiento estricto de las disposiciones dictas para alcanzar dicha Seguridad.

b. Control. El Comando, para cumplir con su responsabilidad de Seguridad, ejerce el control mediante la verificación constante del cumplimiento de las medidas dictadas para alcanzar la Seguridad. Esta norma se cumple mediante el programa de inspecciones de seguridad, periódicas o inopinadas.

c. Selección de Personal. El personal que tiene que trabajar con material clasificado, deberá ser objeto de una cuidadosa selección a base de sus cualidades lealtad, integridad, discreción, moralidad y carácter.

d. Adoctrinamiento del Personal. Es una de las normas básicas más importantes y en la que reposa todo el armazón de la Seguridad. Permite eliminar "la ignorancia" del personal, que es el riesgo interno, más peligrosos. Esta norma consiste en desarrollar en las personas "la conciencia de Seguridad", mediante la ejecución de un buen programa de instrucción, de constante entrenamiento y de control permanente.

e. Limitación de acceso. Es la norma básica destinada a proteger la información y material clasificado, restringiendo su conocimiento o posesión únicamente a las personas autorizadas que por sus funciones oficiales tienen necesidad de ellos y que además disponen del acceso legal respectivo.

f. Custodia Apropiada. Es la norma básica que consiste en la designación de un CUSTODIO, cuya misión es dar la protección adecuada a la información y material clasificados, no permitiendo su conocimiento o posesión a personas no autorizadas, cualquiera que sea su grado, puesto o función.

g. Clasificación, Marcado y Manejo. La CLASIFICACIÓN, es la selección de la información y material, de acuerdo a su importancia y naturaleza, asignándosele un grado de seguridad. La CLASIFICACION se materializa mediante el MARCADO, que consiste en hacer visible el grado de Seguridad asignado. La clasificación y el marcado, condicionan y facilitan el MANEJO en seguridad de la información y material clasificados.

f. Destrucción. Es la norma básica que consiste en que los borradores, desperdicios y residuos de toda información clasificada, deben ser destruidos en forma tal, que no sea posible su reconstrucción.

Principales medidas de seguridad

a) Las normas básicas de seguridad por sí solas no permiten alcanzar la condición de Seguridad deseada, por lo que hay que complementarlas con una serie de medidas de Seguridad.

b) Las medidas de seguridad son múltiples y variadas, tantas como riesgos se hayan determinado mediante el Estudio de Seguridad, pero todas ellas pueden estar incluidas en las siguientes medidas:

   1) Medidas activas. Son aquellas de carácter ofensivo que detectan, neutralizan o eliminan los riesgos contra la seguridad.

   2) Medidas Pasivas. Son aquellas de carácter defensivo, muchas de las cuales las aceptamos como de rutina, por lo que normalmente se encuentran especificadas en el POV de seguridad. Estas medidas que son básicamente preventivas y su mejor expresión se alcanza cuando el personal tiene "conciencia de seguridad".

   3) Medidas de Engaño. Son aquellas que se adoptan para desviar los esfuerzos y acciones del enemigo atentatorios contra la seguridad, orientándolos sobre objetivos falsos, con el fin de engañarlo o despistarlo. Estas medidas pueden ser de carácter activo o pasivo.

c) Cada uno de estos tipos de medidas permite alcanzar determinado grado de seguridad, pero la seguridad deseada solo podrá obtenerse combinando apropiadamente los tres tipos de medidas.

d) De manera general entre las principales medidas de Seguridad, podemos citar las siguientes:

   (1) Buena utilización de la Inteligencia disponible sobre el enemigo para:

      (a) Prevenirlos de las sorpresas.

(b) Prever todas sus acciones a fin de disponer del tiempo y de los medios suficientes para reaccionar oportunamente y evitar, neutralizar o destruir dichas acciones.

(2) Buen empleo de la Contrainteligencia para impedir que el enemigo obtenga inteligencia.

(3) Uso apropiado de las medidas de contraespionaje, para detectar, neutralizar y/o destruir el espionaje del enemigo.

(4) Empleo adecuado de las medidas de Contrasabotaje, para impedir actos de sabotaje.

(5) Utilización de medidas de contrasubverción, para detectar, neutralizar y/o impedir las acciones subversivas.

(6) Reconocimiento y contrarreconocimiento.

(7) Observación y contraobservación.

(8) Alarma oportuna.
(9) Reacción oportuna.

(10) Medidas de protección de las informaciones, del material y de las instalaciones.

(11) Determinación de la lealtad del personal.

(12) Sistema de transmisiones eficientes.

(13) Realización de censura de rutina y especiales.

(14) Uso de fintas y demostraciones.

(15) Difusión de información falsa.

(16) Empleo de ardides y artimañas.

(17) Acción psicológica para crear conciencia de seguridad.

Grado de seguridad

a. El grado de seguridad, se refiere a la condición de seguridad que requiere alcanzar una unidad, instalación o dependencia militar, en función a su importancia para con la defensa Nacional.

b. El grado de seguridad requerido de la Unidad, instalación o dependencia militar puede ser máximo, mediano o mínimo.

- Máximo. Se refiere a la mayor importancia que tiene la Unidad, instalación o dependencia militar en la Defensa Nacional, exigiendo que se adopten las máximas medida de seguridad necesarias a fin de evitar la presencia de grandes riesgos.
- Mediano. Se refiere al mediano grado de importancia que tiene la unidad, instalación o dependencia militar en la Defensa Nacional, exigiendo que se incrementen las medidas de seguridad para evitar la existencia de riesgos.
- Mínimo. Se refiere a la menor importancia de la unidad, instalación o dependencia militar en la Defensa Nacional, exigiendo que se adopten las medidas de seguridad indispensables para evitar la existencia de riesgos.

c. Para determinar el grado de seguridad requerido hay que estudiar la Unidad, instalación o dependencia militar, de acuerdo a los siguientes aspectos:

- Misión. Al punto de vista de su alcance, duración, clasificación, personal que interviene, material almacenado y en uso, etc.

- Costo de reemplazo. Evaluar en dinero y tiempo cuantos costaría reemplazar la instalación estudiada; hay que tener en cuenta especialmente el tiempo que hace falta para adiestrar al personal principal y especializado.

- Ubicación. La ubicación del inmueble con respecto al área que lo rodea, es un aspecto que debe que tenerse en cuenta, para determinar el grado de seguridad requerido, ya que de ella pueden derivar peligros provenientes de la conformación topográfica del área, de las personas que lo habitan o laboran en los alrededores y de la propia naturaleza.

- Existencia de Instalaciones Similares. Si se cuenta con otra u otras instalaciones que puedan, en caso de desaparición de la estudiada, desempeñar la misma misión y absorber sus funciones.

- Documentación Clasificada. Determinar la mayor clasificación de los documentos con que regularmente se trabaja en la instalación.

Seguridad de las instalaciones

a. La seguridad en las instalaciones se alcanza mediante la adopción de medidas destinadas a eliminar los riesgos que las amenazan.

b. Por instalación se entiende la estructura física de un inmueble y los materiales que contiene en forma permanente o en depósito.

c. Aunque este concepto se refiere a cualquier instalación, sea cual fuere su tipo o utilidad, para poder adoptar mejor las medidas que garanticen su seguridad, es necesario tener en cuenta la siguiente clasificación:

- Instalaciones militares.
- Instalaciones civiles.

d. Por instalaciones militares se entiende a todas aquellas que están directamente al servicio de la Fuerza Armada y son utilizadas por sus miembros.

e. Las instalaciones civiles se denominan a las que son dirigidas y utilizadas por personal civil.

f. Los riesgos de seguridad existentes en una instalación, se determinan mediante el Estudio de Seguridad correspondiente, son múltiples y variados, pero pueden señalarse como principales a los siguientes:

Acceso no autorizado.

a) Este riesgo se refiere al ingreso a la instalación por parte de personas que no cuentan con la debida autorización (Agentes de espionaje o sabotaje, ladrones, curiosos, etc.).

b) Los agentes de espionaje o sabotaje necesitan tener acceso al posible objetivo para realizar sus actividades; dicho acceso no solamente debe entenderse como la presencia física del espía o del saboteador en el interior de la instalación (acceso directo), sino también como la posibilidad de que dichos agentes logren llegar a sus objetivos dentro de la instalación misma en forma directa, valiéndose de medios de penetración técnica (audiofónica, física o visual), el envío de artefactos de destrucción por correo o por mensajeros, ataque desde el exterior utilizando armas de tiro curvo (morteros, granadas de mano y de fusil), etc.

c) Se evita el acceso no autorizado mediante la aplicación de medidas de tipo preventivo y correctivo (pasivas y activas)

destinadas a proteger, tanto el perímetro exterior como el área interior de la instalación.

Incendios

a) En cualquier instalación está siempre latente la posibilidad de que se produzca incendios, ya sea por causas naturales, descuidos del personal o, premeditadamente, mediante actos de sabotaje.

b) La forma más eficaz de evitar estos riesgos, está dada por la puesta en ejecución de un programa de contraincendios destinado a instruir al personal sobre los peligros que significan y la manera de combatirlos y la confección de un plan contraincendios, anexo al plan de seguridad de la instalación.

c) En toda instalación militar se tendrá en cuenta la dirección de los vientos en la zona para poder ubicar las cocinas, hornos, incineradores, etc. a fin de evitar cualquier amago de incendio.

Ataque enemigo.

(a) Es un riesgo que corre toda instalación particularmente la de carácter militar, sea en tiempo de paz o de guerra, debido a su propia naturaleza.

(b) La realización de un ataque enemigo debe preverse desde el momento en que se decide ocupar un local y para contrarrestarlo y destruirlo, es necesario confeccionar el plan de defensa de la instalación, que es un anexo al plan de seguridad.

Sabotaje

a) El sabotaje es un riego que se deriva del acceso no autorizado,

es decir, de la instrucción de personas o artefactos destructivos al interior de la instalación; sin embargo, no debe eliminarse la posibilidad de que provenga de actos efectuados por el propio personal o sea, de individuos pertenecientes a organismos enemigos, infiltrados dentro de nuestra institución.

b) Para combatir el riesgo de sabotaje se debe establecer medidas las cuales figuren en el POV de Seguridad de la instalación.

Riesgos provenientes de fenómenos naturales.

a) Son los que se derivan de la propia acción de la naturaleza, tales como terremotos, maremotos, inundaciones, etc. que pueden significar peligro para la existencia de una instalación.

b) Para contrarrestar esta posibilidad de destrucción por causas naturales, se establece el plan de evacuación, anexo también al plan de seguridad.

g. Instalaciones civiles. En algunas oportunidades, sobre todo en situaciones de emergencia nacional, ciertas instalaciones civiles pasan a depender de las FFAA en cuanto a su seguridad, debido a que su producción interesa al esfuerzo de guerra o, en forma general, su funcionamiento está íntimamente ligado a la seguridad nacional; tales por ejemplo las fábricas que elaboran productos para las FFAA, los laboratorios de investigaciones, los depósitos de combustibles, etc., bajo los mismos principios utilizados para las instalaciones militares, pero teniendo en cuenta que en las primeras aparece un problema nuevo, derivado de la naturaleza misma de su estructura y del propio civil.

Medidas de seguridad en las instalaciones militares

a. Medidas de Seguridad contra el acceso no autorizado:

1) Consideraciones generales:

a) Las medidas de seguridad contra el acceso no autorizado, se conocen con el nombre genérico de BARRERAS, las cuales pueden agruparse en los siguientes tipos:

(1) Barreras naturales

(2) Barreras estructurales

(3) Barreras humanas

(4) Barreras animales

(5) Barreras de energía.

b) Teniendo en cuenta el hecho de que para un Gobierno u organización, que estén dispuestos a emplear dinero, material y tiempo necesario y que cuenten con personal suficientemente entrenado, NO HAY BARRERA INFRANQUEABLE, la preocupación principal de quien esté obligado a dictar las medidas que garanticen la seguridad de una instalación debe ser perfeccionando cada vez más estas barreras y colocarlas unas detrás de otras en forma sucesiva, a fin de acumular el mayor número de ellas entre el intruso potencial su posible objetivo.

c) La acumulación de barreras tiene por objeto cambiar obstáculos por tiempo, de tal manera que el intruso se vea obligado a emplear el mayor tiempo posible (tiempo de retardo) como para permitir la intervención de la barrera por excelencia, el hombre, quien en definitiva será el llamado a destruir o neutralizar cualquier penetración.

Medidas de Seguridad Contraincendios

1) Generalidades:

   a) Constituyendo los incendios un peligro real y constante para cualquier instalación, es imprescindible prever la forma de evitarlos o combatirlos.

   b) Con el fin de comprender mejor este peligro, es necesario conocer algunos conceptos básicos acerca de su origen, sus tipos y la forma de combatirlos.

2) El Fuego. Es el producto de la reacción química conocida con el nombre de combustión, que se produce cuando se ponen en contacto tres elementos: Un material combustible, Calor, Oxígeno (aire). Gráficamente se puede representar mediante un triángulo equilátero en el cual un lado representa al oxígeno, el otro al calor y el tercero al combustible.

   Así como un triángulo deja de existir cuando se elimina alguno de sus lados, al eliminar uno de sus tres factores que componen el fuego, éste deja de existir: de aquí nacen los tres procedimientos básicos que se conocen para combatir el fuego.

   a) Enfriamiento. Consiste en la eliminación del calor. Se logra aplicando algún elemento que lo elimine fácilmente, tal como agua que es el medio más común y que puede emplearse pura o mezclándola con diversas sustancias químicas que aumenten su poder de extinción.

   b) Sofocamiento. Consiste en la eliminación del oxígeno. Se consigue básicamente colocando un separador entre el fuego y el aire que lo rodea. Para lograr este objetivo se utiliza diversos procedimientos; el más conocido es el de cubrir el fuego con una manta de material incombustible, una capa de tierra o una sustancia que por ser más pesada que los aires haga sus veces. Tal el caso del polvo químico seco que debido a su composición química que lo hace más pesado que el aire, desplaza a esté ocupando las capas inferiores próximas al fuego y originando su expulsión.

   c) Remoción. Consiste en retirar el material combustible, pero resulta demasiado complicado y peligroso debido a que los individuos que deben hacerlo tienen que acercarse al fuego, con el consiguiente riesgo.

3) Incendios y sus Tipos .- Se denomina incendio a la quemazón total o parcial de una gran cantidad de combustible. Según sea el combustible que se quema y la forma como se desarrolla el fuego, los incendios pueden ser de diversos tipos; los más comunes son:

a) Incendio tipo "A" .- Es el que se produce en materiales comunes tales como la madera, papeles, trapos, desperdicios y en general en materiales sólidos. El fuego de esta clase se combate por enfriamiento con agua o con soluciones que tengan un alto contenido de agua. Se puede emplear también polvo químico, seco especial, de uso múltiple.

b) Incendio tipo "B" .- Es el que se produce en las mezclas de vapores con aire, sobre la superficie de líquidos inflamables tales como la gasolina, aceite, grasa, pinturas y disolventes. La restricción del aire (oxígeno) o la interrupción de la reacción son de importancia primordial en los fuegos incipientes de esta clase. Los chorros directos de agua tienen la tendencia a esparcir el fuego, aumentando su intensidad.

   Se usan generalmente polvo químico seco regular y de uso múltiple, bióxido de carbono, espuma de hidrocarburos, halogenados, según las circunstancias.

c) Incendio tipo "C".- Es el que se produce en o cerca de equipos eléctricos donde no deben emplearse agentes extinguidores conductores de la electricidad. Para su combate se emplean polvos químicos secos, bióxido de carbono, gas inerte comprimido o liquido vaporizante. No se debe emplear espuma ni agua, porque son conductores y pueden exponer a la persona a un riesgo de choque eléctrico. A veces es posible emplear agua finamente pulverizada en algunos equipos, ya que el agua en esa forma no es buena conductora.

d) Incendio tipo "D" .- Es el que se produce en metales combustibles tales como el magnesio, titanio, circonio, litio y sodio. Para controlar los incendios de esta clase se necesitan agentes extinguidores, equipos y técnicas especiales. Los equipos de extintores normales no deben ser usados en los incendios de metales porque existe el riesgo de que se presente una

reacción química entre el agente extinguidor y el metal que arde, creando una explosión o aumentando la intensidad del fuego.

4) Prevención de incendios.- El mejor momento para controlar el fuego es antes de que empiece, pues aunque se cuente con muy buenos equipos de extinción y se esté bien adiestrado en su uso, siempre "Es mejor prevenir que curar". Habiendo comprendido la "Química del Fuego" es fácil entender los factores en que se basa la prevención de incendios. Se dijo al principio que el fuego es la combinación de combustible, calor y oxígeno y que para apagar el fuego basta eliminar uno de estos elementos o interrumpir la reacción en cadena. En las medidas de prevención se consideran solamente los tres primeros elementos, ya que es imposible contar con la interrupción de la reacción en cadena, puesto que ésta sólo se presenta después que el fuego ha comenzado. La prevención de incendios se basa en evitar que estos tres elementos se combinen, a fin de que no se produzca el fuego. Para evitar que el combustible se mezcle con el oxígeno, los materiales deben conservarse en recipientes cerrados. Para evitar que el calor se combine con el combustible se controlan todas las fuentes de calor y se les confina a lugares donde no haya combustibles que puedan incendiarse, siendo dificultoso evitar el contacto del combustible con el oxigeno, la principal medida de prevención consiste en controlar adecuadamente las fuentes de calor.

   a) Causas de incendio. La experiencia y los registros de investigaciones han demostrado que hay algunas causas comunes de incendios, responsables de la mayoría de los casos ocurridos. He aquí las más conocidas y el modo de controlarlas:

      (1) Falta de Orden y Aseo. Acumulación de desperdicios combustibles, trapos con aceite ó grasa, aceites o líquidos inflamables en el piso, rumas de materiales demasiados secos alrededor de los edificios, falta de aseo en maquinaria, en armaduras de techo, etc. se debe hacer limpieza periódica para eliminar todos los desperdicios y materiales sobrantes. Los trapos con aceite, pintura y otros materiales combustible deben ser depositados en recipientes especiales con tapa, que deben

ser desocupados periódicamente y regularmente. Los materiales utilizables y de fácil combustión deben ser guardados en armarios, cajas o recipientes de metal, cerrados.

(2) Cigarrillos y fósforos. Las colillas de cigarrillos tiradas despreocupadamente han sido la causa de muchos incendios. Son muchas las personas que no observan la regla más elemental de precaución de cerciorarse que los fósforos y las colillas estén bien apagados antes de tirarlos en un cenicero apropiado. Aunque lo ideal sería eliminar completamente el hábito de fumar en una instalación sensible, esta regla es muy difícil de implantar y de cumplir. Para esto, deben designarse lugares u horas de fumar, donde no exista riesgo de incendio y sea fácil de controlar en caso de que se produjera. Se debe prohibir de fumar en los talleres donde se trabaja con madera, en los galpones, en los lugares donde almacenan o usan líquidos u otros productos inflamables, etc. tanto los lugares donde se prohíbe fumar como aquellos destinados para ello, deben estar claramente señalados con avisos bien visibles.

b) Todas las inversiones que se hagan en la compra de equipos contraincendios, resultarán inútiles sino se pone en práctica un programa de prevención y combate de incendios dentro de cada instalación, el cual debe contemplar como mínimo, las siguientes actividades:

(1) Desarrollar un programa de instrucción de lucha contra incendios, a fin de que todo el personal conozca los riesgos de incendios inherentes a la instalación y la forma de evitarlos, así como la manera más eficaz de combatirlos una vez que se produzcan, utilizando los medios que para el efecto existan.

(2) Adquirir equipos contra incendios que sean suficientes en tipo, número y calidad para garantizar la extensión de los que puedan producirse, de acuerdo a la naturaleza de la instalación. Estos pueden estar constituidos por:

(a) En las instalaciones de gran magnitud, equipos de bomberos que cuenten con cisternas, bombas, escaleras telescopios y extintores de gran capacidad.

