ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

INGENIERÍA EN SEGURIDAD

TEMA: "SISTEMA INTEGRAL DE SEGURIDAD: REQUERIMIENTOS PARA CONTRARRESTAR LOS RIESGOS Y AMENAZAS QUE PUEDEN AFECTAR LA SEDE DEL CONSEJO NACIONAL ELECTORAL EN EL DM. DE QUITO".

PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SEGURIDAD

ELABORADO POR:

JORGE OSWALDO MUÑOZ RIVADENEIRA

DIRECTOR

Dr. ALEJANDRO RECALDE

CODIRECTOR

Msc. WILMAN GUARNIZO

SANGOLQUI, JUNIO DE 2013

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. JORGE OSWALDO MUÑOZ R., como requerimiento parcial a la obtención del Título de INGENIERO EN SEGURIDAD.

Sangolquí, 16 Junio de 2013.

DIRECTOR: **CODIRECTOR:**

Dr. ALEJANDRO RECALDE Msc. WILMAN GUARNIZO

ESCUELA POLITÉCNICA DEL EJÉRCITO
INGENIERÍA EN SEGURIDAD

DECLARACIÓN DE RESPONSABILIDAD

MUÑOZ RIVADENEIRA JORGE OSWALDO

DECLARO QUE:

El proyecto de grado denominado "SISTEMA INTEGRAL DE SEGURIDAD: REQUERIMIENTOS PARA CONTRARRESTAR LOS RIESGOS Y AMENAZAS QUE PUEDEN AFECTAR LA SEDE DEL CONSEJO NACIONAL ELECTORAL EN EL DM. DE QUITO", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en la referencias bibliográficas correspondientes.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 16 de Junio del 2013

MUÑOZ RIVADENEIRA JORGE OSWALDO

ESCUELA POLITÉCNICA DEL EJÉRCITO
INGENIERÍA EN SEGURIDAD

AUTORIZACIÓN

YO, MUÑOZ RIVADENEIRA JORGE OSWALDO

Autorizo a la Escuela Politécnica del Ejército la publicación, en la bilioteca virtual del proyecto de grado denominado "SISTEMA INTEGRAL DE SEGURIDAD: REQUERIMIENTOS PARA CONTRARRESTAR LOS RIESGOS Y AMENAZAS QUE PUEDEN AFECTAR LA SEDE DEL CONSEJO NACIONAL ELECTORAL EN EL DM. DE QUITO", cuyo contenido, ideas y criterio son de mi exclusiva responsabilidad y autoría.

Sangolquí, 16 de Junio del 2013

MUÑOZ RIVADENEIRA JORGE OSWALDO

DEDICATORIA

Dedico este trabajo a mi Dios, quien me ha dado todo lo que hasta ahora tengo para dedicar y seguir dedicando en mi vida.

A mi madre Katty quien me enseño desde pequeño la importancia de conseguir con esfuerzo lo que deseo y ahora desde el cielo está acompañándome.

A mi padre Franco Oswaldo, quien con amor y responsabilidad me enseña cada día la importancia de planificar cada segundo de mi vida, como cualidad primordial para alcanzar el éxito.

A mi esposa Ibeth, quien con paciencia y entrega me acompaña cada segundo de mi vida para juntos caminar en la misma dirección en búsqueda de nuestros sueños y aspiraciones.

A mi hija Emily y al bebe que está en camino, que son la prolongación de mi existencia, por ser ellos un motivo más para querer seguir luchando.

A mi hermano Andrés, que cada día me sorprende, al estar en otro país, luchando solo, por el amor a su familia.

A mi familia que con su cariño y preocupación han estado siempre en los momentos más difíciles, enseñándome que cuando los amigos y el resto se va, la familia siempre te acompaña.

AGRADECIMIENTO

Agradezco a las personas quienes de alguna forma me ayudaron a culminar con éxito mi carrera, al Dr. Alejandro Recalde y al Msc. Wilman Guarnizo, quienes con su conocimiento y apoyo supieron guiarme para el cumplimiento exitoso de mi tesis, así mismo, agradezco al Consejo Nacional Electoral por haberme brindado un apoyo incondicional para obtener la información necesaria para realizar este trabajo, agradezco a mi familia, amigos, en especial a Fernando Gallegos quien estuvo siempre preocupado para darme una mano cuando más necesitaba.

Gracias a ti mi Dios, por darme una segunda oportunidad de vida, después de haberme acercado al otro lado, tu dejaste que cumpliese con mis sueños.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FOTOGRAFÍAS

RESUMEN

El Consejo Nacional Electoral de la República del Ecuador es el máximo organismo de sufragio. Tiene su sede en la ciudad de Quito, ubicado en la Av. 6 de diciembre y Bosmediano, goza de completa autonomía financiera y administrativa. Sus funciones son organizar, controlar las elecciones, puede sancionar a partidos y candidatos que infrinjan las normas electorales.

El Consejo Nacional Electoral como función Electoral del estado Ecuatoriano, es el organizador de los procesos electorales; esto le convierte en blanco de amenazas por intereses políticos y sociales particulares que podrían afectar la integridad de autoridades y funcionarios del CNE; así como de sus instalaciones, equipos y materiales.

La seguridad del Consejo Nacional Electoral en el país, es de fundamental importancia, razón por la cual debe ser enfocada para contribuir a la ejecución segura de cada evento electoral a desarrollarse en el Ecuador, con un enfoque de seguridad integral, protegiendo personas, activos, información, comunidad en general.

Establecer un sistema de protección de medidas físicas integradas con el propósito de prevenir, controlar, verificar posibles intrusiones, ocupaciones, robos, hurtos, sabotajes, y detectar de manera oportuna posibles ataques. Evidenciar la acción de adversarios, permitiendo que a través de una adecuada comunicación se pueda coordinar la respuesta oportuna y eficaz de los cuerpos de seguridad destinados para este efecto y poder interrumpir y/o neutralizar la acción de adversarios evitando un enfrentamiento violento.

El proceso de la seguridad plantea dar un respuesta, que se anticipe a los diferentes eventos posibles, que pueden afectar a la organización, para lo cual ya no es suficiente elaborar un plan de respuesta, sino mantener un sistema de seguridad que en su mayor parte sea diseñado en materia de prevención y no en la reacción o respuesta.

EL CNE y sus organismos y unidades de la Función Electoral, se comprometen a adaptar dinámicamente los criterios de seguridad ante nuevos desafíos, revaluando de manera permanente sus programas, revisando planes, procedimientos, e implementación tecnológica, alineándose con estándares nacionales e internacionales en búsqueda de la excelencia en la gestión integral de seguridad, para lograr los mejores resultados en beneficio de sus funcionarios, usuarios y comunidad en general.

PALABRAS CLAVES:
ESTUDIO DE SEGURIDAD
SEGURIDAD FÍSICA
ANÁLISIS Y GESTIÓN DE RIESGOS
SEGURIDAD PRIVADA

ABSTRACT

"Concejo Nacional Electoral" of the Republic of Ecuador is the maximum organism of suffrage. Its main office is in Quito, located at 6 de Diciembre Av. and Bosmediano. It has complete financial and administrative autonomy. Its functions are to organize and control elections. Also, CNE can sanction political parties and candidates who violate election rules if necessary.

"Consejo Nacional Electoral" as the Electoral entity of Ecuadorian, is the organizer of the electoral process. This makes it the target of threats because of political interests and social conditions that could affect the integrity of CNE authorities and employees, as well as of their facilities, equipment and materials.

The security of "Consejo Nacional Electoral" it is of fundamental importance for the country; that is why we should be focused to contribute to the security of each electoral process in Ecuador. We need to be focused on integral security protecting people, assets, information, and the community in general.

It is important to establish an integral system of physical protection measures with the propuse to prevent, control, verify intrusions, occupations, robbery, sabotage, and detect beforehand possible attacks. Also, it is important to evidence the action of the adversaries, allowing through an adequate communication a quick response of the security forces destined for this effect in order to interrupt and/or neutralize the action of adversaries avoiding a violent confrontation.

The security process wants to give a response that anticipates different possible events that can affect the organization. For this purpose it is not enough to develop a response plan, but also maintain a security system based on prevention rather than in reaction or response.

CNE, their organizations and units of the Electoral functions are committed to dynamically adapt security criteria to new challenges. CNE needs to permanently revaluate their programs, reviewing plans, procedures, and technological implementation, based on national and international standards in search of excellence in the integral management of security in order to obtain the best results for the benefit of its employees, users, and the community.

KEYWORDS:
SECURITY STUDY
PHYSICAL SECURITY
ANALYSIS AND RISK MANAGEMENT
PRIVATE SECURITY

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. Tema de Tesis

"SISTEMA INTEGRAL DE SEGURIDAD: REQUERIMIENTOS PARA CONTRARRESTAR LOS RIESGOS Y AMENAZAS QUE PUEDEN AFECTAR LA SEDE DEL CONSEJO NACIONAL ELECTORAL EN EL DM. DE QUITO".

1.2. Planteamiento del Problema de Investigación.

La naturaleza competitiva y los intereses contrapuestos en disputa de las elecciones determinan la posibilidad de existencia de una serie de amenazas y riesgos para el Consejo Nacional Electoral en contra de funcionarios, usuarios, contratistas, comunidad, activos, redes e información, por lo que se hace necesario realizar un análisis – estudio de seguridad que permita determinar las condiciones de seguridad existentes y desarrollar un sistema de protección integral.

Existen versiones de que, desde el nacimiento de la república hasta hace pocas décadas el país vivió por efecto de la confrontación conservadora- liberal una lamentable experiencia de fraudes electorales, así como lo señalan investigadores de la talla de Oswaldo Hurtado, en su obra el Poder Político del Ecuador.

> *De los 85 presidentes que ha tenido el país 21 son dictaduras; 25 han sido ejercidos por personas que se les ha encargado el poder por corresponderles el poder constitucionalmente o por así haberlo decidido los "notables"; 20 provienen de asambleas constituyentes o congresos dominados por el dictador o por el caudillo triunfante; y solo 19 han sido elegidos a través del sufragio popular* ***ordinariamente fraudulento****, salvo en las últimas décadas* ***aunque no siempre****." Osvaldo Hurtado en su obra El Poder Político del Ecuador* (Hurtado, 2006)

En nuestro país, es de suma importancia que el Consejo Nacional Electoral (CNE), tenga un adecuado manejo, control y seguridad integrado que contribuya al desarrollo de los Procesos Electorales, los mismos que incidirán directamente con la estabilidad y continuidad del Estado ecuatoriano. Dice nuestra Constitución Política que la soberanía reside en el pueblo y este la ejerce a través de instrumentos democráticos siendo, entre ellos, el más importante, el ejercicio del voto mediante los procesos electorales que permite elegir o ser elegidos para cumplir funciones de representación popular, de ahí que es vital un proceso transparente, con un sistema de seguridad que contribuya a que cada uno de sus procesos se cumplan con parámetros de seguridad y transparencia; como lo estable jurídicamente la Constitución Política del Estado Ecuatoriano.

La integridad y transparencia de los procesos electorales es un factor clave para que en un país exista gobernabilidad democrática. De ahí que los fraudes electorales sean no sólo el más grave atropello a la soberanía popular sino también la más rotunda violación a los derechos políticos y civiles de los ciudadanos y ciudadanas, semilla de justificado descontento, representa una amenaza permanente a la gobernabilidad democrática y a la estabilidad de una nación y consecuentemente del CNE como el máximo organismo de la función electoral.

La seguridad del Consejo Nacional Electoral en el país, es de fundamental importancia, razón por la cual debe ser enfocada para contribuir a la ejecución segura de cada evento electoral a desarrollarse en el Ecuador, con un enfoque de seguridad integral, protegiendo personas, activos, información, comunidad en general. En este sentido el estado debe proveer de garantías para que los candidatos puedan hacer campaña libremente en todo el país, seguridad a sus ciudadanos para que ejerzan su derecho al voto de forma libre y voluntaria y que las autoridades del CNE no sientan presiones o se vean amenazadas dentro del desarrollo de los procesos electorales. De ahí la importancia de la Dirección Nacional de Seguridad Integral del CNE, realice las coordinaciones y acciones pertinentes para el desarrollo de estudios técnicos que permitan determinar los riesgos que deben ser priorizados para una gestión eficiente de los mismos.

En los últimos años, nuestro país ha soportado una vida política muy agitada, por lo cual la democracia ha sido quebrantada innumerables veces con golpes de Estado y cuartelazos dando paso a gobiernos de facto.

El gobierno del Econ. Rafael Correa Delgado, se ha constituido en unos de los periodos presidenciales más estables por la aceptación y respaldo popular, sin embargo la oposición política representan la antesala a un posible escenario que amenace la seguridad del CNE, autoridades, funcionarios y del desarrollo normal del proceso electoral en sus diferentes fases Pre-Electoral, Acto Electoral, Post-Electoral; como ya se evidenció con el problema de las firmas falsas, en donde funcionarios del CNE fueron acusados de la venta de la base de datos del Registro Electoral, esto indica lo vulnerable que es el Consejo Nacional Electoral, al no disponer de un sistema de seguridad integral.

Las actividades que se desarrollan en el CNE por tener un carácter de interés político, estas pueden verse afectadas por diferentes tipos de amenazas, influenciadas por la forma particular de llevarse a cabo, la influencia de la interrelación entre las actividades y las circunstancias específicas de cada elección, determinan el nivel y prioridad del riesgo relacionado con cada una de las diferentes amenazas.

> *Por ejemplo, en la segunda ronda de votaciones para elegir a un presidente (la final entre dos candidatos en competencia), el peligro de asesinato político u atentado representa un riesgo significativamente mayor que en una elección de cientos de parlamentarios para una asamblea.* (ACE Project Red de Conocimientos Electorales,)

Cabe señalar que el Consejo Nacional Electoral tiene personal de contrato como funcionarios permanentes y por temporada que por necesidades y requerimientos propios de cada proceso electoral son contratados sin procesos óptimos de selección de personal lo que puede alterar rápidamente a las actividades normales esto requiere que en forma expedita se vuelvan a priorizar o se invaliden los procedimientos de seguridad iníciales por lo que corresponde a situaciones especiales que tendrían altos perfiles de riesgo y las medidas tendrían que ser de otra naturaleza.

Además, las condiciones circunstanciales que puedan suscitarse y la ausencia de un Sistema de Seguridad Integral, así como el desconocimiento de los funcionarios del CNE con respecto a normas y procedimientos generales de seguridad (temas de seguridad), son aspectos que deben ser evaluados para determinar en base a la vulnerabilidad existente las amenazas y riesgos, de mayor impacto y profundidad que deben ser considerados como base de la planeación de la Dirección Nacional de Seguridad Integral del CNE; para lo cual es necesario establecer lineamientos y estrategias de seguridad muy flexibles.

Con estos antecedentes el Consejo Nacional Electoral y sus autoridades se han visto en la necesidad de llevar a cabo varias estrategias direccionadas a proteger sus bienes, personal e información, con el objetivo de disminuir su vulnerabilidad, ante posibles amenazas, a través del diseño de un Sistema Integral de Seguridad.

1.3. Delimitación y formulación del Problema de Investigación.

1.3.1. Delimitación espacial.

En el aspecto internacional es conocido como el terrorismo ve una oportunidad en el ritual de la democracia que las elecciones despiertan, amenazas de parte de diferentes grupos, cuyas motivaciones pueden no tener conexión con los objetivos nacionales de una elección. Como lo han demostrado sucesos recientes cuando el proyecto maoísta de Sendero Luminoso se puso en acción en precisa y exacta coincidencia con el proceso electoral general de 1980; el asesinato del pre-candidato presidencial de Colombia Luis Carlos Galán (18 de agosto de 1989) partidario de permitir la extradición de los narcotraficantes a los Estados Unidos, y considerado como entre los mejor posicionados para hacerse con la candidatura del Partido Liberal, el intento de asesinato de César Gaviria (27 de noviembre de 1989) quien no subió al vuelo 203 de Avianca por consejo de sus asesores, con un saldo de 107 muertos esta ordenes de asesinato fueron dadas por Pablo Escobar Gaviria líder del Cartel de Medellín. De esta forma podemos evidenciar el gran interés de las organizaciones criminales y terroristas en utilizar un proceso electoral para manifestar sus intereses propios.

El terrorismo internacional tiene la capacidad y motivación para llevar a cabo "ataques espectaculares" con el objetivo de impulsar sus propias agendas. La intensificación de la cobertura en los medios durante una elección hace de este periodo algo altamente visible, por lo que se vuelve una oportunidad atractiva para que ocurran este tipo de ataques.

> *La influencia del narcotráfico sobre los partidos políticos ha sido ampliamente documentada por Comisiones Legislativas que han investigado este problema. Como en países cercanos esta amenaza se cierne sobre el funcionamiento del sistema democrático, a pesar de que no reviste características tan graves como en aquellos en los cuales son centro de procesamiento y distribución donde el Ecuador se ve directamente afectado.*

> *Relacionado con este problema, aunque con causas independientes se encuentran el creciente fenómeno de la corrupción pública. La centralización estatal ha propiciado esto pues al ampliarse el marco de las regulaciones estatales se amplían las oportunidades para los funcionarios de obtener privilegios u ofrecer excepciones a sus deberes, a cambio de la dádiva y del soborno. El aumento de la delincuencia del cuello blanco es un claro reflejo de esta circunstancia*. (Alfonsin, Agenda para la Cosolidación de la Democracia en América Latina, 1990)

Una historia concurrente de paros que por lo general han dejado víctimas fatales y daños a la propiedad tanto pública y privada; como el 30 de Septiembre del 2010, donde existió un levantamiento de la Policía Nacional y un grupo de militares, que originaron el ambiente propicio para causar una conmoción social que dejó grandes pérdidas económicas. Manifestaciones, saqueos y cinco víctimas, son ejemplo de cómo las instituciones públicas a nivel nacional pueden ser un blanco propicio para el descontento social o intereses políticos particulares.

Es así como hace algunos años el Consejo Nacional Electoral, ha sido víctima de amenazas de bomba y atentados sin llegar a materializarse, el problema de la validación de firmas y acreditación de partidos y la verificación de todo el proceso por la denuncia de firmas falsas de incluso, partidos políticos ya acreditados, generaron manifestaciones sin daños a la propiedad, y críticas por los medios de comunicación desprestigiando su imagen; en vista de la naturaleza competitiva y los intereses contrapuestos en disputa de las elecciones; estas presentan una serie de amenazas y riesgos para las autoridades, funcionarios, infraestructura, información, equipos y materiales de la institución por lo que es necesario realizar un plan de seguridad integral acorde a las necesidades estructurales y funcionales del CNE.

El Consejo Nacional Electoral de la República del Ecuador es el máximo organismo de sufragio. Tiene su sede en la ciudad de Quito, ubicado en la Av. 6 de diciembre y Bosmediano, goza de completa autonomía financiera y administrativa. Sus funciones son organizar, controlar las elecciones, puede sancionar a partidos y candidatos que infrinjan las normas electorales.

Hasta el 2008, el organismo máximo electoral del Ecuador era el Tribunal Supremo Electoral de Ecuador (TSE). A partir de la aprobación de la Constitución de Ecuador de

2008, el Consejo Nacional Electoral asumió ciertas funciones del TSE y otras pasaron a manos del nuevo Tribunal Contencioso Electoral.

Este organismo conforma, junto al Tribunal Contencioso Electoral, la Función Electoral.

La seguridad del Consejo Nacional Electoral se requiere que se sustente en el esfuerzo integrado de las autoridades y de la Dirección Nacional de Seguridad Integral, por lo que en este Plan, deberá atender los aspectos de: seguridad física, personal, electrónica, informática, y de la información, que forman parte de la seguridad integral.

1.3.2. Delimitación temporal

La presente investigación se realizará durante el primer semestre de 2013, considerando la información que se dispone de los últimos 10 años y procesos electorales producidos en el país.

1.3.3. Formulación del Problema de Investigación

¿La no disponibilidad de un Sistema de Seguridad Integral que atienda los requerimientos para contrarrestar los riesgos y amenazas que atentan a la SEDE del Consejo Nacional Electoral del DM. de Quito, afectará el normal desenvolvimiento de sus actividades?

1.4. Objetivos de la Investigación.

1.4.1. Objetivo General.

Diseñar un Sistema de Seguridad Integral acorde, flexible y óptimo para el Consejo Nacional Electoral con sede en Quito; que garantice la protección y seguridad de personas, infraestructura, información, equipos y materiales; que permita precautelar el normal desarrollo de sus actividades.

1.4.2. Objetivos Específicos.

- Determinar la situación actual de seguridad en la sede del CNE del Distrito Metropolitano de Quito.
- Identificar los activos críticos del CNE con sede en el Distrito Metropolitano de Quito, que incluya bienes, personal e información y su exposición a riesgos identificados.
- Determinar las amenazas y evaluar los riesgos a los que se encuentra expuesta la sede del CNE, en el DM. De Quito, mediante la relación de riesgos y amenazas y vulnerabilidad existente.
- Determinar los recursos humanos y materiales disponibles en la sede del CNE. en el DM. de Quito, para ser utilizados adecuadamente en diseño del Sistema de Seguridad Integral.
- Determinar los recursos humanos y materiales que se requieren para el diseño de un Sistema de Seguridad Integral en la sede del CNE. en el DM. de Quito.
- Establecer la metodología de planificación más apropiada para la elaboración del Sistema de Seguridad integral para la sede del CNE., en la ciudad de Quito.
- Desarrollar planes, procedimientos, sistemas y subsistemas del sistema de seguridad integral del CNE.

1.5. Justificación de la Investigación

La inseguridad ha tocado las fibras más sensibles de nuestra sociedad y ha mostrado la fragilidad y vulnerabilidad de las instituciones públicas por lo que el presente estudio es una herramienta de apoyo que permitirá prevenir, disminuir, controlar,

responder y recuperarse al CNE de un posible evento disruptivo; por este motivo sus Directivos han visto la necesidad de disponer de un Sistema de Seguridad Integral que le permita garantizar la seguridad optima de personas, equipos, materiales, infraestructura e información.

El Consejo Nacional Electoral como función Electoral del estado Ecuatoriano, es el organizador de los procesos electorales; esto le convierte en blanco de amenazas por intereses políticos y sociales particulares que podrían afectar la integridad de autoridades y funcionarios del CNE; así como de sus instalaciones, equipos y materiales.

Factibilidad Política: El Consejo Nacional Electoral al ser la máxima autoridad del sufragio, con completa autonomía financiera y administrativa, que con apoyo de los organismos de Seguridad del Estado, trabaja en forma conjunta con el Ministerio de Coordinación de Seguridad Interna y Externa, Ministerio de Defensa, Ministerio del Interior, Secretaría Nacional de Inteligencia, Secretaría Nacional de Gestión de Riesgos; materializados en sus órganos operativos FF.AA. y Policía Nacional; y otras instituciones que tienen responsabilidades en el proceso electoral, esto es el Ministerio de Educación, Cruz Roja, Cuerpo de Bomberos y otras, que de forma particular planifican y ejecutan lo pertinente a cada ámbito de su especialidad.

Factibilidad Financiera: Se dispone de los recursos necesarios para desarrollar la investigación que garantice el diseño de un Plan de seguridad para atender todos los requerimientos que implica disponer de un sistema de seguridad integral que presente un ambiente óptimo para el desarrollo de sus actividades.

Factibilidad Administrativa: La estructura organizativa del CNE, facilita la concepción, diseño y ejecución de un Sistema de Seguridad Integral que integre a todos sus participantes en sus diferentes niveles como parte de su planificación.

Para la presente investigación se dispone de la dirección y codirección, aparte del asesoramiento de personal técnico que labora en el Consejo Nacional Electoral.

Las importantes funciones que se encuentran asignadas a este organismo del Estado requiere que dispongan de un Sistema de Seguridad Integral que garantice el normal

desarrollo de sus actividades, que identifique aspectos técnicos, administrativos y de seguridad más sensibles a ser atacados por su vulnerabilidad, y las amenazas y riesgos a los que está expuesto, determinando normas y procedimientos específicos a los diferentes niveles y momentos de los procesos que cumple el organismo, así como a los miembros permanentes y temporales que laboran en el CNE, antes, durante y después de los procesos electorales.

Así la investigación, contribuirá a prevenir, disminuir, controlar, responder y recuperarse al CNE de un posible evento disruptivo derivados de amenazas; y aplicar acciones correctivas oportunas.

Beneficiarios Directos: Autoridades, funcionarios del CNE, usuarios como partidos, movimientos políticos y la ciudadanía en general.

Beneficiarios Indirectos: La comunidad que vive cercana a las instalaciones de la sede del CNE en el Distrito Metropolitano de Quito.

1.6. Interrogantes de Investigación

1. ¿Cuál es la situación actual de la seguridad en la sede del CNE del DM. de Quito?
2. ¿Cuáles son los riesgos y amenazas a los que están expuestos: físicamente el CNE., funcionarios y personal que labora en la instalación, la información que dispone, y los equipos que se utilizan en el proceso electoral?
3. ¿Qué recursos físicos y sistemas técnicos de seguridad tanto pasiva y activa están disponibles en el CNE para ser empleados en el Sistema de Seguridad Integral?
4. ¿Qué recursos físicos y sistemas técnicos de seguridad tanto pasiva y activa se requieren para el diseño del Sistema de Seguridad Integral?
5. ¿Qué conocimientos de seguridad tiene el personal que labora dentro del CNE?
6. ¿Cómo incide los criterios y opiniones del nivel directivo en la aceptación de la necesidad de la implementación de un Sistema de Seguridad Integral?
7. ¿Cómo se puede llevar a cabo la estructuración de un Sistema de Seguridad Integral para Consejo Nacional Electoral con sede en Quito?
8. ¿Qué metodología es la más adecuada para la elaboración del Sistema de Seguridad a ser implementado en el CNE?

1.7. Operacionalización de las interrogantes.

Tabla Nº 1 Operacionalización de las interrogantes de investigación

PROBLEMA	VARIABLES	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	PREGUNTAS DE INVESTIGACIÓN.	INSTRUMENTO
¿La no disponibilidad de un Sistema de Seguridad Integral que atienda los requerimientos para contrarrestar los riesgos y amenazas que atentan a la SEDE del Consejo Nacional Electoral del DM. de Quito, afectará el normal desenvolvimiento de sus actividades?	**INDEPENDIENTE** Requerimientos para contrarrestar los riesgos y amenazas que atentan a la SEDE del Consejo Nacional Electoral del DM. de Quito	Fortalecer y modernizar los mecanismos necesarios para garantizar la seguridad de autoridades electorales, funcionarios del CNE, candidatos, visitantes	**Necesidades del entorno del CNE, sede Quito sobre seguridad.**	- Evaluación de riegos de seguridad en la sede quito. - Identificación de los recursos humanos y materiales que se disponen para seguridad en el CNE sede Quito. - Incorporación de normas y procedimientos de protección pasiva y activa al Sistema de Seguridad del CNE.	2. ¿Cuáles son los riesgos y amenazas a los que están expuestos: físicamente el CNE., funcionarios y personal que labora en la instalación, la información que dispone, y los equipos que se utilizan en el proceso electoral? 3. ¿Qué recursos físicos y sistemas técnicos de seguridad tanto pasiva y activa están disponibles en el CNE para ser empleados en el Sistema de Seguridad Integral? 4. ¿ Qué recursos físicos y sistemas técnicos de seguridad tanto pasiva y activa se requieren para el diseño del Sistema de Seguridad Integral? 5. ¿Qué conocimientos de seguridad tiene el personal que labora dentro del CNE? 7. ¿Cómo se puede llevar a cabo la estructuración de un Sistema de Seguridad Integral para Consejo Nacional Electoral con sede en Quito?	**Encuesta** **5; 6; 7; 11; 12; 15; 16; 18; 19; 21; 22;24; 26; 27; 28** **Lista de chequeo de seguridad** **Entrevista.** **2; 3; 7; 8; 10**
	DEPENDIENTE Sistema de Seguridad Integral	Planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos, así como el resguardo de los activos de la empresa.	**Plan operativo de seguridad integral.**	- Situación actual de la seguridad en el CNE Quito. - Establecimiento de metodología más apropiada para el diseño del Sistema de Seguridad del CNE sede Quito. - Diseño de un Sistema de Seguridad flexible y dinámico.	1. ¿Cuál es la situación actual de la seguridad en la sede del CNE del DM. de Quito? 6. ¿Cómo incide los criterios y opiniones del nivel directivo en la aceptación de la necesidad de la implementación de un Sistema de Seguridad Integral? 8. ¿Qué metodología es la más adecuada para la elaboración del Sistema de Seguridad a ser implementado en el CNE?	**Encuesta.** **1; 2; 3; 4; 5; 6; 8; 9; 10; 13; 14; 17; 18; 20; 23; 25; 29; 30** **Lista de chequeo de seguridad** **Entrevista** **1; 4; 5; 6; 8; 9; 10**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes de la Investigación

La sede del Consejo Nacional Electoral del DM. de Quito, dispone de Planes de Contingencia, Planes de Seguridad para el Proceso Electoral y otros más; se dispone de instructivos y directivas de procesos electorales inmediatos anteriores como las Elecciones Generales 2009, Procesos Electorales de revocatorias y consulta popular 2011, que han sido utilizadas en las operaciones de seguridad, para el cumplimiento y desarrollo de eventos electorales; no existen Planes que establezcan la temática de la seguridad en forma integral y como un sistema que garantice el desarrollo de las actividades del CNE, en paz y tranquilidad.

2.2. Marco legal

Constitución Política de la República.

Capitulo Sexto; de la Función Electoral:

Art. 219.- El Consejo Nacional Electoral tendrá, además de las funciones que determine la ley, las siguientes:

1. Organizar, dirigir, vigilar y garantizar, de manera transparente, los procesos electorales, convocar a elecciones, realizar los cómputos electorales, proclamar los resultados, y posesionar a los ganadores de las elecciones.
2. Designar los integrantes de los organismos electorales desconcentrados.

Art. 158.- Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos.

Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial.

La protección interna y el mantenimiento del orden público son funciones privativas del Estado y responsabilidad de la Policía Nacional.

Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador "Código de la Democracia":

La presente ley dicta las normas y procedimientos con respecto al Sistema Electoral, a la organización de la Función Electoral, a los derechos y obligaciones de participación político electoral de la ciudadanía y la normativa y procedimientos de justicia Electoral.

Art. 16.- Ninguna autoridad extraña a la organización electoral podrá intervenir directa o indirectamente en el desarrollo de los procesos electorales ni en el funcionamiento de los órganos electorales. Las y los integrantes de las Fuerzas Armadas y Policía Nacional, que se encuentren asignados a la seguridad del proceso electoral, solo podrán actuar en el cumplimiento de las órdenes emanadas por los presidentes y presidentas del Consejo Nacional Electoral, de las Juntas Regionales, Distritales, Provinciales Electorales y de las juntas receptoras del voto, en el ámbito de esta ley.

Art. 18.- La Función Electoral garantiza el ejercicio de los derechos políticos que se expresan a través del sufragio, así como los referentes a la organización política de la ciudadanía. La Función Electoral estará conformada por el Consejo Nacional Electoral y el Tribunal Contencioso Electoral. Estos órganos tendrán sede en Quito, jurisdicción nacional, autonomía administrativa, financiera y organizativa, y personalidad jurídica propia y se financiarán con recursos del Presupuesto General del Estado.

Se regirán por principios de autonomía, independencia, publicidad, transparencia, equidad, interculturalidad, paridad de género, celeridad, probidad, certeza, eficacia,

eficiencia, calidad, coordinación, planificación, evaluación y servicio a la colectividad. En el caso del Consejo Nacional Electoral también rige el principio de la desconcentración.

La Función Electoral será representada por la Presidenta o Presidente del Consejo Nacional Electoral.

Art. 21.- Durante el proceso electoral, los organismos electorales dispondrán la colaboración de las autoridades públicas, militares y policiales para la aplicación de las disposiciones de esta ley; asimismo, previo acuerdo, podrán demandar la colaboración de las personas jurídicas de derecho privado.

Ley de Seguridad Pública y del Estado:

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

Ley de Vigilancia y Seguridad Privada:

Art. 1.- Objeto de la Ley.- Esta Ley regula las actividades relacionadas con la prestación de servicios de vigilancia y seguridad a favor de personas naturales y jurídicas, bienes muebles e inmuebles y valores, por parte de compañías de vigilancia y seguridad privada, legalmente reconocidas. Se entiende por prestación de dichos servicios la que sea proporcionada, dentro del marco de libre competencia y concurrencia, a cambio de una remuneración.

De los delitos contra la inviolabilidad del secreto

Art. 197.- Serán reprimidos con prisión de dos meses a un año y multa de cuarenta a cien sucres, los empleados o agentes del Gobierno y los del servicio de estafetas y

telégrafos que hubieren abierto o suprimido cartas confiadas al correo, o partes telegráficos, o que hubieren facilitado su apertura o supresión.

Art. 198.- Los que, siendo depositarios de partes telegráficos, hubieren revelado su existencia o contenido, a excepción de los casos en que fueren llamados a declarar en juicio y de aquellos en que la ley les obligue a hacer conocer la existencia o contenido de dichos despachos, serán reprimidos con prisión de quince días a seis meses y multa de cuarenta a ochenta sucres.

Art. 199.- El que hallándose en posesión de una correspondencia no destinada a la publicación, la hiciera publicar, o presentare en juicio sin orden judicial, aunque haya sido dirigida a él, será reprimido con multa de cuarenta a doscientos sucres, si el acto puede causar perjuicio a terceros; a no ser que se trate de correspondencia en que consten obligaciones a favor del tenedor de ella, caso en el que puede presentarse en juicio.

Art. 200.- En la misma pena incurrirá el que, sin ser empleado público, divulgare actuaciones o procedimientos de que haya tenido conocimiento y que, por ley, deben quedar reservados.

Art. 201.- El que teniendo noticia, por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación puede causar daño, lo revelare sin causa justa, será reprimido con prisión de seis meses a tres años y multa de cincuenta a quinientos sucres.

Art. 202.- Los que sustrajeren cartas confiadas al correo serán reprimidos con prisión de quince a sesenta días, excepto los padres, maridos o tutores que tomaren las cartas de sus hijos, consortes o pupilos, respectivamente, que se hallen bajo su dependencia.