(b) En las instalaciones pequeñas, extintores portátiles en número suficiente para cada uno de los ambientes en los que puedan producirse incendios.

(c) Los extintores sean portátiles o de gran capacidad, deben ser adecuados para eliminar las diferentes clases de incendios.

(d) En todo caso deben existir preparados que son medios de circunstancias para apagar incendios, tales como para agua, recipientes de arena, mantas de asbesto, etc.

(e) Tanto los extintores como los medios de circunstancias, es necesario que vayan acompañados de letreros en los que se explique el modo de empleo, así como la clase de incendio para el cual debe emplearse.

(f) El oficial de seguridad de cada instalación será responsable del mantenimiento de los extintores en condiciones de funcionar, para lo cual gestiona ante la Jefatura de ingeniería correspondiente su revisión y recarga una vez al año. La fecha y condiciones de recarga deben figurar en una tarjeta atada al extintor.

(g) En algunas reparticiones de máxima seguridad, se justifica la instalación de sistemas automáticos de detección y combate de incendio en los ambientes más propensos a sufrirlos. En estos casos será también más el oficial de seguridad el encargado de mantener operativos dichos sistemas, controlando que su mantenimiento se realice de acuerdo a las especificaciones técnicas pertinentes.

5) Instrucción de personal. Instruir al personal en el manejo de los medios contraincendios existentes, especializando si fuera posible, a determinados individuos. Los extintores que estén próximos a la fecha

de recarga, pueden ser usados para demostraciones prácticas, previa autorización y teniendo cuidado de mantener extinguidores en reserva

6) Plan contraIncendios. Confeccionar un plan contraincendios como Anexo al Plan de Seguridad de la instalación, en el que se contemple detalladamente la actividad en caso de incendio de cada uno de los individuos que sirven en la Unidad. El plan contraincendios debe ser dado a conocer por el Oficial de seguridad a los interesados y ensayado en forma periódica (por lo menos bimestralmente), para ser realmente operativo en el momento de su ejecución.

Control de acceso a la instalación

El control de acceso a una instalación o en este caso a la Escuela Militar de Chorrillos CFB a través del perímetro y a las zonas prohibidas en el interior debe ser efectuado, tanto para el personal como para vehículos

a. Control de acceso de personal a la instalación.

1) A las Instalaciones Militares y particularmente a la Escuela Militar de Chorrillos CFB y a aquellas donde exista munición, explosivos o material inflamable, "NO DEBEN INGRESAR PERSONAS QUE NO TRABAJEN EN ELLA".

2) El personal de Oficiales, Cadetes que trabajen en los Áreas de la Escuela Militar de Chorrillos CFB o de otras dependencias militares usará permanentemente la tarjeta de identidad desde que ingresa hasta que sale de la instalación. (Anexo 2)

3) En algunas dependencias existen oficinas de trabajo común y otras donde se labora con material clasificado. A estas últimas se les

designará como "Zonas Reservadas", debiendo el personal que trabaja en ellas usar tarjeta de identidad de color "ROJO"

4) En la Escuela Militar de Chorrillos CFB se entregará la tarjeta de identidad sólo a los Oficiales y personal civil que laboren en las oficinas donde se trabajen con material clasificado.

5) En los días de salida, el comandante de la guardia en la puerta principal de la Escuela Militar de Chorrillos a la guardia a fin de identificar a los soldados en su unidad, que regresan de paseo, y evitar el ingreso de soldados de otras unidades o civiles que portando uniforme traten maliciosamente de ingresar a la unidad. Es conveniente que en la guardia exista un "álbum Fotográfico" del personal de la unida, subunidades, con el objeto de despejar cualquier duda de identificación que pudiera presentarse.

6) A la persona visitante, se le entregará una tarjeta de visitante (Anexo 3). El visitante debe ser acompañado por un "Número" hasta la sala de recibo u oficina del Oficial si así se autorizara, siendo responsabilidad del Oficial visitado hacerlo acompañar con un soldado o clase hasta la Guardia al término de la entrevista.

7) El personal visitante portará la tarjeta en cualquier lugar visible de la camisa o saco, a la altura del pecho.

8) El Oficial, clase o soldado que encontrara a algún visitante transitando aislado por la instalación debe conducirlo ante el Oficial de Guardia, dando cuenta de su actitud, aun cuando sea portador de la tarjeta de visitante.

9) Cuando algún visitante porte maletín o paquete se tendrá especial cuidado de que lo lleve consigo a la salida.

10) Toda autoridad que reciba una visita tendrá especial cuidado de que el visitante no deje olvidado en su oficina, paquete, maletín, lapiceros, cajas de fósforos y objetos de cualquier naturaleza, debiendo avisar del hecho inmediatamente al Oficial de Seguridad, pues puede tratarse de un artificio de sabotaje.

11) Los cantineros y cocineros de las unidades deben ser revisados a su ingreso y salida de la instalación, entregando y recabando diariamente una tarjeta de visitante.

12) Por ningún motivo se permitirá a los cantineros y cocineros el libre tránsito por las instalaciones, debiendo concretarse a la zona de su labor.

13) Los Oficiales peruanos que no laboran en la instalación podrán ingresar a ella previa identificación ante el Oficial de Guardia o el servicio de día.

14) El personal auxiliar y de tropa, solamente podrá ingresar a la sala de recibo después de haberse identificado.

15) Por ningún motivo deberán ingresar Oficiales extranjeros a los cuarteles u otras instalaciones militares, sin una autorización de la Comandancia General de la Región a la cual pertenecen dichas instalaciones. En las guarniciones de frontera cuando no hay tiempo de obtener la autorización mencionada solamente podrán hacerlo a la sala de Guardia o a los locales sociales, si es que existen. En todo caso la autorización de visitante debe ir acompañada de una ficha de personalidad de los interesados, así como de un "programa de visita", y confeccionado por el Departamento de Inteligencia respectivo, en el cual se especifique los detalles de la visita y las actitudes que al respecto deba realizar el personal de seguridad de la instalación.

16) Los familiares de los Oficiales, en las guarniciones en que la escasez de locales sociales lo justifique, podrán ingresar a las instalaciones militares premunidos de su respectivo carnet, pero de ninguna manera saldrán de las zonas específicamente señaladas como locales sociales.

17) El personal de tropa recibirá sus visitas en la sala respectiva o en un lugar especialmente destinado para ello, dichas visitas deben ser observadas en forma disimulada por el personal de seguridad el cual a su ingreso recibirá todos los paquetes que porten a fin de evitar la instrucción subrepticia de artefactos peligrosos.

18) Los agentes vendedores podrán ser autorizados a mostrar sus

productos en la sala de recibo de la Guardia en locales debidamente controlados.

19) A las ceremonias que se realizan en el interior de las instalaciones militares, solamente ingresarán personas especialmente invitadas y a los lugares específicamente señalados.

20) Solamente en casos excepcionales y con especial autorización del Comando del Ejército, se proporcionará alojamiento a personas o a grupos de personas en las instalaciones militares. Esta autorización sola será otorgada si es que en la guarnición no existiesen las condiciones mínimas de alojamiento, compatibles con la naturaleza de las personas.

21) En la Guardia de cada instalación debe llevarse un registro de control de visitantes, en el cual se anotará a todo extranjero, civil o militar, que por algún motivo llegue a la instalación y solamente a los nacionales que ingresen al interior de las mismas. (Anexo 3).

22) Identificación plena del militar y civil que ingresa a las instalaciones militares, exigiendo la presentación de la Tarjeta de Identidad Personal, teniendo en consideración y el hecho de vestir uniforme militar no representa un medio de identificación.

b. Control de acceso en el Área Interna de la Instalación:

1) Generalidades

a) La seguridad perimétrica no es suficiente para obtener la seguridad integral de una instalación debido principalmente a la posibilidad de acceso indirecto, es por eso que debe estudiarse cuidadosamente también el problema del interior de la misma, determinando como consecuencia la forma más adecuada de garantizarlo

b) En muchas circunstancias, las mismas medidas que sirven para dar seguridad al perímetro, son también aplicables al área interna, pero circunscribiéndolas a espacios más reducidos, con lo cual se da cumplimiento al principio de acumular tiempo de retardo basándose

en barredas sucesivas.

2) Como consecuencia del análisis del área interna se debe determinar:

   a) Las ZONAS PROHIBIDAS, o sea los lugares que por su ubicación, por los ingenios que contienen o por su propósito, deban ser restringidas en cuanto a su acceso.

   b) De acuerdo a la importancia que tengan estas zonas para la seguridad, tanto nacional como militar, es decir, al mayor o menor daño que pueda derivarse del acceso a la misma por parte de personas no autorizadas, pueden ser:

      (1) ZONAS DE EXCLUSION, cuando su importancia es tal, que la sola presencia en sus inmediaciones puede considerarse una violación de su seguridad; es el caso de los lugares donde se llevan a cabo trabajos o se exhiben cartas o planos de alta clasificación y a los que solamente podrán ingresar las personas que trabajan en ellos o los que exhiban un permiso especial firmado por la más alta autoridad de la instalación; en este último ingresarán acompañadas por alguien que trabaje en el lugar. La protección de estas zonas además de los elementos de vigilancia y control, deben ser completamente por barrera de energía.

      (2) Las ZONAS LIMITADAS O RESERVADAS, las que por la naturaleza de su función deben ser protegidas del acceso no autorizado, lo cual se hace efectivo por el uso de las guardias, escoltas y vigilantes, etc. El ingreso a estas zonas debe permitirse, con la presentación de simples tarjetas de visitas, que previa constatación de motivos, que serán proporcionados por la guardia. Cuando las instalaciones son pequeñas y en ellas existe un gran número de zonas prohibidas, más económico es considerar a toda la instalación como una sola zona y establecer en ellas medidas de seguridad perimétricas acordes con su importancia.

3) Control de acceso.

a) Una vez determinadas las zonas prohibidas, es necesario decidir la forma más eficaz de darles seguridad impidiendo el acceso de personas no autorizadas, mediante el establecimiento de barreras de diferentes tipos y en número diferente de acuerdo a la importancia de la zona y de procedimientos de control de acceso que ofrezcan garantía suficiente. Como ya se dijo anteriormente, las ZONAS DE EXCLUSION se protegen mediante cercas, sistemas de vigilancia y barreras de energía, en las ZONAS RESERVADAS no son necesarias estas últimas.

b) El control de acceso, que es puesto en ejecución por los componentes del sistema de vigilancia, debe hacerse teniendo en cuenta ciertas consideraciones, entre las cuales es necesario recalcar las siguientes:

(1) El "Reconocimiento Personal", es decir la identificación de los individuos por parte de vigilantes que los conozcan personalmente, es el más efectivo y recomendable, pero es difícil aplicarlo en forma efectiva a instalaciones que tengan un número elevado de personal, o que éste cambie constantemente. En principio el reconocimiento personal sólo será posible cuando un guardia tiene que reconocer a un máximo de cincuenta personas; si fuera más, puede subsanarse la dificultad fijando varias entradas por cada una de las cuales ingresará un máximo de cincuenta, esto, aunque es costoso y requiere de personal de vigilancia que conozca al personal en cada turno de trabajo, se justifica cuando la seguridad prima sobre cualquier otra consideración.

(2) En las zonas prohibidas que por su extensión hagan difícil y poco práctico el reconocimiento personal, pueden utilizarse otros sistemas de control basándose en tarjetas, pases o insignias de identidad fabricadas de tal manera que ofrezcan

un mínimo de seguridad contra las falsificaciones.

(3) Un sistema de control muy práctico es el de pase y ficha; el individuo entrega a su entrada a la zona prohibida su tarjeta de identidad color rojo y recibe en cambio una ficha verde que para el efecto existe en el lugar de control; ambos documentos tarjeta y ficha, contienen la fotografía del sujeto y los mismos datos, prácticamente, la ficha es un duplicado de la tarjeta de identidad. Al abandonar el individuo la instalación se procede a la inversa, es decir se cambia de ficha por el pase.

c. Control de acceso de vehículos.

1) En principio, a una instalación militar sólo deben ingresar vehículos que son orgánicos de la misma o pertenezcan al personal que labora en ella, previa autorización del Jefe de la instalación. En lo posible los vehículos orgánicos deben parquear en los galpones que para efecto existirán en cada instalación o en zonas que no estén expuestos a posibles actos de sabotaje y que cuente con vigilancia efectiva.

2) La mayoría de las instalaciones tienen necesidad de acceso de vehículos para abastecimientos, transportes, mantenimiento, etc, por lo tanto, se debe establecer un control sobre todo tipo de tránsito de vehículos, para evitar que esta actividad sea empleada como un medio de ayuda, por el espía o el saboteador en la penetración a la instalación.

3) Los procedimientos siguientes son generalmente efectivos para proporcionar seguridad:

a) Areas de estacionamiento.

b) Sistema de control:

1 Registro de vehículos

2 Sistema de escolta

3 Centro común de choferes

4) Áreas de estacionamiento. Las áreas de estacionamiento deben estar situadas fuera de la instalación, o por lo menos ubicadas fuera de las áreas de producción o de almacenaje, pero si esto no es factible y tienen que estar dentro o adyacentes a tales áreas, se les debe separar con cercos, para que todos los empleados tengan que ingresar por las entradas destinadas a los peatones. Una medida de seguridad que se debe adoptar cuando se establecen las áreas de estacionamiento, es la de prohibir el estacionamiento de vehículos a una distancia de 6 metros de cualquier edificio, material o equipo que no este a prueba de incendio.

5) Sistema de control. Donde existen áreas de estacionamiento cercanas a las instalaciones o dentro de ellas la guardia debe ejercer vigilancia sobre dichas áreas y sobre todos los caminos que conduzcan a ellas. Una medida para conseguir esta previsión, es el establecimiento de un centro de chequeo para los camiones, debe estar ubicado en la entrada o entradas de la instalación. Este centro de chequeo se usa como el medio de mayor efectividad para controlar el personal y el equipo de un vehículo; hacer que cumplan las restricciones, autorizar que los vehículos vayan a su zona respectiva y anotar en un registro todos los vehículos que entran y salen de la instalación. Hay varios sistemas que se pueden establecer para ayudar a la guardia en el control de las actividades de los camiones de otros vehículos a los cuales se permita el ingreso a la instalación. No se puede decir que uno sea mejor que el otro, por que las diferentes instalaciones requerirán distintos grados de seguridad. Los tres sistemas que se pueden usar para el control del tránsito son: el registro de vehículos, el sistema de escolta y el sistema de centro común de choferes.

   a) El registro de vehículos. Es el más simple y menos seguro de los tres sistemas de control. Este sistema se efectúa haciendo que la guardia, en el punto de chequeo, registre la siguiente información:

      (1) La fecha y hora de entrada de cada vehículo a la instalación.

      (2) El nombre del chofer y su ayudante, si lo hubiera (brevete o

carnet).

(3) El nombre del propietario del vehículo (tarjeta de propiedad).

(4) Una descripción de la carga del vehículo, el análisis de la carga.

(5) El número de la placa del rodaje del vehículo.

(6) El destino del vehículo dentro de la instalación.

(7) La hora de salida del vehículo que se anota en el momento que sale de la instalación.

b) El sistema de escolta. En el sistema de escolta, un miembro de la guardia acompaña al vehículo hacia su destino y a su regreso. El guardia vigila a los ocupantes del vehículo todo el tiempo que permanecen en la instalación.

Este sistema proporciona un alto grado de seguridad, pero tiene la desventaja del aumento de personal si hay un tránsito intenso de vehículos.

c) El centro común de choferes. El sistema del Centro común de choferes se usa en una instalación donde la economía de personal no se toma en consideración y se necesita un alto grado de seguridad. El control de tránsito se efectúa haciendo que los conductores o choferes originales permanezcan en la vecindad de la entrada, donde se controlan sus actividades.

Seguridad de personal

a. La seguridad de personal comprende todas aquellas disposiciones y actividades que permiten conocer determinados rasgos de la personalidad de los individuos que trabajan para la Fuerza Armada o que de alguna manera tienen relación con ella, los peligros que esos rasgos pueden significar para la seguridad militar y nacional y las medidas que deben adoptarse para neutralizar dichos peligros.

b. La finalidad de la seguridad de personal es determinar el grado lealtad,

discreción, integridad, moralidad y el carácter del personal, para prevenir, neutralizar y/o destruir cualquiera de sus posibles actividades que puedan significar riesgos para la seguridad.

c. Las actividades del personal que entrañan peligro para la seguridad y que por lo tanto deben ser prevenidas y combatidas, son:

1) Traición.

2) Espionaje.

3) Sabotaje.

4) Rebelión.

5) Subversión y motines.

6) Las que resultan de las propias debilidades humanas (riesgos internos del propio personal).

d. Para alcanzar un buen grado de seguridad de personal, es necesario dar cumplimiento a las siguientes prescripciones que normalmente deben ser suficientes para asegurar la lealtad de los individuos que trabajan para la Fuerza Armada:

1) Selección de personal

Es un procedimiento general de personal, cuya finalidad es prevenir la infiltración de agentes enemigos o adversarios, así como posibles colaboradores de estos.

La selección de personal que es una medida pasiva, tiene un amplio espectro y se aplica para hacer frente además del espionaje, al terrorismo, sabotaje y otras actividades encubiertas del enemigo o adversario.

Durante la permanencia del personal en una organización, es necesaria también realizarse la selección, cuando tenga que decidirse promociones, asignación de mayores responsabilidades, trabajos especiales, misiones delicadas, autorizaciones para el manejo de documentación clasificada, etc.

Estas investigaciones serán tanto más severas, cuando mayor sea la responsabilidad que le espera al individuo investigado y son de dos clases:

a) Investigación de personal. Es aquella que se realiza con el fin de determinar la lealtad, integridad, valor moral y discreción, carácter y antecedentes de las personas que pertenecen o tienen relación con las Fuerzas Armadas. Las Investigaciones de Personal, a su vez pueden ser de dos tipos:

   - Investigación Básica

   Que se realiza en forma minuciosa, investigando todos los detalles por insignificantes que parezcan; asimismo el investigador debe ser imparcial, dejando de lado los sentimientos de familiaridad o amistad que pudieran existir.
   Los aspectos a tener en cuenta en esta investigación son:

   (1) Antecedentes familiares

   (2) Vínculos personales y familiares con personal extranjero.

   (3) Vinculaciones políticas.

   (4) Vinculaciones sociales (sindicales, laborales, etc)

   (5) Vinculaciones religiosas

   (6) Antecedentes educativos.

   (7) Antecedentes Policiales y judiciales.

   (8) Signos exteriores de riqueza al. ingreso.

   Estos aspectos deben ser investigados periódicamente toda vez que, de acuerdo al puesto que ocupa el personal, tendrá la posibilidad de acceder a información, documentación o material importante para la organización y por lo tanto estará expuesto a las actividades de espionaje del enemigo.

   - Investigación para otorgar acceso a material clasificado.

A la que son sometidas las personas que por su trabajo, necesitan tener acceso a información o material clasificado; dichas personas previamente deben haber obtenido resultados favorables en la investigación básica.

b) Investigación especial. Son las que se realizan para confirmar o desechar las sospechas de actividades de espionaje, sabotaje, traición, sedición y cualquier otro delito contra la seguridad militar o nacional que se detecte durante la permanencia del personal en el trabajo o fuera de él, o como resultado de la investigación básica. Comprende el análisis de los hechos delictivos cuando no han sido descubiertos sus autores, o ha estos autores cuando han sido identificados, sean militares o civiles y trabajen o no para la Fuerza Armada.

2) Adoctrinamiento.

Que se realiza a base de un programa de instrucción de seguridad, que no sólo prevé la forma más adecuada de instruir la personal acerca de sus responsabilidades y crear en él la llamada consciencia de seguridad.

El personal de toda organización debe estar informado sobre los posibles objetivos de los cuales el enemigo o adversario puede intentar obtener información, así como de los medios y procedimientos a los que estará expuesto por la acción del esfuerzo de espionaje enemigo, motivo por el cual será necesario instruir al personal sobre las medidas pasivas de seguridad tendientes a contrarrestar su acción.