De la violación de sellos y documentos

Art. 240.- Cuando hubieren sido rotos los sellos puestos por orden de la autoridad pública, los guardianes serán reprimidos, por simple negligencia, con prisión de ocho días a seis meses.

Art. 241.- Los que hubieren roto intencionalmente los sellos serán reprimidos con prisión de seis meses a dos años; y si el culpado fuere el guardián mismo o el funcionario público que ha ordenado o ejecutado la fijación, será reprimido con prisión de uno a tres años.

Art. 242.- Si los sellos rotos fueren de los fijados sobre papeles o efectos de un individuo acusado de un delito, señalado la pena de reclusión mayor o de reclusión menor extraordinaria, o de un individuo condenado por estas penas, el guardián negligente será reprimido con prisión de tres meses a un año.

Art. 243.- El que hubiere roto intencionalmente los sellos puestos sobre papeles o efectos de la calidad enunciada en el artículo precedente, será reprimido con prisión de uno a tres años; y si el culpado es el guardián o el funcionario público que ha ordenado o ejecutado la fijación, será reprimido con prisión de uno a cinco años.

Art. 244.- Si el rompimiento de los sellos ha sido cometido con violencias, el culpado será reprimido con el máximo de las penas señaladas para la infracción.

Art. 245.- En los casos de los Arts. 241, 242, 243 y 244, el culpado podrá ser condenado, además, a multa de cuarenta a cuatrocientos sucres.

De los delitos contra los medios de comunicación

Art. 422.- (Agregados los tres últimos incisos por el **Art.** 1 de la Ley 99-38, R.O. 253, 12-VIII-99).- Será reprimido con prisión de seis meses a dos años el que interrumpiere la comunicación postal, telegráfica, telefónica, radiofónica o de otro sistema, o resistiere violentamente al restablecimiento de la comunicación interrumpida.

Quienes ofrezcan, presten o comercialicen servicios de telecomunicaciones, sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios o cualquier otra forma de la contratación administrativa, salvo la utilización de servicios de Internet, serán reprimidos con prisión de dos a cinco años.

Estarán comprendidos en esta disposición, quienes se encuentren en posesión clandestina de instalaciones que, por su configuración y demás datos técnicos, hagan presumir que entre sus finalidades está la de destinarlos a ofrecer los servicios señalados en el inciso anterior, aun cuando no estén siendo utilizados. Las sanciones indicadas en este artículo, se aplicarán sin perjuicio de las responsabilidades administrativas y civiles previstas en la Ley Especial de Telecomunicaciones y sus Reglamentos.

2.3. Marco teórico – conceptual

2.3.1. La seguridad su origen y desarrollo en la humanidad

La seguridad es el resultado del proceso histórico derivado del estado de incertidumbre e indefensión del ser humano frente a fenómenos naturales o acciones de otros seres con quienes a compartido supervivencia, desde los albores de la humanidad hasta la presente fecha.

La búsqueda de la seguridad la encontramos entonces inscrito en la humanidad desde los tiempos más remotos. El hombre se enfrenta a un mundo que no entiende y que le agrede constantemente lo cual lo obliga a subsistir por sus propios medios y a defenderse de factores naturales y antrópicos siendo este último uno de los más peligrosos ya que su amenaza es constante y representa uno de los factores psicológicos de percepción de inseguridad más importantes. De esta manera ha escrito Mallet:

> *"El ansia de seguridad ha sido el motor del progreso de la humanidad. La invención de la agricultura fue una forma de asegurarse alimento en vez del aleatorio método de la caza y de la recolección de frutos silvestres. La agrupación en tribus, la formación de aldeas de ciudades, la constitución de estados, traducen el deseo de seguridad frente a un enemigo exterior."* (Mallet, 1983)

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Sun Tzu Cicerón, César, Virgilio, Seutonio, Frontino, han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa, Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.

> *La "Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella"* (Dr. Manunta)

El próximo paso de la Seguridad fue especialización. Así nace la seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas.

2.3.2. Sistema integral de seguridad

> *Desarrollar un sistema de seguridad implica planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos, así como el resguardo de los activos de la empresa, basado en el análisis de la amenaza.* (POA).

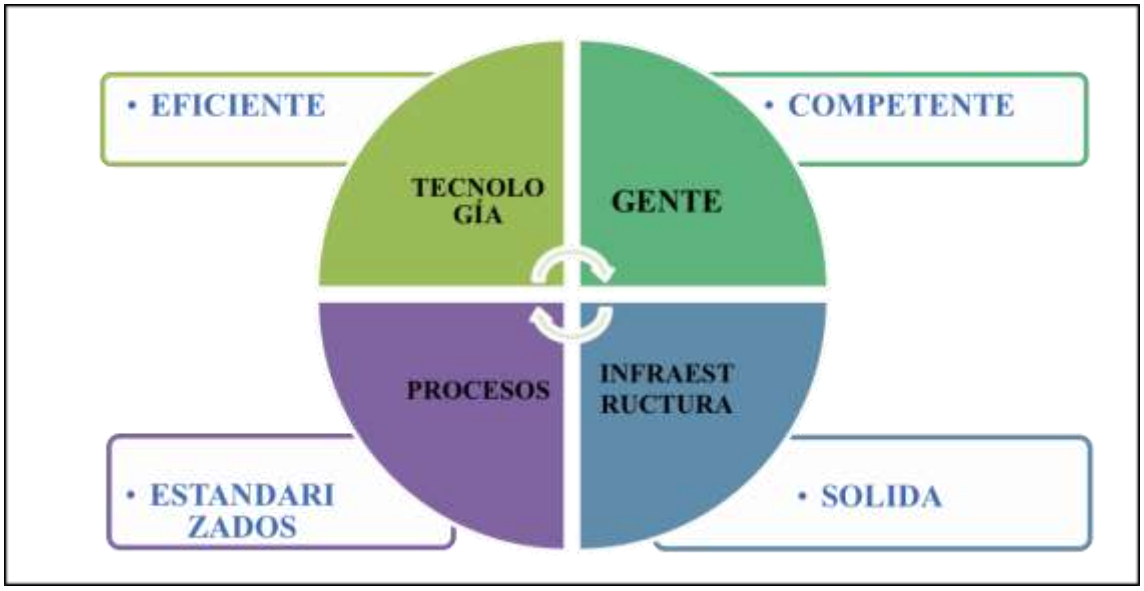
El análisis de los factores de riesgo que se presentan nos permitirán realizar un diagnóstico, que permitirá dar paso a la elaboración de un Sistema de Seguridad Integral el cual, permite plantear la solución a los problemas referidos en el diagnóstico de seguridad, estableciendo participantes, objetivos generales y específicos; niveles de intervención, fijando objetivos, estrategias y actividades a seguir; y, el presupuesto correspondiente.

La misma que es destinada a fortalecer y modernizar los mecanismos necesarios para garantizar la seguridad de autoridades electorales, funcionarios del CNE, candidatos, visitantes. De ahí la importancia de la Dirección Nacional de Seguridad Integral del CNE, contar con un Sistema de Seguridad Integral.

El presente trabajo estará estructurado bajo el análisis de la información referente a seguridad dentro de las instalaciones del CNE, teniendo en cuenta factores como la delincuencia común y organizada, grupos sociales o agrupaciones políticos adversos,

fenómenos atmosféricos adversos y atentados terroristas, por lo que a continuación se exponen varios temas y conceptualizaciones que serán utilizados durante el proceso de análisis.

Gráfico Nº 1 Seguridad integral



Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.3. Integración de subsistemas en la seguridad

La seguridad es un sistema de combinación de métodos, procedimientos, técnicas y elementos diseñados para disuadir, detectar, denegar, demorar y reaccionar con respecto a la amenaza, cuya meta es crear un contexto de tranquilidad para el desarrollo de actividades, la seguridad busca la integración de subsistemas para la optimización de los recursos, con este antecedente aparece el concepto de seguridad integral, en el cual están inmerso la seguridad física que son los elementos tangibles diseñados para la protección y que también incluye el uso de tecnología, que algunos autores la fragmentan como potro subsistema de seguridad electrónica; la seguridad personal busca la protección de la vida e integridad de la personas; la seguridad informática protege equipos informáticos, programas y archivos de ataques externos como virus y hackers; la seguridad de la información permite la preservación, confidencialidad e integridad de la información.

Un sistema integrado de seguridad para prevención de pérdidas puede muchas veces ser omitido por soluciones de seguridad limitadas sin un estudio ni planificación adecuada para la incorporación e integración de medidas de seguridad.

Tipos respuestas que se suelen dar para enfrentar problemas de seguridad:

Unidimensional.- Basada en una sola medida. Ejemplo: Solo Seguros o solo vigilantes.

Fragmentada.- Agregando ingredientes de acuerdo a como surge la necesidad sin un programa coherente.

Reactiva.- Respondiendo únicamente a eventos específicos de perdida.

Empaquetada.- Sistemas estándares de seguridad (equipo, personal o ambos) "porque todos lo hacen" en el supuesto de que un paquete responderá a cualquier clase de problema sin un diagnóstico previo.

Integral.- Basada en el análisis de riesgos y evaluación de vulnerabilidades con cobertura sobre todos los activos materiales y no materiales.

> *Sin embargo ningún plan o programa (sistema) puede ser efectivo sin un entendimiento claro de la problemática a enfrentar. (ASIS, 2012)*

2.3.4. Análisis y gestión de riesgos

El proceso de análisis y gestión de riesgos utiliza instrumentos que sirven de apoyo a esta gestión de administración de los riesgos priorizados de acuerdo al impacto en las organizaciones. La parte central de la gestión de riesgos está comprendida por los medios para analizar y evaluar los riesgos, así como valorar, recomendar o priorizar las medidas, a través de métodos cualitativos y cuantitativos para proceder al análisis.

El análisis de riesgos determina el impacto o afectación al que nos encontramos expuestos; el riesgo existe cuando este afecta directa o indirectamente al ser humano el

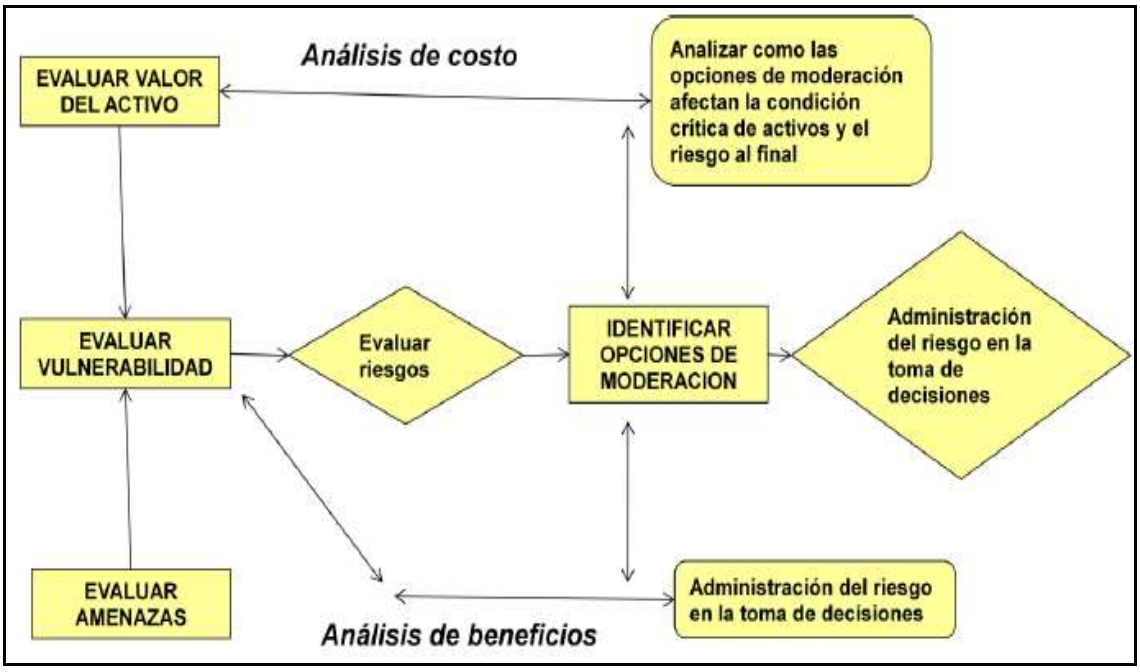
cual puede medir el riesgo a través de la relación de la amenaza por la vulnerabilidad y la capacidad existente para enfrentar la amenaza.

El análisis de riesgos permite identificar los bienes e información que necesitan ser protegidos y los tipos de riesgos que pueden afectarlos, determina la probabilidad de incidencia y el impacto o el efecto.

> *El libro "Risk Analysis and the Security Survey"; escrito por James F. Broder, CPP Security, menciona las siguientes tareas básicas para realizar el análisis del riesgo:* (Broder, 1999)

- Identificar los bienes que necesitan protección.
- Identificar los tipos de riesgos que pueden afectar los bienes involucrados.
- Determinar la probabilidad de incidencia del riesgo.
- Determinar el impacto o el efecto si ocurriera una pérdida determinada.

Gráfico Nº 2 Diagrama de flujo del análisis de riesgos

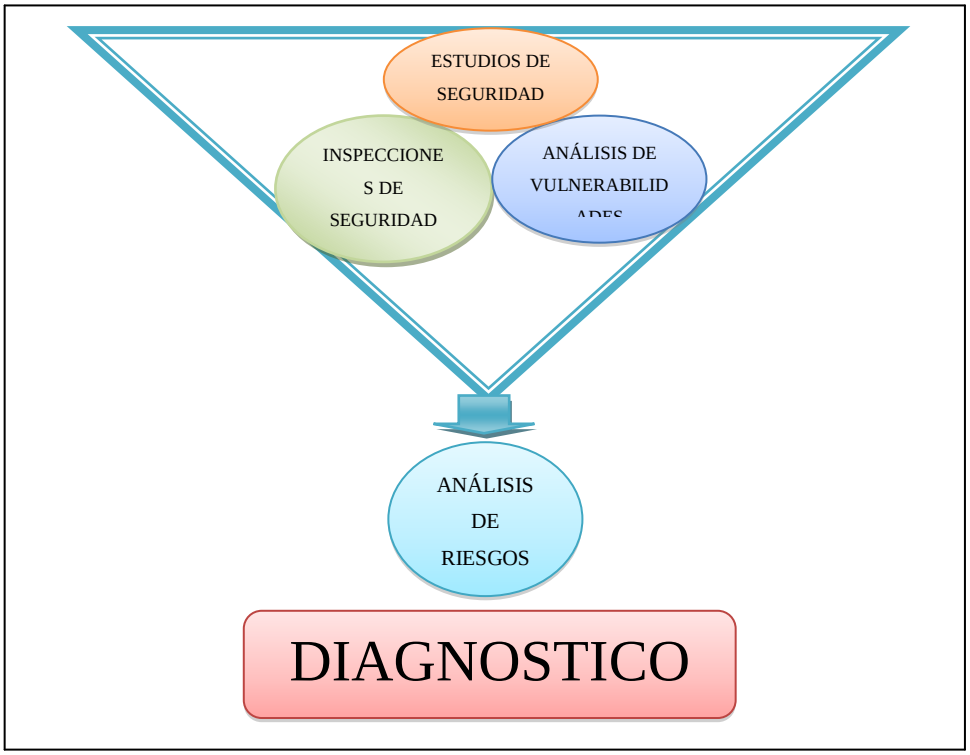


Fuente: Certificación PSP, "Guía de Estudio", David G. Patterson, CPP, PSP

Evaluación de riesgos.- Es un examen detallado de la instalación permite conocer sus procesos y rutas críticas, el valor del activo tangible o intangible, sobre el cual actúan las amenazas y su vulnerabilidad frente a estas, y el impacto en los activos, permite evaluar el riesgo.

Administración del riesgo.- Son las contramedidas y defensas para mitigar las amenazas y reducir las vulnerabilidades incluyendo el costo beneficio de implementarlas.

Gráfico Nº 3 Diagnóstico - Herramientas



Fuente: Fernando M. Chávez, CPP Presentación Herramientas de Diagnóstico.
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.4.1. Variables a considerar en el análisis de riesgos.

Los riesgos y amenazas, se han de analizar desde tres puntos de vista.

Gráfico Nº 4 Variables en el análisis de riesgos

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.4.2. Catálogo de riesgos.

El catálogo de riesgos está constituido por los siguientes riesgos:

Gráfico Nº 5 Catálogo de riesgos

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.5. Metodología en la seguridad

La metodología para el planeamiento de la Seguridad no es única esta se debe ajustar a las necesidades únicas y propias del objeto de estudio de seguridad, para motivo de la presente investigación emplearemos la metodología analítica, hace falta considerar los medios y procedimientos para poner en práctica las técnicas de Seguridad. Eso se contempla en la metodología operativa, que tiene como líneas fundamentales las siguientes: Estudio de se seguridad que incluye estudio del entorno, auditorías de seguridad (internas y externas) y sus correspondientes proyectos subsiguientes: formación y entrenamiento y al final inversiones en material y equipo

2.3.6. Estudio de seguridad

Método sistemático que permite determinar la situación de seguridad existente, las deficiencias o excesos, la vulnerabilidad de los sistemas o de la instalación y establece las recomendaciones de protección y seguridad.

Identifica los riegos y el grado de vulnerabilidad existente para enfrentar un tipo de evento, determina la protección necesaria y recomendaciones para mejorar la seguridad.

> *"Conjunto de procedimientos que permiten la recolección análisis, formulación y evaluación de la información relevante sobre los hechos reales y potenciales relacionados con la Seguridad de un ámbito específico, seguida de un diagnóstico, pronóstico y formulación para determinar las fuentes de riesgo y vulnerabilidad en cada recurso de incidencia, en un espacio y tiempo determinados."* (La Rotta, 2005)

El estudio de seguridad, puede establecer la necesidad de desarrollar un programa de seguridad, por medio de llevar a cabo un estudio completo de la instalación, sus operaciones y procedimientos, donde el experto o consultor de seguridad determinará los factores críticos y el valor activo de mayor importancia para la empresa que afectaría a la imagen y la continuidad de las operaciones normales de la organización. Las principales problemas con la seguridad están relacionados con hurto, fraude, falsificación, fuego, robo con allanamiento de morada, robo, daño intencionado, selección de personal e investigación, robo de secretos comerciales, espionaje industrial, protección a ejecutivos,

secuestro, extorsión, amenaza de bomba y explosión, y planificación de emergencia y desastre, siendo estos unos de los problemas más comunes.

> *R.M. Momboisse ha definido el estudio de seguridad como: "Un examen y análisis crítico, en situ, de una planta industrial, negocio, hogar, institución pública o privada para determinar el estado actual de seguridad, identificar deficiencias o excesos, determinar la necesidad de protección y hacer recomendaciones para mejorar la seguridad de conjunto" (Momboisse, 1968)*

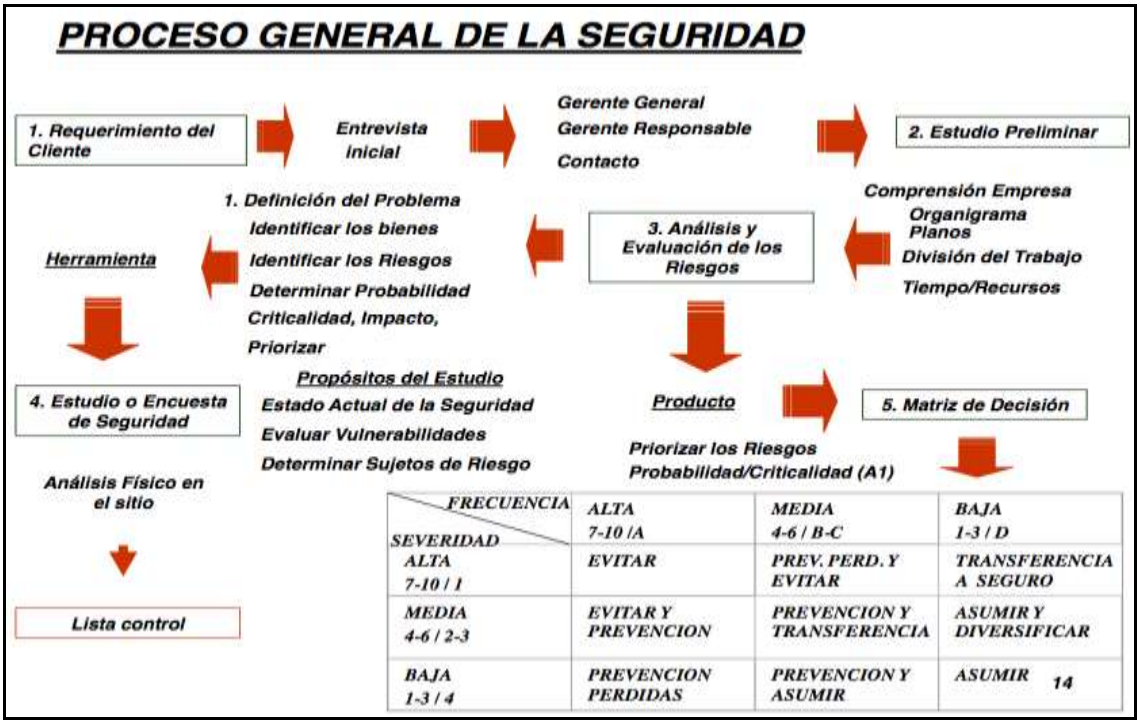
2.3.7. Proceso general de la seguridad

> *Por lo general se lleva a cabo un proceso lógico de acciones y tareas para diseñar e implementar un sistema de seguridad integral, dentro de la metodología que ASIS plantea, la seguridad en las organizaciones debe "participar en un proceso amplio y sistemático de prevención, control, mitigación, respuesta, continuidad y recuperación". (ASIS I. , 2009-2013)*

El proceso de la seguridad plantea dar un respuesta, que se anticipe a los diferentes eventos posibles, que pueden afectar a la organización, para lo cual ya no es suficiente elaborar un plan de respuesta, sino mantener un sistema de seguridad que en su mayor parte sea diseñado en materia de prevención y no en la reacción o respuesta.

Empresas, instituciones públicas y privadas, buscan asegurar la continuidad de sus actividades, por lo que la seguridad se constituye en un proceso continuo, dinámico e interactivo que aumenta la resiliencia organizacional.

Gráfico Nº 6 Proceso general de la seguridad



Fuente: Guillermo Pedraza, CPP "Presentación proceso general de la Seguridad"

Gráfico Nº 7 Proceso general de la seguridad

Fuente: Guillermo Pedraza, CPP "Presentación proceso general de la Seguridad"

Gráfico Nº 8 Proceso general de la seguridad

Fuente: Guillermo Pedraza, CPP "Presentación proceso general de la Seguridad"

2.3.8. Método Mósler

El método tiene por objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación de un riesgo, con la finalidad de que la información obtenida, nos permita calcular la clase y dimensión de riesgo para poder cuantificarlo, contrarrestarlo o asumirlo.

El método es de tipo secuencial y cada fase del mismo se apoya en los datos obtenidos en las fases que le preceden.

El desarrollo del mismo considera las siguientes fases: (Sanchez, 1998)

1º - Definición del riesgo.
2º - Análisis del riesgo.
3º - Evaluación del riesgo.
4º - Cálculo de la clase de riesgo.

1º fase – Definición del riesgo.

Esta fase tiene por objeto, la identificación del riesgo, delimitando su objeto y alcance, para diferenciarlo de otros riesgos. El procedimiento a seguir es mediante la identificación de sus elementos característicos, estos son:

1) El bien.- es toda persona o cosa que, en determinadas circunstancias, posee o se le atribuye una o varias cualidades benéficas y resulta objeto de valoración
2) El daño.- toda consecuencia negativa que experimenta un bien, por lo que sufre una disminución de su valor o precio.

2º fase – Análisis del riesgo.

En esta fase se procederá al cálculo de criterios que posteriormente nos darán la evaluación del riesgo. El procedimiento consiste en:

1) Identificación de las variables específicas.
2) Análisis de los factores obtenidos de las variables y ver en qué medida influyen en el criterio considerado, cuantificando los resultados según la escala penta.

"F" Criterio de función.

Las consecuencias negativas o daños pueden alterar de forma diferente la actividad:

- Muy gravemente 5
- Gravemente 4
- Medianamente 3
- Levemente 2
- Muy levemente 1

"S" Criterio de sustitución.

Los bienes pueden ser sustituidos:

- Muy difícilmente 5
- Difícilmente 4
- Sin muchas dificultades 3
- Fácilmente 2
- Muy fácilmente 1

“P” Criterio de profundidad.

La perturbación y los efectos psicológicos que producirían serían de diferente graduación por sus efectos en la imagen.

- Perturbaciones muy graves. 5
- Perturbaciones graves 4
- Perturbaciones limitadas 3
- Perturbaciones leves. 2
- Perturbaciones muy leves 1

D.- “E” Criterio de extensión.

El alcance de los daños según su amplitud o extensión pueden ser:

- De alcance internacional. 5
- De carácter nacional. 4
- De carácter regional. 3
- De carácter local. 2
- De carácter individual. 1

E.- “A” Criterio de agresión.

La probabilidad de que el riesgo se manifieste es:

- Muy alta 5
- Alta 4
- Normal 3
- Baja 2
- Muy baja 1

F.- “F” Criterio de vulnerabilidad.

La probabilidad de que se produzcan daños es:

- Muy alta 5
- Alta 4
- Normal 3
- Baja 2
- Muy baja 1

3º fase – Evaluación del riesgo.

Tiene por objeto cuantificar el riesgo considerado. El procedimiento a seguir se compone de:

a) Cálculo del carácter del riesgo "C". Para ello recurriremos a los datos obtenidos en la anterior fase, aplicando: C = I + D

   I = Importancia del suceso = F x S
   D = Daños ocasionados = P x E

b) Cálculo de la probabilidad "Pb". Para lo cual recurriremos a los datos obtenidos en la segunda fase, aplicando: Pb = A x V

c) Cuantificación del riesgo considerado. Multiplicaremos los valores obtenidos en a) y b) : ER = C x Pb

4º fase – Cálculo de la clase de riesgo.

Esta clase tiene por objeto clasificar el riesgo en función del valor obtenido en la evolución del mismo. Dicho valor estará comprendido entre 2 y 1.250 y aplicando la Tabla Nº 1 tendremos:

Tabla Nº 2 Cálculo de la clase riesgo

Valor ER	Clase de riesgo
2 - 250	Muy reducido
251 - 500	Reducido
501 - 750	Normal
751 - 1.000	Elevado
1.001- 1.250	Muy elevado

Fuente: SANCHEZ, Manuel, "Seguridad en Entidades Bancarias"
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 3 Método "Mósler"

<table>
<tr><th colspan="5">MÉTODO MÓSLER</th></tr>
<tr><td rowspan="2">DEFINICIÓN DEL RIESGO</td><td>Objetivo</td><td>Elementos</td><td>Detalle</td><td>Clasificación de Riesgos</td></tr>
<tr><td rowspan="2">Identificación del riesgo delimitando su contenido y alcance para diferenciarlo de otros riesgos</td><td>BIEN</td><td>Persona o cosa valorada por sus cualidades o circunstancias</td><td rowspan="2"><u>Riesgos Empresariales</u>: Propios de la actividad
<u>Riesgos de Seguridad</u>: Extraños a la actividad</td></tr>
<tr><td>DAÑO</td><td>Definido por la causa</td></tr>
<tr><td rowspan="7">ANÁLISIS DEL RIESGO</td><td>Objetivo</td><td>Criterios</td><td>Detalles</td><td>Subcriterios</td></tr>
<tr><td rowspan="6">En esta fase se procederá al cálculo de criterios que posteriormente nos darán la evolución del riesgo</td><td>Función (F)</td><td>Consecuencias negativas que pueden afectar o alterar la actividad</td><td>1. Lo daños en la imagen de la entidad pueden afectar.
2. Los daños en las instalaciones.
3. Los daños en las personas (personal, usuarios) de la institución pueden afectar.</td></tr>
<tr><td>Sustitución (S)</td><td>Dificultades que pueden tenerse para sustituir o reponer los bienes o servicios</td><td>1. Lugar donde el bien a sustituir se puede encontrar?
2. Para la reposición de infraestructuras dañadas que debe realizarse?
3. Qué plazo tendrán los trabajos de sustitución?
4. Qué será necesario para los trabajos de sustitución?</td></tr>
<tr><td>Profundidad (P)</td><td>La perturbación y los efectos psicológicos que producirían serían de diferente graduación por sus efectos en la imagen</td><td>1. Qué perturbaciones pueden causar los daños de la imagen en el sector?
2. Qué perturbaciones pueden causar los daños de la imagen frente a sus clientes?
3. Qué perturbaciones pueden causar los daños de la imagen percibida por sus empleados?</td></tr>
<tr><td>Extensión (E)</td><td>Alcance de los daños o perdidas</td><td>1. El alcance de las repercusiones económicas.
2. El alcance de las repercusiones en la imagen de la entidad.</td></tr>
<tr><td>Agresión (A)</td><td>La probabilidad de que el riesgo se manifieste</td><td>1. Ubicación de la agencia o sede.
2. Delincuencia en la zona.
3. Presencia de Fuerzas y Cuerpos de Seguridad del Estado.
4. Qué vigilancia tenemos.</td></tr>
<tr><td>Vulnerabilidad (V)</td><td>La probabilidad de que se produzca daños</td><td>1. Protección perimetral.
2. Control de accesos para el personal y visitantes.
3. Circulación de personas.</td></tr>
</table>

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 4 Evaluación y cálculo “Mósler”

EVALUACIÓN DEL RIESGO	**Objetivo**	**Aspectos**	**Detalles**	
	Cuantificar el riesgo previamente definido y analizado en la instalación estratégica	Cálculo del carácter del riesgo. (C)	C= I+D	I= F*S D= P*E
		Cálculo de la probabilidad (Pb)	PB= A*V	
		Cuantificación del riesgo considerado (ER)	ER= C*Pb	
CÁLCULO DE LA CLASE DE RIESGO	**Objetivo**	**Valor entre**	**Clase de riesgo**	
	Clasificar el riesgo en función del valor obtenido en la evaluación	2 - 250	Muy reducido	
		251 - 500	Reducido	
		501 - 750	Normal	
		751 - 1.000	Elevado	
		1.001 - 1.250	Muy elevado	

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 5 Matriz de ejecución de Mósler

LOCACIÓN / INSTALACIÓN		**CNE**										
No.	Criterio Riesgo	Función	Sustitución	Importancia del Suceso	Profundidad	Extensión	Daños	Agresión	Vulnerabilidad	Probabilidad	Carácter del Riesgo	Cuantificación Riesgo	**Interpretación**
1													
2													

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 6 Valoración del Riesgo "Mósler"

VALORACIÓN	
2 a 250	**Muy Reducido**
251 a 500	**Reducido**
501 a 750	**Normal**
751 a 1.000	**Elevado**
1.001 a 1.250	**Muy Elevado**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

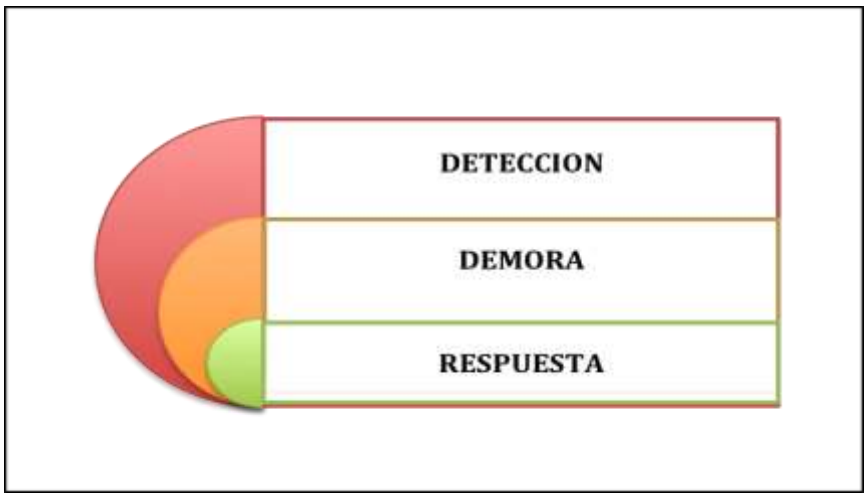
2.3.9. Seguridad física

La seguridad física se refiere a las medidas o conceptos diseñados para proteger al personal y bienes, prevenir el acceso físico o la entrada de personas no autorizadas a una instalación o área protegida, mediante la aplicación de barreras físicas y procedimientos de control, para defenderlos en contra de sabotaje, espionaje, daño y robo.

A medida que se abre el acceso a nuevas tecnologías, como la identificación biométrica, administración remota de datos de seguridad, reconocimiento facial por cámaras inteligentes; permiten rastrear la actividad humana dentro de las instalaciones y sus alrededores.

La seguridad física concibe tres funciones primarias (detección, demora y respuesta) y como secundaria la disuasión, para impedir que la posible amenaza se materialice.

Gráfico Nº 9 Funciones de Seguridad



Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Los medios o dispositivos de detección, son el primer medio de alerta que recibe el equipo de seguridad, su eficiencia y disponibilidad dentro del sistema de seguridad permite impedir el ingreso no autorizado neutralizando la amenaza.

Los medios o dispositivos de demora, son las barreras físicas naturales y artificiales que dispone una instalación con el fin de dificultar el acceso del adversario a su objetivo,

lo que dará tiempo al grupo de seguridad de respuesta en reaccionar y neutralizar la amenaza.

La respuesta es último momento que dispone un sistema de seguridad para evitar el éxito del adversario, del cual dependerá directamente de los anteriores medios para poder reaccionar en el tiempo suficiente. Nunca puede ser mayor el tiempo de respuesta que el tiempo que le lleva al adversario en cumplir con su propósito.

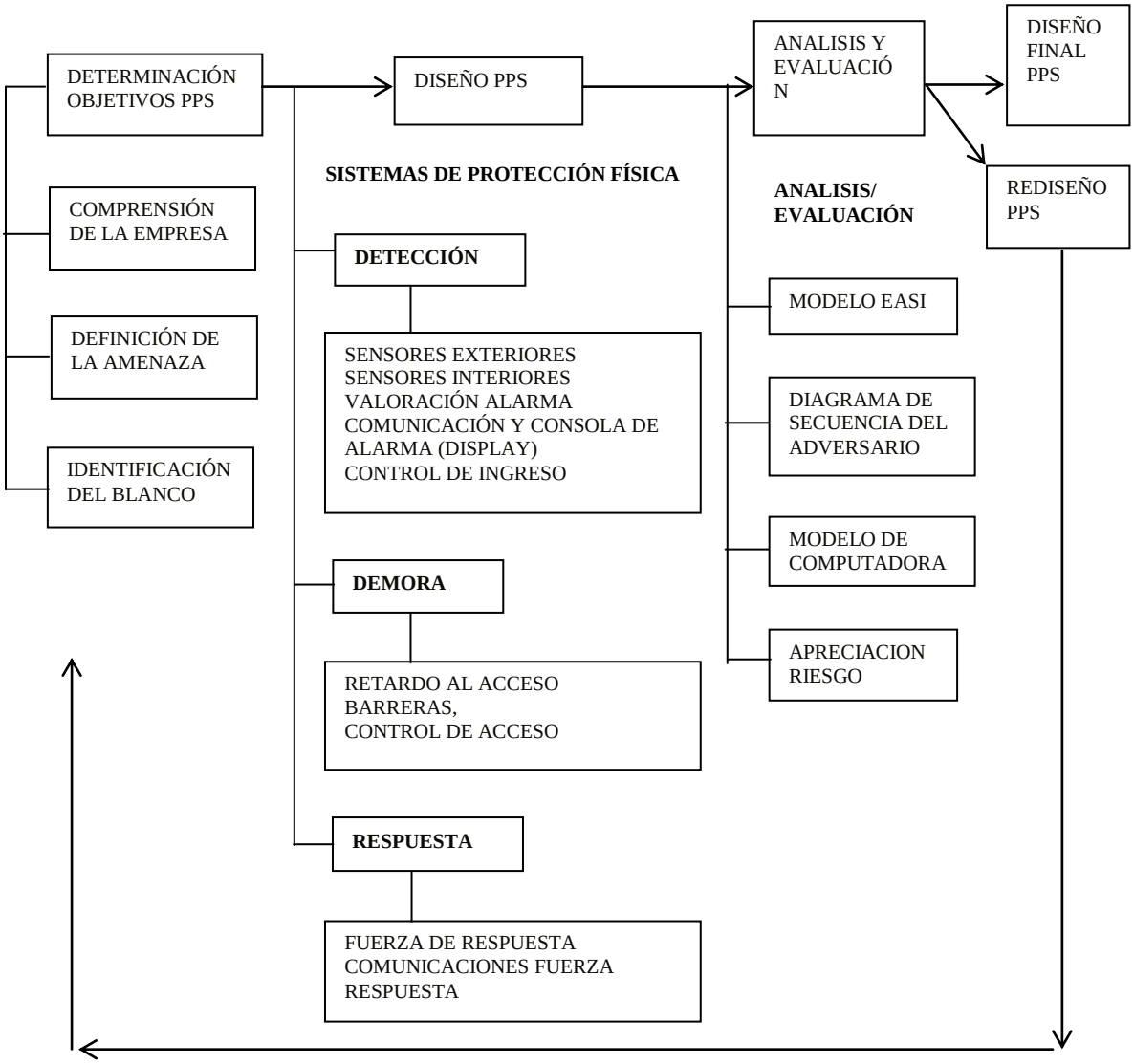
La disuasión, es una función secundaria que consiste en la aplicación de doctrina CPTED la Prevención del Crimen a Través del Diseño Ambiental , que se refiere a que la aplicación de criterios como vigilancia natural, territorialismo, control de acceso natural pueden lograr resultados iguales al endurecimiento con barreras, puertas y rejas y candados.

2.3.10. Programa de Seguridad Física

Un programa de Seguridad Física, no es más que el diseño y evaluación de un Sistema de Protección Física (PPS), que cumple con pasos ordenados basados en el ciclo de mejora continua de Deming, como cualquier otro programa, permite obtener como resultado final su diseño, sin embargo el PPS (*Physical Protection System),* nombre con el que se identifica al Sistema de Protección Física debe ser evaluado para determinar si efectivamente este alcanza con los objetivos de protección esperados, caso contrario este debe ser rediseñado, tomando en cuenta las debilidades encontradas.

> *El plan o programa de seguridad no puede ser efectivo si este no está basado en un claro entendimiento de los riesgos que está destinado a controlar (objetivos de protección). Hasta que no estén claramente evaluadas las amenazas (identificación de la amenaza) contra los activos (sujetos de riesgo), las contramedidas no pueden ser escogidas adecuadamente.* (Broder, 1999)

Gráfico Nº 10 Diseño de un programa de protección



Fuente: MARY LINN GARCÍA "THE DESIGN EVALUATION OF PHYSICAL PROTECTION SYSTEM"

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.10.1. Características de un sistema de protección física

Protección en profundidad

Es la existencia de varios anillos de protección que tendrá que vencer un adversario, para cumplir con su propósito. Esto permite que el adversario no conozca lo que el sistema puede hacer, requiriendo mucha más preparación antes de atacar al sistema (tiempo y

conocimiento); crea pasos adicionales donde un adversario puede fallar o abortar la misión. (Tiempo de detección, demora y respuesta).

Gráfico Nº 11 Protección en Profundidad

Elaborador por: Jorge Oswaldo Muñoz Rivadeneira

Mínima consecuencia por fallas de componentes

La complejidad del sistema obviamente aumenta la probabilidad de fallas, ya sean de orden físico, eléctrico o electrónico o humano, por ello hay que tener un plan para minimizar el tiempo en el cual el sistema no esté operando apropiadamente.

Protección balanceada

Esto significa que: "los elementos del PPS están iguales en cada fase de la facilidad."

Las superficies deben ser iguales en cuanto a nivel de protección:

- Paredes, pisos y techos.
- Puertas.
- Calefacción, ventilación o aire acondicionado.

2.3.10.2. Criterios de diseño.

El sistema debe poseer un criterio con el cual se debe comparar y calificar el funcionamiento del sistema completo.

Conceptos de diseño y objetivos.

Esta sección discute la integración de sensores individuales en un sistema de sensores perimetrales y considera la interacción del sistema perimetral o subsistemas con un sistema físico de protección integrado y balanceado.

Tabla Nº 7 Diseño y Objetivos

DISEÑO Y OBJETIVOS	
Línea continua de detección	Detección uniforme
Protección en profundidad	Múltiples líneas de detección
Sensores complementarios	Redundancia orden de verificación
Combinación de sensores	AND (Y) OR (O)
Zona clara	Mejorar el funcionamiento SES
Configuración del sensor	Aumentar Pd
Sistema específico al lugar	Ambiente físico
Protección del sistema e implementos del mismo	(TAMPER)
Método de prueba	Central de comunicaciones
Reconocimiento del patrón	Patrón de intruso

Fuente: Mary Lynn Garcia "Physical Protection System 2008"

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

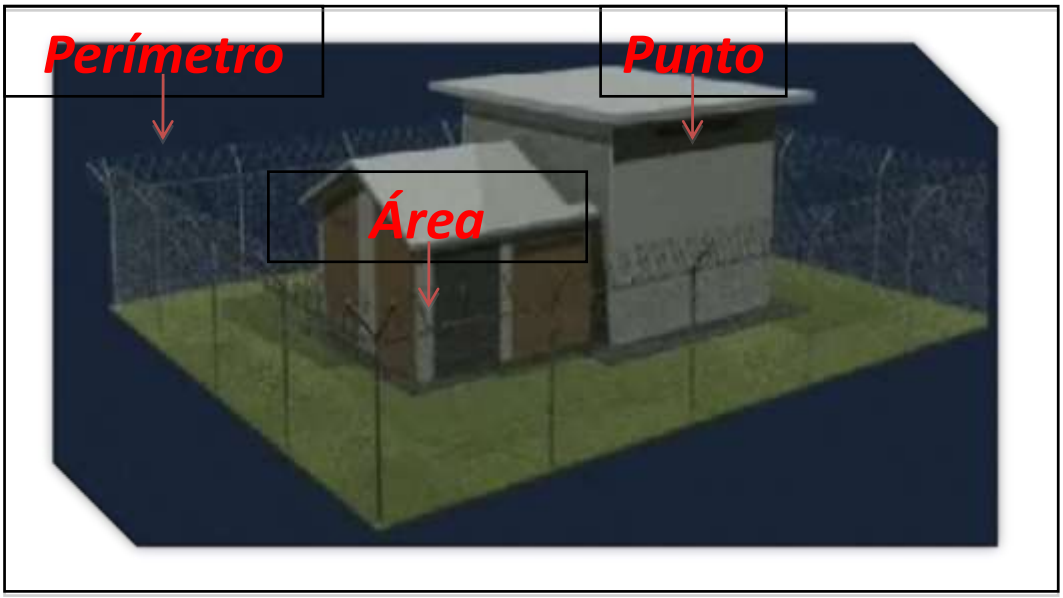
2.3.11. Teoría esférica de la seguridad

Otros autores en relación a la seguridad en profundidad mencionan que: La seguridad debe cubrir el espacio contenido en una esfera cuyo centro será el objetivo a proteger (persona, establecimiento u objeto); la zona a cubrir comprende todo el espacio

que existe por encima, por debajo y a los lados, en una profundidad suficiente para cubrir las necesidades de seguridad exigibles en cada caso.

La seguridad no puede preocuparse de un solo plano, debe tratar de cubrir las tres dimensiones de posibles agresiones (tejados terrazas de los edificios próximos, subsuelos), reconociendo la importancia del plano horizontal por ser el más asequible.

Gráfico Nº 12 Teoría esférica de la seguridad



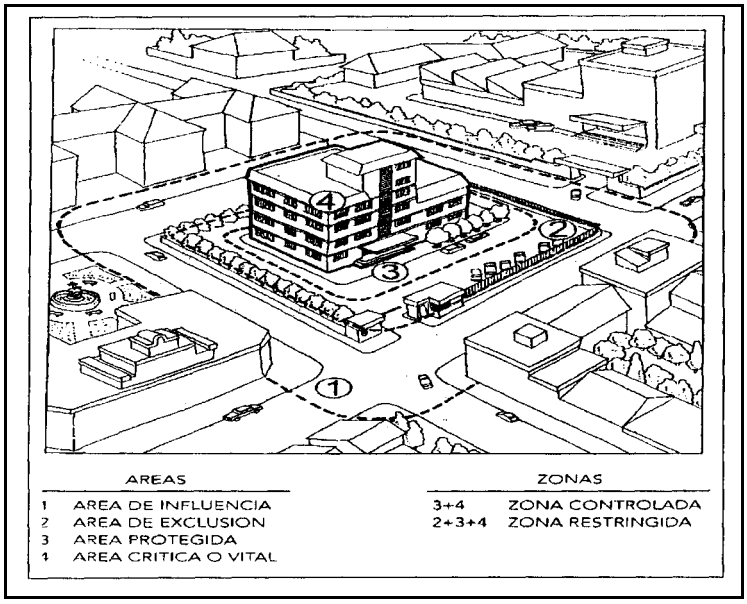
Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.12. Áreas y zonas de seguridad

Identifica las diferentes áreas que existen a través de círculos concéntricos, dentro de los cuales se reforzará las medidas de seguridad; alrededor de la persona, objeto, material o instalación que se desea proteger

> *A estos círculos se los denomina áreas o zonas de seguridad y se puede considerar las siguientes:* (CEAS)

Gráfico Nº 13 Áreas y zonas de seguridad



Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"

Tabla Nº 8 Concepto de áreas y zonas de seguridad

ÁREAS / ZONA	CONCEPTO
ÁREA DE INFLUENCIA	Espacio exterior al área de exclusión, donde existe la factibilidad de realizarse acciones en contra la integridad del área protegida
ÁREA DE EXCLUSIÓN	Espacio exterior al área Protegida, de utilización restringida o acceso limitado.
ÁREA PROTEGIDA	Espacio limitado por barreras físicas y de acceso limitado, se ejerce cierto control sobre los movimientos y permanencia
ÁREA CRITICA O VITAL	Espacio limitado por barreras físicas y de acceso limitado e interior al Área Protegida, cuyo acceso y permanencia son objeto de especiales medidas de control: El movimiento es estrictamente controlado.
ZONA CONTROLADA	Esta zona comprende las áreas Protegida y critica o Vital, aquí se extreman las medidas de seguridad.
ZONA RESTRINGIDA	Esta zona comprende las áreas Protegida, de Influencia y de Exclusión, en esta zona el acceso está sujeto a restricciones específicas o a acciones de control por razones de seguridad de personas o bienes.

Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

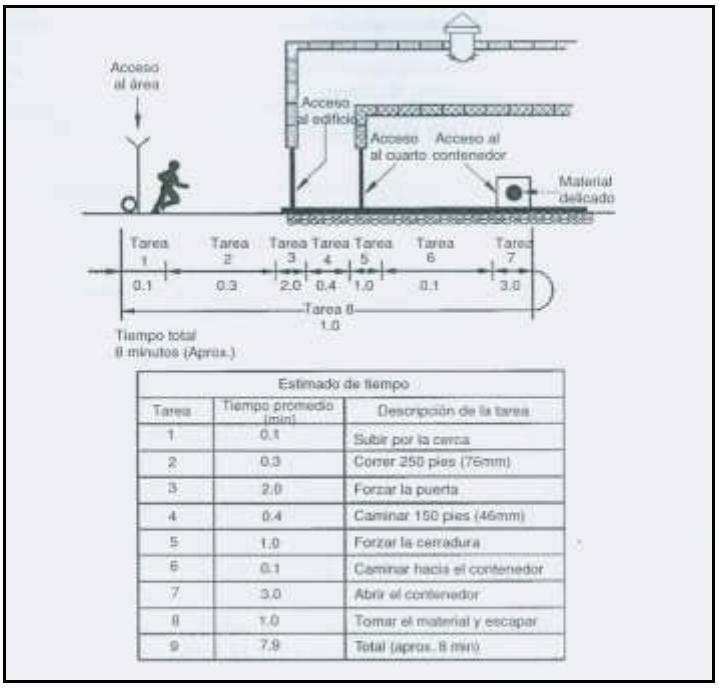
2.3.13. Diagrama de secuencia del adversario

La persona que realiza con intención e interés actos malévolos con el fin de causar daño o prejuicio, se le considera un adversario el mismo que puede ser interno o externo, los diagramas de secuencia de adversario es una herramienta útil que ayuda a determinar el tiempo que requiere un adversario para traspasar la seguridad implementada.

Conocer el tiempo que requiere el adversario para vulnerar los controles o medidas puede ayudarle a complementar más medidas para impedir, demorar y detener al intruso.

La acción específica, que debe ejecutar el adversario a lo largo del camino para cumplir con su propósito de romper los mecanismos de seguridad implementados, se le conoce como tarea del adversario y al conjunto de estas acciones ordenadas contra un blanco que, si es completado, resulta en el éxito de robo o sabotaje es conocido como el camino del adversario.

Gráfico Nº 14 Diagrama de secuencia del adversario



Estimado de tiempo		
Tarea	Tiempo promedio (min)	Descripción de la tarea
1	0.1	Subir por la cerca
2	0.3	Correr 250 pies (76mm)
3	2.0	Forzar la puerta
4	0.4	Caminar 150 pies (46mm)
5	1.0	Forzar la cerradura
6	0.1	Caminar hacia el contenedor
7	3.0	Abrir el contenedor
8	1.0	Tomar el material y escapar
9	7.9	Total (apros. 8 min)

Fuente: Certificación PSP, “Guía de Estudio”, David G. Patterson, CPP, PSP

2.3.14. Los medios o dispositivos técnicos de seguridad

Los dispositivos técnicos de seguridad se dividen en medidas pasivas (medios físicos) o activas (medios electrónicos), capaces de detectar un evento o suceso extraño dentro de su campo de visión o detección, y producir una alarma que permita adoptar contramedidas oportunas en un mínimo de tiempo.

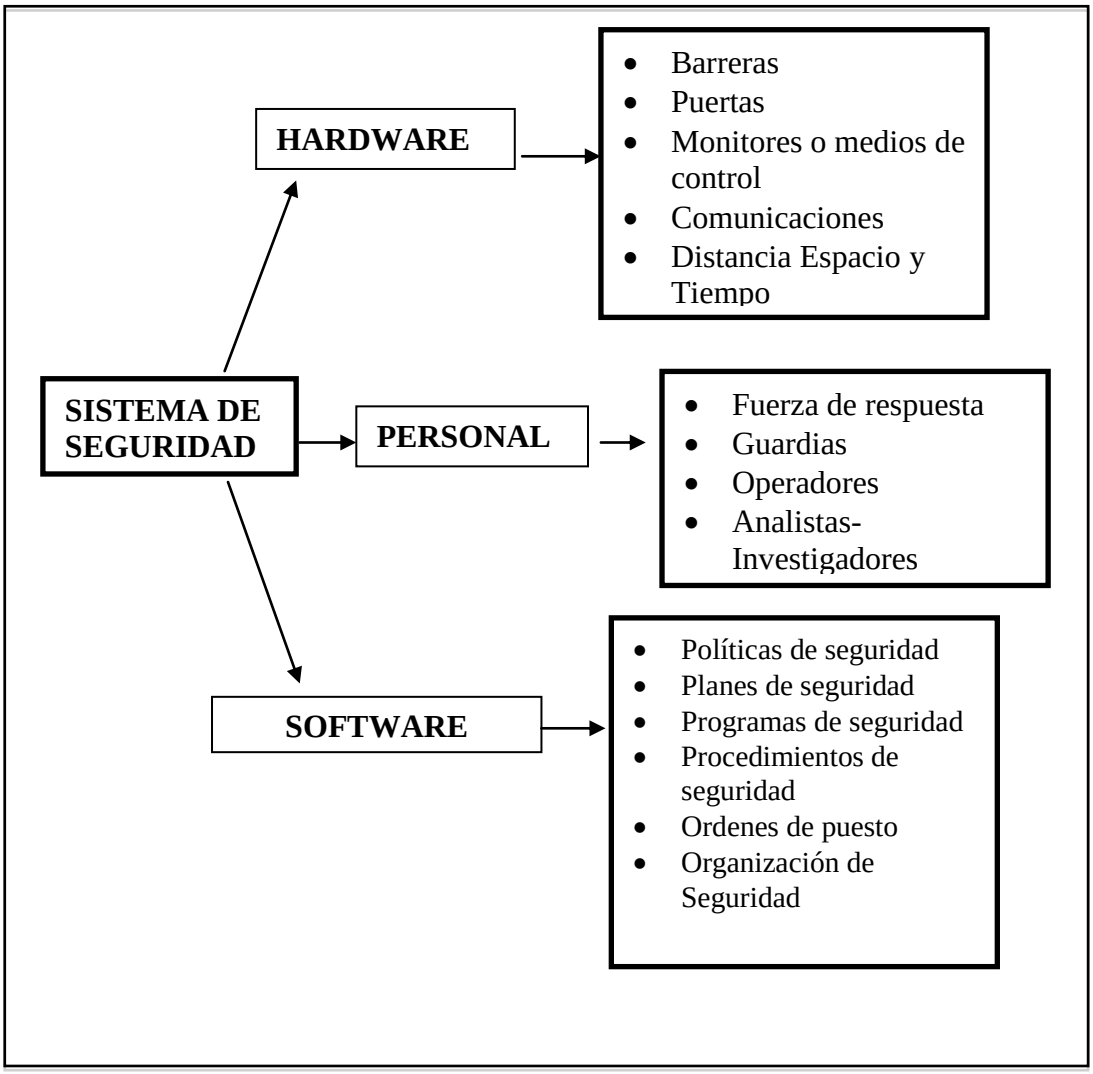
> *Todos los medios o dispositivos que componen un sistema de seguridad integral se interrelacionan e interactúan de forma complementaria con el objetivo dependen mutuamente de tal manera que la eficacia depende de la coordinación y ajuste entre los medios. Un buen sistema debe ser al mismo tiempo defensivo y ofensivo (CEAS).*

Tabla Nº 9 Función de los medios técnicos de seguridad

MISIÓN DEFENSIVA	MISIÓN OFENSIVA
Detectar cualquier intento de agresión Intrusismo peligro real	Proporcionar una garantía máxima y un tiempo mínimo de reacción ante el peligro
Detener y obstaculizar los daños causados por la fuente de peligro	Facilitar una investigación inmediata
Identificar y localizar el peligro para poder actuar en consecuencia.	Neutralizar rápidamente todo intento de agresión intrusión y peligro real.

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 15 Componentes que integran el sistema de seguridad



Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.14.1. Eficacia de un dispositivo de seguridad

Tiempo de demora: Es el que transcurre desde la manifestación de la alarma y esta es evaluada por el operador y comunicada a la fuerza de respuesta, hasta que el intruso alcanza su objetivo en el interior del área controlada.

Tiempo de respuesta: Espacio de tiempo disponible, para que la fuerza que debe reaccionar intercepte al intruso; comprende desde que los censores se activan hasta la neutralización de la amenaza. Un sistema de seguridad es más eficaz cuando el tiempo de demora es mayor que el tiempo de respuesta.

2.3.14.2. Estilo de un dispositivo de seguridad

Estilo Encubierto: La mayoría de medidas de seguridad están ocultas para garantizar su inviolabilidad, o por no dar a conocer el real valor de los bienes en custodia.

Estilo Disuasivo (Aurea de Seguridad): Con este estilo lo que se pretende es la disuasión, considerando que se desconoce el valor real de lo que se custodia, la imagen de seguridad queda deteriorada y potenciada (evaluada).

Estilo mixto: Por lo general se utiliza un sistema de seguridad mixto que reúna elementos de ambos, con el fin de no descubrir todas las medidas de seguridad y mantener un aceptable nivel de protección.

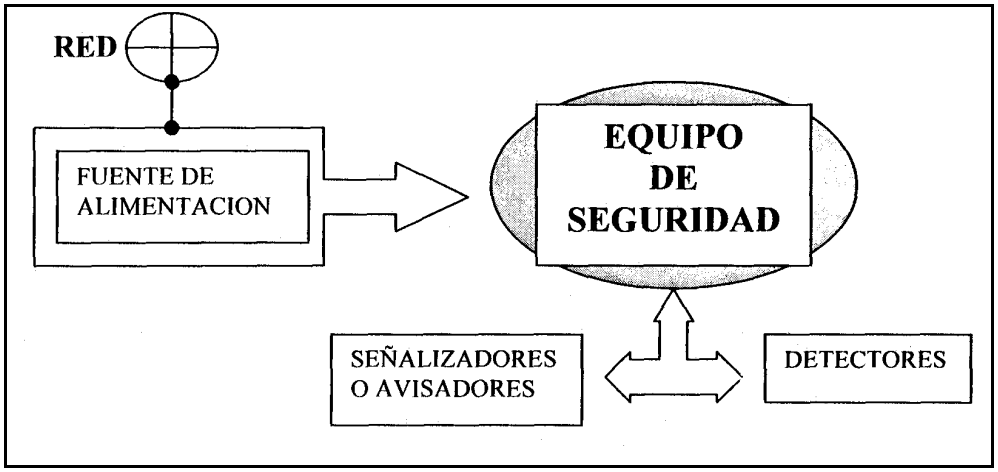
2.3.15. Medios técnicos activos (seguridad electrónica).

> *La función de los medios activos es la de alertar local o remotamente de un intento de violación o sabotaje de las medidas de seguridad física establecidas el conjunto de medios activos constituye lo que se denomina seguridad electrónica sus funciones principales son* (CEAS)*:*

- Detección de intrusos en el interior y en el exterior.
- Control de accesos y tráfico de personas, correspondencia y vehículos.
- Vigilancia óptica por fotografía o circuito cerrado de televisión.
- Intercomunicación por megafonía.
- Protección de las comunicaciones.

Un sistema electrónico de seguridad está formado por el conjunto de elementos electromecánicos y/o electrónicos relacionados entre sí, que a través de la información que nos proporcionan, permiten mantener un nivel de seguridad determinado, en nuestro entorno. De manera esquemática, un sistema electrónico de seguridad consta de los siguientes elementos:

Gráfico Nº 16 Elementos de un sistema electrónico de seguridad



Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"

Los detectores son dispositivos colocados tanto en el exterior como en el interior de una instalación con el fin de proteger los activos críticos de mayor importancia, su objetivo informar a la central de las variaciones del estado ambiental de la zona que están protegiendo, indicando, por tanto, la intrusión de personas en dichos objetivos.

> *Los señalizadores o avisadores permiten conocer adecuadamente lo que está sucediendo y donde está sucediendo, el evento detectado con el fin de reaccionar con oportunidad y eficacia.* (CEAS)

Tabla Nº 10 Sistemas de detección de intrusos

PUNTUALES	**Piezoeléctricos:** vibradores colocados sobre cristales o paredes y denuncian cuando tratan de romperlos **Rotura:** laminas o cintas parecidos al papel, que si se rasgan provocan una alarma **Presión :** dispositivos para ubicar debajo de las alfombras, dan alarma cuando alguien pisa
PERÍMETROS	Protegen todos los puntos exteriores de una área, generalmente se emplea para grandes extensiones de terreno, para ello existen equipos de "electrificación" de las verjas de estos contornos y que nos avisan si algún intruso trata de trepar por la valla "invisible" a base de haces de rayos infrarrojos o de microondas.
VOLUMÉTRICAS	Sistema de detección puntual que direcciona rayos imperceptibles a la vista del hombre en el área donde se ubica el activo a proteger, de suerte que si algún intruso penetra en la zona de su alcance es automáticamente detectado por las perturbaciones que origina dicho movimiento en las condiciones ambientales del volumen protegido.

Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.15.1. Subsistema de Circuito Cerrado de Televisión.

Un subsistema de CCTV, para el caso de la vigilancia, proporciona un elemento eficaz para complementar las patrullas de guardia.

El CCTV es un subsistema de evaluación que apropiadamente integrado proporciona un método rápido y efectivo para determinar la intrusión y causa de las alarmas.

Configuración de un subsistema de CCTV.

Las cámaras de CCTV deberán localizarse en:

- En exteriores, a lo largo de las zonas de aislamiento perimetral del sitio.
- En exteriores, en puntos de acceso controlado (puertas de ingreso).
- En interiores, dentro del área protegida, y el área de visión cercana a los activos protegidos.
- En interiores, en activos escogidos dentro del área protegida.

Tipos de cámaras:

- Cámaras regulares
- Cámaras tipo domo
- Escáner
- Domos y PTZ
- Cámaras megapíxeles
- Cámaras infrarrojas
- Cámaras térmica

Gráfico Nº 17 Tipos de cámaras seguridad

Fuente: Presentación del Sistema de Protección Física, ASIS 231 Ecuador

2.3.15.2. Sistemas de Detección de Incendios.

Los sistemas detectores de incendio son herramientas que permiten dar la alarma oportuna cuando un incendio se encuentra en su fase inicial, dentro de una instalación.

Los sistemas de detección de incendios se clasifican en:

- Detectores de Humo
- Detectores de Llama
- Detectores de Temperatura

Tabla Nº 11 Tipos detectores de humo

FOTOELÉCTRICO	IÓNICO	DE GASES
		

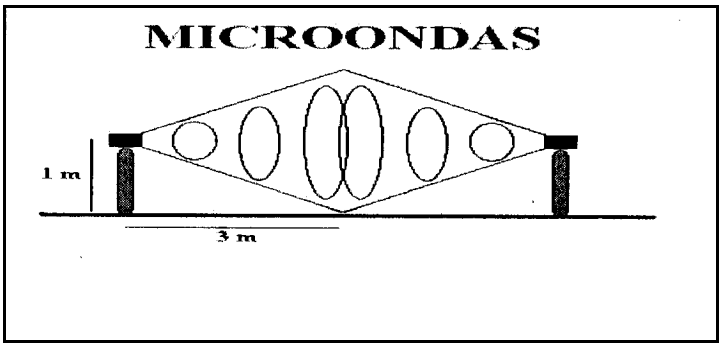
Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD “CEAS - ECUADOR”

2.3.15.3. Sistema de Detección Perimetral

Banda de microondas

Están constituidas por dos equipos emisor y receptor montados en oposición, que al atravesar un cuerpo total o parcialmente el haz de microondas generado por el emisor produce una atenuación de la señal captada por el receptor, la que convenientemente evaluada por el sistema provoca la alarma.

Gráfico Nº 18 Banda de microondas



Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"

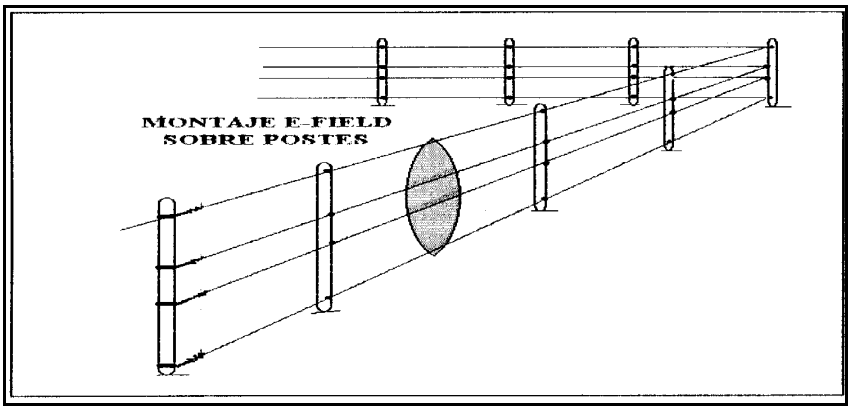
Barrera de infrarrojos

Rayo generadas de tipo infrarrojo, capaces de cubrir distancias entre 60 y 120 metros, 1.80 metros de alto y 20 centímetros de ancho Su principal ventaja estriba en la reducida sección de haz que emite, lo que permite su utilización en instalaciones en las que las zonas de detección resultaran insuficientes para un sistema de microondas.

Campo eléctrico

Este procedimiento (también llamado de detectores capacitivos), consiste en instalar hilos conductores a lo largo del perímetro capaz de generar un campo electrostático. En este sistema el cable es utilizado como sensor y basta la aproximación de un intruso para activar la alarma, Su principal ventaja es que puede instalarse en perímetros irregulares.

Gráfico Nº 19 Campo eléctrico en el perímetro



Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD “CEAS - ECUADOR”

Contactos de tensión

Este procedimiento prevé el empleo de un determinado número alambres de acero, tendidos a distinta altura a lo largo del perímetro, sometiéndolos a tensión por tracción. Cada tramo de alambre incorpora un sensor capaz de captar cualquier vibración brusca de la tensión a la que está sometido.

Tabla Nº 12 Equipos de seguridad activa

SISTEMAS DE PROTECCIÓN ACTIVO Son aquellos materiales, equipos y sistemas de seguridad electrónicos e informáticos que se emplean en la protección y prevención de riesgos en instalaciones estratégicas					
	MATERIALES Y EQUIPOS DE PROTECCIÓN	**CONCEPTO**	**APLICACIÓN**	**TIPOS**	**DETALLES**
PROTECCIÓN CONTRA ACTOS ANTISOCIALES	**Equipos de control e identificación de personas**	Sirven para identificar y controlar a personas no autorizadas	Protección de recintos y zonas de acceso restringido	Autónomo Centralizado	Parámetros de selección
	Detección de interior	Dispositivos que alertan sobre irregularidades	Protección frente a la intrusión	Puntuales Lineales Superficiales Volumétricos	Como: Contactos magnéticos Rayos infrarrojos Barreras de Rayos infrarrojos Microondas
	Centrales de señalización y control	Equipos electrónicos	Sistema electrónico de seguridad	Según su aplicación Según su tecnología	Características técnicas
	Vigilancia con CCTV	Vigilancia remota	Componentes: Cámaras; monitores; ópticas; equipos de control y de computación; equipos auxiliares de monitoreo; video sensores; equipos de registro de imagen.		Parámetros de selección
	Pulsadores de emergencia anti atraco	Dispositivos discretos	Usados en lugares ocultos	**TIPOS** De accionamiento manual, puntual, a presión o de pinza	
	Detección de armas y explosivos	Detección de metales y rayos X	Para identificar armas o explosivos	**TIPOS** Portátiles; por paso; fijos	
	Detección de moneda falsa	Dispositivos de tipo luz ultravioleta	Comprobar efectividad del dinero	**VERIFICAN** Marcas de agua; hilos de seguridad, fibras, papel exento de blanqueado, leyendas e imágenes.	
	Equipos de retardo y bloqueo	Dispositivos que temporizan la apertura de cerraduras	Usados en cajas fuertes, bóvedas, cajeros, etc.	**CONSIDERACIONES** Bloqueo y retardo de apertura Regulación del retardo y bloqueo, etc.	

<table>
<tr><td colspan="6"><u>SISTEMAS DE PROTECCIÓN ACTIVO</u>
Son aquellos materiales, equipos y sistemas de seguridad electrónicos e informáticos que se emplean en la protección y prevención de riesgos en instalaciones estratégicas</td></tr>
<tr><td rowspan="5">PROTECCIÓN CONTRA INCENDIOS</td><td>MATERIALES Y EQUIPOS DE PROTECCIÓN</td><td>CONCEPTO</td><td>APLICACIÓN</td><td>TIPOS</td><td>DETALLE</td></tr>
<tr><td rowspan="3">Sistemas de Detección</td><td rowspan="3">Sistemas instalados para responder ante el inicio de un incendio</td><td rowspan="3">Convencionales
Direccionales
Identificables
Analógicos</td><td colspan="2">Características técnicas generales
Equipos que reciben señales;
Equipos de control</td></tr>
<tr><td>Detectores de incendio</td><td>TIPOS
De humo; por ionización, por temperatura; térmicos; llamas; gases.</td></tr>
<tr><td>Central de Incendio</td><td>CARACTERÍSTICAS TÉCNICAS
Transmitir y activar alarmas y alertas; controlar señales de entrada y salida.</td></tr>
<tr><td>Pulsadores con alarma</td><td>Dispositivos que provocan alarma y transmiten señales de alerta</td><td colspan="3">CARACTERÍSTICAS
El pulsador deberá ser colocado cerca
Existe conexión directa con la central de incendios</td></tr>
<tr><td>Sistemas de extinción automática</td><td>Dispositivos que detectan y extinguen un incendio</td><td>INCLUYEN
Sistema de alarma y alerta inmediata</td><td colspan="2">CARACTERÍSTICAS TÉCNICAS
Clasificación, aplicación, uso, especificaciones, suministros, condiciones de los equipos, parámetros de diseño del sistema, certificación.</td></tr>
<tr><td rowspan="2">SISTEMAS DE CONTROL DE EMERGENCIAS</td><td>Sistemas de control de rondas</td><td>Dispositivos para verificar el paso obligado por un punto determinado</td><td>PARÁMETROS DE SELECCIÓN
Determinar rutas, número de lectores, horarios</td><td colspan="2">CARACTERÍSTICAS TÉCNICAS
Equipos portátiles,
Equipos terminales
Unidad central</td></tr>
<tr><td>Sistemas busca personas</td><td>Dispositivos receptores de mensajes vía radio para casos de emergencia</td><td colspan="3">CARACTERÍSTICAS TÉCNICAS
Transmitir incidencia exacta en el caso de requerirlo
Confirmación de regreso ha estado de calma.</td></tr>
</table>

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 13 Clasificación de dispositivos por su utilización

Detección (sensores)	**a) Interior:** (detectores de movimiento) **b) Perimetral:** (sensores magnéticos de apertura, detectores de rotura de vidrios, barreras infrarrojas). **PROTECCIÓN IDEAL = a + b**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.16. Medios Técnicos Pasivos (Seguridad Física)

Los medios técnicos pasivos o físicos, tienen como función básica disuadir, detener o al menos, retardar la progresión de la amenaza.