El adoctrinamiento de personal, también debe hacerse extensible hacia los familiares directos (padres, esposa e hijos), a fin de evitar que se produzcan acciones que atenta contra la seguridad.

Los aspectos a tenerse en cuenta para el adoctrinamiento son:

a) Conocimiento de las modalidades de espionaje que emplea el enemigo o adversario.

b) Instrucción sobre medidas pasivas de Seguridad y conocimiento de las responsabilidades individuales en cuanto al resguardo de informaciones e inteligencia de interés nacional.

c) Instrucción sobre disciplina del secreto, discreción, censura, acción en caso de captura, infidencia, etc.

d) Responsabilidades en la ejecución de las medidas de contrainteligencia.

e) Normas para crear y mantener la conciencia de seguridad.

f) Acciones penales contempladas en el Código de Justicia Militar (CJM) para el personal que no cumple con las medidas pasivas de seguridad que atenta contra la seguridad de las FFAA o Nacional.

3) Observación

La libertad de sentir y de pensar que goza el hombre, hace que una buena investigación, básica o especial, realizada al personal, a pesar de que comprueba su lealtad e idoneidad en e momento en que se lleva a cabo, no garantiza que esta lealtad sea indefinida y se mantenga a través de toda la vida del sujeto, o por lo menos durante su permanencia en la organización, por lo cual es necesario observar constantemente sus actividades dentro y fuera del lugar de trabajo, a fin de prevenir o detectar posibles desviaciones negativas de su conducta y de su cambio de convicción ideológica que puede afectar la seguridad de la organización.

Los aspectos que deben observarse entre otros son los siguientes:

a) Comportamiento en el trabajo, actitudes negativas, negligencias, descuidos, etc.

b) Signos Exteriores de riqueza.

c) Lugares que visita con cierta frecuencia.

d) Relaciones interpersonales con elementos sospechosos de atentar a la seguridad nacional (nacionales y extranjeros)

e) Relaciones con personal extranjero.

RuvaSeguridad (s.f) sobre los Sistemas perimetrales de videovigilancia nos señala que los sistemas perimetrales de videovigilancia son un sistema de detección basado en cámaras que ofrece la mejor protección porque no puede saltarse. En el momento de la detección la imagen se envía automáticamente al operador de la Central Receptora, que podrá responder rápidamente a la intrusión gracias a la validación visual, sin necesidad de llamadas al abonado.

Los sistemas de **Análisis de Video** actúan como un vigilante virtual, ahorrando costes en personal de seguridad, con unas prestaciones equivalentes y unos costes mensuales muy reducidos.

Los sistemas de **video análisis** funcionan exclusivamente a partir de las imágenes de las cámaras, sin necesidad de instalar otros sensores en el perímetro, y permitiendo ahorrar en costes de obra civil.

Las mismas cámaras utilizadas para vigilar el perímetro le permitirán a Ud. monitorizar su instalación en cualquier momento y desde cualquier parte del mundo a través de Internet. La misma instalación de CCTV servirá para vigilar activamente las intrusiones, sin necesidad de costes adicionales.

El sistema permite:

- Identificar personas o vehículos en los alrededores del perímetro a proteger.
- Detectar una intrusión en su propiedad en el momento en que se está produciendo, para que usted pueda reaccionar a tiempo.
- Detectar el cruce de barreras virtuales definidas por el usuario.
- Visualizar las cámaras de forma remota a través de Internet.

Características

- Discriminación entre personas y vehículos.
- Filtrado automático de otros elementos (cambios de luz, plantas que se mueven con el viento, lluvia, etc.)
- Visualización de incidencias rápida e intuitiva.

Ventajas

- Mayor cobertura de detección que otros sensores.
- Sin falsas alarmas: la Central Receptora de Alarmas le avisa sólo en caso de incidencia real (video verificación).
- Privacidad: Ud. controla el acceso del operador a las cámaras.
- Activación y desactivación desde el teclado de alarma convencional.
- Sin instalación de barreras u otros sensores.

Cámaras térmicas

- Máxima tecnología en verificación de imagen térmica.
- Visión independiente de los cambios climáticos, día, noche, lluvia, niebla, etc...
- La visión siempre es la misma con las cámaras térmicas.
- Una cámara térmica no se ve afectada por la incidencia directa de la luz del sol
- Una cámara térmica no se ve afectada por contrastes en la luminosidad
- Una cámara térmica no se ve afectada por presencia de humo

Holowczak B (s.f) CCTV en sistemas de detección perimetral, señala que con las nuevas tecnologías se ha buscado reducir al mínimo las falsas alarmas. Junto con una buena herramienta de gestión de alarmas en el centro de control, el trabajo de los operadores es cada vez más eficaz y rápido, gracias a que los nuevos sistemas incorporan dos características: activación mediante teclado de alarma convencional y videoverificación mediante grabación inteligente. Esta facilidad de uso se convierte en un valor agregado para el cliente.

Los sistemas perimetrales de detección de intrusos que añaden CCTV y videoanálisis permiten cubrir grandes superficies con un alto grado de eficiencia. De esta forma, se consigue un ahorro de material, costos de obra y mantenimiento y se gana en seguridad, previniendo intrusiones en un área determinada. Si al sistema se le agregan servidores centralizados de videoanálisis, incluso pueden aprovecharse cámaras de CCTV ya existentes, si las hubiera.

Ubicación de las cámaras

A la hora de armar un sistema de protección perimetral que incluya CCTV es conveniente seguir algunas pautas y tener en cuenta algunas consideraciones para la correcta ubicación de las cámaras. Algunas de ellas son: 1. Las cámaras de un sistema de videovigilancia se utilizan tanto en interiores como en exteriores.

En el segundo caso se deben tener en cuenta los accesorios adecuados para soportar condiciones de intemperie.

Se debe evitar instalar cámaras cerca de fuentes directas de calor (radiadores) o bajo sol directo, para evitar el sobrecalentamiento. También se pueden utilizar sobre techo de caja o cajas con ventilador como precaución.

Las cámaras de exterior deben ser instaladas a una altura mínima de 2,30 metros del suelo. Una vez ubicadas a esta altura, conviene inclinarlas levemente hacia abajo para evitar la visión del cielo a distancia. Esto permitirá ver el área de interés: la cámara captará la distancia máxima que permita la longitud focal de la lente utilizada (máximo aprovechamiento de visión de la cámara). Cuanto más alto se instale la cámara, más habrá que inclinarla hacia abajo, reduciendo en gran proporción la información de control.

Cuando las superficies del ambiente a controlar reciban iluminación directa, las cámaras deben ubicarse por detrás de la fuente de luz. Siempre hay que orientarlas evitando que enfoquen faroles de iluminación, ya que éstos impedirán ver bien lo que se encuentre a su alrededor. El iris de las lentes se cerrará ante faroles, ventanas o cielo, con lo cual se tornarán muy oscuros los objetos, reduciendo notablemente la visión.

Es importante ubicar la cámara cerca del/los objeto/s de interés, para poder observarlo/s con mayor detalle.

Según el campo de visión horizontal y la longitud de las zonas de alarma, las cámaras deben ser orientadas del centro longitudinal de la zona de alarma hacia adentro, con el fin de aumentar la capacidad de visión de la intrusión, la cual se desplaza hacia adentro o el interior del predio

Qwantec (s.f) sobre las rondas exteriores señala que es un sistema electrónico encargado de controlar el cumplimiento de las rondas de vigilantes o guardias, permitiendo garantizar que el personal de vigilancia ya no tendrá la posibilidad de "dormir" o realizar otras labores en el turno de vigilancia. El personal de seguridad deberá cumplir la ronda o será descubierto por el control de rondas Qwantec.

Se instalan puntos de control (no necesitan batería) a lo largo de la ronda y cuando el lector portátil lee el punto de control, registra el nombre del guardia, la hora y la fecha en la cual estuvo el guardia en el punto de control. Al final del día o la semana se pueden descargar los datos en un computador y ver los registros de marcaciones y saber cuál guardia estuvo en qué lugar en qué fecha y hora.

CyberPoint (s.f) sobre el control de ronda nos indica que funciona como puntos de control de datos para las rondas de guardias de seguridad y se puede instalar prácticamente en cualquier lugar como un sistema de rondas de vigilancia tradicional, los miembros del equipo de seguridad confirman su presencia en un lugar al colocar una llave inteligente en una etiqueta electrónica.

Cuando una llave inteligente se presenta a un dispositivo de comunicación, un registro completo de la ronda de vigilancia se carga en el software de gestión. Los informes pueden ser generados, enviados por correo electrónico y analizados.

Una ventaja significativa sobre las aplicaciones de rondas de vigilancia tradicionales es que Cyberpoint es parte del sistema de control de acceso. La misma llave inteligente CyberKey que un guardia que se utiliza para verificar su ubicación también se puede cargar con los permisos de acceso para abrir cilindros designados.

En el software Enterprise, los usuarios pueden activar el módulo de mejora de seguridad de la llave inteligente que permite a las etiquetas electrónicas reactivar temporalmente una llave inteligente expirada. Cuando una llave toca un Cyberpoint con esta función activada, puede acceder a cilindros designados. La activación se apaga después de ocho segundos o de cinco minutos, dependiendo de que preferencia de activación esté configurada.

Iluminet (2017) respecto a La iluminación de seguridad o reflectores nos dice que por sí sola tiene un valor que debe considerarse como parte de un paquete integral; cámaras, monitores, alumbrado público, enrejados, etc. Además de proporcionar una medida de disuasión, la iluminación de seguridad puede aumentar la incertidumbre y la vulnerabilidad de un intruso mientras aporta confianza a los particulares. Las personas se sienten más seguras cuando pueden ver con claridad todo lo que les rodea y cuando pueden ver lo que les espera en el lugar a donde se dirigen.

La iluminación exterior está destinada a mejorar la seguridad, sin embargo demasiada iluminación puede tener el efecto opuesto. La visibilidad es la meta. El resplandor de las luces brillantes y las fuentes que no están cubiertas crean un efecto contrario, pues el brillo en nuestros ojos cierra las pupilas y esto no sólo puede ser cegador, sino que también hace más difícil para nuestros ojos adaptarse. Por lo tanto, el factor clave en cualquier instalación no es el nivel absoluto sino la uniformidad.

INACAL (s.f) El Comité Técnico de Normalización CTN en Seguridad Contra Incendios del INACAL presentó la Norma Técnica Peruana NTP/ISO 13943: Vocabulario, importante instrumento que define términos para su aplicación en ese campo, promoviendo el uso de un lenguaje común.

Para tal fin, y gracias al apoyo de la Sociedad Nacional de Industria - SNI, se organizó la conferencia “Los Incendios en las Edificaciones” que reunión al sector público y privado, incluyendo empresas de seguros para conocer esta nueva NTP.

La presentación estuvo a cargo del presidente del comité técnico, Saúl Montenegro Tello, quien también es presidente del Comité de Seguridad Contra Incendios de la SNI. Montenegro expuso los alcances de la nueva norma que busca establecer un lenguaje común entre los actores involucrados en la prevención de este tipo de siniestros.

Mapfre (s.f) sobre las clases de incendio indica:

Clase A

Símbolo: Triángulo verde

Fuego en materiales secos, sólidos que producen brasa (papel, madera, trapos, plástico).

Clase B

Símbolo: Cuadrado Rojo

Fuegos en materiales líquidos, grasas, gases (petróleo y derivados, aceites, resinas, pinturas, GLP).

Clase C

Símbolo: Círculo Azul

Fuegos en equipos eléctricos con energía (conectados).

Clase D

Símbolo: Estrella Amarilla

Fuegos en metales combustibles (zirconeo, magnesio, aluminio en polvo, etc).

Clase K

Símbolo : Un cuadrado negro con una sartén

Fuego en cocina con presencia de grasa.

Métodos de extinción

Enfriamiento:
Consiste en actuar sobre el calor eliminándolo.

Sofocación:
Consiste en actuar sobre oxígeno, evitando su aportación sobre el combustible, o reduciendo su concentración hasta valores que no permitan continuar la combustión.

Eliminación del Combustible:

Consiste en retirar los combustibles presentes en un incendio antes de que sean afectados por el fuego. Una variante es la SEGREGACIÓN, que consiste en retirar los combustibles alrededor del incendio.

Inhibición:
Consiste en la neutralización química de los radicales libres que dan lugar a la reacción en cadena y por lo tanto a la combustión.

Paritarios.Cl (s.f) hace la definición de tarjeta de seguridad definiéndola como que Indica una superficie, (generalmente cartulina, papel, madera, etc.), sobre la cual aparecen letras o marcas para advertencia, instrucción o información a los trabajadores sobre riesgos a los cuales podrían estar eventualmente expuestos.

EIA (2019) respecto a los detectores metálicos señala:

Siempre son más numerosos los eventos de gran concurrencia de público, que necesitan controles de seguridad con Detectores de Metales a tránsito para todos los que ingresan. Dichos eventos incluyen exposiciones, exhibiciones deportivas, conciertos, congresos, celebraciones de fiestas importantes, etc.

Los Detectores de Metales para eventos públicos deben ofrecer elevadísimas prestaciones en términos de capacidad de detección y de flujo y deben ser especialmente compactos para permitir el fácil transporte, la instalación y el desplazamiento al finalizar las operaciones de control. En los

casos en que los controles se efectúen al aire libre, los dispositivos deben ser capaces de funcionar en cualquier condición atmosférica.

REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN

ARTÍCULO 1: El presente Reglamento tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Este Reglamento no sustituye las medidas específicas que norman el procesamiento de la información clasificada y limitada, que son objeto de normativas emitidas por el Ministerio del Interior.

ARTÍCULO 2: El término Seguridad de las Tecnologías de la Información utilizado en este Reglamento está relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos. El empleo de otros términos, tales como seguridad de la información, seguridad de los ordenadores, seguridad de datos o seguridad informática, tienen a los efectos de lo que aquí se establece, el mismo significado.

ARTÍCULO 3: Este Reglamento será de aplicación, en lo que a cada cual concierne, en todos los Órganos y Organismos de la Administración Central del Estado y sus dependencias; otras entidades estatales; empresas mixtas; sociedades y asociaciones económicas que se constituyan de acuerdo a la Ley; entidades privadas radicadas en el país; organizaciones políticas, sociales y de masas y personas naturales que posean o utilicen, en interés propio o de un tercero, tecnologías de la información. El cumplimiento de este Reglamento en áreas sensibles que son objeto de la atención directa del MININT y el MINFAR será realizado por los especialistas de estos órganos designados al efecto.

DEL SISTEMA DE SEGURIDAD INFORMATICA.

ARTÍCULO 4: Cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un Sistema de Seguridad Informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos: • Minimizar los riesgos sobre los sistemas informáticos. • Garantizar la continuidad de los procesos informáticos.

ARTÍCULO 5: A partir del Sistema de Seguridad Informática diseñado, cada entidad elaborará su Plan de Seguridad Informática.

ARTÍCULO 6: El diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 7: Los jefes de entidades responden por la actualización de los Planes de Seguridad Informática, considerando para ello los siguientes factores: a) La aparición de nuevas vulnerabilidades. b) Los efectos de los cambios de tecnología o de personal. c) La efectividad del sistema, demostrada por la naturaleza, número y daño ocasionado por los incidentes de seguridad registrados;

ARTÍCULO 8: En los Órganos y Organismos de la Administración Central del Estado y en aquellas organizaciones en que las tecnologías de la información son determinantes para su gestión se dispondrá de los 2 cargos de especialistas de Seguridad Informática que se requieran para atender esta actividad, los cuales tendrán las siguientes atribuciones y funciones: a) Organizar y controlar la actividad de Seguridad Informática. b) Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia. c) Supervisar el trabajo del personal que responde por la Seguridad Informática en las entidades y organizar su preparación. d) Proponer medidas ante violaciones de la base legal establecida en la materia.

ARTÍCULO 9: Los jefes a las diferentes instancias en los órganos, organismos y entidades responden por la protección de los bienes

informáticos que le han sido asignados y tienen las siguientes obligaciones: a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos. b) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática en la parte que concierne a su esfera de acción y garantizar su cumplimiento. c) Aplicar las medidas y procedimientos establecidos en su área de responsabilidad. d) Especificar al personal subordinado las medidas y procedimientos establecidos y controlar su cumplimiento. e) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas. f) Imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

ARTÍCULO 10: El responsable de la actividad informática en cada entidad tiene las siguientes obligaciones: a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina de cumplimiento. b) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado. c) Garantizar la disponibilidad de los bienes informáticos. d) Asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las tecnologías de la información. e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la Dirección de la Entidad. f) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas. g) Informar a los usuarios de las regulaciones establecidas.

ARTÍCULO 11: Los usuarios de las tecnologías de la información asumen en primera instancia la responsabilidad de las consecuencias que se deriven de la utilización impropia de las mismas.

ARTÍCULO 12: Los usuarios de las tecnologías de información en órganos, organismos y entidades tienen las siguientes obligaciones: a)

Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.

b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.

c) Utilizar las tecnologías de información solo en interés de la entidad.

d) No transgredir ninguna de las medidas de seguridad establecidas.

e) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.

f) No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.

g) Cumplir las reglas establecidas para el empleo de las contraseñas.

h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

Clasificación y control de bienes informáticos

ARTÍCULO 13: Los bienes informáticos de una entidad deben ser utilizados en las funciones propias del trabajo

en correspondencia con su objeto social.

ARTÍCULO 14: Todos los bienes informáticos de una entidad deberán estar identificados y controlados, para lo

cual se conformará y mantendrá actualizado un inventario de éstos incluyendo sus componentes y las

especificaciones técnicas de aquellos que pudieran ser suplantados.

ARTÍCULO 15: Cada uno de los bienes informáticos de una entidad tienen que ser puestos bajo la custodia

documentada legalmente de una persona, que actuando por delegación de la dirección de la entidad, es

responsable de su protección.

ARTÍCULO 16: Los jefes de entidades instrumentarán los procedimientos que se requieran para garantizar la

autorización y el control sobre el movimiento de los bienes informáticos, los cuales deberán ser considerados a

esos efectos de igual forma que el resto de los medios de la entidad.

Sección Segunda

Del personal

ARTÍCULO 17: Las funciones y responsabilidades de seguridad, tanto general como específica, serán

documentadas y se incluirán dentro de las responsabilidades laborales del personal.

ARTÍCULO 18: El personal previsto para ocupar cargos vinculados a la actividad informática en órganos,

organismos, entidades, organizaciones políticas, sociales y de masas, incluyendo personal eventual,

estudiantes insertados y otros casos similares con acceso a sistemas críticos, a información de valor o a la

supervisión y seguridad de los sistemas, deberá ser seleccionado adecuadamente.

ARTÍCULO 19: Los términos y condiciones del contrato de empleo incluirán la obligación de la entidad

contratante en cuanto a la preparación del contratado, así como la responsabilidad del trabajador hacia la

Seguridad Informática, precisando que este último aspecto mantiene su vigencia una vez finalizada la relación

laboral. Deberán incluirse las acciones a tomar en caso que el trabajador pase por alto los requerimientos de

seguridad.

ARTÍCULO 20: La utilización de las tecnologías y sus servicios asociados en cada entidad estará aprobada

previamente por la dirección de la misma y basada en cada caso en la necesidad de uso por interés de la

propia entidad.

ARTÍCULO 21: El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una

violación de los derechos de la entidad que es sancionable. Es un deber y un derecho de la dirección de cada

entidad la supervisión del empleo de las tecnologías de la información por parte de los usuarios.

ARTÍCULO 22: Los Jefes a cada nivel, garantizarán que el personal vinculado a las tecnologías de la

información esté capacitado para la utilización de las mismas, así como que conozca sus deberes y derechos

en relación con el Sistema de Seguridad Informática implementado, los cuales deberán firmar una declaración

como constancia de su conocimiento y compromiso de cumplimiento, que se incluirá en el contrato de trabajo.