El conjunto de los medios pasivos, constituye lo que se denomina seguridad física, la misma que está constituida por (CEAS):

- Elementos de carácter estático y permanente, es el primer obstáculo que se presenta a la penetración de los intrusos formando lo que conocemos como protección perimetral.(vallas, cercados, setos)
- Otros elementos también estáticos, que impiden el acceso al propio edificio principal o núcleo de la seguridad, formando lo que denominaremos protección periférica (puertas, rejas, cristales)
- Para la protección focalizada del bien, que la constituyen los recintos o habitáculos cerrados (cajas fuertes, cámaras acorazadas)

Tabla Nº 14 Protección perimetral

ELEMENTOS	DETALLE
Mampostería	Cerramientos realizados con materiales de albañilería.
Metal	Cerramientos realizados mediante cercas metálicas: alambradas acordadas en la parte superior, concertinas de alambre dentado.
Otros	De diversos tipos atendiendo a la topografía del terreno con obstáculos naturales y/o artificiales, así como la vegetación natural o implantada para dificultar el paso.

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.16.1. Protección Periférica

- Puertas blindadas, instaladas en los puntos principales de acceso al edificio o establecimiento.
- Instalación de sistemas de esclusas en dichos puntos de acceso, de forma que no se pueda acceder directamente al interior.
- Cristales blindados en ventanas, al menos en aquellos despachos sujetos a un riesgo especial, y de nivel que se considere conveniente.
- Rejillas y emparrillados protectores en huecos necesitados de ventilación.

2.3.16.2. Protección del Bien

- Cámaras acorazadas, construidas conforme a especialidades reguladas reglamentariamente. Disponen de un acceso que puede estar temporizado.
- Cajas fuertes.

2.3.16.3. Fiabilidad de un sistema de protección

Es el grado de confianza que otorga un sistema de protección en el cumplimiento de una misión.

Parámetros:

- Seguridad de reacción
- Porcentajes de falsas alarmas
- Vulnerabilidad al sabotaje

2.3.17. Seguridad de la información

El manejo de los riesgos en contra de la información es una de las responsabilidades de cada Gerente de Seguridad.

Todo programa de Seguridad de IT, debe contemplar dos procesos fundamentales:

- Identificación de riesgos y activos a proteger.
- Control y neutralización de riesgos.

Dentro del proceso de seguridad de la información intervienen tres grandes comunidades (Chavez , 2013)*:*

1. Grupo de Seguridad de Información.

Miembros que entienden mejor las amenazas y los ataques que pueden producir riesgos, encargados de identificar y crear barreras de protección.

2. Grupo de la Información Tecnológica.

Encargados de construir los sistemas de seguridad necesarios para asegurar una operación confiable, que permita desarrollar un adecuado procedimiento de respaldo de la información, para controlar el riesgo de fallas en discos duros.

3. Administradores y usuarios del sistema.

El conocimiento y entrenamiento adecuado, permite mantenerlos alejados de los riesgos identificados por la organización, este grupo toma parte en los procesos de detección temprana y respuesta.

La identificación de activos informáticos de la organización, por su utilidad, importancia, es un proceso debe ser realizado para identificar las debilidades y amenazas que se pueden presentar.

Tabla Nº 15 Componentes en la seguridad de la información

Componentes del Sistema IT	Componentes del Manejo de Riesgos	
Personas	Personas dentro de la organización	• Empleados de confianza • Otro personal
Procedimientos	Procedimientos	• Procedimientos estándar de negocios y de IT. • Procedimientos sensitivos de negocios y de IT
Datos	Datos/ Información	• Transmisión • Procesamiento • Almacenamiento
Software	Software	• Aplicaciones • Sistemas operativos • Componentes de seguridad
Hardware	Hardware	• Sistemas y periféricos • Componentes de seguridad
Redes	Componente de la Red	• Componentes de Intranet • Componente de Internet

Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.17.1.Modelo de Clasificación de la Información.

Los esquemas parar clasificar la información son diferentes y se ajustan de acuerdo al criterio y necesidad particular de cada organización.

Información Confidencial.

Constituida por aquella que necesita ser controlada cuidadosamente inclusive dentro de la empresa. El acceso a estos activos de información está restringido bajo la norma de "LA NECESIDAD DEL SABER" o bajo requerimientos estrictamente contractuales. La información que ingrese en esta clasificación puede llamarse también información propietaria o sensible.

Información Interna.

Toda aquella información interna que no encaje en los parámetros de información confidencial. A estos activos solo pueden tener acceso los empleados de la organización, contratantes autorizados y terceras personas muy específicas.

Información Externa.

Todos los activos de información que hayan sido autorizados por la gerencia general de dominio público.

> *Esta clasificación debe ser revisada por lo menos una vez al año para asegurar que su información se encuentre correctamente clasificada y que los controles apropiados se encuentren implementados* (Chavez , 2013).

Manejo de la información clasificada.

El manejo de los activos de información, debe incluir consideraciones sobre almacenamiento, distribución, portabilidad y destrucción. Todo activo deberá estar claramente identificado como clasificado o desclasificado.

2.3.17.2. Identificación de amenazas a la seguridad de la información.

La adecuada clasificación de los activos de información, permiten determinar las debilidades potenciales que presentan cada uno de ellos y las amenazas que podrían incidir sobre estas.

Tabla Nº 16 Amenazas para la seguridad de la información

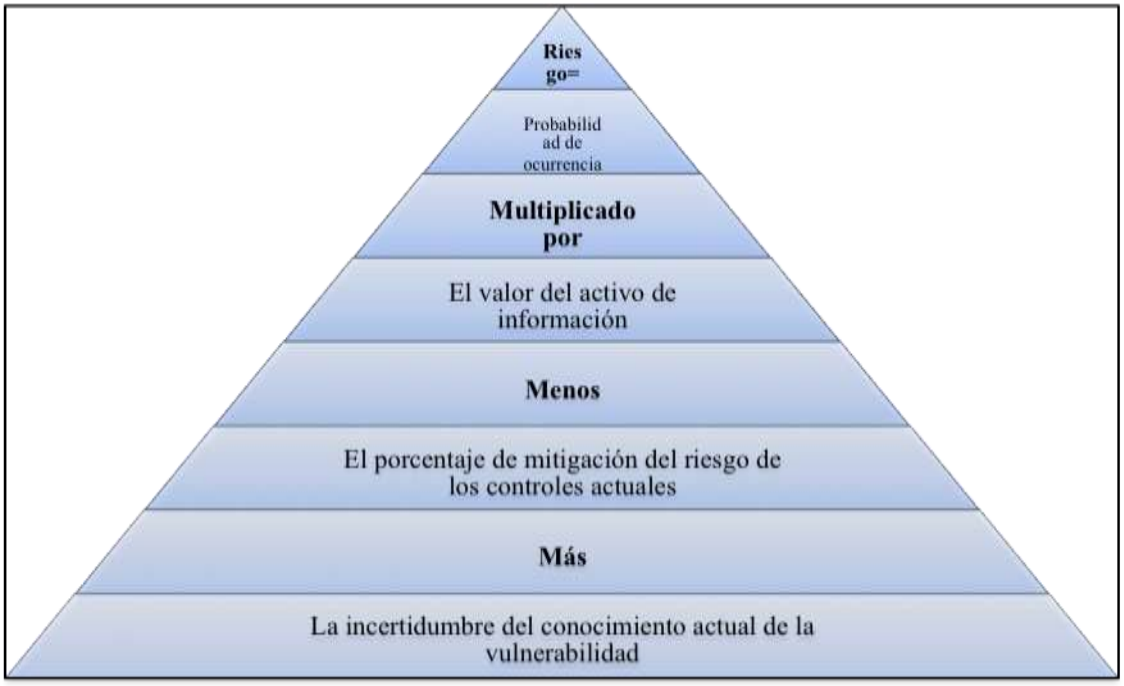
Tipos de amenazas	Ejemplos
Actos de errores o fallas humanas	Accidentes, errores de empleados
Comprometimiento de la propiedad intelectual	Piratería, infracciones a los derechos de autor
Actos deliberados de espionaje	Accesos no autorizados
Actos deliberados de extorsión de información	Accesos a correos electrónicos
Actos deliberados de vandalismo o sabotaje	Destrucción de sistemas o información
Actos deliberados de robo	Confiscación ilegal de equipos o información
Actos deliberados de ataque al software	Virus
Fuerza de la naturaleza	Fuego, terremotos, relámpagos
Calidad de los servicios de proveedores	Potencia y calidad de servicios de internet, comunicaciones, transmisión de datos, etcétera.
Fallas técnicas en el hardware.	Fallas en el equipo
Fallas técnicas en el software o errores	Bugs, problemas de códigos
Tecnología obsoleta	Tecnología no actualizada o adecuada

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

2.3.17.3. Especificación del riesgo informático.

La determinación del riesgo asigna valor a cada vulnerabilidad, que permite relacionar el riesgo relativo con cada activo vulnerable y facilita la creación posterior de ratings comparativos en el proceso de control de riesgos.

Gráfico Nº 20 Ecuación del Riesgo de la información



Fuente: Presentación del Sistema de Protección Física ASIS 231 Ecuador

2.3.17.4. Seguridad Informática.

En el mundo actual el principal activo de las organizaciones es la información, la mayor parte de las organizaciones se encuentran conectadas a Internet y hacen de esta herramienta una de las más importantes para acceder a información, comunicarse, enviar y recibir información; facilitando la comunicación interna y externa.

El intercambio de información a través del internet, trae consigo una serie de problemas, que si no se detectan y se resuelven de una manera eficaz y proactiva pueden generar un caos.

Uno de los problemas de la seguridad de la información, es garantizar su confidencialidad, integridad y disponibilidad. Cada vez son más sofisticadas las formas en que los diferentes tipos de intrusos realizan ataques para hacer espionaje, sustraer y/o alterar información. Es por esto la importancia de contar con una adecuada estrategia de seguridad que les permita proteger adecuadamente su información, identificar sus vulnerabilidades y detectar e impedir proactivamente intentos de ataques a sus sistemas de información.

2.3.17.5. Seguridad en la Infraestructura Tecnológica.

Comprende el diseño de la red segura y las tecnologías necesarias para poder identificar vulnerabilidades en la red, minimizar los riesgos potenciales y detectar y prevenir ataques en la red realizadas por intrusos internos y/o externos y cubre los siguientes ítems:

- Topología general de la red.
- Conexiones externas y tipo de acceso a la infraestructura tecnológica de la Organización.
- Control de Acceso.
- Identificación y Autenticación.
- Disponibilidad.
- Confidencialidad.
- Recuperación en caso de Desastre.
- Integridad de la Información.
- Certificación de la Información.
- Seguridad física.

Seguridad en los Procesos, Administración de la Seguridad y Gestión del Riesgo**:**

Comprende la revisión del flujo de la información, entendiendo como la información entra y sale de los procesos de la organización.

Los ítems que se evalúan son:

- Medidas de clasificación y control, que busca mantener una apropiada protección a los bienes de la organización.

Flujo de información y clasificación a nivel de:

- Reportes.
- Medios magnéticos.
- Mensajería electrónica.
- Transferencia de archivos.

Seguridad del personal, que incluye ítems relacionados con la reducción del riesgo generado por error humano, robo, fraude o mal uso.

- Responsabilidad en seguridad con el cargo.
- Acuerdos de confidencialidad.
- Filtrado de personal.
- Entrenamiento a usuarios.
- Procesos disciplinarios.

Desarrollo y Mantenimiento está orientado a verificar la inclusión de la seguridad en el desarrollo de aplicativos:

- Requerimientos de seguridad en sistemas.
- Requerimientos de seguridad en aplicaciones.
- Seguridad en sistemas de archivos.
- Seguridad en procesos de desarrollo y soporte.

Comunicación y operación que busca asegurar el correcto y seguro uso de operación del procesamiento de información.

- Procesos de operación.
- Procesos para manejo de incidentes.
- Segregación de funciones.
- Planeación y aceptación de sistemas.
- Protección de código malicioso.
- Manejo de Logs.

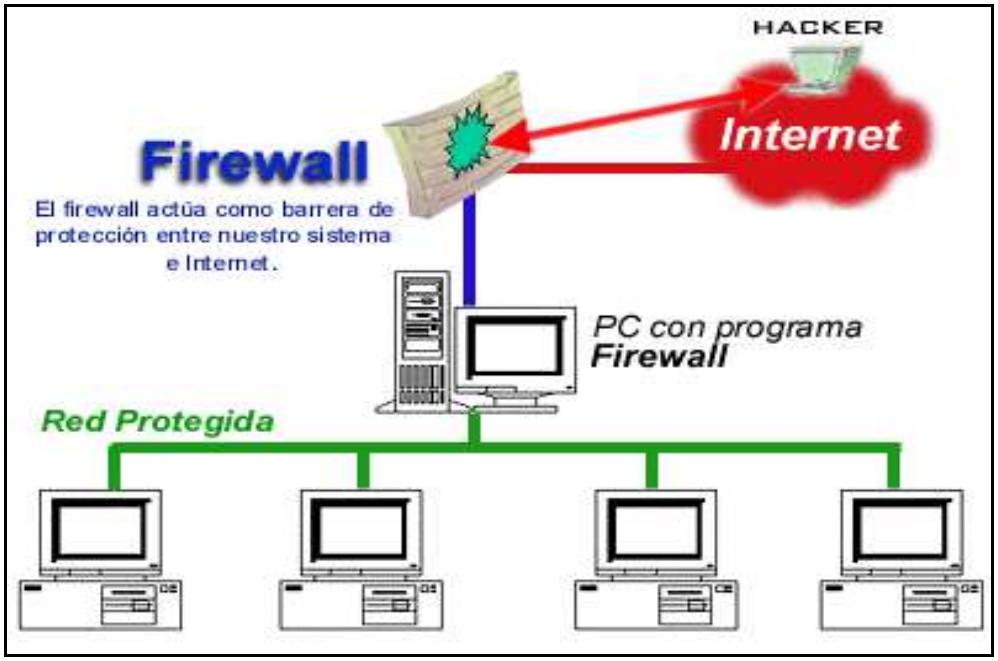
Concientización y cultura organizacional en el tema de seguridad informática:

Consiste en el desarrollo de un programa de culturización y concientización, que permitirá integrar a los administradores directos e indirectos de la información con el fin de dar un estricto cumplimiento de las políticas de seguridad.

Firewall

Herramienta de seguridad, que impide que ciertos comandos o paquetes de datos anormales penetren en nuestro sistema. Comúnmente son traducidos como barreras de fuego, que detectan ataques o entradas forzadas en los puertos de nuestro sistema.

Gráfico Nº 21 Función del Firewall



Fuente: CORPORACIÓN EUROAMERICANA DE SEGURIDAD "CEAS - ECUADOR"

Los Firewalls o muros de fuego, son la solución para tapar el agujero de esta segunda puerta. Este programa puede identificar quien solicita el servicio de nuestro ordenador además e impedir que entren datos a nuestro ordenador. Estos firewalls pueden reconocer comandos dañinos o peligrosos para nuestro terminal.

2.3.18. Seguridad Ciudadana.

El proceso de consolidación de los sistemas democráticos construyen consensos y alianzas estratégicas, tanto la sociedad civil como las organizaciones del estado que trabajan y comprometen esfuerzos en la construcción de un marco de convivencia que permita el desarrollo individual y colectivo de los ciudadanos y ciudadanas.

Los problemas de seguridad ciudadana, orden público, narcotráfico, daño ecológico, violencia, etcétera, son factores que afectan al desarrollo social por lo cual todos los organismos involucrados y que tienen competencia legal y jurídica necesitan coordinarse efectivamente para cumplir el objetivo de garantizar la seguridad de la población que permita el normal desarrollo de sus actividades productivas, sociales y recreativas en un ambiente de paz y tranquilidad.

CAPITULO III

3. METODOLOGÍA

3.1. Paradigma de Investigación.

El presente trabajo de investigación será desarrollado con la utilización y el aporte de los dos principales paradigmas de investigación: cuantitativo y cualitativo.

El paradigma de investigación cualitativa nos ayudará a identificar las opiniones de quienes participan en la investigación, tanto de expertos en el tema, niveles directivo, planificador y operadores en general. Con toda esta información se considera que se podrá analizar cómo está la situación de la Seguridad en el CNE, Sede. DM. Quito, para en lo posterior poder elaborar un diseño de una planificación que se ajuste a las necesidades de seguridad integral de la institución.

El paradigma de investigación cuantitativo nos permitirá apoyarnos, para a través de la recopilación de datos, tabulación y procesamiento de los mismos obtener conclusiones y recomendaciones valederas que nos permitan plantear propuestas de alternativas de solución a los diferentes problemas identificados.

No solamente se trata de realizar el estudio de la seguridad en el CNE. Sede. DM. Quito, sino de plantear una alternativa o propuesta de solución al análisis y evaluación de riesgos y amenazas a los que se ve abocada la institución en su integralidad nacional.

La investigación se realizará a través de la utilización de fuentes primarias y secundarias, como fuentes primarias la utilización de:

- Encuestas dirigidas los niveles directivo, planificador y operadores.
- Entrevistas a expertos en relación al problema sujeto de análisis y,

- Fuentes secundarias a través de la utilización de bibliografía que haga referencia a la temática motivo de la investigación.

Una vez obtenida está información sobre los principales objetivos, se procederá a continuar con la aplicación de técnicas de observación en función de las interrogantes planteadas a fin, tabular, analizar y sintetizar dicha información que nos permitirá extraer conclusiones y resultados significativos que contribuyan a una aplicación eficiente de una propuesta de diseño de una planificación de seguridad integral e implementación que permita mitigar, disminuir, neutralizar o eliminar las potenciales riesgos y amenazas que atenten al cumplimiento de los objetivos planteados.

En el desarrollo de la presente investigación seguiremos los siguientes pasos:

- Se realizará un diagnóstico de la situación actual de seguridad en la sede del CNE del Distrito Metropolitano de Quito.
- Se realizará una evaluación de los riesgos a los que se encuentra expuesta la sede del CNE, en el DM. de Quito.
- Establecimiento de los recursos humanos y materiales disponibles en la sede del CNE, en el DM. de Quito.
- Establecimiento de los recursos humanos y materiales que se requieren para el diseño de un Plan de seguridad integral en la sede del CNE, en el DM. de Quito.
- Establecimiento de una metodología de planificación apropiada para la elaboración del Plan de Seguridad integral para la sede del CNE, en la ciudad de Quito.
- Elaboración de un Sistema de Seguridad para el CNE.

3.2. Nivel y Tipo de Investigación

Los métodos empleados en este estudio serán:

Método Inductivo.- A partir del estudio de casos particulares relacionados con los problemas de inseguridad, se obtendrán conclusiones o leyes universales que explican los fenómenos estudiados. Inicia desde lo particular hasta llegar a inferencias generales; por lo cual será utilizado para plantear estrategias y tácticas a seguir para la implementación de procesos de seguridad en el CNE.

Método Deductivo.- Obtener conclusiones particulares a partir de una ley universal. Inicia desde lo general hasta llegar a situaciones particulares; por lo que este método será utilizado para determinar oportunidades y/o problemas que se presentan dentro de un sistema de seguridad integral. Analizaremos en el contexto de la seguridad del CNE, emitiendo posibles soluciones y deduciendo de la aplicación de las mismas los resultados esperados.

Método Estadístico.- El método estadístico consiste en una serie de procedimientos para el manejo de los datos cualitativos y cuantitativos de la Investigación a fin de obtener conclusiones y recomendaciones. Dicho proceso se realizará a la aplicación a la población muestra de los diferentes niveles y de acuerdo a las interrogantes planteadas.

Método analítico – sintético El Método analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de cada uno de los procesos de seguridad en particular. Es necesario conocer la naturaleza de la seguridad que se estudia para comprender su esencia. Este método nos permitirá conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

El método sintético va de la mano con el analítico, pues una vez que hemos desagregado las partes de los procesos de seguridad, los iremos uniendo o agregando, con la finalidad de entender la dinámica de acción de cada uno de los componentes, dentro del fenómeno de la seguridad como un todo dinámico y no disperso.

Utilizaremos la tabulación de encuestas y entrevistas, con el consiguiente análisis de sus resultados y la elaboración de pasteles que reflejen los mismos.

3.3. Población y Muestra.

3.3.1. Población.

“Es el conjunto de todos los elementos que son objeto del estudio estadístico”.

La población de encuestados del CNE son de 380 personas, pero de acuerdo a los requerimientos y relacionamiento con las interrogantes de investigación establecemos los siguientes niveles:

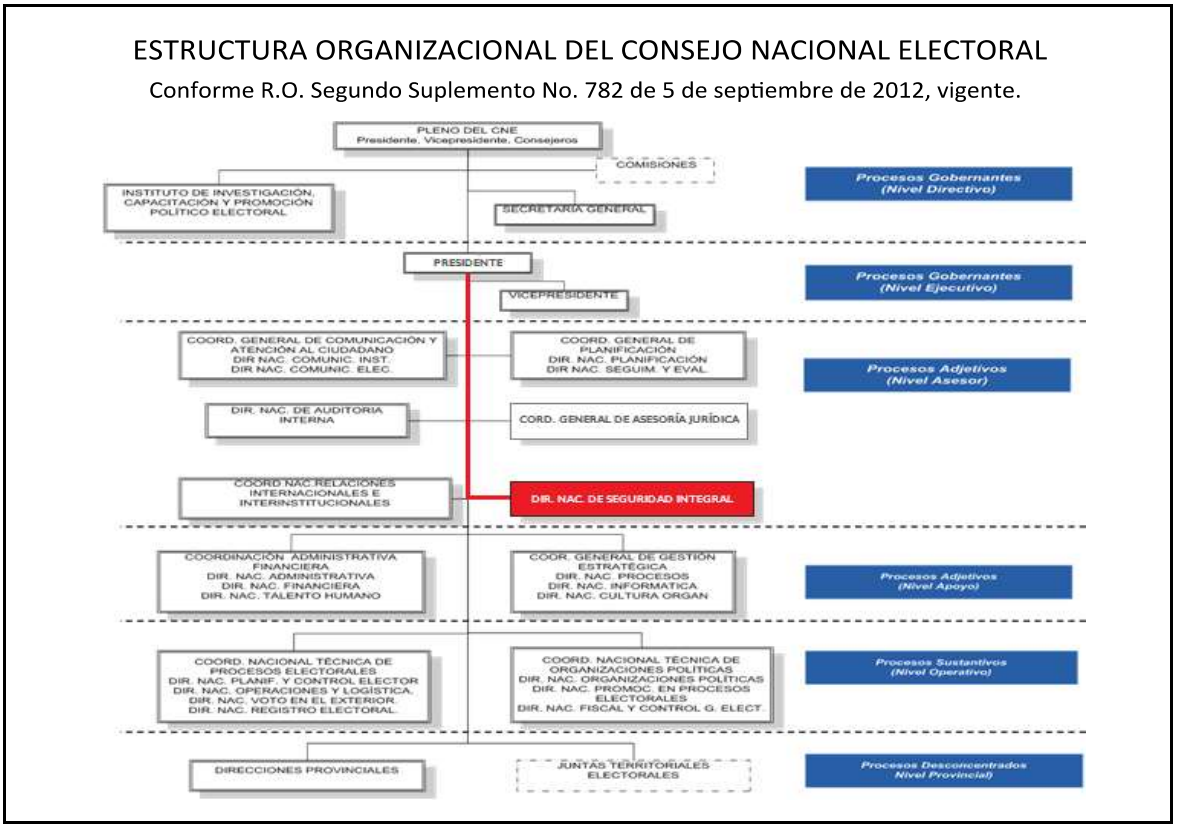
En el presente trabajo de investigación trabajaremos con dos grupos de estudio de diferente número poblacional. El cálculo de la muestra se realizará para el nivel directivo y planificador de la seguridad y para el nivel operativo de acuerdo a la fórmula más de 200 personas.

Tabla Nº 17 Población y muestra

Departamento	Número de Personas
Nivel Directivo y Planificador de Seguridad	3 personas que corresponde al 60 % de la población.
Nivel Operativo	380 personas, de las cuales se trabajaran con 195 personas que corresponde al 51.3% del total de la población

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 22 Estructura organizacional del CNE



Fuente: CNE "Estructura Orgánica del Consejo Nacional Electoral", 2012

3.3.2. Muestra.

"Es un subconjunto, extraído de la población (mediante técnicas de muestreo), cuyo estudio sirve para inferir características de toda la población".

Con este dato se procede al cálculo de la muestra a través de la siguiente fórmula.

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

En donde:

n= tamaño de la muestra

e= margen de error

m= tamaño de la población

$$n = \frac{380}{(0.05)^2\,(380-1)+1}$$

$$n = \frac{380}{0{,}0025 \text{ x } (379)+1}$$

$$n = \frac{380}{1.94.75}$$

$$n = \frac{380}{1.9475}$$

n = 195.12 de donde se tomaran 195 encuestas al personal dentro del nivel operativo

3.4. Técnicas de Recolección de Información

Los datos y respuestas serán recolectados de la fuente primaria de información, detallando de forma directa a fin de que la información sea procesada con actualidad sobre el problema a ser investigado.

Entre las principales técnicas de recolección de datos que utilizaremos para nuestra investigación están:

- **La Observación:** Permite verificar la situación actual de la seguridad en el CNE. Sede DM. Quito.
- **La Encuesta:** Para determinar la opinión por parte de los participantes en la seguridad del CNE. Sede DM. Quito.

El proceso investigativo, funcionarios de los diferentes niveles, expertos en seguridad integral.

- **La Entrevista:** Servirá para conocer la realidad y diferentes concepciones de la problemática a ser investigada.

Como fuentes secundarias, tomaremos en cuenta, opiniones de expertos, libros, revistas, textos, manuales, documental y visitas al Internet, que sirvan como guías para poder realizar la investigación de campo de una manera más eficaz.

Como corresponde al proceso investigativo y en la parte correspondiente a tratamiento y análisis de datos, una vez que se han obtenido, los datos correspondientes de acuerdo a la aplicación de las diferentes técnicas de recolección de información, se procederá realizar la tabulación respectiva y posteriormente el análisis de los resultados que permita levantar conclusiones que aporten a la resolución de los objetivos planteados en la presente investigación.

3.5. Análisis y Discusión de Resultados

3.5.1. Observación en campo “LISTA DE CONTROL DE SEGURIDAD”

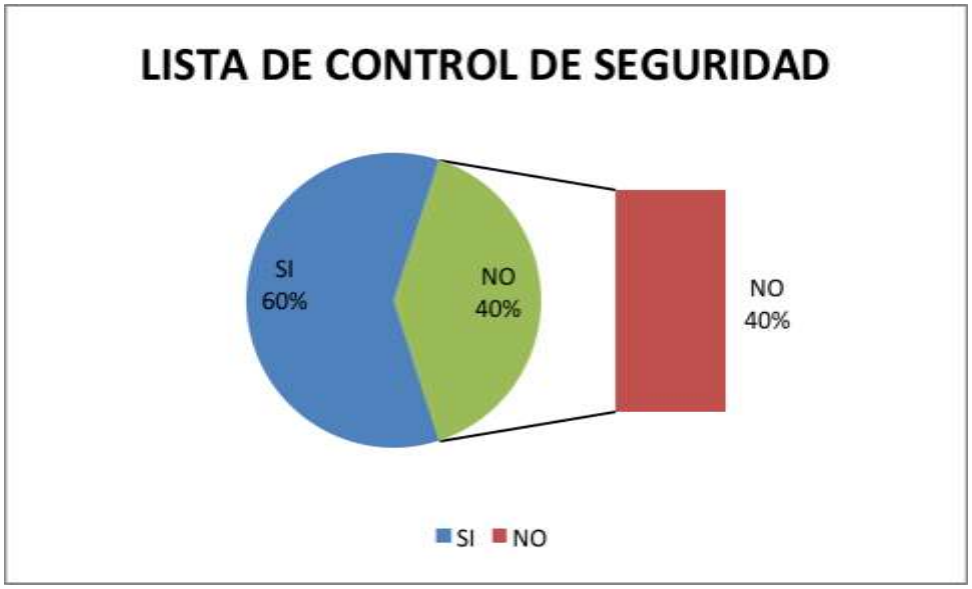
Tiene el propósito de proveer un registro lógico de información y asegurar que ninguna cuestión importante quede sin respuesta.

Tabla Nº 18 Lista de control de seguridad

ORD.	ITEMS	SI	NO
1	Existen barrearas físicas en el perímetro?	X	
2	Existe un medio de seguridad para el registro y control de accesos?	X	
3	La seguridad es 24 horas, 7 días a la semana?	X	
4	Existe medios electrónicos de seguridad?	X	
5	Existe controles adicionales de seguridad en el centro de datos?	X	
6	Se verifica y solicita la identificación de todas las personas que ingresan?	X	
7	Se emiten tarjeta de identificación para todos los funcionarios del CNE?	X	
8	Existen tarjetas para visitantes que indiquen el área a la que están autorizados?	X	
9	Se mantiene un registro de los incidentes?		X
10	Existe una adecuada señalética de seguridad para el establecimiento?		X
11	Existe procedimientos de seguridad de la información?		X
12	Se ejecutan trabajos clasificados?	X	
13	Las instalaciones están propensas a sufrir destrozos por amenazas naturales?	X	
14	Existe escaleras de emergencia?		X
15	Se emplea CCTV para el control interno y externo?	X	
16	Están las oficinas equipadas con equipos de detección y respuesta contra incendios?		X
17	Existe un punto seguro establecido?		X
18	Existe procedimientos específicos para recepción de paquetes?		X
19	Existe suficiente alumbrado en las zonas exteriores?		X
20	Se dispone de iluminación adecuada al interior?	X	
21	Se dispone de generador de energía alterna o UPS?	X	
22	Existen adecuado control en áreas de acceso restringido?		X
23	Existe control para el uso del parqueadero?		X
24	Existe un sistema de control para los desechos?		X
25	Las instalaciones que dispone el CNE brindan seguridad para funcionarios y visitantes?		X
26	Existe departamento médico en el CNE?	X	
27	El programa de seguridad física cuenta con suficiente personal?	X	
28	Se realizan simulaciones y simulacros en caso de desastres?		X
29	Existen procedimientos de seguridad?	X	
30	El personal de seguridad está armado?	X	
	TOTAL	**60%**	**40%**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 23 "Lista de Control de Seguridad"



Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Los resultados de la observación en campo a través de la Lista de Control de Seguridad, indica que existe parcialmente disponibilidad de medios con una deficiente incorporación de políticas, programas y planes de seguridad, siendo necesario fortalecer estos aspectos, para una adecuada articulación del hardware, software y personal, dentro del programa de seguridad física, que tiene como objetivo salvaguardar personas, prevenir ingresos no autorizados a instalaciones, equipos, materiales y documentos.

3.5.2. Encuesta para personal que trabaja en Consejo Nacional Electoral, con sede en el Distrito Metropolitano de Quito.

Objetivo.

La presente encuesta, tiene como finalidad recabar información de uso exclusivo para mi trabajo de tesis, por lo cual agradezco de antemano su colaboración, y solicito señalar en cada pregunta planteada el indicador de evaluación que Ud., considere el más adecuado

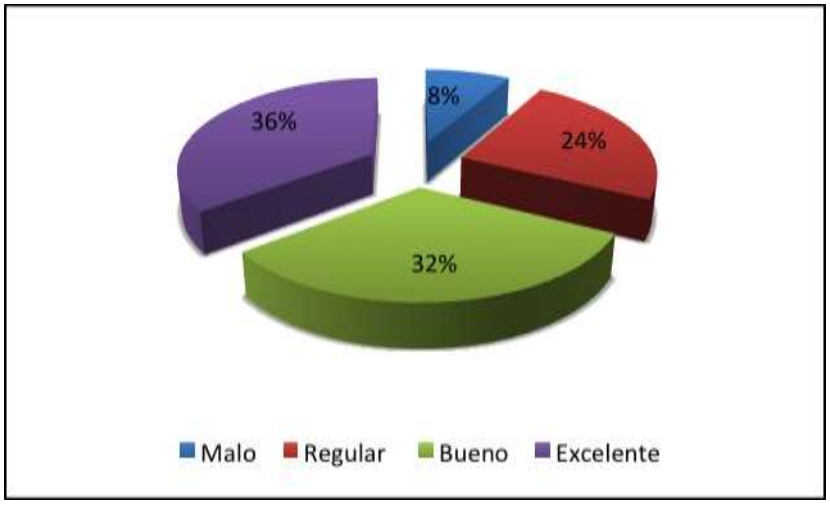
Tabla Nº 19 “Nivel de seguridad que dispone el CNE”

Concepto	Frecuencia	Porcentaje
Malo	16	8%
Regular	47	24%
Bueno	63	32%
Excelente	69	36%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 24 “Nivel de seguridad que dispone el CNE”



Fuente: MUÑOZ, Jorge, 2013, Encuesta de la Tesis, pregunta 1

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Los datos nos pueden indicar que un 32% de la muestra poblacional percibe que la seguridad que dispone el CNE, no es lo suficientemente representativa como para generar un ambiente de seguridad propicio para el normal desarrollo de sus actividades; un 32% tiene un sentido de percepción aceptable de seguridad y solo 36% considera que se encuentran en un ambiente seguro, lo que indica las falencias existentes y la necesidad de mejorar el sistema o programa de seguridad actual.