ARTÍCULO 23: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por

parte de personal que no forme parte de la plantilla será en todos los casos objeto de una estricta autorización y

control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir se

establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

ARTÍCULO 24: Los usuarios de las tecnologías de la información están en la obligación de informar de

inmediato cualquier incidente de seguridad, debilidad o amenaza a sistemas o servicios y las direcciones

correspondientes exigirán su cumplimiento.

ARTÍCULO 25: Constituye una violación grave de la seguridad la realización de acciones de comprobación de

vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

ARTÍCULO 26: Ninguna persona está autorizada a introducir, ejecutar, distribuir o conservar en los medios de

cómputo programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, así como

información contraria al interés social, la moral y las buenas costumbres, excepto aquellas aplicaciones

destinadas a la comprobación del sistema instalado en la organización para uso por especialistas expresamente

autorizados por la dirección de la misma. En ningún caso este tipo de programas o información se expondrá

mediante las tecnologías para su libre acceso.

Sección Tercera

Seguridad Física y Ambiental

ARTÍCULO 27: La dirección de cada entidad determinará las tecnologías de información que por las funciones a

que estén destinadas, la información que contengan y las condiciones de los locales en que se encuentren

ubicadas, requieran la aplicación específica de medidas de protección física.

ARTÍCULO 28: Las tecnologías de la información se ubicarán en áreas que garanticen la aplicación de medidas

alternativas que permitan la creación de una barrera de protección a estos medios e impidan su empleo para

cometer acciones malintencionadas o delictivas.

ARTÍCULO 29: En los edificios e instalaciones de cada entidad se determinarán áreas o zonas controladas con

requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la

importancia de los bienes informáticos contenidos en ellas y su utilización, de acuerdo con los criterios y

denominaciones siguientes:

a) Áreas limitadas, son aquellas donde se concentran bienes informáticos de valor medio cuya

afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.

b) Áreas restringidas, son aquellas en que se concentran bienes informáticos de alto valor e

importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o

sectores de la economía o de la sociedad; territorios o entidades.

c) Áreas estratégicas, son aquellas en que se concentran bienes informáticos de alto valor e

importancia crítica que inciden de forma determinante en la seguridad y la defensa nacional; la

seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las

redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la

economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de

la población; la salud pública y el suministro de agua.

ARTÍCULO 30: Las áreas o zonas controladas estarán protegidas con medidas adecuadas para garantizar el

acceso exclusivamente al personal autorizado.

ARTÍCULO 31: La selección y diseño de las áreas controladas tomará en cuenta la posibilidad de daño por

fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

ARTÍCULO 32: El equipamiento instalado en las áreas controladas estará protegido contra fallas de

alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los

procesos que deban continuar en caso de un fallo de electricidad prolongado y será ubicado y protegido de

manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso

no autorizado.

ARTÍCULO 33: En las Áreas Limitadas se aplicarán las medidas de protección física siguientes:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros;

b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán

medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo;

c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.

d) Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización

por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su

verificación en caso de necesidad.

ARTÍCULO 34: En las Áreas Restringidas, además de las medidas requeridas en las Áreas Limitadas, se

aplicarán las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las

mismas debe ser controlado mediante los documentos de registro que para ello se establezcan;

b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.

c) Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren

fuera del alcance de estas áreas ni a redes públicas de transmisión de datos;

d) Se aplicarán sistemas de detección y alarma que permitan una respuesta , efectiva ante accesos no

autorizados cuando no se encuentre el personal que labora en las mismas;

e) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas

áreas;

f) Se prohíbe la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido

autorizados de forma expresa por la dirección de la entidad.

g) Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de

almacenamiento digital ajeno a la misma.

ARTÍCULO 35: En las Áreas Estratégicas, además de las medidas requeridas en las Áreas Restringidas y

Limitadas, se aplicarán las siguientes:

a) Todo el personal que labora en ellas o que por razones de servicio sea autorizado a permanecer en las

mismas, deberá contar con una identificación personal visible que distinga el área.

b) Se implementarán medios especiales de supervisión de la actividad que en ellas se realiza;

c) El acceso a estas áreas por personas ajenas a la misma solo se realizará de manera excepcional,

restringida y bajo supervisión, mediante un permiso especial en cada caso emitido por la dirección de la

entidad.

ARTÍCULO 36: Todas las tecnologías de información, independientemente de su importancia, se protegerán

contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que

contienen.

ARTÍCULO 37: En las redes de las entidades los cables de alimentación o de comunicaciones que transporten

datos o apoyen los servicios de información se protegerán contra la intercepción o el daño. Los cables de

alimentación deberán estar separados de los cables de comunicaciones para evitar la interferencia.

ARTÍCULO 38: Los jefes de entidades garantizarán que el equipamiento reciba el mantenimiento correcto de

acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante para asegurar su

disponibilidad e integridad continuas. En caso de necesidad de envío de equipamiento fuera de las

instalaciones para que reciban mantenimiento, se realizará en correspondencia con los procedimientos que se

establezcan previamente para ello, observando las regulaciones establecidas en el país en materia de

protección a la información.

ARTÍCULO 39: El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de

información tiene que estar autorizado legalmente por la dirección de la misma mediante el documento

correspondiente. La seguridad que se le garantice deberá ser equivalente a la que tiene en las instalaciones

habituales el equipamiento usado para el mismo propósito, tomando en cuenta los riesgos de trabajar fuera de

la instalación.

ARTÍCULO 40: El equipamiento que cause baja o sea destinado para otras funciones será objeto de un

procedimiento adecuado para evitar que la información que contiene pueda resultar comprometida. Los

dispositivos de almacenamiento que contengan información crítica para la entidad deberán destruirse

físicamente o sobrescribirse mediante un proceso completo en lugar de borrarlos como usualmente se hace.

ARTÍCULO 41: Se prohíbe el movimiento sin autorización de los equipos, la información o el software y en caso

de que se autorice será realizado mediante un documento oficial que demuestre su legalidad y el movimiento

deberá registrarse a la salida y a la entrada al reintegrarse el medio a su origen. Se deberán realizar

inspecciones sorpresivas para detectar las extracciones no autorizadas.

Sección Cuarta

Seguridad de Operaciones

ARTÍCULO 42: Al determinar las responsabilidades que se asignan al personal se tendrá en cuenta el principio

de separación de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona,

a fin de reducir oportunidades de modificación no autorizada o mal uso de los sistemas informáticos.

ARTÍCULO 43: La introducción en una entidad de nuevos sistemas informáticos, actualizaciones y nuevas

versiones será aprobada previamente a partir de su correspondencia con el sistema de seguridad establecido y

los resultados de las pruebas que se realicen para determinar si cumple los criterios de seguridad apropiados.

ARTÍCULO 44: Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema

deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que:

a) solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a

los datos;

b) todas las acciones de emergencia tomadas sean documentadas detalladamente;

c) la acción de emergencia sea reportada a la dirección y realizada de manera ordenada;

Sección Quinta

Identificación, autenticación y control de accesos

ARTÍCULO 45: En los sistemas en que es posible el acceso por múltiples usuarios se dispondrá para cada uno

de ellos de un identificador de usuario personal y único. Las personas a las que se asignen identificadores de

usuarios responden por las acciones que con ellos se realicen.

ARTÍCULO 46: La asignación de nuevos identificadores de usuarios en los sistemas se realizará a partir de un

procedimiento que incluya la notificación del jefe inmediato del usuario. En caso de terminación de la necesidad

del uso de los sistemas por el cese de la relación laboral u otras causas, se procederá de forma análoga para la

eliminación del identificador de usuario.

ARTÍCULO 47: Para la utilización de contraseñas como método de autenticación de usuarios, se cumplirán los

siguientes requisitos:

a) Serán privadas e intransferibles.

b) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado

para el acceso que protegen.

c) Combinarán en todos los casos letras y números sin un significado evidente, con una longitud

mínima de 6 caracteres.

d) No pueden ser visualizadas en pantalla mientras se teclean.

e) No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.

ARTÍCULO 48: En cada entidad se definirán de manera estricta los derechos y privilegios de acceso a sistemas

y datos que tiene cada usuario y se implementará un procedimiento escrito en cada caso para otorgar o

suspender dichos accesos.

Sección Sexta

Seguridad ante programas malignos

ARTÍCULO 49: Se prohíbe el diseño, la distribución o intercambio de códigos de virus informáticos u otros

programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la

autoridad competente para el análisis e investigación de programas malignos.

ARTÍCULO 50: En cada entidad se implementarán los controles y procedimientos para protegerse contra virus y

otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su

generalización. Para la protección contra virus se utilizarán los programas antivirus de producción nacional u

otros autorizados oficialmente para su uso en el país, debidamente actualizados.

ARTÍCULO 51: Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no

conectados a redes, se procederá al cese de la operación de los medios implicados y a su desconexión de las

redes cuando corresponda, preservándolos para su posterior análisis y descontaminación por personal

especializado y se revisarán los soportes con los cuales haya interactuado el medio contaminado.

ARTÍCULO 52: La contaminación por virus informáticos u otros programas malignos se considera un incidente

de seguridad y se cumplirá en este caso lo establecido en el Artículo 89 del presente Reglamento. En todos los

casos se determinará el origen y la responsabilidad de las personas involucradas.

Sección Séptima

Respaldo de la información

ARTÍCULO 53: Todas las entidades están en la obligación de implementar un sistema fiable de respaldo de la

información esencial para su funcionamiento que permita la recuperación después de un ataque informático,

desastre o fallo de los medios, para lo cual ejecutarán los procedimientos que aseguren la obtención

sistemática de las copias que se requieran.

ARTÍCULO 54: La información de respaldo, conjuntamente con informes precisos y completos de las copias de

respaldo y los procedimientos de recuperación documentados deberá almacenarse en otra ubicación que le

permita no afectarse en caso de desastre en la ubicación principal.

ARTÍCULO 55: La información de respaldo deberá tener una protección física y ambiental consecuente con las

normas aplicadas en la ubicación principal. Los controles aplicados a los medios en la ubicación principal

deberán extenderse a la ubicación de los medios de respaldo.

ARTÍCULO 56: Los medios de respaldo deberán probarse regularmente y verificar su estado de actualización

con el fin de asegurar que pueda confiarse en ellos para un uso de emergencia cuando sea necesario.

Sección Octava

Seguridad en Redes

ARTÍCULO 57: Los órganos, organismos y entidades están en la obligación de implementar los mecanismos de

seguridad de los cuales están provistas las redes, así como de aquellos que permitan filtrar o depurar la

información que se intercambie.

ARTÍCULO 58: En todas las redes se habilitarán las opciones de seguridad con que cuentan los sistemas

operativos de forma tal que se garantice la protección de los servidores y las terminales, el acceso a la

información solamente por personal autorizado y los elementos que permitan el monitoreo y auditoria de los

principales eventos por un tiempo no menor de un año.

ARTÍCULO 59: Para la fiscalización y el monitoreo del empleo que se le da a las redes de datos y de los

servicios en ellas implementadas las entidades instalarán los productos autorizados en el país para esos

propósitos.

ARTÍCULO 60: La arquitectura y la configuración de los diferentes componentes de seguridad de una red y la

implementación de sus servicios estarán en correspondencia con las políticas definidas y aprobadas para su

empleo y en ningún caso deben ser el resultado de la iniciativa de una persona con independencia de la

preparación que ésta posea.

ARTÍCULO 61: Toda red de computadoras deberá contar para su operación con la existencia de al menos una

persona encargada de su administración.

ARTÍCULO 62: El Administrador de una red tiene, en relación con la Seguridad Informática, las siguientes

obligaciones:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.

b) Realizar el análisis sistemático de los registros de auditoria que proporciona el sistema operativo de la red.

c) Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.

d) Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier

violación o anomalía detectada en los existentes.

h) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y

acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.

i) Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas

periódicas.

e) Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.

f) Participar en la confección y actualización del Plan de Seguridad Informática.

ARTÍCULO 63: La gestión de administración de las redes implica la concesión de máximos privilegios,

debiéndose realizar directamente desde los puestos de trabajo habilitados al efecto. Se prohíbe la

administración remota de estas redes mediante conexiones conmutadas a través de las redes públicas

de transmisión de datos.

ARTÍCULO 64: Se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software en una

red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la

dirección de la entidad, garantizando su compatibilización con las medidas de seguridad establecidas para la

protección de dicha red.

ARTÍCULO 65: Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las

redes son responsables por su propia conducta. Los usuarios deben conocer las políticas de seguridad para las

computadoras y redes a que ellos acceden y están en la obligación de cumplir estas políticas.

ARTÍCULO 66: En las redes que prevean conexiones desde o hacia el exterior de una entidad es obligatorio

instalar los medios técnicos que aseguren una barrera de protección entre las tecnologías de información de la

entidad y la red externa, mediante los mecanismos de seguridad que sea necesario implementar.

ARTÍCULO 67: Las entidades instrumentarán la ejecución de procedimientos periódicos de verificación de la

seguridad de las redes con el fin de detectar posibles vulnerabilidades, incluyendo para ello cuando sea

procedente la comprobación de forma remota por entidades autorizadas oficialmente a esos efectos, debido a la

sensibilidad de estas acciones.

ARTÍCULO 68: Las entidades autorizadas oficialmente para la comprobación de la seguridad de las

redes de otras entidades están en la obligación de:

a) Garantizar la profesionalidad que requiere esta actividad.

b) Obtener la aprobación previa de las entidades que requieren estos servicios para su realización.

c) Mantener el máximo de discreción con relación a las posibles vulnerabilidades detectadas.

d) Abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio

propio.

e) Informar a la Oficina de Seguridad para las Redes Informáticas de los resultados de las

comprobaciones realizadas.

ARTÍCULO 69: En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras

redes o usuarios externos se implementarán mecanismos de seguridad que garanticen la confidencialidad, la

integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

ARTÍCULO 70: Las entidades que coloquen información en servidores para su acceso público, establecerán las

medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su

contenido con los intereses de la propia entidad y del país.

ARTÍCULO 71: Si por necesidades de conectividad u otros intereses se requiere hospedar un sitio en

servidores ubicados en un país extranjero, siempre se hará como espejo o réplica del sitio principal en

servidores ubicados en Cuba, estableciendo las medidas requeridas para garantizar su seguridad,

particularmente durante el proceso de actualización de la información.

ARTÍCULO 72: Se prohíbe la colocación de páginas o sitios Web desde entidades estatales en servidores

extranjeros que ofrecen estos servicios de forma gratuita.

ARTÍCULO 73: Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior

de las mismas no serán instalados en las máquinas en que se instalen los servidores destinados para el uso

interno de dicha red.

ARTÍCULO 74: En los casos de redes corporativas que prevean la extrapolación de servicios internos, esto se

realizará por puertos bien identificados y mediante la protección con dispositivos que garanticen el acceso a

esos servicios por el personal autorizado.

ARTÍCULO 75: Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas solo

se utilizarán en interés de la misma. La asignación de cuentas para el empleo de estos servicios será aprobada

en todos los casos por la dirección de la entidad sobre la base de las necesidades requeridas para su

funcionamiento.

ARTÍCULO 76: Se prohíbe el establecimiento de cuentas de correo electrónico desde entidades

estatales en servidores que se encuentran en el exterior del país, considerando la inseguridad que el

empleo de los mismos implica para la entidad por hallarse fuera del control del Estado Cubano. Si de

manera excepcional por no haber otra alternativa, surgiera esta necesidad de forma puntual, tiene que

ser aprobada previamente y por escrito por la dirección de la entidad, a partir de la valoración de las

razones existentes, especificando claramente el tipo de información que se va a transmitir y el plazo de

vigencia de esta modalidad.

ARTÍCULO 77: Se prohíbe vincular cuentas de correo electrónico de un servidor de una entidad a un

servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo.

ARTÍCULO 78: La suscripción a listas de correo electrónico y el empleo de servicios de conversación en

tiempo real (chat) por parte del personal de una entidad será autorizado en todos los casos por la

dirección de la misma en correspondencia con sus intereses y de las normas particulares establecidas

para estos servicios, debiendo documentarse esta autorización de manera que pueda ser objeto de

comprobación.

ARTÍCULO 79: Se prohíbe la difusión a través de las redes públicas de transmisión de datos de información

contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la

Seguridad Nacional, por cualquier persona natural o jurídica. Las entidades instalarán los controles y

mecanismos que permitan detectar y obstaculizar este tipo de actividades. Las violaciones detectadas serán

informadas oportunamente a las instancias pertinentes.

ARTÍCULO 80: Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico

no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sean de carácter informativo, comercial,

cultural, social, con intenciones de engaño (hoax) u otros.

ARTÍCULO 81: Las redes proveedoras de servicios tomarán las medidas que se requieran para impedir la

sobrecarga de los canales de comunicaciones, restringiendo el envío o recepción de grandes volúmenes de

información y la generación de mensajes a múltiples destinatarios.

ARTÍCULO 82: Las entidades implementarán controles dirigidos a impedir e interrumpir la generación de cartas

en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

ARTÍCULO 83: Las entidades con redes destinadas a proveer servicios a otras personas naturales o jurídicas

mediante conexiones remotas están en la obligación de cumplir los aspectos siguientes:

a) Establecer las medidas y procedimientos de Seguridad Informática que garanticen la protección de los

servicios a brindar y los intereses de seguridad de los que los reciben.

b) Implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones,

incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año.

c) Dar a conocer a los clientes de estos servicios los requerimientos de Seguridad Informática que deben

cumplir en correspondencia con las políticas de seguridad establecidas en la red que los brinda.

d) Facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar con las

mismas en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

ARTÍCULO 84: Ninguna persona, natural o jurídica está autorizada para explorar o monitorear las redes

públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales

de las mismas.

ARTÍCULO 85: El acceso no autorizado o la agresión a cualquier sistema de cómputo conectado a las redes

públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente

autorizados se consideran violaciones del presente Reglamento, independientemente de otras implicaciones

legales que puedan derivarse de estas acciones.

2.3. Definición de términos básicos

- Amenaza: Acción consistente en el anuncio de un mal futuro, injusto y aparentemente real, con el fin de intimidar el ánimo de aquel a quien se dirige
- Auditoría: Examen de la información por terceras partes, distintas de quienes la generan y quienes la utilizan, con la intención de establecer su suficiencia y adecuación, e informar de los resultados del examen con objeto de mejorar su calidad
- Autenticación: La acción de verificar la elegibilidad del usuario para tener acceso a la información. Por lo general diseñada para proteger la actividad de logon mal intencionada
- Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada
- Contraseña: Palabra o cadena de caracteres, normalmente secreta, para acceder a través de una barrera. Se usa como herramienta de seguridad para identificar usuarios de una aplicación, archivo o red. Puede terner la forma de una palabra o frase de carácter alfanumérico y se usa para prevenir accesos no autorizados a información confidencia
- Control interno: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos de negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos
- Controles correctivos: Controles diseñados para corregir errores, omisiones, usos no autorizados e intromisiones una vez éstos han sido detectados
- Controles de detección: Controles para detectar e informar de la ocurrencia de errores, omisiones y utilización o carga no autorizada

- Dato de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables
- Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio
- Plan de seguridad: Correcta planificación de la seguridad que permita la adopción de las medidas adecuadas en cuanto a su tipo (prevención, detección y recuperación) y naturaleza (física, técnica y administrativa)
- Responsable de seguridad: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables
- Riesgo: La probabilidad de ocurrencia de una acción o evento adverso
- Seguridad: Facultad de estar a cubierto de algún riesgo o amenaza
- Seguridad física: Trata de la protección física de los datos, programas, equipos, redes, soportes, instalaciones y personas
- Control de riesgos: Es el proceso de toma de decisión, basado en la información obtenida en la evaluación de riesgos. Se orienta a reducir los riesgos, a través de proponer medidas correctoras, exigir su cumplimiento y evaluar periódicamente su eficacia.
- Cultura de seguridad o cultura de prevención: Conjunto de valores, principios y normas de comportamiento y conocimiento respecto a la prevención de riesgos en el trabajo que comparten los miembros de una organización.
- Emergencia: Evento o suceso grave que surge debido a factores naturales o como consecuencia de riesgos y procesos peligrosos en el trabajo, que no fueron considerados en la gestión de seguridad y salud en el trabajo.
- Evaluación de riesgos: Proceso posterior a la identificación de los peligros, que permite valorar el nivel, grado y gravedad de los mismos, proporcionando la información necesaria para que la empresa esté en condiciones de tomar una decisión apropiada sobre la oportunidad, prioridad y tipo de acciones preventivas que debe adoptar.
- Gestión de la Seguridad y Salud: Aplicación de los principios de la administración moderna a la seguridad y salud, integrándola a la producción, calidad y control de costos.

- Gestión de Riesgos: Es el procedimiento, que permite una vez caracterizado el riesgo, la aplicación de las medidas más adecuadas para reducir al mínimo los riesgos determinados y mitigar sus efectos, al tiempo que se obtienen los resultados esperados.
- -Identificación de Peligros: Proceso mediante el cual se localiza y reconoce que existe un peligro y se definen sus características.
- Medidas de Prevención: Acciones que se adoptan ante los riesgos identificados con el fin de evitar lesiones a la salud y/o disminuir los riesgos presentes en el trabajo, dirigidas a proteger la salud de los trabajadores. Medidas cuya implementación constituye una obligación y deber de parte de los empleadores.
- Peligro: Situación o característica intrínseca de algo capaz de ocasionar daños a las personas, equipo, procesos y ambiente.
- Prevención de Accidentes: Combinación de políticas, estándares, procedimientos, actividades y prácticas en el proceso y organización del trabajo, que establece una organización en el objetivos de prevenir riesgos en el trabajo.
- Primeros Auxilios: Protocolos de atención de emergencia que atiende de inmediato en el trabajo a una persona que ha sufrido un accidente o enfermedad ocupacional.
- Proactividad: Actitud favorable en el cumplimiento de las normas de seguridad y salud en el trabajo con diligencia y eficacia.
- Seguridad: Son todas aquellas acciones y actividades que permiten al trabajador laborar en condiciones de no agresión tanto ambientales como personales, para preservar su salud y conservar los recursos humanos y materiales.
- Enemigo: Nación extranjera, agrupación política, persona extranjera o del país que realiza actos contra la Seguridad Nacional o Institucional, en forma intencional y consciente.
- - Seguridad: Estado de confianza y tranquilidad de una persona o grupo humano basado en el convencimiento que no hay ningún peligro que temer, después de haber adoptado una serie de medidas o normas que supriman todos los riesgos que se presenten.

- Seguridad Integral (Nacional): Conjunto de acciones que tiene que realizar un Estado para garantizar su soberanía y libertad de acción para alcanzar sus objetivos nacionales.
- - Seguridad Militar: Estado de confianza y tranquilidad del Jefe y demás integrantes de una unidad, instalación o dependencia militar y del área de su responsabilidad, que se basa en el convencimiento de que no hay ningún peligro que temer, al haberse adoptado las medidas necesarias para evitar todo riesgo en el personal, la información, las instalaciones, el material y el equipo.
- - Medidas de Seguridad: Actos, acciones y operaciones de carácter activo, pasivo y de engaño que se toman para alcanzar la condición de seguridad.
- Contrainteligencia: Conjunto de medidas adoptadas para neutralizar o impedir las actividades de inteligencia del enemigo.
- Contrasabotaje: Conjunto de medidas destinadas a detectar, neutralizar y/o impedir los actos de sabotaje del enemigo.
- Contraespionaje: Conjunto de medidas a detectar, neutralizar y/o impedir el espionaje enemigo.
- Contrasubversión: Conjunto de medidas destinadas a descubrir, neutralizar y/o impedir las actividades subversivas.
- Riesgos de Seguridad: Peligros evidentes o encubiertos contra la Seguridad.
- Estudio de Seguridad: Actividades que se realizan para detectar los riesgos de seguridad existentes en una unidad, dependencia e instalación.
- Plan de Seguridad: Plan que se formula para prevenir a una instalación contra los riesgos internos o externos que pudieran amenazarla. Se formula siguiendo los lineamientos de un Plan de Seguridad. Este documento forma parte de la Guía de Procedimientos de la unidad, dependencia e instalación.
- POV de Seguridad: Documento que contiene las medidas de seguridad que por ser rutinarias no se consideran en el Plan de Seguridad. Este documento forma parte de la Guía de Procedimientos de la unidad, dependencia e instalación.

- Inspección de Seguridad: Actividad que se realiza para verificar la forma como se están cumpliendo las medidas de seguridad adoptadas en una unidad, dependencia e instalación.
- Conciencia de Seguridad: Es el conocimiento permanente de los riesgos de seguridad y de la obligación que se tiene de adoptar las medidas que sean necesarias.
- Guía de Procedimientos: Documento clasificado que contiene los procedimientos que se ejecutan en guarnición, relacionados con la seguridad militar de la Unidad, dependencia o instalación

2.4. Hipótesis

2.4.1. Hipótesis General

Existe relación significativa entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.4.2. Hipótesis General Nula

No existe relación significativa entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.4.3. Hipótesis Específica 1

Existe relación significativa entre las medidas de seguridad y el control de acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.4.4. Hipótesis Especifica 1 Nula

No existe relación significativa entre las medidas de seguridad y el control de acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.4.5. Hipótesis Específica 2

Existe relación significativa entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.4.6. Hipótesis Específica 2 Nula

No existe relación significativa entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

2.5. Variables

2.5.1. Definición conceptual

2.5.1.1. Medidas de seguridad:

Acciones que se adoptan ante los riesgos de espionaje o sabotaje por parte de elementos desconocidos, con el fin darle protección a los recursos humanos, económicos y materiales de una determinada instalación.

2.5.1.2. Control de Acceso:

Identificación y chequeo que se hace a personas propias o visitas que desean ingresar a una determinada instalación.

2.5.2. Definición operacional

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ITEM
Medidas de seguridad	Acciones que se adoptan ante los riesgos de espionaje o sabotaje por parte de elementos desconocidos, con el fin darle protección a los recursos humanos, económicos y materiales de una determinada instalación.	1. Medidas de seguridad externa	1.1 M. contra el sabotaje 1.2 Cámaras perimétricas 1.3 Rondas externas 1.4 Reflectores externos	1. ¿Cree ud que las medidas de seguridad contra el sabotaje que se aplican en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar? 2. ¿Considera ud que las cámaras de seguridad instaladas en el exterior mejoran el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar? 3. ¿Piensa ud que las rondas externas ayudan con el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar? 4. ¿Cree ud que los reflectores instalados en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?
		.2. Medidas de seguridad interna	2.2 Rondas internas 2.3 Chapas y candados	5. ¿Cree ud que las rondas internas facilitan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar? 6. ¿Considera ud que las chapas y candados colocados en las puertas obstaculizan el acceso de personas a las oficinas y ambientes internos de las instalaciones?
Control de Acceso	Identificación y chequeo que se hace a personas propias o visitas que desean ingresar a una determinada instalación.	1. Control de acceso para el personal que labora en las instalaciones	1.1 Registro de personal 1.2 Control de ingreso a Áreas reservadas 1.3 Tarjetas de seguridad	7. ¿Cree ud que el registro de personas y vehículos pertenecientes a la Escuela Militar facilita el control de acceso a dichas instalaciones? 8. ¿Piensa ud que el control de ingreso a áreas reservadas por parte del personal que labora en la Escuela Militar es una medida de seguridad vital dentro las instalaciones militares? 9. ¿Considera ud que las tarjetas de seguridad (fotochek) es importante para identificar al personal que labora en las instalaciones de la Escuela Militar?

		2.Control de acceso para visitas	2.1 Registro de visitas 2.2 Detector de metales 2.3 Tarjeta de visitas 2.4 Centinelas	10. ¿Cree ud que el registro de visitas facilita el control de acceso a las instalaciones de la Escuela Militar? 11. ¿Considera ud que el detector de metales es una medida de seguridad importante para el control de personas que ingresan a las instalaciones militares? 12. ¿Cree ud que las tarjetas de visitas contribuye al control de ingreso a las instalaciones de la Escuela Militar? 13. ¿Considera ud que el empleo de centinelas distribuidos en zonas críticas contribuye al control de acceso a las instalaciones de la Escuela Militar?

CAPÍTULO III. MARCO METODOLÓGICO

3.1. Enfoque

Mixto: Cuantitativo

El trabajo de investigación se sustenta en el enfoque cuantitativo:

(Hernández, Fernández y Baptista - 2007)

3.2. Tipo

Básico, descriptivo- correlacional.

Es descriptivo porque describe situaciones y eventos. Esto es, como es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Miden o evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar.

Un estudio correlacional determina si dos variables están correlacionadas o no. Esto significa analizar si un aumento o disminución en una variable coincide con un aumento o disminución en la otra variable.
(Hernández, Fernández y Baptista - 2007)

3.3. Diseño

No experimental – de corte transversal

El diseño no experimental-transversal las variables independientes no se manipulan porque ya han sucedido. Las inferencias sobre las relaciones entre variables se realizan sin influencia directa y experimental, dichas relaciones se observan tal y como se han dado en su contexto natural.
(Hernández, Fernández y Baptista - 2007)

3.4. Método

El método empleado en esta investigación es hipotético – deductivo toda vez que se plantean hipótesis general y específicas que se contrastan para conocer las conclusiones e inferir las recomendaciones; asimismo se emplea la deducción que es un método científico que va de lo específico a lo general.

3.5. Población y muestra

3.5.1. Población:

La población la conforma doscientos veinticinco (225) cadetes de cuarto año de la Escuela Militar de Chorrillos, estratificados de la siguiente manera:

- **INFANTERÍA : 89**
- **ARTILLERÍA : 26**
- **CABALLERÍA : 32**
- **INGENIERÍA : 25**
- **COMUNICACIONES : 20**
- **MATERIAL DE GUERRA : 07**
- **INTENDENCIA : 10**
- **INTELIGENCIA : 16**

TOTAL : 225

La población es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado. Cuando se vaya a llevar a cabo alguna investigación se debe tener en cuenta algunas características esenciales al seleccionarse la población bajo estudio.

(Hernández, Fernández y Baptista - 2007)

3.1.1. Muestra:

Para hallar la muestra no se empleó la fórmula tradicional. Se empleó calculadora de internet denominada "Calculo del tamaño de muestra" en Excel, la misma que se muestra a continuación:

MUESTREO ALEATORIO ESTRATIFICADO CON AFIJACIÓN PROPORCIONAL

Tamaño de la población objetivo……	225
Tamaño de la muestra que se desea obtener……	143
Número de estratos a considerar……..…	8

Estrato	Identificación	Nº sujetos en el estrato	Proporción	Muestra del estrato
1	**INFANTERÍA**	89	39,6%	**57**
2	**ARTILLERÍA**	26	11,6%	**17**
3	**CABALLERÍA**	32	14,2%	**20**
4	**INGENIERÍA**	25	11,1%	**16**
5	**COMUNICACIONES**	20	8,9%	**13**
6	**MATERIAL DE GUERRA**	7	3,1%	**4**
7	**INTENDENCIA**	10	4,4%	**6**
8	**INTELIGENCIA**	16	7,1%	**10**
			100,0%	**143**

> Cuando la población es grande, la muestra es un subconjunto extraído de la población, cuyo estudio sirve para inferir características de la población.
> (Hernández, Fernández y Baptista - 2007)

3.6. Técnicas e instrumentos para recolección de datos

Se empleó como técnica una encuesta conformada por 15 ítems redactada de manera clara y simple en base a cada uno de los indicadores de las dimensiones.

Se empleó como instrumento el cuestionario por medio del cual se ha obtenido información sintetizada que se ha utilizado para interpretar los resultados. Los datos recolectados están íntimamente relacionados con las variables de estudio y con los objetivos planteados.

(Hernández, Fernández y Baptista - 2007)

3.7. Validación y confiabilidad del instrumento

Para validar los instrumentos se sometieron los Ítems a juicio de expertos, los cuales evaluaron y asignaron un atributo para cada Ítem, en base a estos resultados se procedió a llenar la hoja resumen de opinión de expertos para determinar el atributo promedio que corresponde a cada Ítem.

Para establecer la confiabilidad de los instrumentos se implementó una prueba piloto para luego someter los resultados de dicho instrumento a la prueba del Alfa de Cronbach con el programa de SPSS 22, aceptando solo aquellos ítems que obtuvieran un atributo mayor a 0.8 de coeficiente de confiabilidad.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,816	13

3.8. Procedimientos para el tratamiento de datos

Consiste en procesar los datos (dispersos, desordenados, individuales) obtenidos de la muestra objeto de estudio durante el trabajo de campo y tiene como fin generar resultados (datos agrupados y ordenados), a partir de los cuales se ha realizado el análisis según los objetivos de hipótesis de la investigación.

Se ha empleado el paquete estadístico SPSS para elaborar las tablas de frecuencia y las figuras correspondientes a cada ítem.

3.9. Aspectos éticos.

La presente investigación se ha desarrollado teniendo en cuenta el aspecto moral de la investigadora (honestidad, práctica de valores, etc.), prueba de ello adjunto documentos importantes:

- Base de Datos.
- Instrumento de recolección de datos
- Validación del instrumento
- Constancia de la entidad donde se realizó la investigación.
- Compromiso de autenticidad del instrumento

CAPÍTULO IV. RESULTADOS

4.1. Descripción

Este párrafo se refiere a la descripción de las gráficas. Los resultados que arroja la investigación de los escritos sometidos a análisis, demuestran, en primer lugar, la justificación del trabajo llevado a cabo porque nos ha permitido identificar en la dimensión adecuada, la existencia de un problema motivo de una investigación.

Las gráficas son el instrumento que nos ha permitido despejar nuestras dudas para darnos la certidumbre de que el problema, de persistir, se puede corregir para luego arribar a conclusiones y recomendaciones.

Hernández (2015) dice que la investigación descriptiva permite detallar situaciones y eventos, es decir como es y cómo se manifiesta determinado fenómeno y busca especificar propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis.

La investigación correlacional es un tipo de método de investigación no experimental en el cual un investigador mide dos variables. Entiende y evalúa la relación estadística entre ellas sin influencia de ninguna variable extraña.

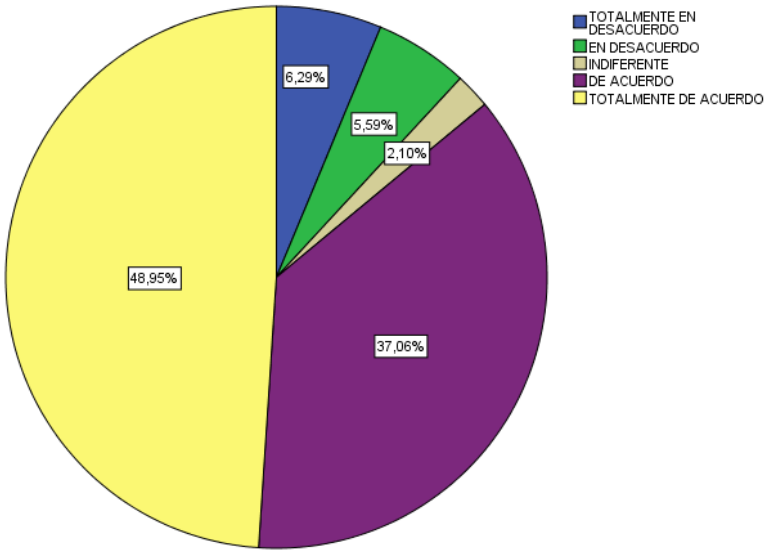
1 VARIABLE INDEPENDIENTE: Medidas de Seguridad

Tabla1

¿Cree ud que las medidas de seguridad contra el sabotaje que se aplican en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		9	6,3	6,3	6,3
	EN DESACUERDO		8	5,6	5,6	11,9
	INDIFERENTE		3	2,1	2,1	14,0
	DE ACUERDO		53	36,8	37,1	51,0
	TOTALMENTE DE ACUERDO		70	48,6	49,0	100,0
	Total		143	99,3	100,0	

.



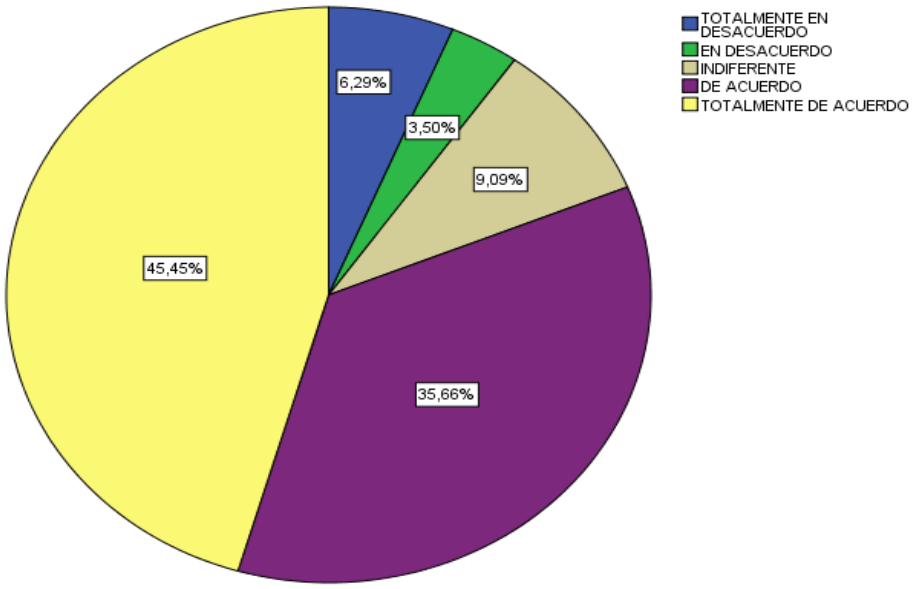
Descripción: Respecto de que si cree que las medidas de seguridad contra el sabotaje que se aplican en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar, el 6% contestó que está totalmente en desacuerdo, el 6% que está en desacuerdo, el 2% que es indiferente, el 37% que está de acuerdo mientras que el 49% que está totalmente de acuerdo

Figura 1. M*edidas de seguridad contra el sabotaje.*

Tabla 2

¿Considera ud que las cámaras de seguridad instaladas en el exterior mejoran el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		9	6,3	6,3	6,3
	EN DESACUERDO		5	3,5	3,5	9,8
	INDIFERENTE		13	9,0	9,1	18,9
	DE ACUERDO		51	35,4	35,7	54,5
	TOTALMENTE DE ACUERDO		65	45,1	45,5	100,0
	Total		143	99,3	100,0	



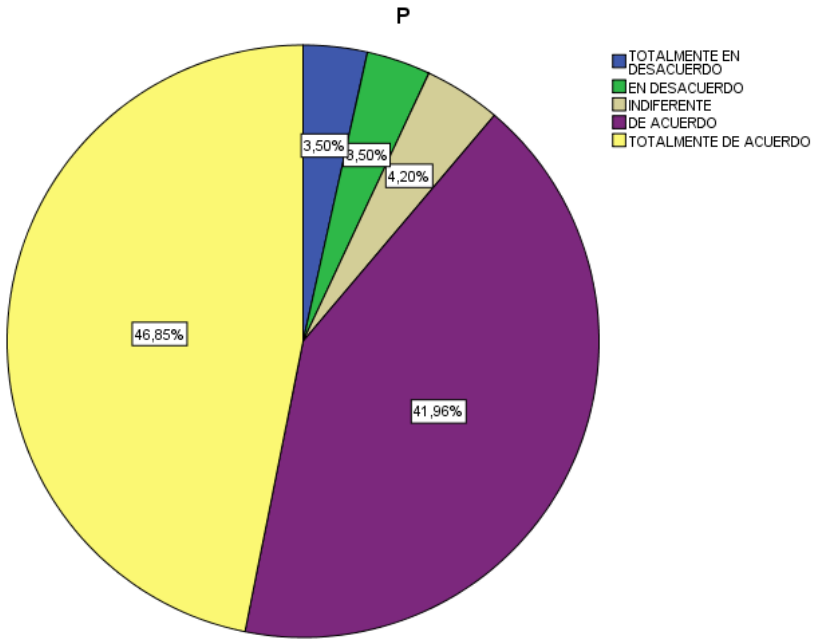
Descripción: Respecto de que si cree que las cámaras de seguridad instaladas en el exterior mejoran el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar el 6% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 9% que es indiferente, el 36% que está de acuerdo mientras que el 46% que está totalmente de acuerdo.