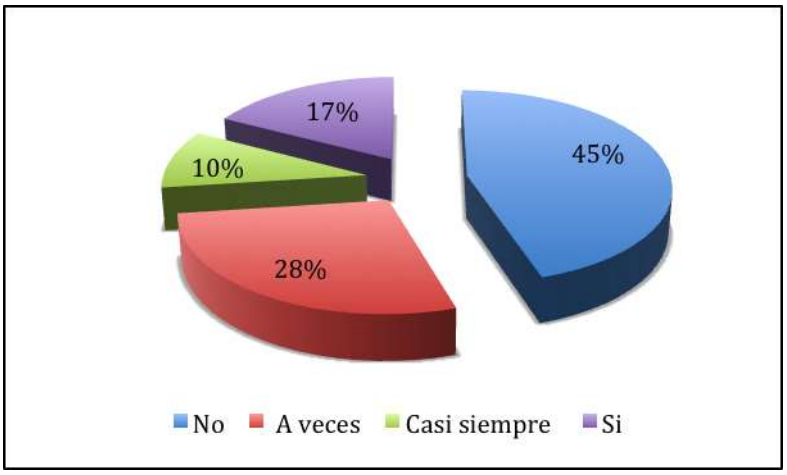
Tabla Nº 20 "Conocimiento de los funcionarios en los sistemas de seguridad que dispone el CNE"

Concepto	Frecuencia	Porcentaje
No	88	45%
A veces	54	28%
Casi siempre	19	10%
Si	34	17%
Total	195	100%

Fuente: Encuesta de la Tesis pregunta 2

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 25 "Conocimiento de los funcionarios en los sistemas de seguridad que dispone el CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Los datos nos pueden indicar que un 73% de los encuestados no tienen conocimiento de los sistemas de seguridad que posee el CNE para el control de los activos, una deficiente socialización puede ser la causa del gran porcentaje de desconocimiento.

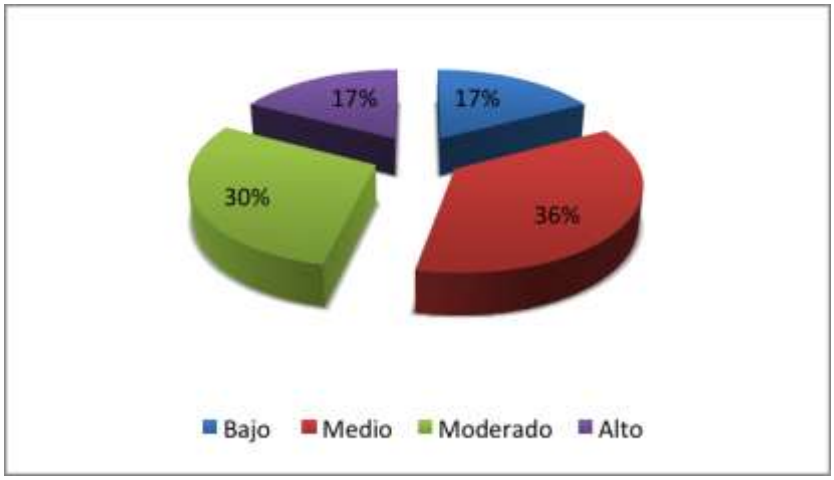
Tabla Nº 21 "Nivel de riesgo al trabajar como funcionarios en el CNE"

Concepto	Frecuencia	Porcentaje
Bajo	34	17%
Medio	70	36%
Moderado	57	30%
Alto	34	17%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 26 "Nivel de riesgo al trabajar como funcionarios en el CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 66% de los encuestados consideraron que están expuestos a un riesgo medio y moderado; y un 17% que se encuentran expuestos a un riesgo alto al trabajar como funcionarios del CNE, en consecuencia a las diferentes amenazas que podrían incidir directamente en el cargo de sus funciones, siendo este dato un antecedente contundente para generar programas de seguridad para el personal.

Tabla Nº 22 "Se difunden normas y procedimientos de seguridad personal"

Concepto	Frecuencia	Porcentaje
No	72	37%
A veces	44	22%
Casi siempre	35	18%
Siempre	44	23%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 27 "Se difunden normas y procedimientos de seguridad personal"

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 59% de los funcionarios encuestados, no han recibido normas y procedimientos en seguridad personal, por parte del departamento de seguridad, lo que indica la vulnerabilidad a la que están sujetos los funcionarios y la necesidad de mejorar los mecanismos de comunicación para dar a conocer procedimientos y normas de seguridad.

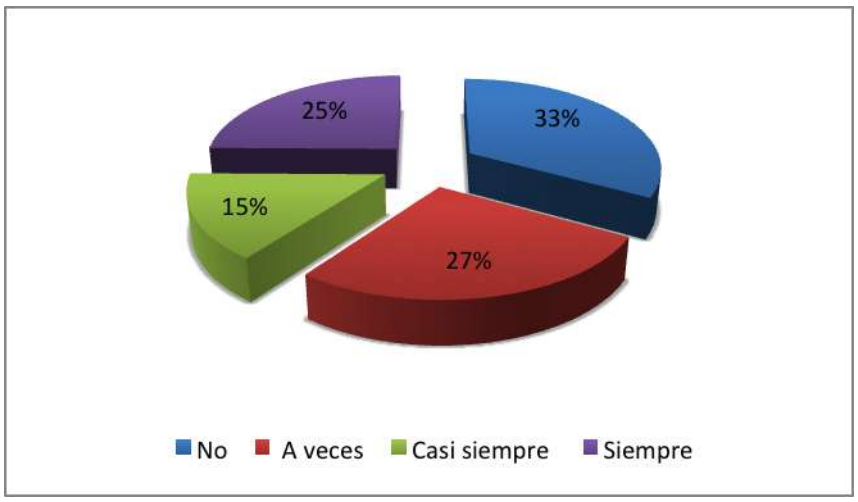
Tabla Nº 23 “Se difunden normas y procedimientos de seguridad de la información”

Concepto	Frecuencia	Porcentaje
No	65	33%
A veces	53	27%
Casi siempre	29	15%
Siempre	48	25%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 28 “Se difunden normas y procedimientos de seguridad de la información”



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis

La seguridad y protección de la información es vulnerable debido a un desconocimiento del 60% de los encuestados acerca de normas y procedimientos causando problemas en la confidencialidad, integridad, disponibilidad y preservación de la información.

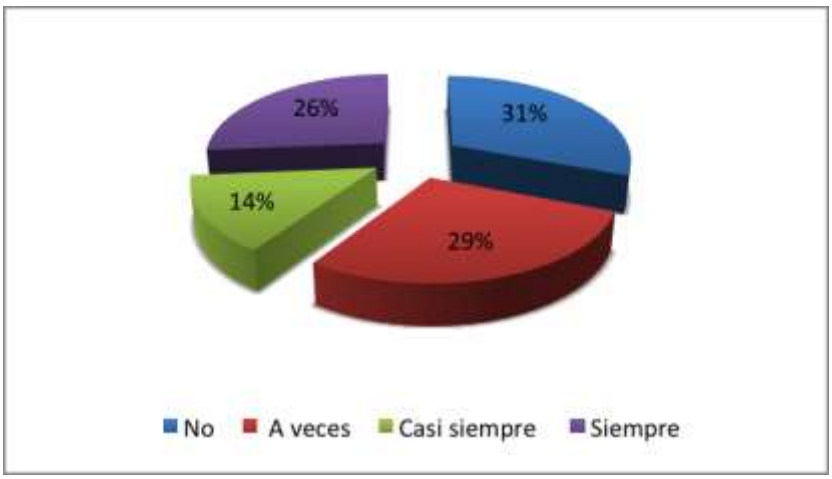
Tabla Nº 24 “Se difunden normas y procedimientos de seguridad física”

Concepto	Frecuencia	Porcentaje
No	60	31%
A veces	56	29%
Casi siempre	28	14%
Siempre	51	26%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 29 “Se difunden normas y procedimientos de seguridad física”



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

La seguridad de los activos no puede estar completamente protegida sin el involucrar a todos los funcionarios dentro un programa de protección física, un 60% de los encuestados manifiestan un desconocimientos de normas y procedimientos en seguridad física lo que dificultara la cooperación necesaria entre los encargados de la seguridad y los funcionarios del CNE.

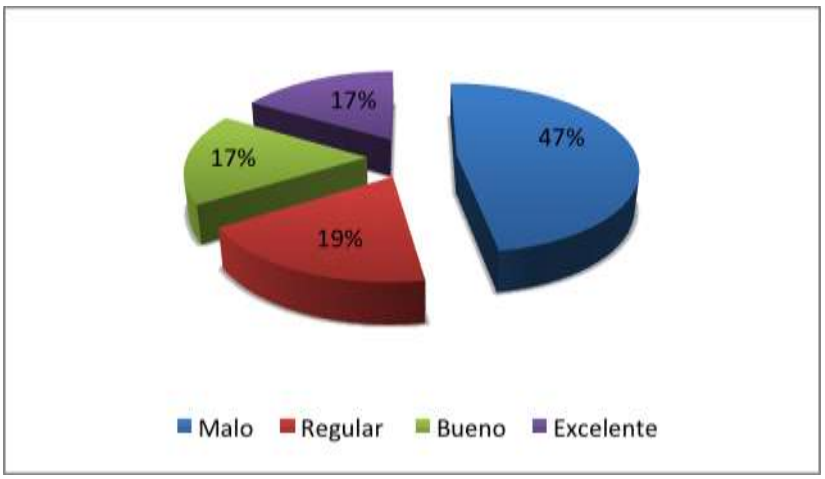
Tabla Nº 25 " Nivel de satisfacción de cursos recibidos en el CNE"

Concepto	Frecuencia	Porcentaje
Malo	92	47%
Regular	37	19%
Bueno	34	17%
Excelente	32	17%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 30 " Nivel de satisfacción de cursos recibidos en el CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 66% de los encuestados consideran deficiente el programa de capacitaciones en temas de seguridad, y la necesidad de aumentar y mejorar la cantidad y secuencia de talleres y seminarios para mantener un alto nivel de comprometimiento y conocimiento en temas de seguridad necesarios para fortalecer un programa de seguridad.

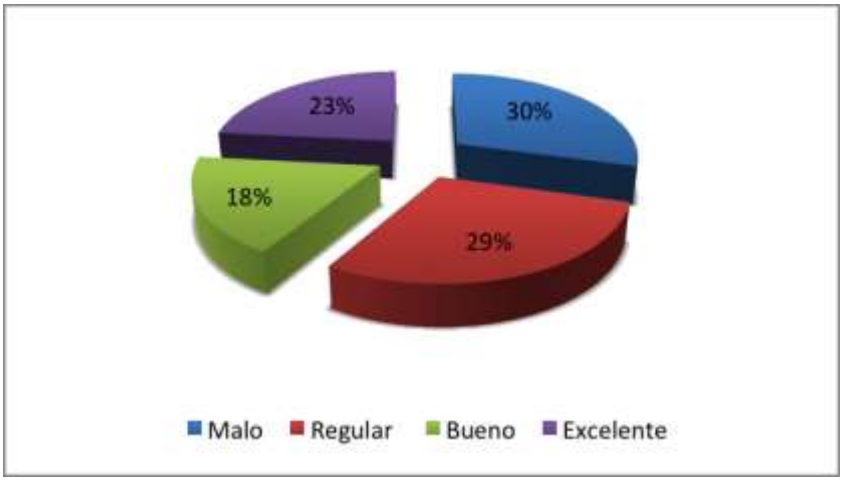
Tabla Nº 26 "Nivel de cumplimiento en la difusión de normas de seguridad en el CNE"

Concepto	Frecuencia	Porcentaje
Malo	58	30%
Regular	57	29%
Bueno	35	18%
Excelente	45	23%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 31 "Nivel de cumplimiento en la difusión de normas de seguridad en el CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 59% de los encuestados ha indicado que existen falencias en el cumplimiento de los encargados de seguridad en difundir normas de seguridad, esto indica que existe un relativo desconocimiento de las mismas lo que dificulta el correcto cumplimiento de los objetivos de un programa de seguridad.

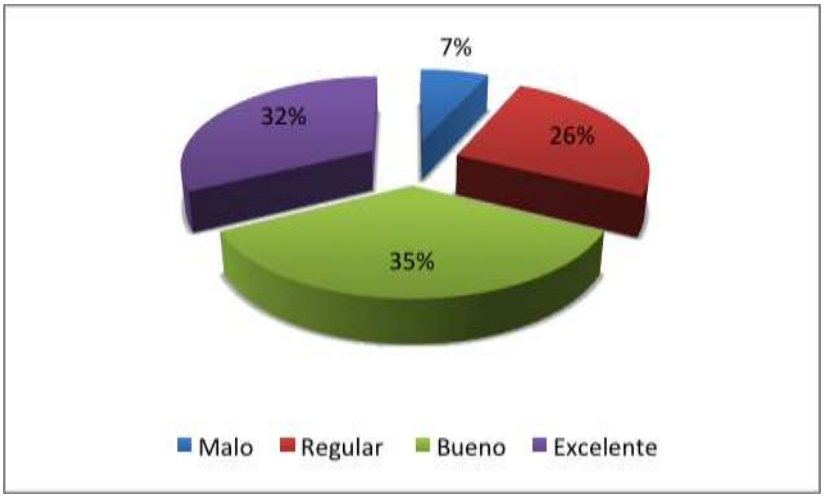
Tabla Nº 27 "Calificación del servicio de seguridad privada por parte de los funcionarios del CNE"

Concepto	Frecuencia	Porcentaje
Malo	13	7%
Regular	50	26%
Bueno	69	35%
Excelente	63	32%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 32 "Calificación del servicio de seguridad privada por parte de los funcionarios del CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

EL servicio de seguridad es contratado y el personal de encuestados en un 33% han considerado que no cumple con eficiencia con su cometido, un 67% está conforme, lo que indica que es necesario incorporar un programa de seguridad integral que permita aumentar y mejorar el cumplimiento de objetivos y propósitos.

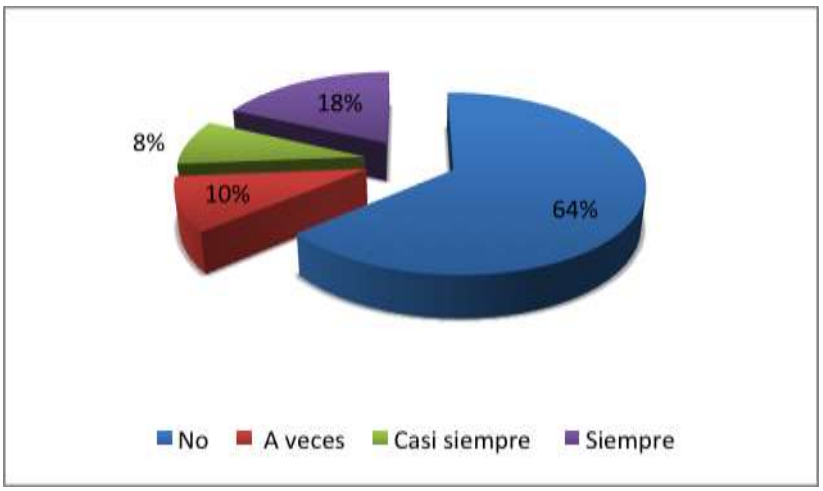
Tabla Nº 28 "Simulacros de evacuación en el presente año"

Concepto	Frecuencia	Porcentaje
No	125	64%
A veces	19	10%
Casi siempre	16	8%
Siempre	35	18%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 33 "Simulacros de evacuación en el presente año"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Los resultados indican que no se han realizado simulacros en el CNE, lo que manifiesta la falta de preparación de los funcionarios para actuar en emergencias al momento de una evacuación, siendo necesario realizar simulacros para preparar al personal que labora en el CNE.

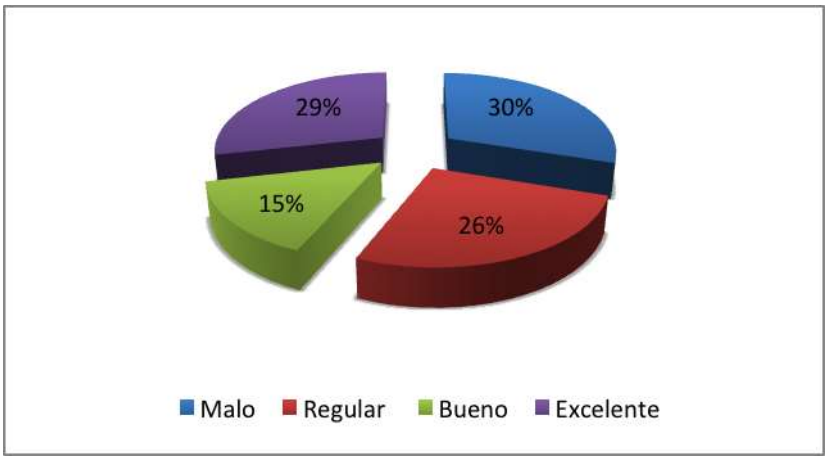
Tabla Nº 29 "Calificación del sistema contra incendios y señalética de emergencia"

Concepto	Frecuencia	Porcentaje
Malo	59	30%
Regular	51	26%
Bueno	29	15%
Excelente	56	29%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 34 "Calificación del sistema contra incendios y señalética de emergencia"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 56% de los encuestados, encuentran deficiente el sistema contra incendios y la señalética que dispone el CNE, lo que permite notar la necesidad de mejorarlos para en momento de actuar frente un incendio tener los mecanismos de respuesta necesarios en óptimo funcionamiento.

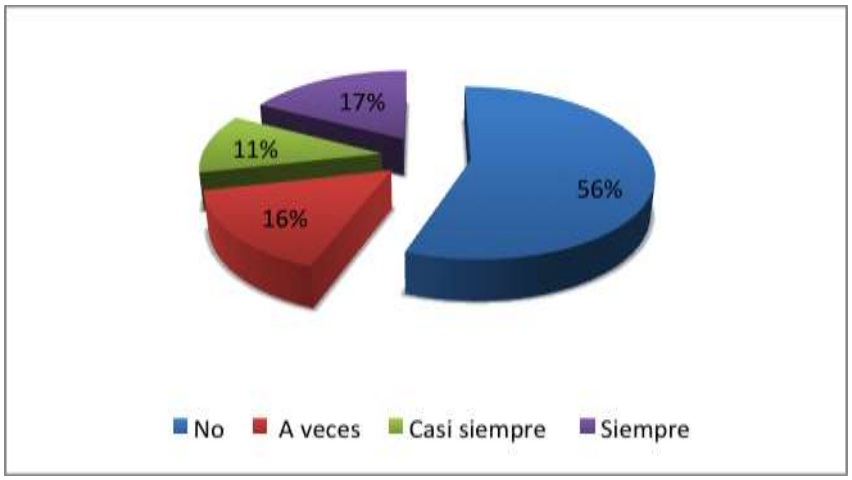
Tabla Nº 30 "Capacitación del personal en planes de emergencia"

Concepto	Frecuencia	Porcentaje
No	108	56%
A veces	31	16%
Casi siempre	22	11%
Siempre	34	17%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 35 "Capacitación del personal en planes de emergencia"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Existe un 72% de encuestados que no han tenido capacitación de cómo actuar frente a emergencias, lo que denota la falta de capacidades que dispone el CNE, para actuar y dar respuesta en eventos no deseados.

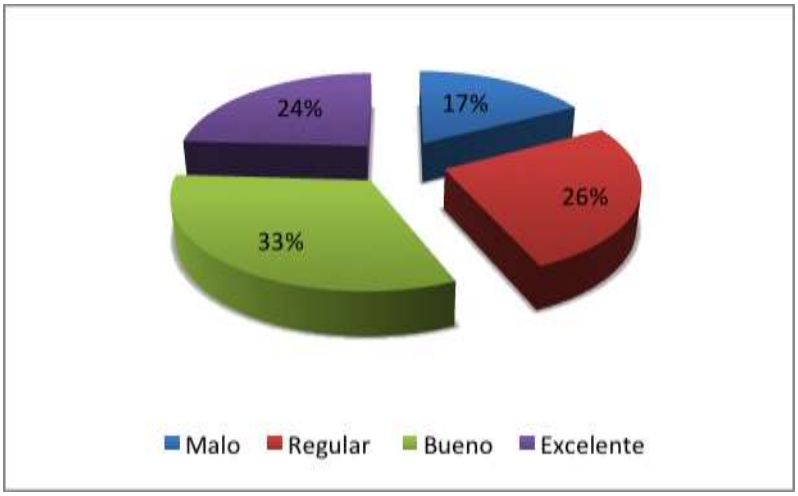
Tabla Nº 31 "Nivel de confidencialidad de la información"

Concepto	Frecuencia	Porcentaje
Malo	34	17%
Regular	51	26%
Bueno	63	33%
Excelente	47	24%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 36 "Nivel de confidencialidad de la información"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Uno de los valores activos con mayor importancia para el CNE, es la información, interpretar un 43% de deficiencia en su manejo, demuestran que es necesario realizar una mayor gestión en la mejora de mecanismos de seguridad, confidencialidad y protección de la información.

Tabla Nº 32 "Conocimiento del personal en medios internos para reportar incidentes y accidentes"

Concepto	Frecuencia	Porcentaje
No	62	32%
A veces	58	30%
Casi siempre	34	17%
Si	41	21%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 37 "Conocimiento del personal en medios internos para reportar incidentes y accidentes"

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

En los resultados de la encuesta, un 52% indican que no existe un correcto sistema de reportes de incidentes y accidentes lo que impide tener una base de datos adecuada, que permite identificar falencias dentro de un programa de seguridad, e imposibilita realizar un auditoria del mismo.

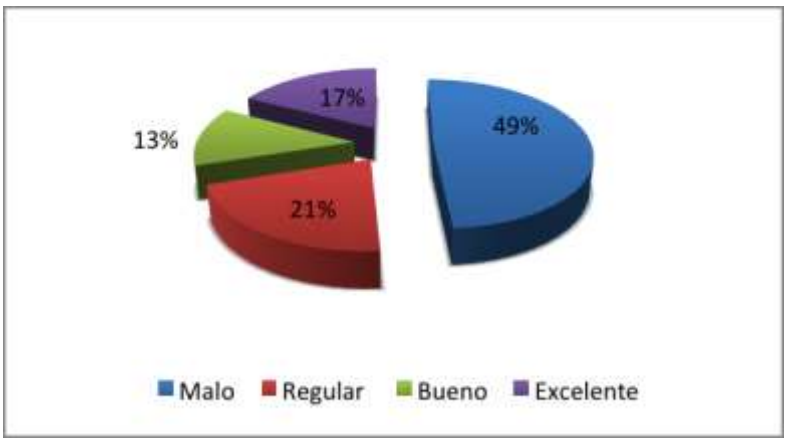
Tabla Nº 33 "Nivel de capacitación que dispone el personal para enfrentar emergencias"

Concepto	Frecuencia	Porcentaje
Malo	95	49%
Regular	41	21%
Bueno	25	13%
Excelente	34	17%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 38 "Nivel de capacitación que dispone el personal para enfrentar emergencias"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 70% de los encuestados consideran que no se encuentran preparados para actuar ante una emergencia debido al desconocimiento de planes de emergencia, rutas de evacuación que necesariamente deberán ser consideradas, para mejorar la respuesta ante las emergencias consideradas.

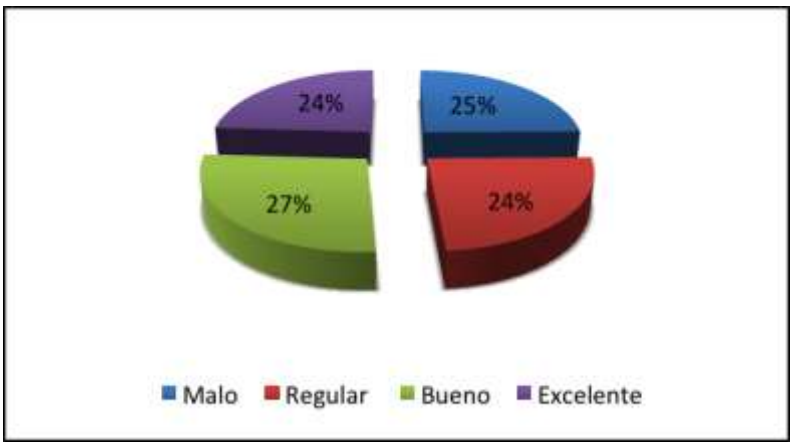
Tabla Nº 34 "Nivel de conocimientos en seguridad del personal del CNE"

Concepto	Frecuencia	Porcentaje
Malo	48	25%
Regular	47	24%
Bueno	53	27%
Excelente	47	24%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 39 "Nivel de conocimientos en seguridad del personal del CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Considerando los datos obtenidos de las encuestas nos permiten observar que aproximadamente un 49% de los encuestados no tienen conocimientos de seguridad, un 27% conocimientos promedio y un 24% si poseen conocimientos en seguridad, entendiendo que los conocimientos a los que nos referimos son básicos de carácter general. Estos datos nos permiten dimensionar nuestra intervención en comunicación y socialización necesaria para generar una cultura de seguridad dentro de los funcionarios del CNE.

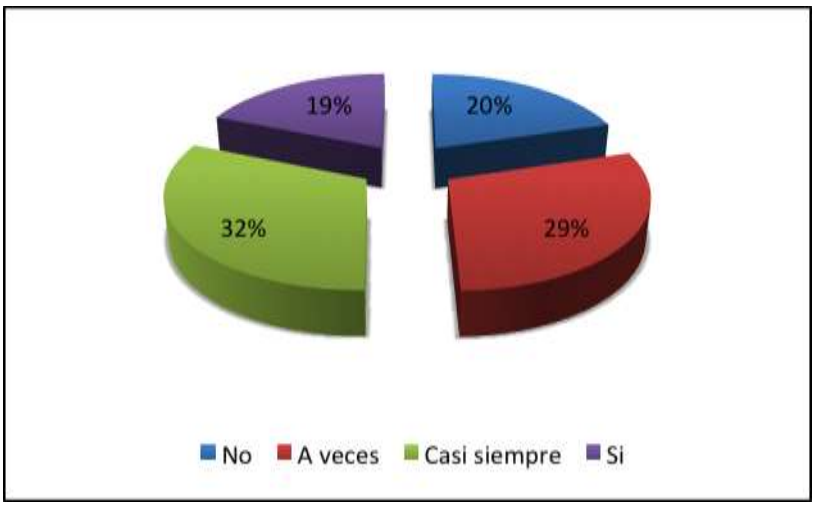
Tabla Nº 35 "Comprometimiento del personal del CNE en el cumplimiento óptimo de la seguridad"

Concepto	Frecuencia	Porcentaje
No	39	20%
A veces	57	29%
Casi siempre	62	32%
Si	37	19%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 40 "Comprometimiento del personal del CNE en el cumplimiento óptimo de la seguridad"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Analizando los datos entre un 49% que no considera que existe un ambiente de solidaridad y trabajo en conjunto, a un 51% que siente que su ambiente trabajo es bueno y propicio para el cumplimiento óptimo de los objetivos de seguridad, permite visualizar una división interna que necesita ser mejorada con la intención de fortalecer las relaciones y comprometimiento personal.

Tabla Nº 36 “Nivel de riesgo que tiene la información a cargo de los funcionarios”

Concepto	Frecuencia	Porcentaje
Bajo	35	18%
Medio	39	20%
Moderado	65	33%
Alto	56	29%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 41 “Nivel de riesgo que tiene la información a cargo de los funcionarios”

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

En una análisis de los datos obtenidos podemos observar que un 82% de los encuestados consideran que la información que manejan, está sujeta algún tipo de riesgo por el valor e interés que esta tiene para determinados grupos políticos.

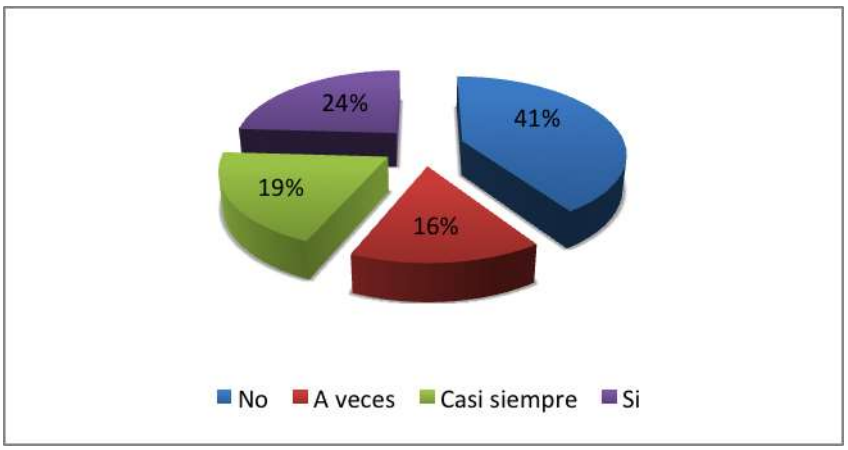
Tabla Nº 37 “Conocimientos impartidos sobre el uso de información clasificada”

Concepto	Frecuencia	Porcentaje
No	79	41%
A veces	31	16%
Casi siempre	38	19%
Si	47	24%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 42 “Conocimientos impartidos sobre el uso de información clasificada”



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Interpretando los datos obtenidos podemos observar la deficiencia en el manejo de información clasificada, el 57% de los encuestados desconoce cómo manejar la información que les ha sido entregada, para efecto de control es necesario clasificar la información confidencial y publica.

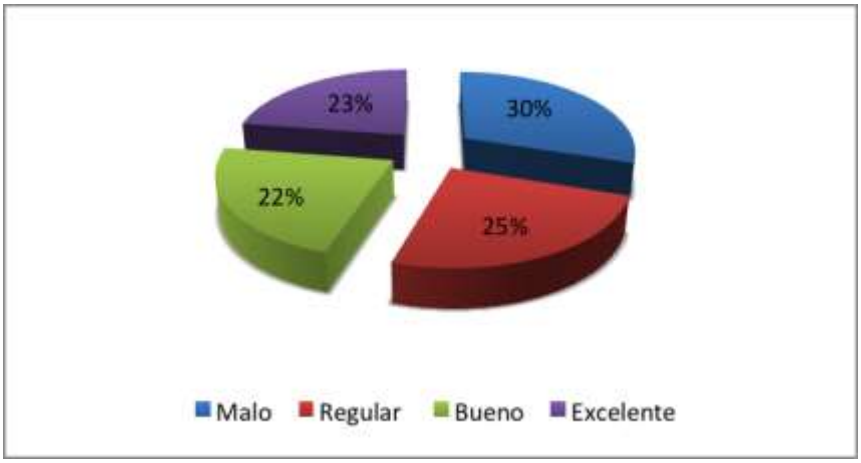
Tabla Nº 38 "Calificación de la respuesta a emergencias por parte del personal del CNE"

Concepto	Frecuencia	Porcentaje
Malo	59	30%
Regular	48	25%
Bueno	44	22%
Excelente	44	23%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 43 "Calificación de la respuesta a emergencias por parte del personal del CNE"



Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 55% de los encuestados consideran deficiente la preparación ante emergencias, el análisis de este dato porcentual, es un indicador para determinar que el Consejo Nacional Electoral, presenta problemas en la organización y respuesta ante una emergencia, por lo que es necesario diseñar e implementar un plan de emergencias y desastres, para dar continuidad a los procesos que lleva acabo la institución.

Tabla Nº 39 "Calificación de la implementación del sistema electrónico de seguridad por parte del personal del CNE"

Concepto	Frecuencia	Porcentaje
Malo	33	17%
Regular	37	19%
Bueno	60	31%
Excelente	65	33%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 44 "Calificación de la implementación del sistema electrónico de seguridad por parte del personal del CNE"

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

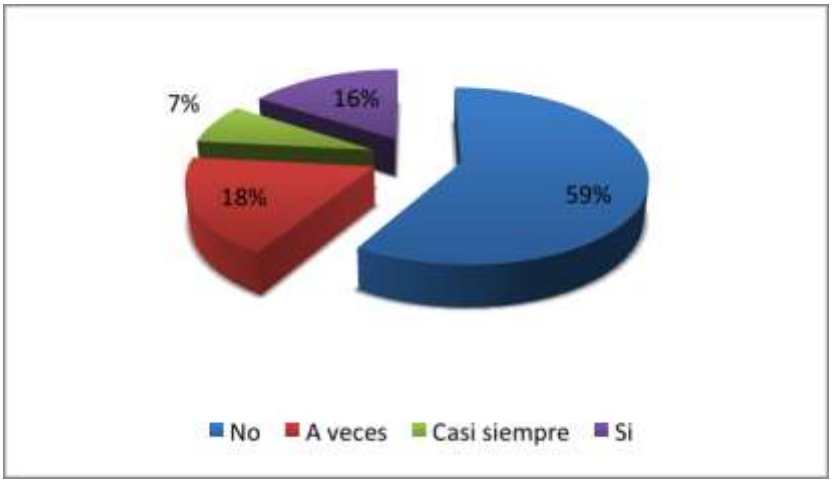
Con un 64% de encuestados, que perciben que la seguridad electrónica es buena, permite aprovechar los recursos disponibles y verificar su funcionalidad y operatividad; y de ser necesario el rediseño del sistema para cubrir las deficiencias identificadas en el estudio de seguridad.

Tabla Nº 40 "Simulaciones y simulacros en caso de amenaza de bomba"

Concepto	Frecuencia	Porcentaje
No	114	59%
A veces	35	18%
Casi siempre	15	7%
Si	31	16%
TOTAL	195	100%

Fuente: Encuesta De La Tesis
Elaborado Por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 45 "Simulaciones y simulacros en caso de amenaza de bomba"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Al considerar un 77% de respuestas negativas, podemos determinar que no ha existido la consideración para realizar un simulacro en caso de amenaza de bomba, situación que debe ser prevista ya que este puede ser un mecanismo de presión y desestabilización al interior del CNE.

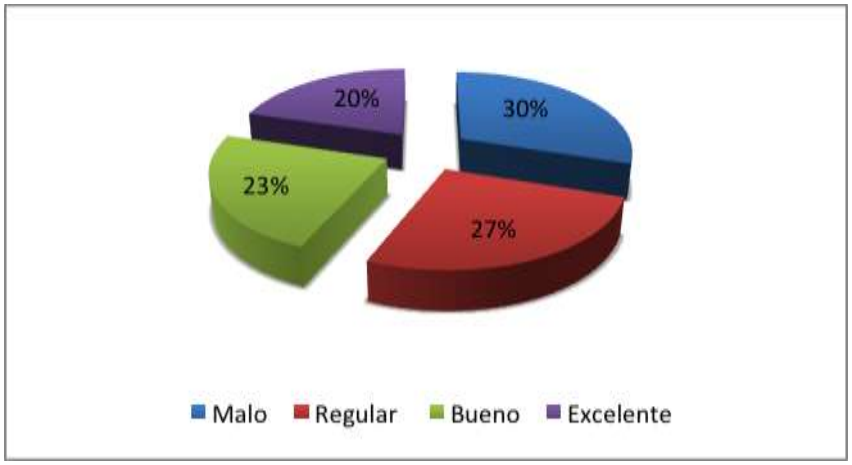
Tabla Nº 41 "Calificación de la tarea ejecutada de la Dirección Nacional de Seguridad Integral"

Concepto	Frecuencia	Porcentaje
Malo	59	30%
Regular	51	27%
Bueno	45	23%
Excelente	40	20%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 46 "Calificación de la tarea ejecutada de la Dirección Nacional de Seguridad Integral"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Un 57% de los encuestados tienen una concepción negativa con la gestión que ha tenido la Dirección Nacional de Seguridad Integral, por lo que es necesario aumentar presencia y gestión de forma transversal en cada área y proceso. Que los objetivos de esta Dirección estén directamente alineados con las políticas del CNE.

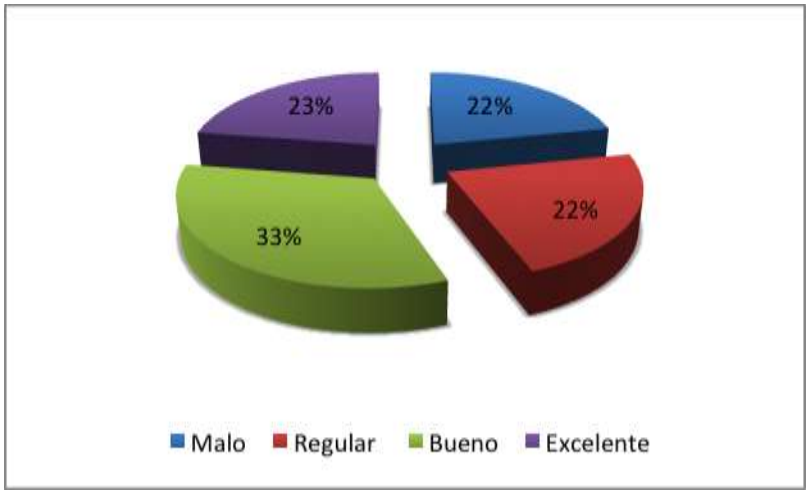
Tabla Nº 42 "Criterio para incorporar un sistema de seguridad en la infraestructura actual"

Concepto	Frecuencia	Porcentaje
Malo	43	22%
Regular	44	22%
Bueno	64	33%
Excelente	44	23%
Total	195	100%

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 47 "Criterio para incorporar un sistema de seguridad en la infraestructura actual"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

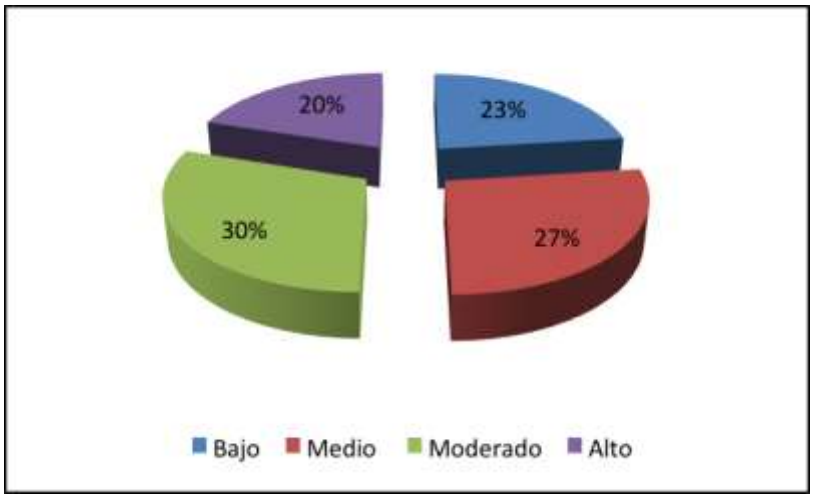
Los datos indican un resultado parcial un 44% en aspectos negativos y un 56% en aspectos positivos, indican que la infraestructura del CNE, podría acoger el programa de protección física, previo análisis de la vulnerabilidad e identificación de las amenazas que podrían incidir en ella.

Tabla Nº 43 "Percepción de inseguridad al interior y exterior de las instalaciones del CNE"

Concepto	Frecuencia	Porcentaje
Bajo	44	23%
Medio	52	27%
Moderado	59	30%
Alto	40	20%
Total	195	100

Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 48 "Percepción de inseguridad al interior y exterior de las instalaciones del CNE"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Considerando que existe un 50%, de percepción de inseguridad al interior y alrededores del CNE, nos pone en manifiesto la necesidad de aumentar medidas y contramedidas que pongan en atención la necesidad de disminuir los riesgos a los que se encuentran expuestos los activos materiales y no materiales.

Tabla Nº 44 "Conocimiento del punto de seguridad en el CNE"

Concepto	Frecuencia	Porcentaje
No	90	46%
A veces	29	15%
Casi siempre	32	16%
Si	44	23%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 49 "Conocimiento del punto de seguridad en el CNE"

Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

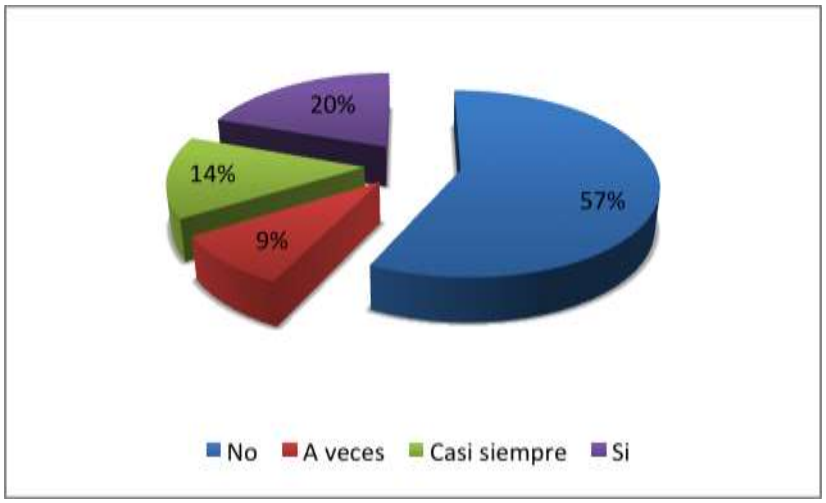
Los resultados indican que no existe conocimiento del punto seguro, en momento de una evacuación por parte del personal del CNE, lo que aumentaría los accidentes y fatalidades en el caso de emergencia, siendo necesario identificar y establecer el punto seguro, para su socialización y conocimiento general.

Tabla Nº 45 "Difusión de información en autoprotección"

Concepto	Frecuencia	Porcentaje
No	111	57%
A veces	18	9%
Casi siempre	28	14%
Si	38	20%
Total	195	100 %

Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 50 "Difusión de información en autoprotección"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Al considerar un 66% de respuestas negativas, podemos indicar que el personal que labora en el CNE, no dispone de información de autoprotección, por lo que es necesario aumentar este conocimiento con el fin de disminuir los eventos delincuenciales que pueden suscitarse a las fueras del Consejo Nacional Electoral.

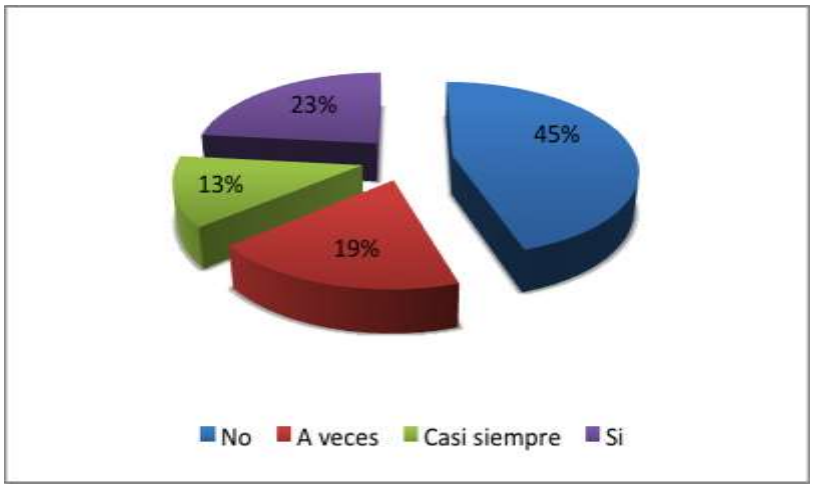
Tabla Nº 46 "Comunicación de procedimientos de seguridad de estricto cumplimiento"

Concepto	Frecuencia	Porcentaje
No	88	45%
A veces	37	19%
Casi siempre	25	13%
Si	45	23%
Total	195	100 %

Fuente: Encuesta de la Tesis

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 51 "Comunicación de procedimientos de seguridad de estricto cumplimiento"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

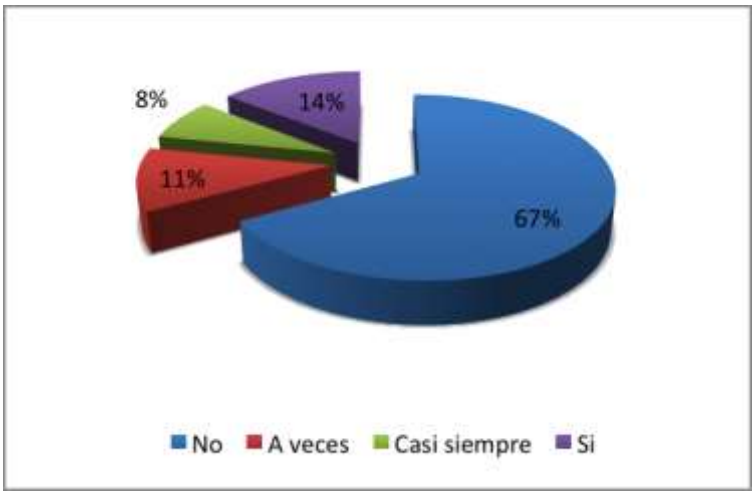
Al considerar un resultado de 64% de respuestas negativas, es un indicador de la falencia existente de normar e indicar procedimientos de seguridad para procesos internos, que deben cumplirse estrictamente con el fin mejorar la relación de un programa de seguridad en el cual interactúan software hardware y personal.

Tabla Nº 47 "Conocimiento de robos o hurtos al interior del CNE"

Concepto	Frecuencia	Porcentaje
No	130	67%
A veces	22	11%
Casi siempre	15	8%
Si	28	14%
Total	195	100 %

Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 52 "Conocimiento de robos o hurtos al interior del CNE"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

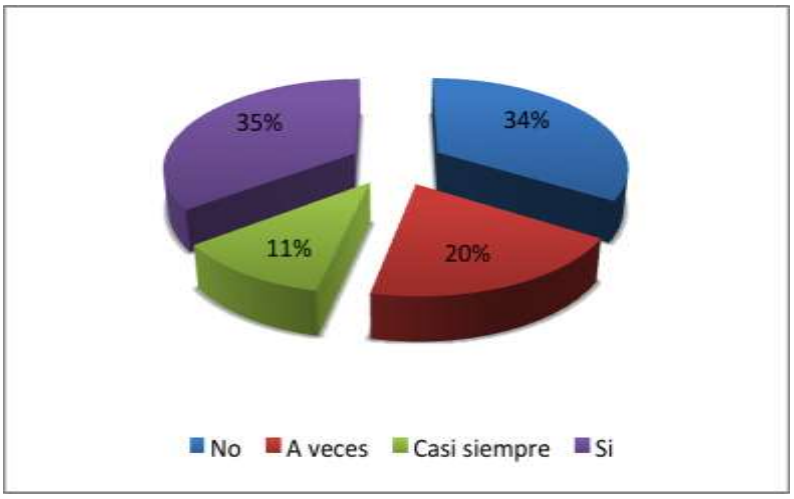
El resultado de comparación en eventos de robos y hurtos, en un 33% de encuestados que mencionan que si han sido sujetos a alguno de estos dos eventos, dejan en manifiesto que es necesario mejorar la seguridad interna del CNE.

Tabla Nº 48 "Conocimiento de robos o hurtos a terceras personas al interior del CNE"

Concepto	Frecuencia	Porcentaje
No	66	34%
A veces	38	20%
Casi siempre	22	11%
Si	69	35%
Total	195	100 %

Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Gráfico Nº 53 "Conocimiento de robos o hurtos a terceras personas al interior del CNE"



Fuente: Encuesta de la Tesis
Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Análisis.

Únicamente un 34% de los encuestados, no han tenido conocimiento de robos o hurtos a terceras personas, frente a un 66%, esto indica la necesidad de implementar un programa de seguridad integral, que disminuya los niveles de inseguridad que percibe el personal de autoridades, funcionarios, usuarios y visitantes.

3.5.3. Análisis de las entrevistas realizadas a los responsables de la seguridad del CNE.

Los entrevistados consideran a la seguridad como parte fundamental de todos los procesos que lleva a cabo el Consejo Nacional Electoral, en el cual se incluye el bienestar del personal y materiales, sin embargo concuerdan que existe deficiencia en la aceptación de las políticas de seguridad, por la falta de una cultura, lo que dificulta la aceptación de las normas y procedimientos de seguridad.

El requerimiento de contar con un sistema de seguridad integral, ajustado a las necesidades de la institución, basado en el diseño del análisis de la amenaza, es considerado de forma general por los entrevistados indispensable para el cumplimiento de los objetivos de protección.

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

1. No existe una política definida en base a la declaración de amenaza para el CNE, su personal, sus usuarios, proveedores y contratistas.
2. El CNE, no tiene una estructura definida para el área de protección de activos (seguridad), lo que dificulta su acción y toma de decisiones.
3. La implementación de medidas de protección existentes no han sido aplicadas en base a un estudio de seguridad ni análisis de la vulnerabilidad, más bien han estado basadas en experiencia de sus funcionarios de seguridad, que han contribuido en su implementación y a planes establecidos en base a una apreciación heurística de riesgos.
4. El CNE, tiene una exposición importante frente a diferentes amenazas antrópicas y las de tipo cibernético no son la excepción, ya que el desarrollo tecnológico puede permitir ataques desde el exterior de las instalaciones, hackers, crackers, virus espía, etc.
5. El CNE, por ser un sitio público donde existe información privilegiada, puede enfrentar adversarios que utilicen la fuerza como arma principal y puedan atacar directamente sus facilidades, sin embargo en el área de informática en el estudio realizado, no se pudo conocer de la implementación de sistemas de extinción modernos (FM200-HALON).
6. El CNE puede también ser objeto de infiltración de indeseables o complicidad de internos aumentando la vulnerabilidad existente.
7. Las comunicaciones se limita a comunicaciones convencionales y radio frecuencia, las mismas que pueden ser fácilmente interceptadas

8. No existe un plan específico en relación al personal que maneja información crítica y/ o privilegiada.
9. El CNE tiene responsabilidad sobre procesos críticos que se desenvuelven fuera de sus instalaciones, donde existe una exposición importante de información vital para la vida política del país. En estos procesos se limita a la custodia de Fuerzas Armadas en situ y Policía Nacional, sin embargo no se utilizan medios tecnológicos para evidenciar la información física.
10. Los procedimientos de control de entrada son deficientes tanto para el control de personas como de correspondencia, así como procedimientos control de visitantes, proveedores, contratistas, etc.

4.2. Recomendaciones

1. Establecer la Política de Seguridad para el CNE, su personal, usuarios, proveedores y contratistas, en base a la declaración de la amenaza determinada, luego de haber realizado el estudio de seguridad y análisis de las diferentes amenazas y riesgos que pueden afectar al CNE.
2. Desarrollar una estructura del área de protección, la misma que tenga la capacidad de interactuar transversalmente con las unidades gerenciales y que reporte a nivel de Vicepresidencia o Presidencia, convirtiéndose en un ente asesor permanente en todas las actividades críticas.
3. Desarrollar procedimientos y considerar en el diseño de protección normas 27001: 2005 para protección de la información, poniendo énfasis en el acceso a sitios como áreas de servidores, antenas de comunicación, repetidores, procesamiento de información, etc.
4. Considerar barreras de retardo que incluyan barreras predecibles activadas, de manera que se logre la interrupción de posibles ocupaciones o ataques anarquistas.
5. Aplicar al personal, pruebas de pre-empleo, honestidad, veracidad, integridad en medida de la responsabilidad y la información que este bajo su custodia. Complementándose con capacitación en prevención de pérdidas
6. Incorporar barreras de retardo y sistemas de alarma en sitios donde existan conexiones, switches, antenas, servidores, etc. Integrándolo al sistema físico de protección

7. Generar procedimientos de Seguridad del personal, planes de respuesta, contingencia, investigación de antecedentes y estilos de vida entre otros.
8. Considerar en el desarrollo de los sistemas de protección: Operaciones satélite remotas o requeridas en tiempo de elecciones, con extensión de planes de respuesta y contingencias en caso de incidentes que pudieran presentarse.
9. Implementar tecnología en control de entrada, con identificación biométrica.
10. Considerar la implementación de tecnología para evidenciar incidentes en operaciones remotas, para que puedan ser monitoreadas.
11. Diseñar un sistema de protección física, basado en detección, retardo y respuesta, con criterios como: seguridad en profundidad, línea continua de detección, evitando fallas en los sistemas, considerando contingencias y redundancia para lograr un nivel de seguridad alto en las facilidades del CNE con planes de respuesta y contingencias, que obedezca al análisis de las diferentes amenazas.

CAPITULO V

5. PROPUESTA

DISEÑO DE UN SISTEMA DE SEGURIDAD INTEGRAL PARA EL CNE CON SEDE EN EL DMQ

5.1. Presentación

Con los lineamientos y las políticas construidas desde el nuevo enfoque de la seguridad, se promueven un grupo de lineamientos y metodologías que pretenden incluir una visión estratégica, en el entendimiento inmutable de que el ser humano es la razón de toda acción estatal y social.

Esta Planificación, construida desde un enfoque integral, refleja el accionar de un trabajo coordinado, altamente técnico, que garantice la articulación adecuada de las políticas de seguridad, en este nuevo paradigma que el Estado ecuatoriano está inmerso, poniendo énfasis en el respeto a la Constitución Política del Estado, las leyes de seguridad, y con mayor realce el plan nacional del buen vivir.

Toda entidad gubernamental, está llamada a respetar y llevar adelante procesos de calidad que involucren aspectos como: el manejo técnico y responsable de los bienes o materiales bajo su cuidado, articulación de sus acciones con las acciones de otras entidades del estado, uso adecuado de la tecnología en el procesamiento y despacho de sus actividades, responder eficientemente a los problemas o dudas que se desarrollen dentro de los momentos de su accionar. Por ende el que estas entidades cuenten con el desarrollo de procesos técnicos de calidad les permitirán de mejor manera enfrentar todo este accionar que de ellas hoy se demanda, para la paz y tranquilidad de los mandantes.

5.2. Objetivos de la Propuesta

- Reducir o minimizar los riesgos y amenazas que atentan al óptimo funcionamiento y desarrollo de las actividades del Consejo Nacional Electoral con Sede en la ciudad de Quito; y que garantice la protección y seguridad de personas, infraestructura, información, equipos y materiales.

5.3. Desarrollo de la propuesta.

Este Plan basa su desarrollo en los requerimientos de las actividades y procesos que realiza el Consejo Nacional Electoral con sede en el Distrito Metropolitano de Quito; por lo que al desarrollar el estudio de seguridad en situ, se identifican las posibles amenazas.

La identificación de Amenazas, la situación de seguridad, la vulnerabilidad de sistemas existentes y deficiencias señaladas en el estudio de seguridad, nos permite realizar el análisis de la amenaza y de la vulnerabilidad, necesarios para el desarrollo correcto del plan de seguridad integral.

5.4. Política de Seguridad Integral del CNE.

Dado que la misión y actividades que cumple el CNE., tienen una connotación de orden estratégico, se estima la necesidad de disponer de un alto nivel de seguridad, que se base en el grado de riesgos y amenazas que tiene el CNE, por ser una de las funciones del Estado, y tomando en cuenta el interés político y social que esta tiene, su seguridad se dirige a proteger a la población fija y móvil, además de las instalaciones, sus muebles e inmuebles, información y las actividades propias de la función electoral.

5.5. ANÁLISIS Y EVALUACIÓN DE RIESGOS

5.5.1. Estudio de Seguridad.

5.5.1.1. Introducción.

> *El Consejo Nacional Electoral es una de las funciones del Estado y tiene un rol muy importante en garantizar la democracia del Ecuador en elecciones seguras y transparentes, tiene como misión fundamental garantizar el ejercicio de los derechos políticos de la ciudadanía y promueve el fortalecimiento de la democracia mediante la organización de procesos electorales y apoyo a las organizaciones políticas y sociales; asegurando una participación equitativa, igualitaria, paritaria, intercultural, libre, democrática y justa para elegir y ser elegidos. (htt8)*

Se rige por las normas de la Constitución Política del Estado, la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador "Código de la Democracia", el Reglamento Interno y el Código de Ética.

5.5.1.2. Objetivos del estudio.

Identificar eventos riesgosos, que puedan afectar el normal desenvolvimiento de las actividades del CNE, utilizando un procedimiento mediante el cual se establecen,

categorizan y detallan situaciones adversas en las respectivas áreas de estudio; esto nos permitirá prever y planificar acciones que controlen y corrijan dichos eventos riesgosos; dictando una normativa cuyo fin principal sea la de capacitar al personal de seguridad (SEPRIV), población permanente y población móvil que circunda el recinto Electoral, creando un ambiente seguro en las instalaciones del CNE en la sede del DMQ.

5.5.1.3. El Grado de seguridad que deseamos imponer

Se estima la necesidad de un alto nivel de seguridad, que se base en el grado de riesgos y amenazas que tiene el CNE, por ser una de las funciones del Estado, y tomando en cuenta el interés político y social que esta tiene, su seguridad se dirige a proteger a la población fija y móvil, además de las instalaciones, sus muebles e inmuebles, información y las actividades propias de la función electoral.

5.5.1.4. Análisis del entorno.

El Consejo Nacional Electoral, mantiene su sede central en la provincia de Pichincha, en el cantón Quito, DM. Ubicado en la Avenida 6 de Diciembre N33-122 y José Bosmediano.

Límites:

- **Norte:** SERVIRECORD, asistencia técnica de equipos electrónicos, ubicado en la 6 de Diciembre N 36- 88 y José Bosmediano.
- **Sur**: EDIFICIO TORRES DEL NORTE, edificio residencial, ubicado en la Av. 6 de diciembre N 33-74.
- **Oriente**: APROFE (Asociación Pro Bienestar de la Familia Ecuatoriana), clínica de atención médica, ubicado en las calles Gral. Giacomo Roca y José Bosmediano.
- **Occidente**: Avenida 6 de Diciembre con 2 carriles de tránsito vehicular y un carril utilizado para ECOVÍA de circulación de dirección norte a sur y de la misma forma dispuesto de sur a norte, asfaltada, considerada como vía principal.

Rutas de acceso a la instalación:

Primaria: Av. 6 de Diciembre en sentido (Sur - Norte), vía de ingreso principal al CNE.
Secundaria: Calle José Bosmediano sentido oriente-occidente, vía alterna de ingreso al CNE.

5.5.1.5. Descripción de la instalación:

- El CNE, es una construcción de concreto, de material sólido y ventanales de vidrio, en la parte exterior está recubierto de alucobon que cubre el edificio en 70%, en la parte interior presenta estructuras de madera en gradas, pisos y en mayor parte en el salón de la democracia.
- La edificación se encuentra dividida en un patio central, con dos ingresos ubicados en Av. 6 de Diciembre (Ingreso Principal – Peatonal) y José Bosmediano (Ingreso secundario – peatonal y vehicular); 4 pisos y un subsuelo, en donde funcionan las diferentes direcciones, secretarias, departamentos de coordinación del CNE

5.5.1.6. Distribución de la instalación.

El CNE se encuentra dividido de la siguiente forma, partiendo desde el subsuelo:

Subsuelo:

- Cuarto de impresión, bodegas para material electoral y suministros, almacenamiento de equipos, parqueadero para personal ejecutivo.

Planta Baja:

- Puesto de guardia ingreso peatonal en la Av. 6 de Diciembre.
- Garita de ingreso de personal y vehicular en la calle José Bosmediano

Primer piso:

- Informática electoral
- Sistemas Informáticos
- Análisis y programación
- Redes

- Procesos electorales
- Voto en el exterior
- Mantenimiento equipos
- Logística y operaciones
- Geografía y registro electoral

Segundo piso:

- Presidencia
- Vicepresidencia
- Coordinación Técnica Institucional
- Sala Múltiple
- Relaciones Internacionales
- Dirección Financiera
- Almacén
- Organizaciones Políticas
- Presupuesto

Tercer piso:

- Salón del pleno
- Consejerías
- Promoción electoral
- Inventarios
- Departamento Medico

Cuarto Piso:

- Asesoría Jurídica
- Aula de capacitación
- Capacitación Cívica
- Actas
- Consejería
- CIDE
- Diseño Grafico
- Comedor Institucional

Terraza:

- Terraza con acceso permanente, que conecta al servicio de comedor.

5.5.1.7. Distribución del talento humano.

El Personal que labora en la edificación es un total de 400 empleados, 2 de ellos con capacidades especiales (físicas), una gran parte de este número es personal de contrato, que por periodo de elecciones cumplirán determinados procesos en un tiempo establecido, e inmediatamente cumplida la tarea saldrán de la institución. En elecciones presidenciales y de diferentes dignidades el Consejo Nacional Electoral realiza turnos para cumplimiento de su agenda doblando turnos, incorporando mesas de información por todo el país, por lo que el aumento de personal es representativo, quedando un número de funcionarios de planta.

La distribución del personal que labora dentro de las instalaciones del CNE se divide de la siguiente forma:

- Subsuelo: 57 funcionarios
- Planta baja: 54 funcionarios
- Primer piso: 31 funcionarios
- Segundo piso: 39 funcionarios
- Tercer piso: 34 funcionarios
- Cuarto piso: 29 funcionarios

5.5.1.8. Consideraciones internas de seguridad

Sistema de emergencia:

Energía eléctrica.- El suministro de energía eléctrica es proporcionado por la Empresa Eléctrica Quito a través de sus redes de conexión; en caso de un corte de energía el CNE cuenta con una planta de emergencia que de forma inmediata se enciende hasta que se normalice el servicio, además dispone de UPS para mantener los equipos de

informática y monitoreo de seguridad prendidos evitando daños en los equipos, perdida de información y paralización de actividades

Agua potable.- El CNE se encuentra conectado a la red de agua potable de la EPMAPS, cuenta con una cisterna de almacenamiento, para proveer de agua mientras exista un corte del servicio.

Contra incendio.- El total de extintores en las instalaciones del CNE es de 23 (21 fijos y 2 móviles), con fecha de caducidad Agosto del 2014, distribuidos de la siguiente manera:

- Garita de ingreso vehicular y peatonal: 1 extintor móvil CO_2 de 20 lbs.
- Subsuelo (Sala de impresión): 5 extintores fijos CO_2 de 10 lbs.
- Primer piso: 9 extintores fijos CO_2 de 10 lbs. y 1 extintor móvil CO_2 de 20 lbs.
- Segundo piso: 3 extintores fijos CO_2 de 10 lbs.
- Tercer piso: 2 extintores fijos CO_2 de 10 lbs.
- Cuarto piso: 2 extintores fijos CO_2 de 10 lbs.
- En la parte exterior del CNE, una bocatoma de agua ubicada, en la Av. 6 de Diciembre.
- Subsuelo donde se encuentra la caja de brakers eléctricos y la bodega de materiales, un gabinete contra incendios fuera de funcionamiento.

Escalera de emergencia.- Cuenta con una escalera de emergencia fuera de norma por no cumplir con las dimensiones adecuadas (65cm del ancho de descanso), ubicada en la parte trasera del edificio, cerca del auditorio. No existe señalización que indique la ubicación de la escalera de emergencia

Salidas y puerta de emergencia.- No cuenta con salidas ni puertas de emergencia.

Ascensor.- El CNE posee un ascensor que es utilizado exclusivamente como montacargas para transporte de alimentos, al comedor.

Electricidad.- El CNE cuenta con el panel de energía y caja de brakers central localizada en el subsuelo, posee a su vez en cada piso las cajas de interruptores manuales para cortar la iluminación de las diferentes áreas.

5.5.1.9. Sistema de control interno.

Personas.- Toda persona que ingresa al CNE, en calidad de empleado o visitante debe pasar la primer línea de seguridad que se encuentra en la entrada principal de la Av. 6 de Diciembre que funciona hasta las 18H00, sitio donde se ubica una área de seguridad con dos vigilantes de seguridad, quien controla el acceso al CNE previa identificación, a partir de las 18H00 el control para ingreso de personas se realiza en el ingreso de la Bosmediano, con un puesto vigilancia.

Empleados.- Los Empleados del CNE registran su entrada y salida del edificio en un Biométrico implementado por el Departamento de Recursos Humanos.

Visitas.- Para el ingreso de visitantes el agente de seguridad solicitara una identificación, y a cambio entregara una tarjeta de visitante en la que consta a que piso se dirige.

Correspondencia.- La correspondencia es revisada en la recepción, se le entrega una tarjeta de visitante al mensajero y este se dirige al piso correspondiente únicamente con el sobre o la encomienda. Se cuenta con un intercomunicador o teléfono de extensiones a las oficinas para confirmar la autorización de ingreso de correspondencia.

5.5.1.10. Consideraciones externas del lugar.

Accesos con que cuenta la instalación:

Fotografía Nº 1 Entrada principal

Fuente: Jorge Oswaldo Muñoz Rivadeneira

Principal: Av. 06 de Diciembre, ingreso peatonal, entrada principal al CNE que funciona desde las 7H00 hasta las 18H00.

Fotografía Nº 2 Entrada secundaria

Fuente: Jorge Oswaldo Muñoz Rivadeneira

Secundario: Calle José Bosmediano, ingreso vehicular y peatonal a partir de las 18H00.

Emergencia: No existe.

Área de ingreso y evacuación: No existe áreas de evacuación, salidas de emergencia y puntos seguros en las instalaciones del CNE.

Topografía:

- Se observarán las características topográficas del lugar, es decir las fortalezas y vulnerabilidades de la zona (ubicación, centros de educación, bancos, etc.), que rodean el CNE.
- Es importante conocer que por ser considerado un sector comercial y negocios, muchas de las edificaciones cuentan con seguridad privada, lo que ayuda a mantener un nivel medio de seguridad.
- Entre las características del terreno podemos encontrar en su mayoría edificios, parqueaderos, y pocas viviendas que han sido adecuadas para el funcionamiento de locales comerciales alrededor del CNE.
- Con la falta de espacio físico suficiente y sin contar con un parqueadero subterráneo ha llevado a utilizar la calle José Bosmediano en ambos sentidos como sitios de parqueo incluyendo la guardianía privada informal de dos personas que desarrollan esta actividad sin dependencia laboral a ninguna empresa de seguridad privada, lo que ocasiona dificultades para la circulación de vehículos y peatonal; por esta misma razón a ciertas horas del día se puede observar congestión vehicular. Es importante destacar que estos factores influyen en el cometimiento de delitos como robo de accesorios de vehículos y el asalto y robo a peatones en las inmediaciones del CNE.
- Se debe considerar la posibilidad de la colocación de señalización indicando: Señalización vial (letreros, señalización horizontal y vertical), Sitios de parqueo, y mayor control por parte del servicio de Transito de la Policía Nacional.

5.5.1.11. Áreas inmediatas.

A. BANCO BOLIVARIANO Entidad que presta diferentes servicios bancarios a la comunidad el sector, ubicado en la calle José Bosmediano E 11-9 y General Roca. La empresa PRISEGUR CIA. LTDA. está a cargo de la seguridad inmediata, con dos vigilantes.

B. APROFE: Institución ecuatoriana de derecho privado, sin fines de lucro que atiende a la población en el área de la salud y planificación familiar, edificio que funciona en la calle Gral. Giacomo Roca N 33-165 y José Bosmediano; La empresa SERMONSEG CIA. LTDA. está a cargo de la seguridad inmediata, con un vigilante.

C. FARMACIAS NAVARRETE: Venta de medicinas para la comunidad del sector, ubicada en la Av. 6 de Diciembre N 33-95.

D. SERVIENTREGA: Empresa encargada de entrega y envío de correspondencia, ubicada en la Av. 6 de Diciembre N 35-81.

E. EDESA: Distribuidora de cerámica y baños Edificio esquinero entre la Av. 6 de Diciembre y Eloy Alfaro. La empresa VIGAR CIA. LTDA. está a cargo de la seguridad inmediata, con un vigilante.

F. ESTACIÓN ECOVÍA BELLAVISTA: Servicio de transporte público que se conecta al norte hasta la Estación Río Coca y al Sur a la Estación de la Marín e incluso a la Estación Quitumbe. La empresa SEGRES CIA. LTDA. está a cargo de la seguridad inmediata, con un vigilante

G. EDIFICIO TORRES DEL NORTE: Edificio residencial, en la planta baja cuenta con un minimarket y dos tiendas con el servicio de cabinas telefónicas e Internet, ubicado en la Av. 6 de diciembre N 33-74. La empresa ROJAS Y PAREDES CIA. LTDA. está a cargo de la seguridad inmediata, con un vigilante.