Figura 2. Cámaras de seguridad instaladas en el exterior

Tabla 3

¿Piensa ud que las rondas externas ayudan con el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		5	3,5	3,5	3,5
	EN DESACUERDO		5	3,5	3,5	7,0
	INDIFERENTE		6	4,2	4,2	11,2
	DE ACUERDO		60	41,7	42,0	53,1
	TOTALMENTE DE ACUERDO		67	46,5	46,9	100,0
	Total		143	99,3	100,0	



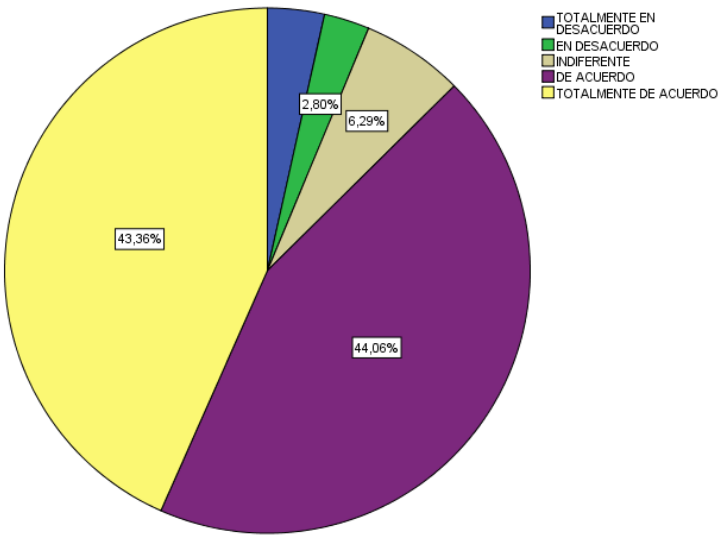
Descripción: Respecto de que si cree que las rondas externas ayudan con el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar, el 4% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 4% que es indiferente, el 42% que está de acuerdo mientras que el 47% que está totalmente de acuerdo.

Figura 3. R*ondas externas.*

Tabla 4

¿Cree ud que los reflectores instalados en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		5	3,5	3,5	3,5
	EN DESACUERDO		4	2,8	2,8	6,3
	INDIFERENTE		9	6,3	6,3	12,6
	DE ACUERDO		63	43,8	44,1	56,6
	TOTALMENTE DE ACUERDO		62	43,1	43,4	100,0
	Total		143	99,3	100,0	



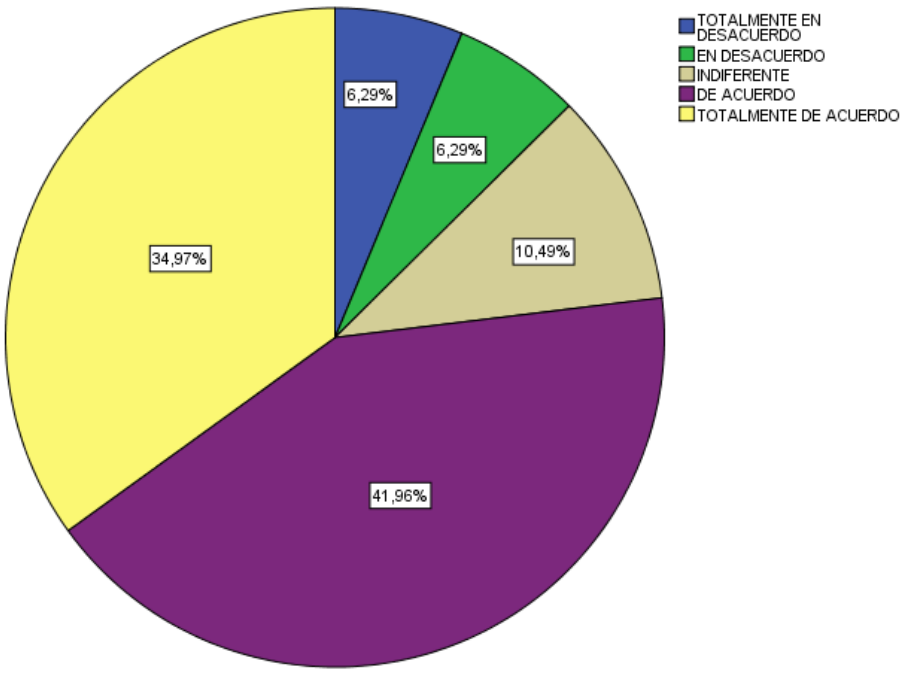
Descripción: Respecto de que si cree que los reflectores instalados en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar, el 4% contestó que está totalmente en desacuerdo, el 3% que está en desacuerdo, el 6% que es indiferente, el 44% que está de acuerdo mientras que el 43% que está totalmente de acuerdo

Figura 4. R*eflectores instalados.*

Tabla 5

¿Cree ud que las rondas internas facilitan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		9	6,3	6,3	6,3
	EN DESACUERDO		9	6,3	6,3	12,6
	INDIFERENTE		15	10,4	10,5	23,1
	DE ACUERDO		60	41,7	42,0	65,0
	TOTALMENTE DE ACUERDO		50	34,7	35,0	100,0
	Total		143	99,3	100,0	



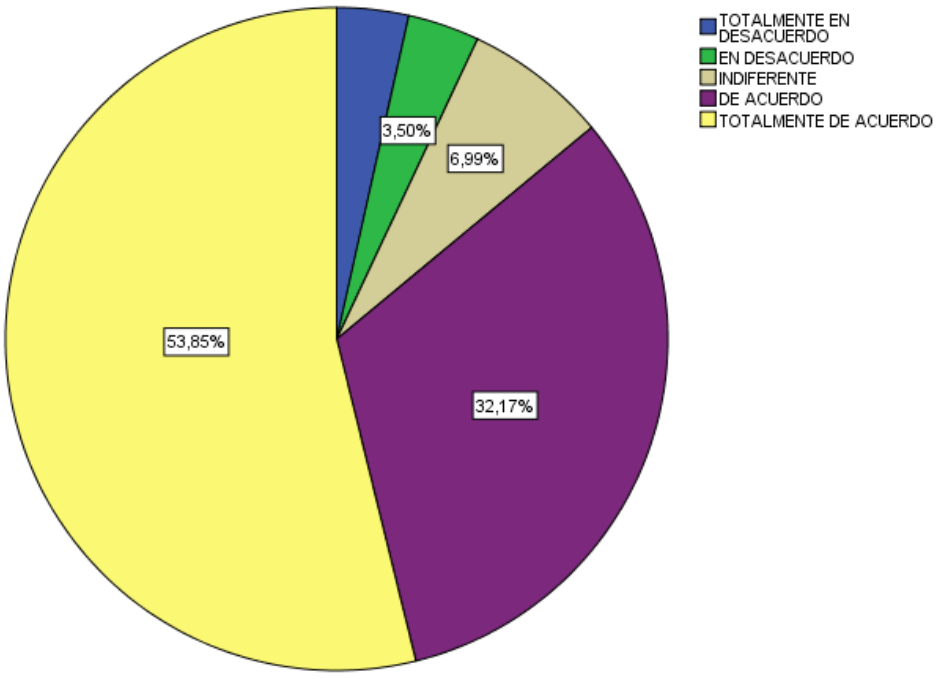
Descripción: Respecto de que si cree que las rondas internas facilitan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar, el 6% contestó que está totalmente en desacuerdo, el 6% que está en desacuerdo, el 11% que es indiferente, el 42% que está de acuerdo mientras que el 35% que está totalmente de acuerdo

Figura 5. R*ondas internas.*

Tabla 6

¿Considera ud que las chapas y candados colocados en las puertas obstaculizan el acceso de personas a las oficinas y ambientes internos de las instalaciones?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		5	3,5	3,5	3,5
	EN DESACUERDO		5	3,5	3,5	7,0
	INDIFERENTE		10	6,9	7,0	14,0
	DE ACUERDO		46	31,9	32,2	46,2
	TOTALMENTE DE ACUERDO		77	53,5	53,8	100,0
	Total		143	99,3	100,0	



Descripción: Respecto de que si cree que las chapas y candados colocados en las puertas obstaculizan el acceso de personas a las oficinas y ambientes internos de las instalaciones, el 4% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 7% que es indiferente, el 32% que está de acuerdo mientras que el 54% que está totalmente de acuerdo

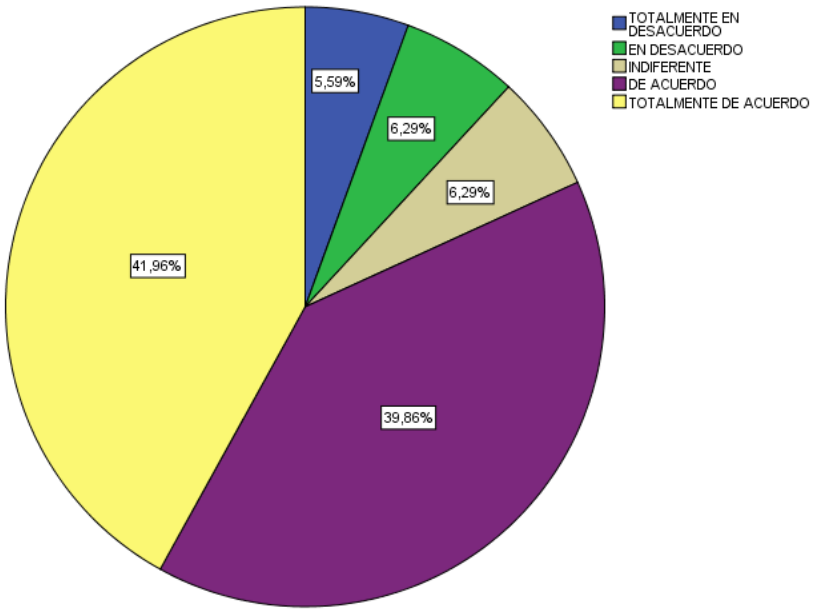
Figura 6. Chapas y candados.

VARIABLE DEPENDIENTE: Control de Accedo a la Escuela Militar

Tabla 7

¿Cree ud que el registro de personas y vehículos pertenecientes a la Escuela Militar facilita el control de acceso a dichas instalaciones?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		8	5,6	5,6	5,6
	EN DESACUERDO		9	6,3	6,3	11,9
	INDIFERENTE		9	6,3	6,3	18,2
	DE ACUERDO		57	39,6	39,9	58,0
	TOTALMENTE DE ACUERDO		60	41,7	42,0	100,0
	Total		143	99,3	100,0	



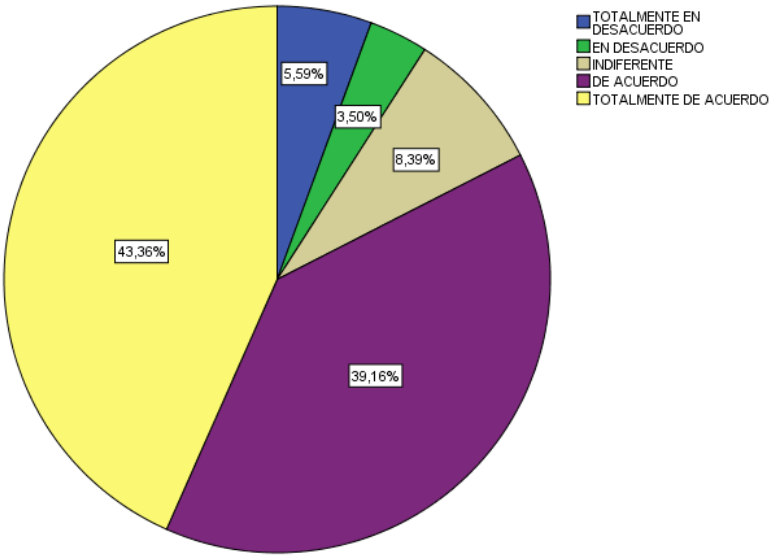
Descripción: De acuerdo al resultado obtenido de que el registro de personas y vehículos pertenecientes a la Escuela Militar facilita el control de acceso a dichas instalaciones, el 6% contestó que está totalmente en desacuerdo, el 6% que está en desacuerdo, el 6% que es indiferente, el 40% que está de acuerdo mientras que el 42% que está totalmente de acuerdo.

Figura 7. R*egistro de personas y vehículos.*

Tabla 8

*¿Piensa ud que el control de ingreso a áreas reservadas por parte del personal que labora en la Escuela Militar es una medida de seguridad vital dentro las instalaciones militares**?***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO	8	5,6	5,6	5,6
	EN DESACUERDO	5	3,5	3,5	9,1
	INDIFERENTE	12	8,3	8,4	17,5
	DE ACUERDO	56	38,9	39,2	56,6
	TOTALMENTE DE ACUERDO	62	43,1	43,4	100,0
	Total	143	99,3	100,0	



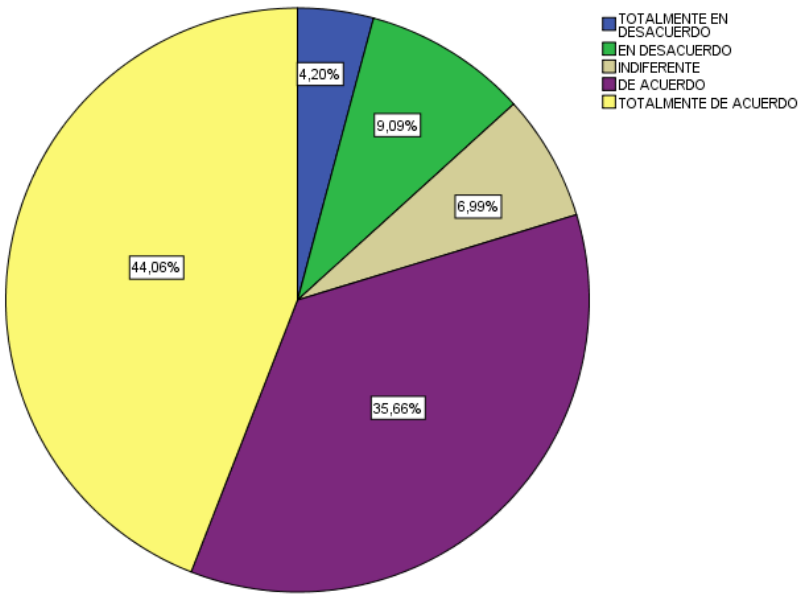
Descripción: Respecto de que el control de ingreso a áreas reservadas por parte del personal que labora en la Escuela Militar es una medida de seguridad vital dentro las instalaciones militares, el 6% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 8% que es indiferente, el 39% que está de acuerdo mientras que el 43% que está totalmente de acuerdo

Figura 8. Control de ingreso a áreas reservadas.

Tabla 9

¿Considera ud que las tarjetas de seguridad (fotochek) es importante para identificar al personal que labora en las instalaciones de la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO	6	4,2	4,2	4,2
	EN DESACUERDO	13	9,0	9,1	13,3
	INDIFERENTE	10	6,9	7,0	20,3
	DE ACUERDO	51	35,4	35,7	55,9
	TOTALMENTE DE ACUERDO	63	43,8	44,1	100,0
	Total	143	99,3	100,0	



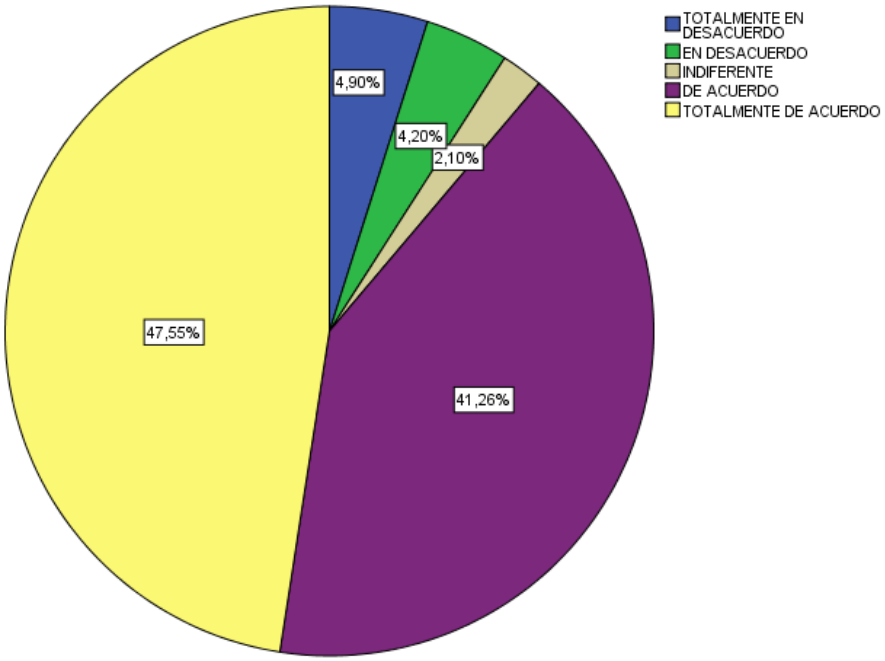
Descripción: Respecto de que las tarjetas de seguridad (fotochek) es importante para identificar al personal que labora en las instalaciones de la Escuela Militar, el 4% contestó que está totalmente en desacuerdo, el 9% que está en desacuerdo, el 7% que es indiferente, el 36% que está de acuerdo mientras que el 44% que está totalmente de acuerdo

Figura 9. T*arjetas de seguridad (fotochek)*

Tabla 10

¿Cree ud que el registro de visitas facilita el control de acceso a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		7	4,9	4,9	4,9
	EN DESACUERDO		6	4,2	4,2	9,1
	INDIFERENTE		3	2,1	2,1	11,2
	DE ACUERDO		59	41,0	41,3	52,4
	TOTALMENTE DE ACUERDO		68	47,2	47,6	100,0
	Total		143	99,3	100,0	



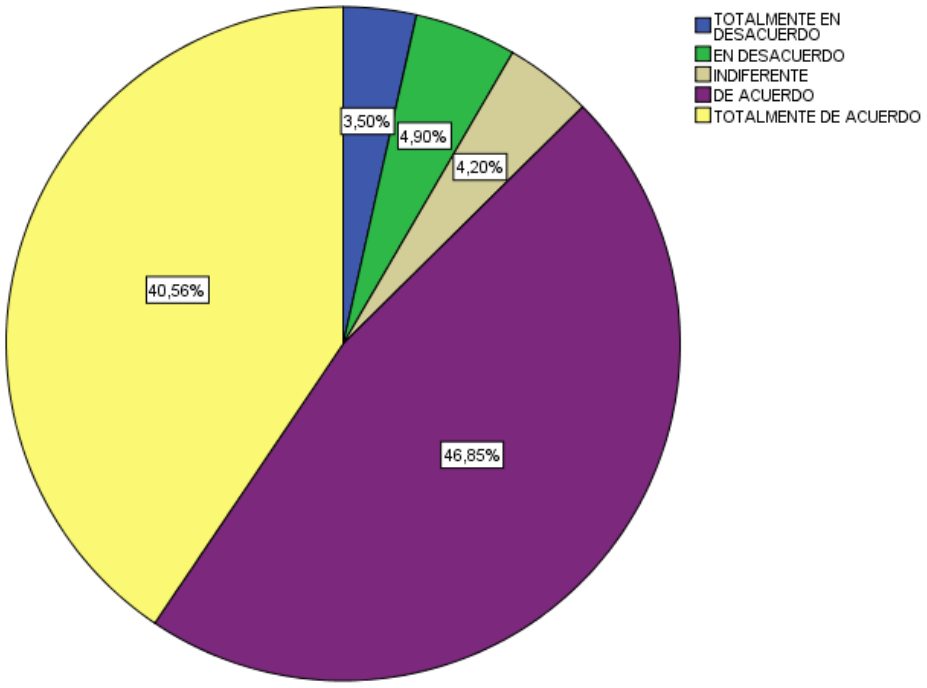
Descripción: Respecto de que el registro de visitas facilita el control de acceso a las instalaciones de la Escuela Militar, el 5% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 2% que es indiferente, el 41% que está de acuerdo mientras que el 48% que está totalmente de acuerdo