H. EDIFICIO TITANIUM: Funcionan Seguros "Constitución" y ASISTA.MED (atención médica primaria), ubicado en la Av. 6 de diciembre N 33-42. La empresa SEGRES CIA LTDA está a cargo de la seguridad inmediata, con cuatro vigilantes.

I. EDIFICIO MONASTERIO PLAZA: Edificio comercial, ubicado en la Av. 6 de diciembre y Av. Eloy Alfaro N 21-29. La empresa TECNISEGURITY CIA. LTDA. está a cargo de la seguridad inmediata, con tres vigilantes.

J. EDIFICIO TORRE SUIZA: Funciona centro médico BIODIMED (Urgencias médicas ambula), ubicado en la Av. Eloy Alfaro N 33-109. La empresa SEGUGIC CIA. LTDA. está a cargo de la seguridad inmediata, con tres vigilantes

K. ALIANZA FRANCESA: Centro cultural y de enseñanza de francés, ubicado en la Av. Eloy Alfaro N32-468 y Bélgica. La empresa LAAR CIA. LTDA. está a cargo de la seguridad inmediata, con tres vigilantes.

L. CENTRO INFANTIL DEL BUEN VIVIR MANUELA CAÑIZARES: Guardería que ofrece cuidado y educación a niños de bajos recursos económicos, ubicado en la calle Ignacio Bossano E10-96. La empresa IRVIN CIA. LTDA. está a cargo de la seguridad inmediata, con dos vigilantes.

M. CLÍNICA SANTA LUCIA: Especialidades médicas, ubicada en la Av. Eloy Alfaro y Suiza 209. La empresa MACETOVI CIA. LTDA. está a cargo de la seguridad inmediata, con tres vigilantes.

N. SISTEMAS MEDICOS DE LA UNIVERSIDAD SAN FRANCISCO DE QUITO: Clínica de especialidades médicas, ubicada en la calle Noruega y Suiza 210. La empresa ECUASPARTAN CIA. LTDA. está a cargo de la seguridad inmediata, con un vigilante.

Gráfico Nº 54 Áreas inmediatas

Fuente: Google Earth

5.5.1.12. Áreas con mayor influencia delictiva cercanas al CNE.

En el sector se han registrado varios casos de secuestro exprés, robos de vehículos y asaltos a personas; la Unidad de Policía Comunitaria (UPC) de Bellavista que pertenece al Circuito Iñaquito, "ha realizado una investigación georeferencial, que permite saber cómo funciona el delito en el sector. Gracias a esto se ha determinado que la mayoría de robos se producen entre la Eloy Alfaro y 6 de Diciembre, principalmente los viernes de 17:00 a 21:00." (HORA)

Información proporcionada por la Jefatura de la Policía Judicial con el índice y categoría de Criminalidad de los meses Enero a Diciembre del 2012.

Inseguridad

Puntos conflictivos

Av. Eloy Alfaro y Portugal

Av. González Suárez

Av. Colón y 6 de diciembre

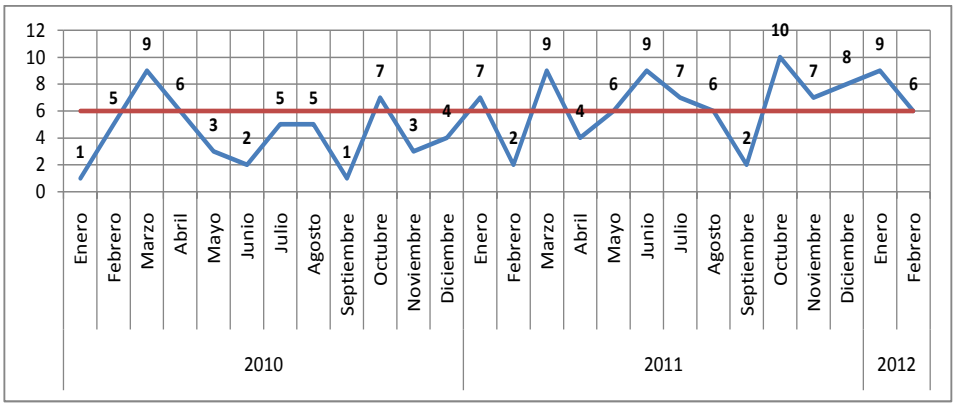
Av. Eloy Alfaro y 6 de diciembre

Diego de Almagro, entre Whimper y Alpallana

Reporte estadístico denuncias de delitos cometidos en las inmediaciones del CNE.- Para efectos del presente análisis se tomaron en cuenta las denuncias de delitos ocurridos dentro de un radio de 200 metros desde la intersección de la Av. 6 de diciembre y Bosmediano.

Es importante indicar que, no se presentan cifras correspondientes a las variables robo total del automotor ni muertes por causas externas.

Gráfico Nº 55 Denuncias por delitos contra la propiedad y las personas en las inmediaciones del CNE Comportamiento por mes Enero 2010 a Febrero 2012



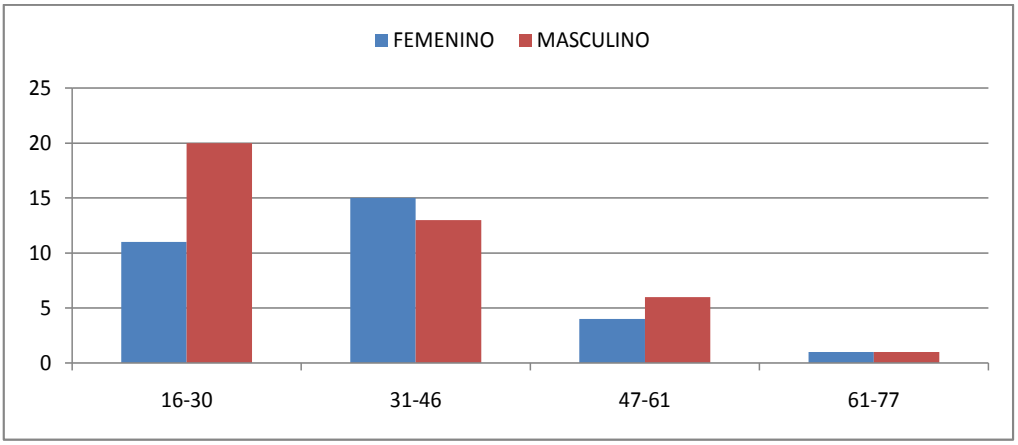
Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Tabla Nº 49 Denuncias por delitos contra la propiedad y las personas en las inmediaciones del CNE Comportamiento por mes Enero 2010 a Febrero 2012

Mes	Frecuencias			Variación			
				Absoluta		Porcentual	
	Año 2010	Año 2011	Año 2012	2010 -2011	2011 - 2012	2010 -2011	2011 - 2012
Enero	1	7	9	6	2	600,0%	28,6%
Febrero	5	2	8	-3	6	-60,0%	300,0%
Total general	6	9	17	3	8	50,0%	88,9%

Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Gráfico Nº 56 Denuncias por delitos contra la propiedad y las personas en las inmediaciones del CNE según edad y sexo



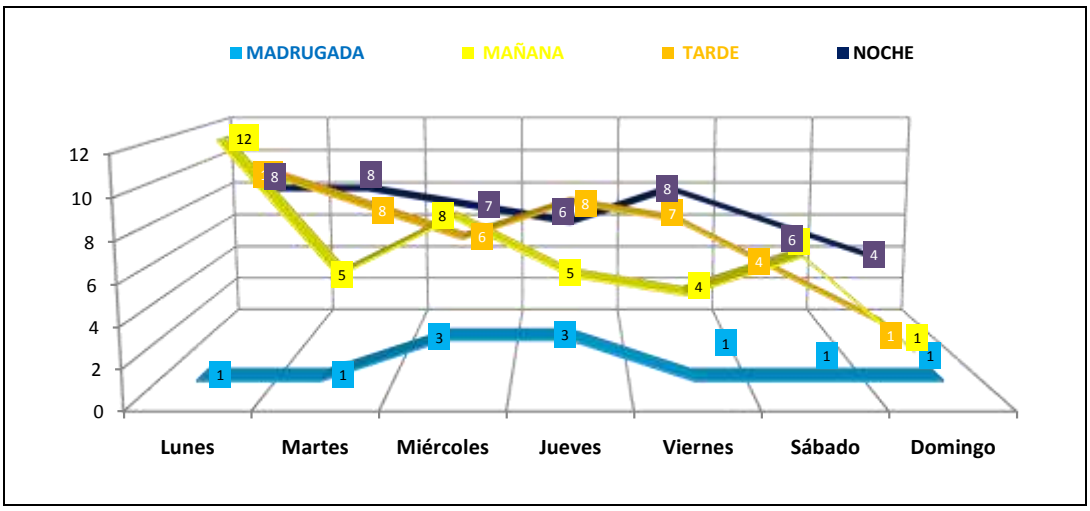
Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Tabla Nº 50 Denuncias por delitos contra la propiedad y las personas en las inmediaciones del CNE por afectado 2011, 2012 y Enero a Febrero 2013

AFECTADOS	2011	2012	A Febrero 2013
DOMICILIOS	2	4	4
EMPRESAS	5	12	5
ENTIDAD PÚBLICA		2	2
PERSONAS	44	60	6
Total general	51	78	17

Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Gráfico Nº 57 Denuncias por delitos contra la propiedad y las personas en las inmediaciones del CNE según día y horario de ocurrencia 2011, 2012 y Enero a Febrero 2013



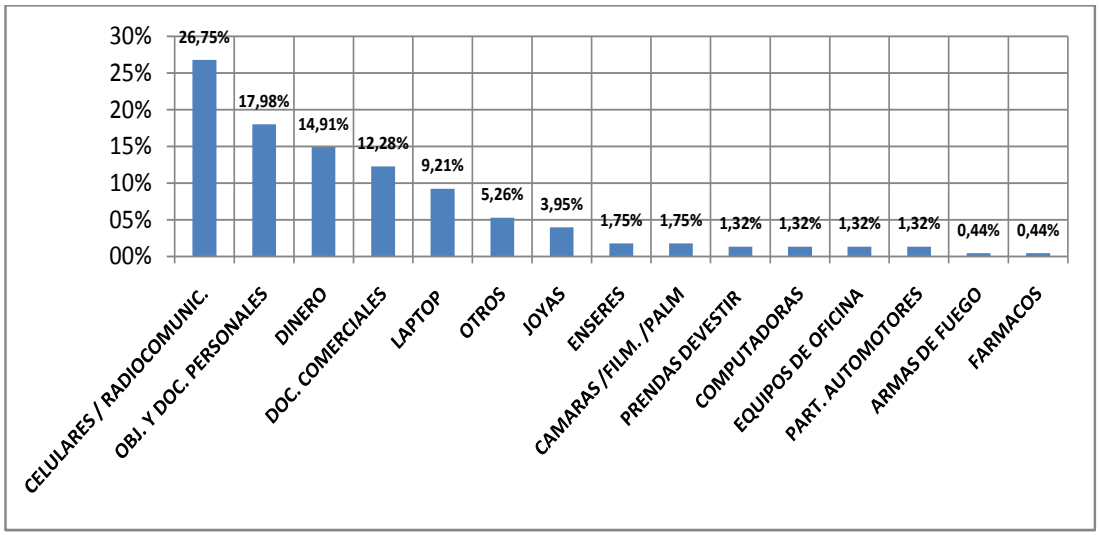
Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Tabla Nº 51 Denuncias por delitos contra personas en las inmediaciones del CNE según Tipo de delito 2011, 2012, a Febrero 2013

TIPO DE DELITO	2011	2012	A Febrero 2013
ASALTO Y ROBO	22	30	2
ROBO	14	25	2
HURTO	8	5	
Total general	44	60	4

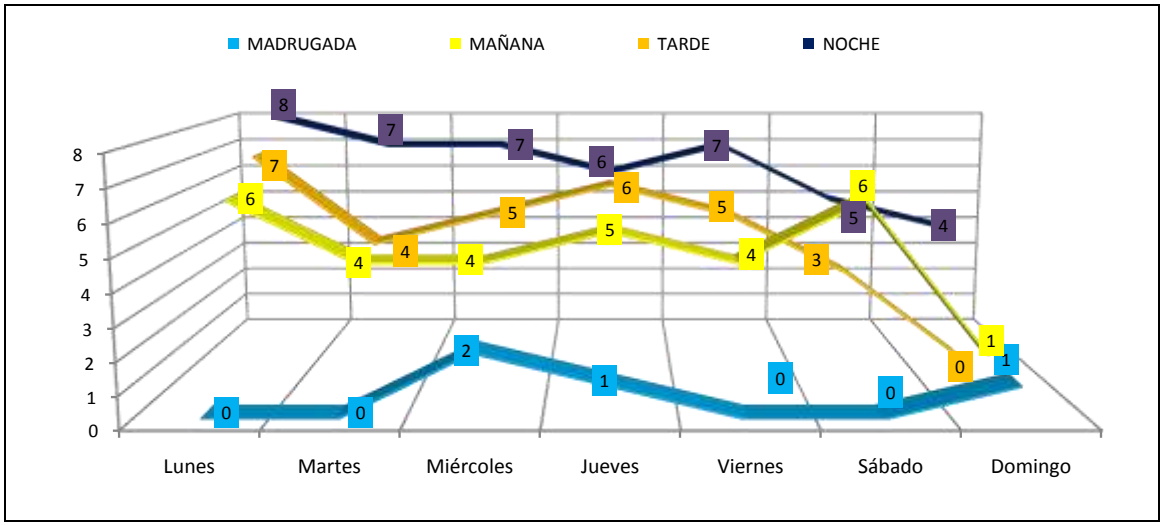
Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Gráfico Nº 58 Denuncias por delitos contra personas en las inmediaciones del CNE según objeto delinquido 2011, 2012 y Enero a Febrero 2013



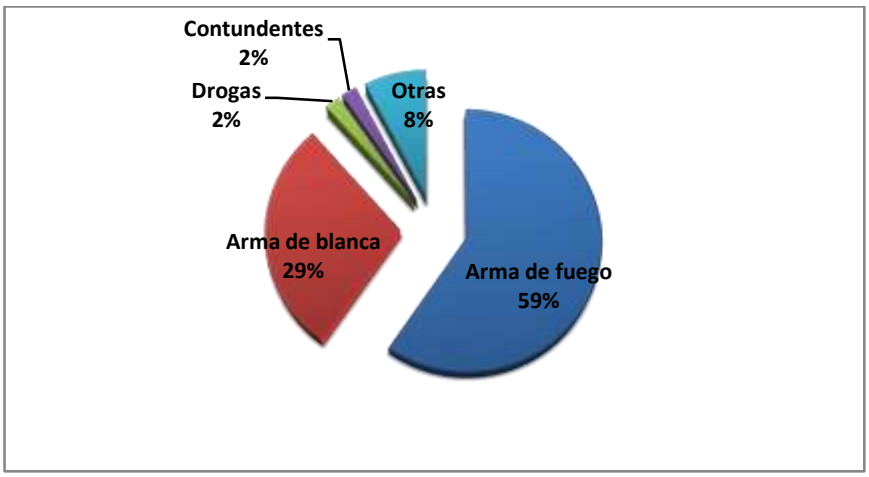
Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Gráfico Nº 59 Denuncias por delitos contra personas en las inmediaciones del CNE según día y horario de ocurrencia 2011, 2012 y Enero a Febrero 2013



Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

Gráfico Nº 60 Denuncias por delitos contra personas en las inmediaciones del CNE según día arma utilizada 2011, 2012 y Enero a Febrero 2013



Fuente: Fiscalía general del Estado
Desarrollado por: Observatorio Metropolitano de Seguridad Ciudadana

El riesgo es la probabilidad de que suceda un daño, es decir el personal de seguridad deberá estar atento y altamente capacitado para solventar cualquier situación que atente contra la seguridad de las personas o bienes del CNE, entonces nuestra tarea es la de disminuir el riesgo al que se encuentran expuestos personas, bienes e información.

5.5.1.13. Barreras de seguridad de la instalación:

Naturales:

- No existen

Artificiales:

- Muro de piedra combinado con alambrado eléctrico que cerca el perímetro del CNE, con una altura de 2,40 metros en la parte frontal que da a la Av. 6 de Diciembre y en la calle José Bosmediano, con una altura de 4,30 metros de altura aproximadamente.

Fotografía Nº 3 Muro de piedra entrada principal

Fuente: Jorge Oswaldo Muñoz Rivadeneira

Fotografía Nº 4 Muro de piedra combinado con cerca eléctrica

Fuente: Jorge Oswaldo Muñoz Rivadeneira

- En la entrada principal el CNE presenta una puerta metálica de aproximadamente 2,13 metros.

Fotografía Nº 5 Entrada principal puerta metálica

Fuente: Jorge Oswaldo Muñoz Rivadeneira

Humanas:

La empresa SEPRIV Cía. Ltda. es la encargada del control de accesos e ingreso de los predios de la institución para este fin se dispone de siete vigilantes de seguridad y supervisor en el horario de 06H30 a 18H00 de lunes a viernes, ubicados como se detalla:

- 2 Vigilantes de seguridad en el ingreso peatonal (Av. 6 de Diciembre).
- 1 Vigilante de seguridad en el ingreso vehicular (calle José Bosmediano).
- 1 Radio Operador en Sala de Monitoreo (primer piso).
- 1 Vigilante de seguridad en la puerta de ingreso de presidencia (segundo piso).
- 1 Vigilante de seguridad en el hall del tercer piso.
- 1 Vigilante de seguridad de Ronda.
- 1 Vigilante de seguridad en fiscalización

En la noche se reduce a cuatro vigilantes de seguridad en el horario de 18H30 a 06H30; y los fines de semana cuenta con cuentan con total de 4 vigilantes de seguridad, ubicados como se detalla:

- 1 Vigilante de seguridad en el ingreso vehicular y peatonal (calle José Bosmediano).
- 1 Radio Operador en la Sala de Monitoreo (primer piso).
- 2 Vigilantes de seguridad de Ronda.

Sistemas técnicos:

- Cuenta con un sistema de CCTV que cubre pasillos y áreas consideradas restringidas.

Las 30 cámaras que dispone el CNE se encuentran distribuidas de la siguiente manera:

- Tres cámaras IP en digitación
- Dos cámaras PTZ y ocho cámaras IP en el auditorio

- Dos cámaras IP en el ingreso al auditorio
- Dos cámaras IP en el pasillo del segundo piso
- Dos cámaras IP en el pasillo del tercer piso
- Una cámara IP ubicada en Recursos humanos
- Una cámara IP en la entrada principal
- Una cámara IP en el área de comunicación social
- Una cámara IP ubicada en el ingreso del edificio central
- Una cámara IP en presidencia
- Una cámara IP en el ingreso principal a Presidencia
- Una cámara IP ubicada en el ingreso al parqueadero interno en el subsuelo
- Una cámara IP en procesos electorales
- Una cámara IP en el ingreso a Sistemas
- Dos cámaras IP en el área perimetral en la Av. 6 de Diciembre y José Bosmediano.
- Sistema de seguridad informática que cuenta con protecciones lógicas y físicas con el fin de proteger la integridad, disponibilidad, control de cambios y confidencialidad de la información.
- Protecciones lógicas: firewall, antivirus, programa de encriptación y respaldo periódico.
- Protecciones físicas: control de accesos, cámaras de seguridad y extinción automática de incendios en el centro de datos.
- Sistema de alarma de señal de incendios ubicada en la sala de monitoreo que se activa mediante censores de humo ubicados en presidencia, informática departamento médico, subsuelo, procesos electorales, geografía y registro electoral, auditorio, comedor y generador eléctrico.

5.5.1.14. Ubicación de los servicio de emergencia.

UNIDADES POLICIALES.

Unidad de Policía Comunitaria "Bellavista".- Ubicada en Calle Diego de Brieda y Camilo Casares, referencia junto al Centro Salud Bellavista, teléfono de contacto 023331516. Cuenta con el siguiente personal y equipo:

2 Patrulleros Vehiculares (camionetas)

5 Motorizados que prestan servicios en horario de 07H00 a 20H00

Nómina de Personal: un oficial y nueve policías

BOMBEROS.

Estación Nº 13 Parque Metropolitano.- Ubicada en Mariano Calvache y Lorenzo Chávez (Batán Alto) teléfono 3332 330.

Equipamiento:

Personal: **15**

Autobomba: **1**

Tanquero: **1**

Camioneta: **1**

CENTROS ASISTENCIALES:

Centro de salud de "Bellavista".- Atención medica primaria, ubicada en calle Diego de Brieda y Camilo Casares en horario de 08H00 a 17H00 de lunes a viernes.

APROFE.- Atención a la población en el área de la salud y planificación familiar, edificio que funciona en la calle Gral. Giacomo Roca N 33-165 y José Bosmediano, teléfono 2440 440 / 2452 060.

Clínica Pasteur.- Atención médica, ubicada en la Av. Eloy Alfaro 552 e Italia, teléfono 2992 400.

Hospital Metropolitano.- Atención médica, ubicada en la Av. Mariana de Jesús y Nicolás Arteta, teléfono 3998 000 / 2269824.

Hospital de la Policía.- Atención médica, ubicada en la Av. Mariana de Jesús y Occidental, teléfono 224 7478 / 224 7488 / 224 7491

Asistencia Pública Hospital "Eugenio Espejo".- Ubicada en Av. Gran Colombia y Piedrahita, teléfono 2565 949 (Caso de Emergencia).

Cruz Roja Ecuatoriana, ubicada en la Av. 6 de Diciembre y Av. El Inca, teléfono 2416514 / 2404696 / 2413864.

Gráfico Nº 61 Ubicación de servicios de emergencia

Fuente: Google Earth

UNIDADES POLICIALES:

CASAS DE SALUD.

BOMBEROS.

CONCEJO NACIONAL ELECTORAL

CRUZ ROJA ECUATORIANA

5.5.1.15. Análisis del estudio de seguridad

El estudio de seguridad aplicado en las facilidades del CNE, permite determinar las amenazas existentes, la situación de seguridad, la vulnerabilidad y deficiencias de sistemas existentes; la valoración de estos aspectos permiten realizar el siguiente análisis de la amenaza:

Análisis de la amenaza.

Luego de establecer la probabilidad de que delincuencia común, crimen organizado, organizaciones políticas o sociales antagónicas o terroristas intenten desarrollar acciones violentas o subrepticias, obligan a que sea necesario desarrollar estrategias para estas condiciones adversas para la protección de personas, bienes e información, por lo que se deben plantear todos los posibles escenarios acerca de las intenciones y capacidades de los adversarios identificadas en el presente análisis.

El estudio de las capacidades e intenciones de potenciales adversarios proporciona los fundamentos para estos escenarios que se los plantea en base a la experiencia de los técnicos de protección, posibles experiencias históricas, el medio ambiente político, el medio ambiente físico, entre otros.

Enunciado de la amenaza

Considerando que el CNE, es la Institución que representa la democracia en el País y que por la naturaleza competitiva y los intereses contrapuestos en disputa de las elecciones, presentarían una serie de amenazas en contra de procesos electorales transparentes y eficientes. El CNE enfrenta amenazas que pueden ir desde pequeños disturbios hasta atentados a sus instalaciones e información, así como a funcionarios, contratistas y proveedores.

La información es el activo más crítico y por lo tanto los sistemas de procesamiento, almacenamiento, distribución y tecnologías de la comunicación, podrían ser atentados con ciberataques.

La gamma de adversarios va desde grupos antagónicos, delincuencia común, crimen organizado con intereses transnacionales que para cumplir con sus objetivos están en la capacidad una serie de operaciones de alto nivel tecnológico y cibernético.

Tabla Nº 52 Matriz de Amenazas

AMENAZAS	PROBABILIDAD		
	ALTA	MEDIA	BAJA
OCUPACIONES DISTURBIOS CIVILES (INSTALACIONES)		X	
ROBOS A LA PROPIEDAD (BIENES)		X	
ATENTADOS, CRÍMENES, EXTORSIONES, SECUESTROS (PERSONAS)			X
ROBO, DESTRUCCÓN, INTERCEPTACIÓN	X		

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 53 Matriz de Adversarios y Capacidades

POSIBLES ADVERSARIOS	CAPACIDADES				
	HERRAMIENTAS	ARMAS BLANCAS	ARMAS DE FUEGO	EQUIPOS DE COMUNICACIÓN	TECNOLÓGICAS
GRUPOS ANTAGÓNICOS	X	X	X		
CRIMEN ORGANIZADO	X	X	X	X	X
DELINCUENCIA COMÚN	X	X	X		

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Evaluación de vulnerabilidad

Se ha utilizado la siguiente escala que permite determinar la vulnerabilidad existente:

Alta: Se han identificado una o varias debilidades principales que hacen que los activos sean extremadamente susceptibles ante un agresor o peligro.

Media: Se ha identificado una debilidad que hace que el activo sea bastante susceptible ante un agresor o peligro.

Baja: Se ha identificado una debilidad menor que aumenta levemente la susceptibilidad del activo ante un agresor o peligro.

Tabla Nº 54 Matriz de Vulnerabilidades

VULNERABILIDADES	VALORACIÓN		
	ALTA	MEDIA	BAJA
OCUPACIONES DISTURBIOS CIVILES (INSTALACIONES)	X		
ROBOS A LA PROPIEDAD (BIENES)		X	
ATENTADOS, CRÍMENES, EXTORSIONES, SECUESTROS (PERSONAS)	X		
ROBO, DESTRUCCÓN, INTERCEPTACIÓN DE (INFORMACIÓN)		X	

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Matriz de Riesgos

Se ha establecido para el impacto una escala lingüística de 3 niveles, que son:

- **Impacto alto:** La pérdida o daño de los activos, personas e información tendría consecuencias graves excepcionales, como pérdida de vida de gran propagación,

lesiones graves de gran alcance o pérdida total de información, servicios primordiales, procesos centrales y funciones.

- **Impacto medio**: La pérdida o daño de los activos, información personas tendría consecuencias moderadas a graves, como lesiones o deterioro de funciones y procesos centrales.
- **Impacto bajo:** La pérdida o daño de los activos y personas o información tendría consecuencias moderadas, como lesiones de menor gravedad o deterioro de menor seriedad de funciones y procesos centrales.

Al determinar la posibilidad o probabilidad de incidencia de una amenaza. La probabilidad de impacto no se basa en certeza matemática, es la consideración de la probabilidad de que un evento de riesgo de pérdida pueda ocurrir en el futuro, con base en datos históricos del lugar, la historia de eventos parecidos en instalaciones similares, la estructura de la comunidad y comunidad inmediata, ubicación general geográfica, condiciones políticas y sociales, cambios en la economía y algún otro factor que podría afectar el que una amenaza pudiera ocurrir, con la siguiente escala a criterio del Equipo Consultor:

- **Probabilidad baja:** Existen pocas posibilidades de que suceda en los próximos 3 a 5 años posteriores.
- **Probabilidad media:** Existe la probabilidad de que suceda de 1 a 3 años posteriores.
- **Probabilidad alta:** Existe la probabilidad de que suceda en el transcurso del próximo año posterior.

Tabla Nº 55 Matriz de Impacto Probabilidad

PROBABILIDAD	IMPACTO EN LA COMUNIDAD		
	ALTO	MEDIO	BAJO
ALTA	ROBO, DESTRUCCIÓN, INTERCEPTACIÓN DE (INFORMACIÓN)		
MEDIA	ROBOS A LA PROPIEDAD (BIENES)	OCUPACIONES DISTURBIOS CIVILES (INSTALACIONES)	
BAJA	ATENTADOS, CRÍMENES, EXTORSIONES, SECUESTROS (PERSONAS)		

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Matriz de recomendaciones de manejo de riesgos

La siguiente matriz, refleja las recomendaciones de Administración de Riesgos, basada en el Impacto y la Probabilidad de los mismos, lo que permite priorizar el manejo de los riesgos.

Tabla Nº 56 Matriz de Recomendaciones Manejo de Riesgos

PROBABILIDAD	IMPACTO EN LA COMUNIDAD		
	ALTO	**MEDIO**	**BAJO**
ALTA	• Prevenir el riesgo controlando su causa y consecuencia. • Mitigar el riesgo implementando controles. • Implementar un programa de Protección.		
MEDIA	• Mitigar el riesgo implementando controles.	• Mitigar el riesgo implementando controles	
BAJA	• Prevenir el riesgo evitando su causa y consecuencia. • Limitar el riesgo implementando controles.		

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 57 Matriz de análisis de riesgos con el método “Mósler”

LOCACIÓN / INSTALACIÓN		CNE											
No.	Criterio Riesgo	Función	Sustitución	Importancia del Suceso	Profundidad	Extensión	Daños	Agresión	Vulnerabilidad	Probabilidad	Carácter del Riesgo	Cuantificación Riesgo	Interpretación
1	Amenaza Bomba/Paquete sospechoso	5	4	20	5	4	20	3	4	12	40	**480**	**Reducido**
2	Ataque armado/Acción Violenta	4	4	16	2	3	6	3	2	6	22	**132**	**Muy Reducido**
3	Manifestaciones y disturbios civiles	5	4	20	4	3	12	5	3	15	32	**480**	**Reducido**
4	Espionaje	5	4	20	5	5	25	3	5	15	45	**675**	**Normal**
5	Fraude	2	1	2	2	2	4	4	2	8	6	**48**	**Muy Reducido**
6	Sabotaje	5	5	25	5	5	25	4	3	12	50	**600**	**Normal**
7	Robo de información	5	4	20	5	4	20	4	5	20	40	**800**	**Elevado**
8	Secuestro	5	4	20	5	4	20	4	4	16	40	**640**	**Normal**
9	Riesgos laborales	3	2	6	3	2	6	2	2	4	12	**48**	**Muy Reducido**
10	Incendio	5	5	25	5	4	20	4	5	20	45	**900**	**Elevado**
11	Extorsión	4	2	8	3	3	9	3	2	6	17	**102**	**Muy Reducido**
13	Sismo	4	3	12	3	3	9	4	3	12	21	**252**	**Reducido**
												430	**Reducido**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Conclusión

El análisis de riesgos, de la metodología MOSLER, de acuerdo a la ponderación de los diferentes riesgos le da un nivel de riesgo reducido a la Sede del Consejo Nacional Electoral.

La mayor cantidad de riesgos se encuentran en los rangos de 2 a 250 (Muy Reducido) y 251 – 500 (Reducido), por lo que la ocurrencia de estos riesgos podrian ser manejables, excepto las consecuencias o daños a la imagen del CNE y que afectarian gravemente no solo a la institución sino a todo un país al vulnerarse la seguridad y transparencia de un proceso electoral, entre estos riesgos está el espionaje con un nivel de riesgo normal, robo de información con un nivel de riesgo elevado y sabotaje con un nivel de riesgo normal; estos riesgos son planificados y efectuados por grupos con intereses particulares dentro de un proceso electoral.

La evaluación de los riesgos a través de un método cuantitativo y cualitativo como el de Mósler permite priorizar adecuadamente las medidas de protección para los riesgos con mayor impacto y profundidad.

El riesgo de mayor valoración es el de incendio con un valor de 900, por las pérdidas y consecuencias que dejarían como resultado, en vista de esto es necesario adoptar medidas técnicas activas de prevención como detectores de humo, extintores, alarmas de incendio, cámaras de video, hidrantes externos, sistema hídrico contra incendios y medidas técnicas pasivas como puertas contra fuego, cajas para protección de equipo sensible; y la conformación de equipos y medios de respuesta mediante la conformación de Brigadas de Emergencias. El CNE no dispone de medidas ni medios suficientes para evitar este riesgo por lo que existe una alta probabilidad de que este ocurra ocasionado grandes perjuicios, afectando a la continuidad de las actividades.

En el área de sistemas el riesgo de robo de información es elevado con una valoración de 800, debido a los problemas registrados con la venta de bases digitales del padrón electoral, el cual llevo al CNE, a una temporada de críticas disminuyendo notablemente su credibilidad como el organismo rector de la democracia del país, por lo que es necesario fortalecer las medidas de protección tanto internas como externas a través

de firewalls, mejora de procesos de codificación, contraseñas de alto grado seguridad, encriptación de mensajes e información, procedimientos de almacenamiento y respaldo de la información, debido a lo sensible y confidencial de la misma.

El riesgo de secuestro tiene una clasificación de normal con una valoración de 640, por lo que se debe mantener en un perfecto estado de funcionamiento de los sistemas electrónicos de seguridad y la capacitación del personal de seguridad como a los funcionarios en el conocimiento de las medidas preventivas de seguridad personal.

5.6. MEDIDAS DE PROTECCIÓN

5.6.1. Sistema de protección física integrado

5.6.1.1. Objeto.

Establecer un sistema de protección de medidas físicas integradas con el propósito de prevenir, controlar, verificar posibles intrusiones, ocupaciones, robos, hurtos, sabotajes, y detectar de manera oportuna posibles ataques y poder evidenciar la acción de adversarios, permitiendo que a través de una adecuada comunicación se pueda coordinar la respuesta oportuna y eficaz de los cuerpos de seguridad destinados para este efecto y poder interrumpir y/o neutralizar la acción de adversarios evitando un enfrentamiento violento.

5.6.1.2. Determinación de objetivos de protección.

Los objetivos de Protección que se han determinado:

1. Instalaciones del CNE ubicadas en Av. 6 de Diciembre N33-122 y José Bosmediano
2. Activos del área informática, tecnología y comunicaciones
3. Procesamiento, almacenamiento, disponibilidad de información crítica.
4. Procesos críticos de logística de actividades electorales
5. Talento Humano y Personal con manejo de información privilegiada.

5.6.1.3. Funciones del sistema físico integrado de protección.

Las Funciones del sistema de protección física, son detección de un adversario malévolo, retardo de la acción del adversario malévolo y la interrupción de la acción del adversario a través de la respuesta que debe procurar la neutralización.

Sin embargo el diseño de las facilidades, la integración de componentes externos como cámaras PTZ y otros elementos de protección visibles podrán disuadir la acción de adversarios.

Detección.