Figura 10. Registro de visitas

Tabla 11

¿Considera ud que el detector de metales es una medida de seguridad importante para el control de personas que ingresan a las instalaciones militares?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		5	3,5	3,5	3,5
	EN DESACUERDO		7	4,9	4,9	8,4
	INDIFERENTE		6	4,2	4,2	12,6
	DE ACUERDO		67	46,5	46,9	59,4
	TOTALMENTE DE ACUERDO		58	40,3	40,6	100,0
	Total		143	99,3	100,0	



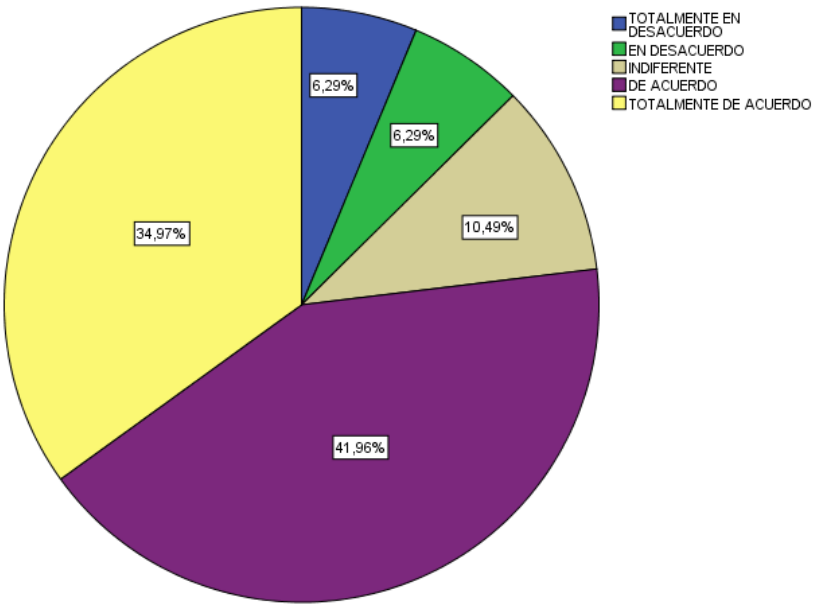
Descripción: Respecto de que el detector de metales es una medida de seguridad importante para el control de personas que ingresan a las instalaciones militares, el 4% contestó que está totalmente en desacuerdo, el 5% que está en desacuerdo, el 4% que es indiferente, el 47% que está de acuerdo mientras que el 41% que está totalmente de acuerdo

Figura 11. D*etector de metales.*

Tabla 12

¿Cree ud que las tarjetas de visitas contribuye al control de ingreso a las instalaciones de la Escuela Militar?

			Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO		9	6,3	6,3	6,3
	EN DESACUERDO		9	6,3	6,3	12,6
	INDIFERENTE		15	10,4	10,5	23,1
	DE ACUERDO		60	41,7	42,0	65,0
	TOTALMENTE DE ACUERDO		50	34,7	35,0	100,0
	Total		143	99,3	100,0	



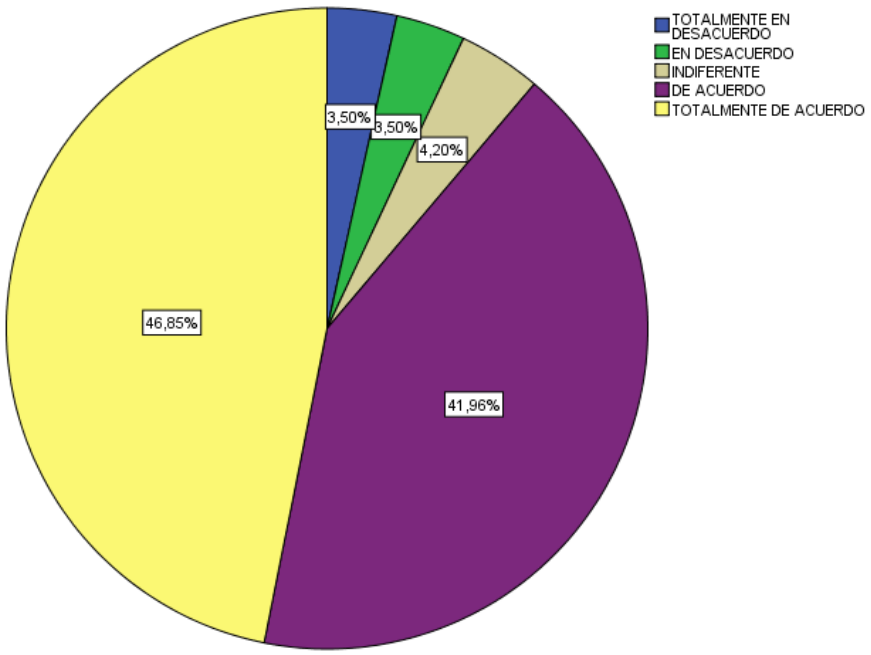
Descripción: Respecto de que las tarjetas de visitas contribuye al control de ingreso a las instalaciones de la Escuela Militar, el 6% contestó que está totalmente en desacuerdo, el 6% que está en desacuerdo, el 11% que es indiferente, el 42% que está de acuerdo mientras que el 35% que está totalmente de acuerdo

Figura 12. T*arjetas de visitas*

Tabla 13

¿Considera ud que el empleo de centinelas distribuidos en zonas críticas contribuye al control de acceso a las instalaciones de la Escuela Militar?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	TOTALMENTE EN DESACUERDO	5	3,5	3,5	3,5
	EN DESACUERDO	5	3,5	3,5	7,0
	INDIFERENTE	6	4,2	4,2	11,2
	DE ACUERDO	60	41,7	42,0	53,1
	TOTALMENTE DE ACUERDO	67	46,5	46,9	100,0
	Total	143	99,3	100,0	



Descripción: Respecto de que el empleo de centinelas distribuidos en zonas críticas contribuye al control de acceso a las instalaciones de la Escuela Militar, el 4% contestó que está totalmente en desacuerdo, el 4% que está en desacuerdo, el 4% que es indiferente, el 42% que está de acuerdo mientras que el 47% que está totalmente de acuerdo

Figura 13. Centinelas.

4.2 Interpretación

Tabla 14

Grado de correlación y nivel de significación entre las Medidas de Seguridad con el Control de Acceso a las instalaciones de la Escuela Militar de Chorrillos

			MEJORAMIENTO INSTRUCCION	CAPACITACION TECNICA
Rho de Spearman	MEDIDAS DE SEGURIDAD	Coeficiente de correlación	1,000	,870
		Sig. (bilateral)	.	,000
		N	143	143
	CONTROL DE ACCESO INSTAL	Coeficiente de correlación	,870	1,000
		Sig. (bilateral)	,000	.
		N	143	143

De los resultados que se aprecian en la tabla adjunta, se presenta el Rho de Spearman cuyo coeficiente de correlación es 0,870 (de 0,8 a 1,0 corresponde correlación muy buena), lo que significa que existe una correlación positiva entre las variables Medidas de Seguridad con el Control de Acceso; luego tenemos que el nivel de significación o valor p = 0,000 < 0,05 es decir que el error de correlación es menor a 5% vale decir que dicho error es mínimo, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna, confirmando que existe relación entre ambas variables y estos resultados coinciden con la tesis.

Tabla 15

Grado de correlación y nivel de significación entre las Medidas de Seguridad con el Control de Acceso del Personal que labora en las instalaciones de la Escuela Militar de Chorrillos

			MEJORAMIENTO INSTRUCCION	EMPLEO EFICIENTE DEL EQUIPO
Rho de Spearman	MEDIDAS DE SEGURIDAD	Coeficiente de correlación	1,000	,850
		Sig. (bilateral)	.	,000
		N	143	143
	PERSONAL QUE LABORA EMCH	Coeficiente de correlación	,850	1,000
		Sig. (bilateral)	,000	.
		N	143	143

De los resultados que se aprecian en la tabla adjunta, se presenta el Rho de Spearman cuyo coeficiente de correlación es 0,850 (de 0,8 a 1,0 corresponde correlación muy buena), lo que significa que existe una correlación positiva entre las variables Medidas de Seguridad con el Control de Acceso del Personal que labora en las instalaciones de la Escuela Militar de Chorrillos; luego tenemos que el nivel de significación o valor p = 0,000 < 0,05 es decir que el error de correlación es menor a 5% vale decir que dicho error es mínimo, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna, confirmando que existe relación entre ambas variables.

Tabla 16

Grado de correlación y nivel de significación entre las Medidas de Seguridad con el Control de Acceso para visitas que acuden a las instalaciones de la Escuela Militar de Chorrillos

			MEJORAMIENTO INSTRUCCION	CONOCIMIENTO DEL EQUIPO
Rho de Spearman	MEDIDAS DE SEGURIDAD	Coeficiente de correlación	1,000	,860
		Sig. (bilateral)	.	,000
		N	143	143
	VISITAS QUE ASISTEN A EMCH	Coeficiente de correlación	,860	1,000
		Sig. (bilateral)	,000	.
		N	143	143

De los resultados que se aprecian en la tabla adjunta, se presenta el Rho de Spearman cuyo coeficiente de correlación es 0,860 (de 0,8 a 1,0 corresponde correlación muy buena), lo que significa que existe una correlación positiva entre las variables Medidas de Seguridad con el Control de Acceso para visitas que acuden a las instalaciones de la Escuela Militar de Chorrillos; luego tenemos que el nivel de significación o valor p = 0,000 < 0,05 es decir que el error de correlación es menor a 5% vale decir que dicho error es mínimo, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna, confirmando que existe relación entre ambas variables.

4.3 Discusión

Para Hernández, Fernández y Baptista (2007) la discusión es el análisis y explicación de los resultados obtenidos con los resultados esperados (hipótesis) y los resultados publicados por otros autores (antecedentes), valores teóricos y creencias de sentido común.

Los resultados obtenidos en la presente investigación están respaldados con las investigaciones tomadas en cuenta como antecedentes en este estudio (tesis formuladas por otros autores), vale decir que son investigaciones que tienen similares resultados con el estudio actual.

De allí que podemos afirmar que existe una relación positiva entre las variables de estudio, vale decir entre las Medidas de Seguridad con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos, lo que además se sustenta con las bases teóricas tomadas en cuenta en esta investigación.

De igual manera se corrobora la existencia de una relación positiva entre las Medidas de Seguridad con el Control de Acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos.

Asimismo la relación positiva entre las Medidas de Seguridad con el Control de Acceso para las visitas que llegan a las instalaciones de la Escuela Militar de Chorrillos.; evidenciando lo que estipulan los antecedentes así como las bases teóricas consideradas en el marco teórico.

A continuación se presenta las tablas de contrastación de la hipótesis general y las específicas cuyas variables guardan una relación positiva entre sí.

CONCLUSIONES

Primera Conclusión

Existe relación significativa entre las medidas de seguridad y el control del acceso a las instalaciones de la Escuela Militar de Chorrillos CFB- 2019

Segunda Conclusión

Es importante tomar medidas para controlar al personal que trabaja en la EMCH de esta manera vamos a evitar que se introduzca o se saque material clasificado, documentos reservados, equipos, etc. lo que podría perjudicar a la institución

Tercera Conclusión

De esta manera se va a tomar acciones de seguridad para controlar a las visitas que ingresan a la EMCH evitando que este personal ingrese a zonas reservadas y pueda sustraer documentos clasificados, material, equipos, armamento, Perjudicando el patrimonio de la instalación.

RECOMENDACIONES

Los investigadores del presente tema respetuosamente recomendamos al Sr. Gral de Brigada, Director de la Escuela Militar de Chorrillos que se digne disponer lo siguiente:

Primera Recomendación

Que se continúe prestando especial atención a las Medidas de Seguridad para ejercer un eficiente Control de Acceso de personas y vehículos a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” con la finalidad de evitar actos de espionaje, ataques, pérdidas de armamento y equipos, así mismo para proteger al personal que labora en esta dependencia principalmente a los cadetes del Batallón.

Segunda Recomendación

Que se optimice las Medidas de Seguridad a efectos de ejercer un adecuado Control de Acceso para el Personal tanto Civil como Militar que labora en las Instalaciones de la Escuela Militar de Chorrillos de tal manera de evitar pérdida de documentos, equipos y otro material, así como limitar el ingreso a áreas restringidas.

Tercera Recomendación

Que se potencie las Medidas de Seguridad con la finalidad de ejercer un adecuado Control de Acceso a las Visitas que concurren de la Escuela Militar de Chorrillos cuyo propósito es evitar pérdida de material y equipos, así como el ingreso a oficinas reservadas.

REFERENCIAS

- CyberPoint (s.f) Control de ronda. Consultado el 15 de marzo 2019. Recuperado de:

  http://www.cybertek-peru.com/control-acceso/cyberpoint/index.html

- EIA (2019) Los detectores metálicos. Consultado el 20 de marzo del 2019. Recuperado de:
  https://www.ceia.net/security/ap_events.aspx?lan=esp

- Enriquez A (2015) "*La seguridad electrónica en el fuerte militar Rumiñahui*" Tesis para optar el título de ingeniero en seguridad - mención seguridad pública y privada. Universidad de las fuerzas armadas "ESPE" Quito. Ecuador.

  https://repositorio.espe.edu.ec/bitstream/21000/10720/1/T-ESPE-049374.pdf

- Enciclopedia.US. Sabotaje (delito). Consultado el 2 de Marzo del 2019. Recuperado de:

  http://enciclopedia.us.es/index.php/Sabotaje_(delito)

- Granado J (2015) *Las distintas formas de sabotaje y delitos por computadoras.* Consultado el 10 de Marzo del 2019. Recuperado de:

  https://prezi.com/fg60ax5d1wnv/las-distintas-formas-de-sabotaje-y-delitos-por-computadoras/

- Holowczak B (s.f) Uso del CCTV en sistemas de detección perimetral. Consultado el 15 de marzo del 2019. Recuperado de: **http://www.rnds.com.ar/articulos/085/RNDS_84-92W.pdf**

- Iluminet (2017) La iluminación de seguridad. Consultado el 18 de Marzo del

2019. Recuperado de: https://www.iluminet.com/consideraciones-diseno-iluminacion-seguridad/

- INACAL (s.f) Norma técnica de seguridad contra incendios. Consultado el 19 de marzo 2019. Recuperado de: https://www.inacal.gob.pe/cid/noticia/incendios

- Qwantec (s.f) sobre las rondas exteriores. Consultado el 16 de maro del 2019. Recuperado de:

https://www.qwantec.com/cl/control-de-rondas?gclid=CjwKCAjwy7vlBRACEiwAZvdx9iamvQ-2N-ZyLNbRJ4JjFbM5km1S6Kq9w-6P5-G1azrriyR6Wu1DhRoCn5oQAvD_BwE

- RuvaSeguridad (s.f) Sistemas perimetrales de videovigilancia . Consultado el 13 de Marzo del 2019. Recuperado de: **https://www.camarasdevigilanciabarcelona.com/noticias/sistemas-perimetrales-de-videovigilancia/index.html**

- Reglamento De Seguridad Para Las Tecnologías De La Información. Consultado el 20 de Diciembre del 2019 . Recuperado de: http://www.fcmjtrigo.sld.cu/resoluciones/reglamento_s_i_tecn_informac..pdf

- Mapfre (s.f) tipos de incendio. Consultado el 18 de Marzo 2019. Recuperado de: https://www.mapfre.com.pe/negocios/sctr/prevencion-incendios.jsp

- Paritarios.Cl (s.f) Letreros, señales y tarjetas de seguridad. Consultado el 19 de marzo del 2019. Recuperado de: http://www.paritarios.cl/especial_letreros_tarjetas_seguridad.htm

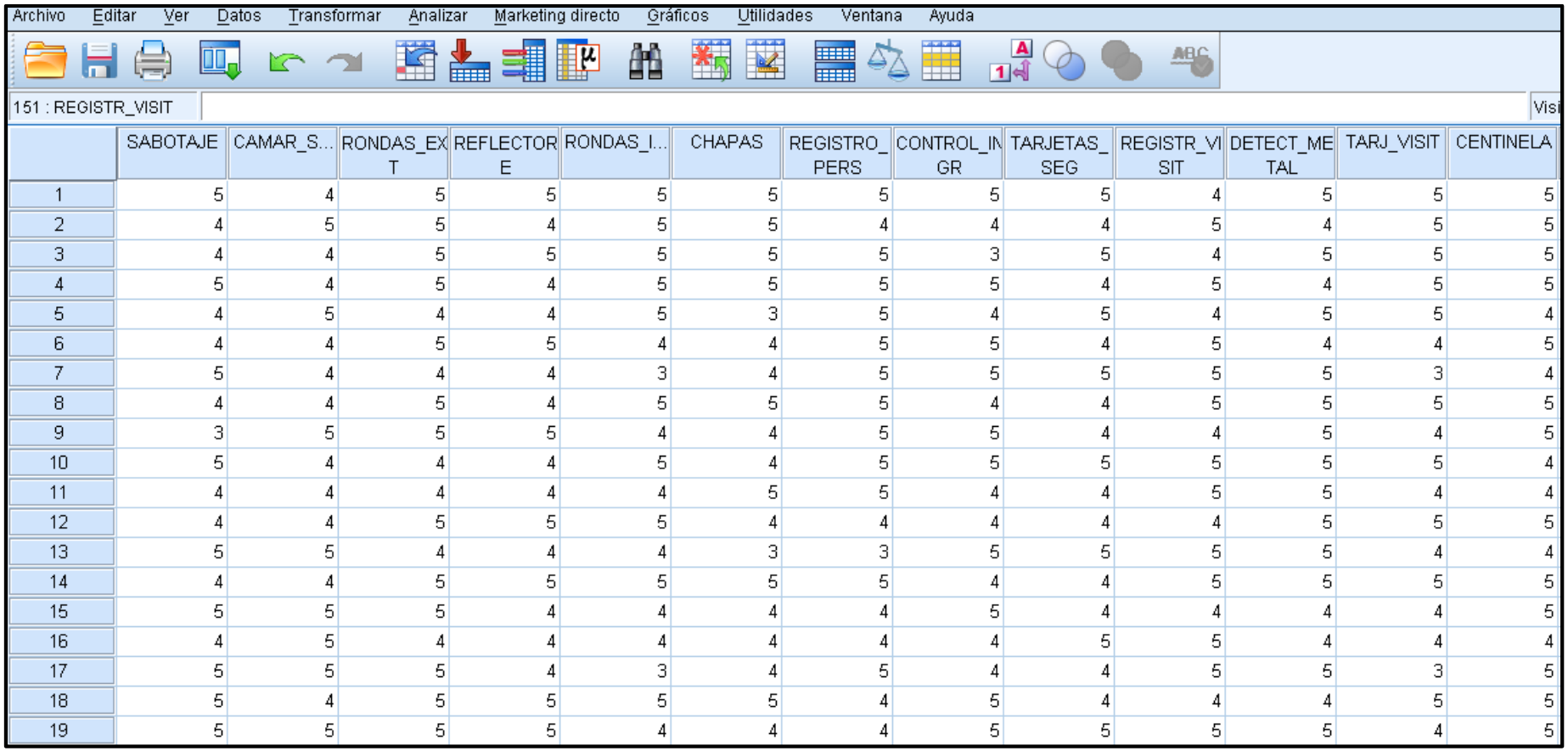
- Salvador C. (2017) Propuesta del Sistema de Video Vigilancia en la Seguridad Ciudadana distrito de Pueblo Libre 2016-2020. Tesis para optar el grado de Maestro en Gestión Pública. Universidad Cesar Vallejo. Lima Perú.

http://repositorio.ucv.edu.pe/bitstream/handle/UCV/7150/Sierra_GCS.pdf?sequence=1&isAllowed=y

ANEXOS

- **Anexo 1.** Base de Datos.
- **Anexo 2.** Matriz de Consistencia
- **Anexo 3.** Instrumento de recolección de datos
- **Anexo 4.** Documento Validación del instrumento
- **Anexo 5.** Constancia de la entidad donde se realizó la investigación.
- **Anexo 6.** Compromiso de autenticidad del instrumento

Anexo 1. Base de Datos.



Archivo Editar Ver Datos Transformar Analizar Marketing directo Gráficos Utilidades Ventana Ayuda

151 : REGISTR_VISIT

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
1	5	4	5	5	5	5	5	5	5	4	5	5	5
2	4	5	5	4	5	5	4	4	4	5	4	5	5
3	4	4	5	5	5	5	5	3	5	4	5	5	5
4	5	4	5	4	5	5	5	5	4	5	4	5	5
5	4	5	4	4	5	3	5	4	5	4	5	5	4
6	4	4	5	5	4	4	5	5	4	5	4	4	5
7	5	4	4	4	3	4	5	5	5	5	5	3	4
8	4	4	5	4	5	5	5	4	4	5	5	5	5
9	3	5	5	5	4	4	5	5	4	4	5	4	5
10	5	4	4	4	5	4	5	5	5	5	5	5	4
11	4	4	4	4	4	5	5	4	4	5	5	4	4
12	4	4	5	5	5	4	4	4	4	4	5	5	5
13	5	5	4	4	4	3	3	5	5	5	5	4	4
14	4	4	5	5	5	5	5	4	4	5	5	5	5
15	5	5	5	4	4	4	4	5	4	4	4	4	5
16	4	5	4	4	4	4	4	4	5	5	4	4	4
17	5	5	5	4	3	4	5	4	4	5	5	3	5
18	5	4	5	5	5	5	4	5	4	4	4	5	5
19	5	5	5	5	4	4	4	5	5	5	5	4	5

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
19	5	5	5	5	4	4	4	5	5	5	5	4	5
20	4	4	5	5	4	4	5	4	4	4	5	4	5
21	5	4	4	4	3	3	4	3	5	5	5	3	4
22	5	5	4	4	5	5	4	5	5	4	5	5	4
23	4	4	5	4	4	4	5	4	4	3	4	4	5
24	5	5	5	5	3	2	5	4	4	4	4	3	5
25	5	5	4	4	3	4	5	5	5	4	4	3	4
26	4	5	5	3	5	5	5	3	3	4	3	5	5
27	5	4	4	5	3	4	5	4	5	4	5	3	4
28	5	5	4	4	4	3	4	3	5	4	4	4	4
29	5	5	5	5	5	4	4	5	5	4	4	5	5
30	5	5	4	5	3	5	5	4	5	5	5	3	4
31	5	4	4	4	4	4	5	4	5	4	5	4	4
32	4	5	5	5	5	2	4	5	4	4	5	5	5
33	5	5	4	5	3	2	4	4	4	4	5	3	4
34	4	4	5	4	4	3	5	3	5	5	4	4	5
35	4	5	4	5	5	4	5	5	3	5	4	5	4
36	5	5	4	3	2	2	4	4	1	4	5	2	4
37	3	5	4	3	4	4	4	3	4	4	5	4	4

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
37	3	5	4	3	4	4	4	3	4	4	5	4	4
38	4	3	5	5	4	5	4	5	3	5	4	4	5
39	5	5	4	4	5	4	5	4	5	5	5	5	4
40	4	4	5	5	4	4	3	4	4	4	5	4	5
41	3	5	5	4	3	3	4	5	3	3	4	3	5
42	5	3	5	5	5	5	5	4	5	4	4	5	5
43	2	4	5	5	4	4	3	3	4	5	5	4	5
44	5	5	5	4	2	3	4	4	3	2	4	2	5
45	4	3	5	5	2	2	5	5	5	4	4	2	5
46	5	4	4	4	4	3	5	4	4	5	5	4	4
47	2	5	3	3	5	4	4	4	5	2	4	5	3
48	4	3	5	5	4	3	5	4	3	4	5	4	5
49	5	3	5	5	2	4	3	5	4	5	4	2	5
50	4	3	5	5	3	5	4	4	3	5	5	3	5
51	5	5	3	5	5	3	4	3	5	4	2	5	3
52	4	3	5	5	4	4	3	4	4	4	5	4	5
53	2	4	4	4	2	1	4	5	4	4	4	2	4
54	5	3	3	5	3	5	4	4	5	4	4	3	3
55	4	3	4	3	4	4	3	3	4	4	4	4	4
56	2	5	4	4	5	1	4	4	3	4	5	5	4
57	5	5	4	5	4	5	4	5	4	5	3	4	4
58	4	3	5	3	3	4	5	3	5	4	4	3	5

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
58	4	3	5	3	3	4	5	3	5	4	4	3	5
59	5	3	4	4	4	1	5	4	4	4	4	4	4
60	4	5	4	5	5	1	5	4	3	5	5	5	4
61	2	3	3	5	5	5	4	5	5	5	4	5	3
62	5	5	4	5	5	4	5	3	4	5	5	5	4
63	4	3	5	2	5	4	5	4	3	4	4	5	5
64	2	4	4	4	2	5	5	5	4	5	4	2	4
65	5	5	3	2	4	4	5	4	5	4	4	4	3
66	4	2	5	5	5	5	3	3	4	5	4	5	5
67	5	4	4	5	5	1	4	5	1	5	4	5	4
68	4	5	3	5	2	4	4	4	4	4	5	2	3
69	1	5	5	5	4	5	3	5	5	5	4	4	5
70	5	2	4	2	5	5	5	2	4	5	4	5	4
71	4	4	4	5	1	5	4	4	4	4	4	1	4
72	5	5	2	4	5	5	4	2	4	5	4	5	2
73	2	5	4	4	4	4	2	5	5	5	5	4	4
74	4	5	5	4	5	5	4	4	2	4	5	5	5
75	1	5	4	5	4	5	4	2	2	5	5	4	4
76	4	4	4	4	4	5	5	5	4	5	5	4	4

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
76	4	4	4	4	4	5	5	5	4	5	5	4	4
77	1	2	2	5	5	5	3	4	4	4	4	5	2
78	5	5	4	4	5	5	4	4	5	5	4	5	4
79	4	5	4	4	5	5	4	5	4	5	5	5	4
80	2	5	4	5	5	4	2	2	2	5	5	5	4
81	5	4	5	4	3	5	4	4	2	4	4	3	5
82	4	2	4	4	4	5	4	2	5	5	4	4	4
83	4	5	4	4	3	5	4	5	4	4	4	3	4
84	5	5	4	5	1	4	2	4	2	5	5	1	4
85	4	5	4	4	2	5	4	1	4	4	4	2	4
86	4	5	2	5	4	5	5	5	2	2	3	4	2
87	5	5	4	4	5	5	5	4	5	5	4	5	4
88	4	2	5	5	4	4	5	1	2	5	5	4	5
89	4	5	5	4	3	5	5	1	5	4	2	3	5
90	5	5	5	4	4	5	5	5	5	5	2	4	5
91	4	5	4	5	5	5	2	4	5	5	4	5	4
92	4	5	4	5	4	4	4	1	5	4	4	4	4
93	5	1	5	4	2	5	2	5	5	5	4	2	5
94	4	5	5	4	4	5	4	4	5	5	4	4	5

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
94	4	5	5	4	4	5	4	4	5	5	4	4	5
95	1	5	5	4	1	5	2	1	2	4	5	1	5
96	5	5	5	5	4	5	5	1	2	5	4	4	5
97	5	4	5	5	4	5	4	5	5	3	4	4	5
98	5	5	2	5	5	5	1	4	2	4	4	5	2
99	5	5	4	5	5	5	2	1	2	1	5	5	4
100	5	5	5	5	5	5	4	5	2	4	4	5	5
101	1	4	5	5	5	5	5	4	5	4	3	5	5
102	4	5	5	5	4	5	2	5	5	5	5	4	5
103	5	4	4	5	4	5	4	5	5	5	4	4	4
104	4	4	5	4	1	5	2	4	5	4	3	1	5
105	5	5	5	4	4	5	4	5	2	5	5	4	5
106	4	4	4	2	1	4	1	5	1	5	4	1	4
107	5	1	5	4	5	5	1	5	5	4	2	5	5
108	5	4	5	5	4	5	4	4	5	5	5	4	5
109	5	5	5	1	1	5	1	5	4	5	4	1	5
110	4	4	4	4	4	5	4	5	4	5	5	4	4
111	4	4	2	1	1	5	5	5	5	5	4	1	2
112	5	4	5	4	4	5	1	4	4	1	4	4	5

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
112	5	4	5	4	4	5	1	4	4	1	4	4	5
113	1	5	5	4	4	4	4	5	4	4	5	4	5
114	5	4	4	4	5	5	5	5	5	2	4	5	4
115	4	4	4	4	4	5	5	5	4	5	3	4	4
116	1	4	5	5	4	5	4	5	4	1	4	4	5
117	5	5	1	4	1	4	1	5	5	1	4	1	1
118	4	1	5	5	4	5	5	5	4	4	4	4	5
119	1	4	1	4	4	5	5	4	4	5	4	4	1
120	5	1	4	5	4	5	5	4	4	4	5	4	4
121	4	5	4	1	5	4	1	5	5	1	5	5	4
122	1	4	5	4	4	5	5	4	4	4	1	4	5
123	5	1	4	4	4	5	5	5	4	1	5	4	4
124	4	1	5	5	4	5	4	4	5	5	5	4	5
125	5	4	4	4	4	4	4	5	5	1	1	4	4
126	5	1	1	1	4	5	4	5	4	4	4	4	1
127	5	4	5	4	5	4	5	4	5	5	2	5	5
128	5	4	4	1	4	4	4	5	1	5	5	4	4
129	5	4	5	5	5	5	5	5	5	2	5	5	5
130	4	1	1	4	4	4	5	5	5	2	2	4	1

	SABOTAJE	CAMAR_S...	RONDAS_EXT	REFLECTORE	RONDAS_I...	CHAPAS	REGISTRO_PERS	CONTROL_INGR	TARJETAS_SEG	REGISTR_VISIT	DETECT_METAL	TARJ_VISIT	CENTINELA
130	4	1	1	4	4	4	5	5	5	2	2	4	1
131	4	4	4	4	1	5	4	5	5	5	5	1	4
132	5	1	5	4	5	5	4	4	5	5	4	5	5
133	5	5	4	4	5	5	5	5	5	4	5	5	4
134	5	4	5	3	4	5	4	4	5	5	4	4	5
135	5	5	4	5	4	4	1	5	1	5	4	4	4
136	5	4	1	3	5	4	4	4	5	5	2	5	1
137	4	5	5	3	4	5	4	1	5	4	5	4	5
138	5	4	4	4	4	4	5	4	5	5	4	4	4
139	5	5	5	4	4	5	5	5	4	5	1	4	5
140	4	4	4	5	4	4	5	4	5	4	4	4	4
141	5	5	5	4	5	5	5	5	1	4	4	5	5
142	5	4	4	5	5	5	4	5	5	4	1	5	4
143	5	4	5	5	5	5	5	5	5	5	1	5	5
144													

Anexo 2: Matriz de Consistencia

Título: **Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" – 2019**

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	DISEÑO METODOLÓGICO E INSTRUMENTOS
Problema General ¿Qué relación existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019?	**Objetivo General** Determinar la relación que existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019	**Hipótesis General** Existe relación significativa entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019	Medidas de Seguridad	1. Medidas de seguridad externa	1.1 M. contra sabotaje 1.2 Cámaras perimétricas 1.3 Rondas externas 1.4 Reflectores externos	**-Tipo/Nivel investigación:** Descriptivo/correlacional **-Diseño de investigación:** No experimental, transversal **-Enfoque de investigación:** cuantitativo **-Técnica/Instrumentos:** Encuesta/cuestionario **-Población:** 225 cadetes de cuarto año **-Muestra:** 143 cadetes de cuarto año **-Métodos de análisis de datos:** Paquete Estadístico SPSS
				2.Medidas de seguridad interna	2.1 Rondas internas 2.2 Candados	
Problema Específico 1 ¿Qué relación existe entre las medidas de seguridad y el control de acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019?	**Objetivo Específico 1** Determinar la relación que existe entre las medidas de seguridad y el control de acceso a las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019	**Hipótesis Específica 1** Existe relación significativa entre las medidas de seguridad y el control de acceso para el personal que labora en las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019	Control de Acceso a las instalaciones	1. Control de acceso para el personal que labora en las instalaciones	1.1Registro de personal 1.2Áreas reservadas 1.3Tarjetas de seguridad	
Problema Específico 2 ¿Qué relación existe entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019?	**Objetivo Específico 2** Determinar la relación que existe entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019	**Hipótesis Específica 2** Existe relación significativa entre las medidas de seguridad y el control de acceso para visitas en las instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019		2.Control de acceso para visitas	2.1 Registro de visitas 2.2 Detector de metales 2.3 Tarjeta de visitas 2.4 Centinelas	

ANEXO 3

INSTRUMENTO DE RECOLECCIÓN DE DATOS

ENCUESTA

Instrucciones:

Gracias por su colaboración en contestar el presente cuestionario, es anónimo. Por favor coloque una X en la respuesta que usted considere pertinente.

---

1. ¿Cree ud que las medidas de seguridad contra el sabotaje que se aplican en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

2. ¿Considera ud que las cámaras de seguridad instaladas en el exterior mejoran el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

3. ¿Piensa ud que las rondas externas ayudan con el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

4. ¿Cree ud que los reflectores instalados en el exterior optimizan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

5. ¿Cree ud que las rondas internas facilitan el control de acceso de personas y vehículos a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

6. ¿Considera ud que las chapas y candados colocados en las puertas obstaculizan el acceso de personas a las oficinas y ambientes internos de las instalaciones?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

7. ¿Cree ud que el registro de personas y vehículos pertenecientes a la Escuela Militar facilita el control de acceso a dichas instalaciones?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

8. ¿Piensa ud que el control de ingreso a áreas reservadas por parte del personal que labora en la Escuela Militar es una medida de seguridad vital dentro las instalaciones militares?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

9. ¿Considera ud que las tarjetas de seguridad (fotochek) es importante para identificar al personal que labora en las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

10. ¿Cree ud que el registro de visitas facilita el control de acceso a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

11. ¿Considera ud que el detector de metales es una medida de seguridad importante para el control de personas que ingresan a las instalaciones militares?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

12. ¿Cree ud que las tarjetas de visitas contribuye al control de ingreso a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

13. ¿Considera ud que el empleo de centinelas distribuidos en zonas críticas contribuye al control de acceso a las instalaciones de la Escuela Militar?

Totalmente de Acuerdo	De acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo

ANEXO 4. VALIDACIÓN DEL INSTRUMENTO POR EXPERTO

TÍTULO DEL TRABAJO DE INVESTIGACIÓN /TESIS:

Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” – 2019

AUTORES: - Bach. Samaniego Romero, Yosimar Stevie
- Bach. Vergaray Rojas, Nataly del Milagro

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado.										X
2.OBJETIVIDAD	Está expresado en conductas observables										X
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										X
4.ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.									X	
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad										X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación									X	
7.CONSISTENCIA	Basado en bases teóricas científicas.										X
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										X
9. METODOLOGÍA	El diseño responde al propósito de la investigación										X
10. PERTINENCIA	Es útil y adecuado para la investigación.									X	

PROMEDIO DE VALORACIÓN DEL EXPERTO: 97

OBSERVACIONES REALIZADAS POR EL EXPERTO: Ninguna

GRADO ACADÉMICO DEL EXPERTO:

APELLIDOS Y NOMBRES DEL EXPERTO:

FIRMA:

…….

DNI:

ANEXO 4. VALIDACIÓN DEL INSTRUMENTO POR EXPERTO

TÍTULO DEL TRABAJO DE INVESTIGACIÓN /TESIS:

Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” – 2019

AUTORES: - Bach. Samaniego Romero, Yosimar Stevie
- Bach. Vergaray Rojas, Nataly del Milagro

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado.									X	
2.OBJETIVIDAD	Está expresado en conductas observables										X
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										X
4.ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.									X	
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad										X
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación									X	
7.CONSISTENCIA	Basado en bases teóricas científicas.										X
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										X
9. METODOLOGÍA	El diseño responde al propósito de la investigación									X	
10. PERTINENCIA	Es útil y adecuado para la investigación.									X	

PROMEDIO DE VALORACIÓN DEL EXPERTO: 95

OBSERVACIONES REALIZADAS POR EL EXPERTO: Ninguna

GRADO ACADÉMICO DEL EXPERTO:

APELLIDOS Y NOMBRES DEL EXPERTO:

FIRMA:

…….

DNI:

ANEXO 4. VALIDACIÓN DEL INSTRUMENTO POR EXPERTO

TÍTULO DEL TRABAJO DE INVESTIGACIÓN /TESIS:

Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” – 2019

AUTORES: - Bach. Samaniego Romero, Yosimar Stevie
- Bach. Vergaray Rojas, Nataly del Milagro

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

CRITERIOS	DESCRIPCIÓN	VALOR ASIGNADO POR EL EXPERTO									
		10	20	30	40	50	60	70	80	90	100
1.CLARIDAD	Está formado con el lenguaje adecuado.									X	
2.OBJETIVIDAD	Está expresado en conductas observables										X
3.ACTUALIDAD	Adecuado de acuerdo al avance de la ciencia.										X
4.ORGANIZACIÓN	Existe una cohesión lógica entre sus elementos.									X	
5. SUFICIENCIA	Comprende los aspectos requeridos en cantidad y calidad									X	
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de la investigación									X	
7.CONSISTENCIA	Basado en bases teóricas científicas.										X
8. COHERENCIA	Hay correspondencia entre dimensiones, indicadores e índices.										X
9. METODOLOGÍA	El diseño responde al propósito de la investigación									X	
10. PERTINENCIA	Es útil y adecuado para la investigación.									X	

PROMEDIO DE VALORACIÓN DEL EXPERTO: 94

OBSERVACIONES REALIZADAS POR EL EXPERTO: Ninguna

GRADO ACADÉMICO DEL EXPERTO:

APELLIDOS Y NOMBRES DEL EXPERTO:

FIRMA:

…….

DNI:

ANEXO 5: Constancia de entidad donde se efectuó la investigación

ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"

CONSTANCIA

El que suscribe Sub Director Académico de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

HACE CONSTAR

Que los Cadetes que se mencionan han realizado la investigación en esta dependencia militar sobre el tema titulado: Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" – 2019

Investigadores:

- Bach. Samaniego Romero, Yosimar Stevie
- Bach. Vergaray Rojas, Nataly del Milagro

Se le expide la presente Constancia a efectos de emplearla como anexo en su investigació

Chorrillos,….. de…….. del 2019

……

ANEXO 6: COMPROMISO DE AUTENTICIDAD DEL INSTRUMENTO

Los Cadetes que suscriben líneas abajo, autores del trabajo de investigación titulado: Medidas de Seguridad y su relación con el Control de Acceso a las Instalaciones de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” – 2019

HACEN CONSTAR:

Que el presente trabajo ha sido íntegramente elaborado por los suscritos y que no existe plagio alguno, ni temas presentados por otra persona, grupo o institución, comprometiéndonos a poner a disposición del COEDE (EMCH “CFB”) los documentos que acrediten la autenticidad de la información proporcionada si esto lo fuera solicitado por la entidad.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada.

Nos afirmamos y ratificamos en lo expresado, en fe de lo cual firmamos el presente documento.

Chorrillos,….. de ……del 2019

……..……

……

Bach. Samaniego Romero, Yosimar Stevie

Bach. Vergaray Rojas, Nataly del Milagro