La Detección es la posibilidad de descubrir la acción de un adversario, esta puede realizarse a través de varios elementos entre estos sistemas de alarma, cámaras, sensores, detección por videos, estas alarmas deben ser evaluadas para evitar reacción frente a eventos que pueden no ser reales, por lo que el monitoreo de los sistemas es básico que se lo realice a través de un Centro de Control de Manejo de Incidentes, el cual está conformado por personal con un adecuado entrenamiento en monitoreo con el fin de lograr una adecuada evaluación para la coordinación de la respuesta. En este caso específico se establece los siguientes elementos integrados para cumplir con la función de detección.

1. Cámaras fijas ubicadas en accesos. Especificaciones cámaras día y noche integrados con iluminación infrarroja, de 1.3 a 5 mega pixeles, comprensión de video mínimo MJPEG, ideal H264.
2. Cámaras fotográficas integradas para control de velocidad, con equipo integrado por ECU 911.
3. Cámaras móviles ubicadas como redundancia y respaldo de cámara fijas para cobertura del área perimetral. Especificaciones cámaras de 1.3 mega pixeles, de 23 a 35x de zoom, IR, día y noche, comprensión de video MJPEG, H264.
4. Sistemas de alarma integrados con cerca eléctrica existente en perímetro. Se establece la integración de pánicos inalámbricos para guardias del perímetro y botones de pánico en recepción y escritorios de funcionarios principales. Estos

sistemas deben tener comunicación GPRS, GSM, integrada a un panel de control (receptora de alarmas) en el centro de control ECU911.

5. Implementar Iluminación blanca (LED) o vapor de mercurio en: perímetros accesos, parqueaderos.

Retardo (demora).

La Demora o el retardo consiste en establecer una serie de barreras a fin de que haga que los adversarios requieran de un tiempo adicional para lograr sus objetivos, Se establece las siguientes barreras:

1. Rompe velocidades en las calles laterales integrados con cámaras fijas, para poder identificar vehículos que puedan utilizar posibles adversarios.
2. Instalar control del ingreso electrónico en la segunda línea de defensa puertas de (paredes propias del edificio), integradas con cámaras fijas para verificación.
3. Instalar puertas de control automáticas reforzadas en acceso parqueadero y acceso principal.
4. Reforzar puertas de segunda línea de defensa, incluyendo paredes colaterales y jambas.
5. Reforzar ventanas de primeros pisos (PB-1) con rejas interiores, integradas con sensores de rotura de cristal y sensores electromecánicos.

Respuesta.

La función de respuesta consiste en acciones realizadas por elementos de (Fuerza pública o privada) para evitar el éxito del adversario. La respuesta como se emplea aquí, consiste en la interrupción y/o neutralización de la acción del adversario.

Interrupción se define como un número suficiente de personal de la fuerza de respuesta que llega a una ubicación específica para detener el progreso del adversario. Es importante la comunicación con la fuerza de respuesta, desde un centro de monitoreo con información precisa en relación a las acciones del adversario y el despliegue de la fuerza de respuesta, jugando un papel importante el monitoreo y verificación por video.

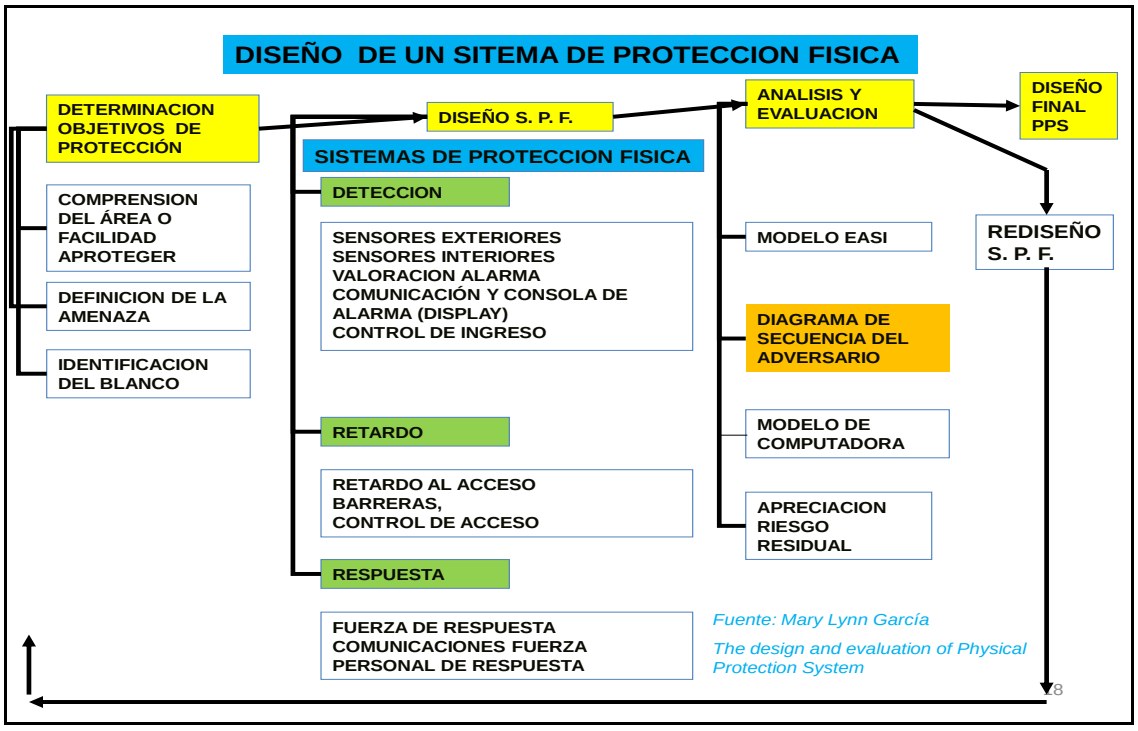
La efectividad de la respuesta dependerá de:

1. El tiempo entre la recepción de la comunicación hacia la fuerza de respuesta referente al inicio de ataque o de la acción del adversario.
2. El tiempo de traslado hasta el sitio de ataque y la interrupción o neutralización.
3. La posibilidad de interrupción del ataque del adversario.

La respuesta integrada al sistema de seguridad física está basada en las siguientes recomendaciones.

1. Un contingente de Policía Nacional, en número suficiente para interrumpir el ataque del adversario.
2. Guardias en posiciones fijas o como barreras predecibles que se activen el momento de un ataque.
3. Las consideradas en Plan Nacional "DEMOCRACIA"

Gráfico Nº 62 Diseño Sistema de Protección Física



Fuente: García Mary Lynn "The design and evaluation of Physical Protection System"

Tabla Nº 58 Equipos de protección activa para el sistema físico integrado de protección de instalaciones del centro de control

UBICACIÓN	Cámaras ptz	Cámaras mini domos	Cámaras profesionales	Scanner/Magnetómetro	Sensores de movimiento	Sensores de rotura de vidrio	Sensores de humo	Lectoras tarjetas	Biométricos	Lineales
Planta baja	4	36	4	1	33	17	75	5	2	24
Planta piso # 1	0	19	2	0	24	28	23	17	4	0
Planta piso # 2	0	13	4	0	20	28	22	15	4	7
Entre piso sistemas-auditorio	0	4	1	0	6	1	8	2	2	0
Planta piso # 3	0	9	3	0	15	20	17	11	0	0
Subsuelo calle Bosmediano	0	9	3	0	15	0	13	6	4	0
TOTAL	**4**	**90**	**17**	**1**	**113**	**94**	**158**	**56**	**16**	**31**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 59 Listado de elementos pasivos del sistema físico de protección de instalaciones

UBICACIÓN	Cerramiento de piedra	Cerca eléctrica	Puerta acorazada	Cámara acorazada	Gabinetes contra incendios
Planta baja	1	1	2	0	1
Planta piso # 1	0	0	0	0	1
Planta piso # 2	0	0	0	1	1
Entre piso sistemas-auditorio	0	0	0	1	1
Planta piso # 3	0	0	0	0	1
Subsuelo calle Bosmediano	0	0	0	0	1
TOTAL	**1**	**1**	**2**	**2**	**6**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Tabla Nº 60 Ubicación del personal de seguridad para sistema físico de protección de instalaciones

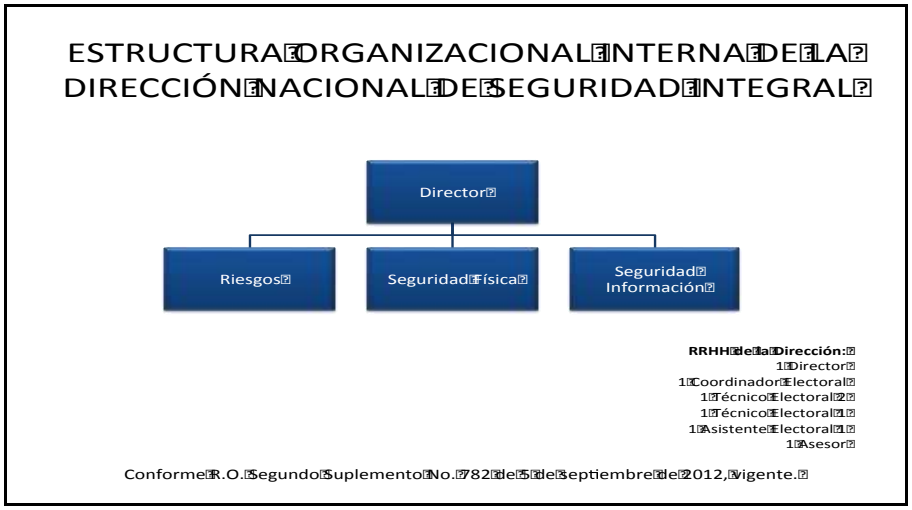
UBICACIÓN	Coordinador de seguridad	Vigilantes de seguridad	Radio operador	Operador de consola CCTV	Supervisor de seguridad
Planta baja	1	2	0	0	0
Planta piso # 1	0	0	1	2	0
Planta piso # 2	0	1	0	0	0
Entre piso sistemas-auditorio	0	0	0	0	0
Planta piso # 3	0	0	0	0	0
Subsuelo calle Bosmediano	0	1(ronda)	0	0	0
TOTAL	**1**	**3**	**1**	**2**	**1**

Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

Se considera que los puestos de seguridad son de 24 horas, correspondiendo a la empresa encargada de la seguridad proveer del saca francos y personal de reemplazo permanentemente.

Estructura interna de Seguridad "Dirección Nacional de Seguridad Integral"

Gráfico Nº 63 Estructura organizacional interna de la Dirección Nacional de Seguridad Integral



Elaborado por: Jorge Oswaldo Muñoz Rivadeneira

La misión de la Dirección Nacional de Seguridad Integral es la organización, coordinación, ejecución y control de actividades dirigidas a garantizar la seguridad integral de los procesos electorales y de Democracia Directa, de la institución; de las autoridades nacionales y extranjeras, y en general de las personas vinculadas a la gestión o a los procesos electorales y de Democracia Directa.

Unidad Administrativa: Dirección Nacional de Seguridad Integral.
Responsable: Director (a) Nacional de Seguridad Integral.

Atribuciones y Responsabilidades

- Diagnosticar la situación de riesgos y seguridad institucional a nivel nacional y desconcentrado del Consejo Nacional Electoral y del Instituto de Investigación, Capacitación y Promoción Política Electoral;
- Proponer políticas que aseguren la confidencialidad, integridad y disponibilidad de la información de la institución;
- Identificar y proponer correctivos para solucionar las falencias de seguridad institucional a nivel nacional y desconcentrado;
- Planificar en relación con la Coordinación Nacional Técnica de Procesos Electorales, la seguridad integral de los procesos electorales.
- Coordinar con la Dirección de Logística y Operaciones, la intervención de la fuerza pública para dar seguridad en los procesos electorales y de Democracia Directa;
- Implementar, monitorear y controlar la ejecución del Plan Operativo de Seguridad Electoral, en relación con la Coordinación Nacional Técnica de Procesos Electorales, durante los procesos electorales y de Democracia Directa;
- Implementar sistemas integrales de seguridad institucional, físicos, mecánicos y electrónicos;
- Coordinar la seguridad física de las personas y bienes institucionales en el ámbito nacional;
- Elaborar Planes de Contingencia, Continuidad de las Operaciones, Recuperación de Desastres y otros que se requiera, para prevenir riesgos que se puedan presentar en la institución así como en los procesos electorales;

- Evaluación de los planes de contingencia y planes de seguridad institucional en coordinación con las unidades responsables de los mismos; y,
- Dirigir, organizar y supervisar las actividades, productos y servicios relacionados con el funcionamiento de la dirección.

RIESGOS

- Diagnósticos georeferenciados de situaciones de riesgos y de seguridad institucional en el ámbito nacional.
- Informes situacionales sobre peligros y falencias de los sistemas de seguridad institucional en el ámbito nacional.
- Planes de Contingencia, Continuidad de las Operaciones y recuperación de Desastres y otros que se requiera.
- Planes de implementación de sistemas de seguridad institucional integral tanto físicos como mecánicos y electrónicos.
- Esquemas de seguridad de los sistemas informáticos implementados.
- Informes de actividades, productos y servicios

SEGURIDAD FÍSICA

- Informes del desarrollo del tema seguridad en los procesos electorales y de Democracia Directa.
- Informe de necesidades identificadas en el área de seguridad física electoral.
- Informe de acompañamiento en la intervención de la fuerza pública para dar seguridad en los procesos electorales.
- Planes de implementación de sistemas de seguridad integral físicos de procesos electorales.
- Informes de actividades, productos y servicios.

SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL

- Propuestas de políticas, normativas, procesos y procedimientos de seguridad de la información.

- Esquemas de seguridad de los sistemas informáticos implementados.
- Informe de cumplimiento institucional de la seguridad de la información.
- Propuesta de plan de difusión de medidas de seguridad de la información.
- Informes de análisis y evaluación de riesgos de la seguridad de la información.
- Propuestas de planes de contingencia para la continuidad y recuperación de desastres de los procesos.
- Informes de auditorías de seguridad de la información.
- Informes de seguimiento a los planes de remediación.
- Informes de actividades, productos y servicios.

5.6.2. Normativa de seguridad del CNE

Aparte de lo especificado en el Marco Teórico – Marco Legal Capítulo II, página 10 a 14 la siguiente normativa:

5.6.2.1. Disposiciones generales y transitorias

Los criterios y directrices emitidos hasta ahora bajo otras formas de disposición o instrucción y los referidos en cualquier otro documento normativo al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente, con excepción de lo regulado en esta materia en la Constitución Política y lo Normado por MRL y Riesgos Laborales.

5.6.2.2. Contenido

La Política de Seguridad Integral del CNE, se orienta a la seguridad y protección de las personas, los intereses, los bienes, la información y el conocimiento de la institución de las agresiones internas y externas que pudieran sobrevenir, adoptando las medidas preventivas, de respuesta y recuperación planificadas, apropiadas y oportunas que garanticen la continuidad de la Función Electoral frente a cualquier evento disruptivo, desarrollando permanentemente una Cultura de Seguridad de sus funcionarios a nivel Nacional.

Para lograrlo, el CNE y sus organismos se comprometen a la generación de un ambiente seguro de trabajo sobre la base de los siguientes principios:

1. Cumplimiento de legislación, de normativa interna y difusión de criterios de seguridad

El CNE cumplirá y hará cumplir en todos los organismos y unidades de la Función Electoral los requisitos legales vigentes en materia de seguridad y protección en todas las provincias y Cantones a Nivel Nacional y definirá la normativa interna necesaria, estableciendo estándares comunes de comportamiento para toda la Función Electoral comprometiéndose a la difusión de los criterios que permitan una conducta común de actuación.

2. Respeto a los derechos humanos

El CNE, en cumplimiento de su misión valores adoptará las mejores prácticas vigentes, tomando como referencia de actuación en esta materia, todos los tratados internacionales de Seguridad y Derechos Humanos. Asimismo, velará porque el personal perteneciente a empresas de Vigilancia y Seguridad que la institución contrate, actúe siempre en el más estricto respeto de estos derechos y de los principios contenidos en cualquier acuerdo al que la Función Electoral pueda o deba adherirse en materia de seguridad.

Todos los empleados que desarrollen funciones de seguridad, tanto del CNE como sus organismos y unidades, dispondrán de una sólida formación en Derechos Humanos.

3. Regulación del uso de armas

La Función Judicial limitará el uso de armas en la vigilancia y protección de personas a los supuestos autorizados en los ordenamientos jurídicos de aplicación.

Dicho uso queda limitado al personal habilitado de Seguridad Privada y Personal de Escolta, valorándose cada supuesto en función de lo que determine la legislación vigente en el País.

Se acudirá a los servicios de las Fuerzas Armadas y Cuerpos de Seguridad ante situaciones extremas o en aquellas ocasiones donde los lugares o actividades a desarrollar impliquen consideraciones de muy alto riesgo.

4. Contribución a la creación de una conciencia de seguridad

El CNE se comprometerá a facilitar los medios oportunos para la protección y salvaguarda de los recursos necesarios para el desempeño de la actividad profesional de sus funcionarios así como de su propia integridad.

Todos los funcionarios del CNE en todos sus organismos y unidades, han de velar por su propia seguridad, para lo cual adecuarán su actividad a los criterios que en esta materia establezca la Institución.

5. Promoción de un ambiente seguro de trabajo

El CNE realizará diagnósticos de seguridad, con el fin de identificar: Riesgos, Amenazas, Deficiencia, Vulnerabilidades y/o excesos, para implementar medidas para prevenir y/o minimizar sus consecuencias y ajustar los programas de Seguridad Integral.

6. Coordinación de la información

El CNE establecerá y mantendrá canales de información interna y externa que permitan conocer la situación de seguridad en los diferentes organismos y unidades de la Función Electoral, con el propósito de minimizar los riesgos y garantizar la seguridad de sus funcionarios, usuarios y comunidad en general.

7. Provisión de recursos

El CNE proveerá los recursos necesarios para alcanzar los estándares de seguridad requeridos para una Función Electoral segura y eficiente y promoverá la formación de las personas involucradas en la gestión de seguridad.

8. Colaboración en la evaluación de riesgos

El CNE, a través de la Dirección Nacional de Seguridad Integral contribuirá en el establecimiento de parámetros adecuados para asegurar una oportuna y acertada evaluación de riesgos en todos los Organismos y Unidades de la Función Electoral.

9. Mejora continua

EL CNE y sus organismos y unidades de la Función Electoral, se comprometen a adaptar dinámicamente los criterios de seguridad ante nuevos desafíos, revaluando de manera permanente sus programas, revisando planes, procedimientos, e implementación tecnológica, alineándose con estándares nacionales e internacionales en búsqueda de la excelencia en la gestión integral de seguridad, para lograr los mejores resultados en beneficio de sus funcionarios, usuarios y comunidad en general.

5.7. MANUALES Y NORMAS DE PROCEDIMIENTOS

5.7.1. Medidas de Protección de Instalaciones.

5.7.1.1. Objeto

Establecer un Plan para prevenir, intrusiones, ocupaciones, robos, extorsiones, sabotajes, detectar amenazas, retardar la acción de posibles adversarios y establecer la respuesta frente a estos eventos, con el fin de mitigar los posibles riesgos que puedan afectar a la actividad normal del CNE

5.7.1.2. Alcance

Este Plan tiene un alcance para el Edificio del CNE, sus propiedades, personal e información

5.7.1.3. Referencias

- Constitución de la Republica.
- Normativa y Reglamentación M.R.L.
- Ley de Vigilancia y Seguridad Privada
- Reglamento a la Ley de Vigilancia Seguridad Privada.

5.7.1.4. Definiciones

Instalaciones:

Se refiere a un edificio o grupo de edificios provistos de los medios necesarios para llevar a cabo la actividad de la Función Electoral.

5.7.1.5. Desarrollo

Responsabilidades.

El Responsable del Área de Protección (Seguridad Física) será el encargado de elaborar y coordinar con los técnicos y asistentes administrativos de Seguridad Física los procedimientos. Además será responsable de implementar y supervisar el cumplimiento de lo establecido en los mismos.

El Coordinador de la Dirección de Seguridad Integral será el encargado de aprobar los planes y procedimientos previamente a la aprobación de la Dirección y una vez aprobados será responsable de controlar la implementación y el cumplimiento de cada uno de los procedimientos del Sistema de Protección Seguridad Física.

5.7.1.6. Estructura para la protección de instalaciones y Tics.

Detección

Los estudios de seguridad y los análisis de riesgos de las instalaciones determinarán la cantidad de elementos de protección, así también determinarán el numérico de personal de vigilancia fija y móvil. Sin embargo deberán cumplirse necesidades mínimas establecidas para cada instalación, que consideren todos los elementos de protección de las medidas integradas.

La Detección está dada por los siguientes elementos:

Sistemas de alarma y cámaras perimetrales en las instalaciones:

a) Cercas electrificadas.
b) Sensores infrarrojo activos.
c) Cámaras de vigilancia perimetral D/N IR.

Sistemas de detección acceso a las instalaciones:

a) Cámaras de vigilancia en acceso D/N IR.
b) Vigilancia fija en accesos
c) Vigilancia móvil rondas.
d) Vigilancia fija en scanners
e) Vigilancia fija en revisión de correspondencia.
f) Arcos detectores de metales.
g) Magnetómetros
h) Scanners
i) Controles de acceso.
j) Lectoras de proximidad y biométricas (data center)

Sistemas de detección en el interior de las instalaciones:

a) Sistema de sensores PIR.

b) Sistema de sensores PIR y magnéticos
c) Cámaras de vigilancia en aéreas interiores IR.
d) Vigilancia móvil (rondas)
e) Monitoreo de alarmas.

5.7.1.7. Retardo.

Las Instalaciones en su gran mayoría no cumplen con espacios de defensa perimetral, por lo que la primera línea de defensa constituyen las paredes propias de los edificios.

El retardo está dado por los siguientes elementos:

Sistemas de retardo

a) Cerca electrificada de perímetro
b) Barreras estructurales de perímetro
c) Barreras estructurales de ventanas.
d) Barreras estructurales de puertas
e) Puestos de vigilancia fija.
f) Controles de acceso exteriores.
g) Puertas de seguridad.
h) Seguridades de puertas
i) Control de acceso interiores
j) Cerraduras electromagnéticas

5.7.1.8. Respuesta.

Como personal de respuesta, se dispone de personal Policial, quienes cumplen con la misión de protección de funcionarios y personal de apoyo a la protección de instalaciones. El número de efectivos es asignado por la comandancia de Policía y constituye una fuerza de reacción inmediata ante cualquier evento o incidente disruptivo o ataque.

Personal de seguridad Privada como equipo de respuesta permite impedir, evitar o neutralizar al adversario en el cumplimiento de su objetivo.

5.7.1.9. Procedimientos.

El área de protección (Seguridad Física) y la Dirección Nacional de Seguridad Integral en su programa cuentan con los siguientes procedimientos que se han desarrollado inicialmente para la integración con el sistema de protección física de las instalaciones.

- Procedimiento control de ingreso a instalaciones
- Procedimiento de revisión de correspondencia.
- Procedimiento control de ingreso vehicular
- Procedimiento rondas vigilancia móvil
- Procedimiento operadores centro de control

Estos procedimientos son aplicables a la Función Electoral y se desarrollarán o ajustarán los mismos de acuerdo al requerimiento de cada organismo.

5.7.2. Procedimiento Vigilantes de Seguridad Privada

5.7.2.1. Introducción:

Los Vigilantes de Seguridad Privada, son parte del sistema de Protección Física de las instalaciones y Tics, por lo tanto forman parte integral de este programa seguridad del CNE. Sus funciones y responsabilidades han sido asignadas de acuerdo a la aprobación de las recomendaciones propuestas en los estudios de seguridad aprobados por el nivel Directivo del CNE.

5.7.2.2. Objetivos:

Integrar al sistema de protección de Instalaciones, Tecnología y Comunicaciones, a través de procedimientos del subsistema de Vigilantes que permita optimizar de manera eficaz y eficiente la implementación de subsistemas de protección como: subsistema de cámaras, subsistema de alarmas, subsistema de detección de incendios, y subsistema de

comunicaciones y monitoreo. Contribuyendo también con los otros programas al cumplimiento de sus objetivos específicos.

5.7.2.3. Aspectos Generales:

Asignación y Distribución:

La asignación y distribución de guardias, obedecerá a los estudios de diagnóstico y las recomendaciones derivadas de estos. Por lo tanto los vigilantes deberán estar en condiciones de cumplir con cualquiera de las funciones asignadas, para esto deben conocer las responsabilidades y procedimientos generales de cada uno de los puestos.

5.7.2.4. Terminología:

Vigilante de Seguridad Física:

Es un profesional de la Seguridad con un nivel de educación de mínimo bachiller, certificado de acuerdo a la Ley De Seguridad Privada, por la capacitación mínima recibida para prestar sus servicios, del cual se han verificado sus antecedentes y su hoja de vida, tanto por la contratista, así como el contratante que desempeñará funciones de vigilancia y observación, específicas en los distintos sectores de responsabilidad en las instalaciones a las cuales ha sido asignado.

Vigilancia Fija:

Puesto de vigilancia fija como: garitas, recepciones, controles de ingreso, donde el vigilante realiza tareas de observación y vigilancia, cumpliendo tareas y procedimientos establecidos previamente, que contribuyen a cumplir los objetivos de protección de las instalaciones a la cual ha sido asignado.

Vigilancia Móvil:

Puestos de vigilancia y observación móviles, es decir que pueden trasladarse y cumplir funciones específicas trasladándose en sectores previamente establecidos, tal es el

caso de: Supervisores, personas encargados de protección de funcionarios o usuarios, patrullas de apoyo, etc.

Fuerzas de Respuesta:

Grupo de vigilantes privados y /o fuerza pública, con capacidad y medios para dar apoyo en casos de emergencia, ubicados en sitios estratégicos o patrullando en áreas cercanas a las instalaciones protegidas.

Procedimiento:

Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación. Todo procedimiento involucra actividades y tareas del personal, determinación de tiempos de métodos de trabajo y de control para lograr el cabal, oportuno y eficiente desarrollo de las operaciones. Ejemplo: Procedimiento de registro de ingreso de vehículos.

Bitácora:

Es el registro de todas las actividades cumplidas durante las actividades en cada puesto de vigilancia fija o móvil, que refleja el cumplimiento de las funciones asignadas.

Monitoreo:

El monitoreo, a rasgos generales, consiste en la observación del curso de uno o más parámetros para detectar eventuales anomalías. En el ámbito de la protección, el monitoreo puede realizarse efectivamente a través de un monitor (que transmite las imágenes captadas por una cámara) o mediante el trabajo de algún vigilante. Si esta persona descubre algún movimiento extraño (como un intruso dentro de una empresa o un paquete sospechoso en un banco), tendrá que actuar para evitar una situación de riesgo.

Observación:

La observación es la acción y efecto de observar (examinar con atención, mirar con recato, advertir). Se trata de una actividad realizada por los seres vivos para detectar y asimilar información. El término también hace referencia al registro de ciertos hechos mediante la utilización de instrumentos.

Comunicación:

El proceso comunicativo implica la emisión de señales (sonidos, gestos, señas, informes, etc.) con la intención de dar a conocer un mensaje. Para que la comunicación sea exitosa, el receptor debe contar con las habilidades que le permitan decodificar el mensaje e interpretarlo. El proceso luego se revierte cuando el receptor responde y se transforma en emisor (con lo que el emisor original pasa a ser el receptor del acto comunicativo). Esto incluye en el caso de vigilantes la comunicación interna, la codificada y la comunicación hablada o escrita con todas las personas que interactúa en el desarrollo de sus actividades.

Consigna:

Orden que recibe una persona o un grupo que va a intervenir en una acción determinada, en este caso específico, todas aquellas órdenes impartidas por el nivel superior y que debe ser cumplida de manera obligatoria ya que es de alta importancia para la protección y seguridad de las instalaciones.

Novedad:

Hecho que cambia o altera algo, es decir cualquier hecho, suceso, incidente o accidente que altera el normal funcionamiento de las actividades de una instalación, puede ser considerada como novedad y por lo tanto debe ser reportada a través de los canales correspondientes.

Reporte o Informe:

Comunicación escrita u oral en la que se dan informaciones, explicaciones y opiniones sobre una persona, asunto, hecho o actividad determinada, para un reporte escrito completo el personal de vigilancia debe llenar el formato correspondiente.

5.7.2.5. Funciones específicas

Puesto vigilancia fija: Ingreso Principal (SCANER)

El vigilante que está asignado al puesto de vigilancia fija del scanner, cumplirá el siguiente procedimiento:

a) Recibir el puesto realizando el chek list correspondiente para asegurarse del buen estado del equipo y herramientas de trabajo.
b) Recibir las consignas y novedades existentes, revisando que estén debidamente reportadas y registradas.
c) Encender el equipo de SCANNER, para asegurarse de que este en optimo funcionamiento para iniciar sus labores.
d) Proceder a indicar a los visitantes que procedan a retirarse todas sus pertenencias que puedan disparar una alarma que indique la presencia de metales, las pertenencias que deben ser retiradas por los visitantes son: correas metálicas, relojes, celulares, esferos, llaveros, monedas u otros que contengan piezas metálicas.
e) Proceder a entregar un recipiente para que se puedan depositar estas pertenencias.
f) Retener laptops, pen drivers, discos duros, a menos que su ingreso sea autorizado por directivos de las instalaciones, en este caso se procederá a registrar los equipos con número de serie y datos específicos del equipo como marca, características y emitir un documento para el control de salida.
g) Observar y Monitorear la pantalla del SCANNER con el fin de detectar algún objeto que puede representar una amenaza dentro de las instalaciones.
h) Reportar inmediatamente sobre cualquier irregularidad que encuentre durante el monitoreo de la pantalla.

i) Solicitar la asistencia del personal de respuesta (Fuerza Pública asignada a la instalación o personal de patrullas privadas), para que tome el procedimiento respectivo.
j) Comunicar al supervisor en caso de detectar personas armadas con su autorización de portación de armas, para que se proceda a retener temporalmente el arma, siguiendo el procedimiento respectivo.
k) Entregar a los visitantes sus maletas o portafolios, luego de haber sido monitoreados y revisados, si no existe ninguna irregularidad que represente una amenaza para la instalación.
l) Proceder a revisar con el SCANNER los paquetes que por requerimiento del personal de recepción de correspondencia, requieran ser revisados.
m) Elevar el reporte correspondiente en caso de existir novedades durante su turno de trabajo, utilizando el formato respectivo.

Puesto vigilancia fija: Ingreso Principal (magnetómetro-arco detector de metales)

El vigilante que se encarga de verificar las señales positivas del arco detector de armas o metales (MAGNETOMETRO), cumplirá el siguiente procedimiento:

a) Dirigir a los visitantes para que procedan a pasar la revisión del SCANNER.
b) Vigilar que los visitantes y usuarios ocasionales de la instalación, cumplan con pasar por los controles previstos.
c) Revisar a los visitantes y usuarios ocasionales, cuando se den señales positivas de detección de metales o armas.
d) Revisar minuciosamente a la persona que diera positivo en el detector. Cumpliendo los siguientes pasos:
e) Revisión de la cabeza: aretes, moños, peinados con vinchas, cadenas, brazaletes u otros que puedan llamar su atención.
f) Revisión de hombros, hombreras de sacos o blazers, brazaletes, cadenas, etc.
g) Revisión de tronco: pechos, posibles adhesivos, protuberancias. Se debe tener especial cuidado con las personas de sexo femenino, en caso de tener alguna duda, apoyarse con personal femenino de seguridad.
h) Revisión de cintura: tras la hebilla del cinturón, revisar todo el contorno del cinturón, revisar la pretina del pantalón.

i) Revisión de muslos: revisar todo el contorno del muslo, fijarse en abultamientos o protuberancias, revisar la parte interior hasta la sínfisis y caderas.
j) Revisión de piernas: revisar todo el contorno de la pierna, fijarse en abultamientos o protuberancias, revisar la parte interior hasta la sínfisis y caderas.
k) Revisión de pies y zapatos: si considera necesario obligue a pasar los zapatos por el SCANER.
l) Obligue a pasar cualquier objeto que considere que puede representar una amenaza por el SCANNER.
m) Solicitar la presencia de un supervisor en caso de encontrar algún tipo de arma y si no porta los documentos de autorización para portar armas, comunicar al personal policial a que proceda como corresponda.

Puesto de vigilancia fija: Registro de Visitantes Prevención.

El Vigilante que se encarga de realizar el registro de visitantes, cumplirá el siguiente procedimiento:

a) Solicitar al visitante la cédula de ciudadanía.
b) Consultar a que persona visita.
c) Consultar motivo de visita.
d) Confirmar con persona que visita
e) Entregar tarjeta para el piso que visite.
f) Solicitar que se coloque la tarjeta en lugar visible.
g) Informar que su identificación será entregada a la salida.
h) Llenar el formato de control de visitantes si no se ha registrado en el software correspondiente.

Puesto de vigilancia fija: Control de ingreso vehicular.

El Vigilante que se encarga de realizar el control de ingreso vehicular, cumplirá el siguiente procedimiento:

a) Mantener despejada el área de ingreso a parqueadero.

b) Confirmar el adecuado funcionamiento del sistema automático de control de ingreso.
c) Impedir el paso peatonal por el parqueadero a menos que se trate del personal de protección de Dignatarios.
d) Registrar vehículos que eventualmente sean autorizados a ingresar como: proveedores, visitas especiales, o de servicios públicos. Para esto llenará el formato correspondiente.
e) Realizar un inventario de los vehículos que permanezcan en el parqueadero antes y después de su turno, verificando su registro.
f) Revisar al ingreso todos los vehículos utilizando equipo de revisión vehicular para evitar el ingreso de explosivos.
g) Dirigir el tráfico vehicular para evitar accidentes.
h) Informar del límite de velocidad permitido en parqueadero.
i) Observar y reportar de situaciones sospechosas en su área de trabajo.
j) Cerrar y abrir la puerta del parqueadero a las horas indicadas, o en caso de disturbios civiles que puedan representar una amenaza a la instalación.
k) Colaborar con el equipo de protección de dignatarios para facilitar su trabajo.

Puesto de vigilancia móvil: Ronda, acompañamiento y apoyo.

a) Realizar recorrido de pisos y subsuelos, observando posibles irregularidades que puedan representar amenaza para la instalación, sus bienes, personas e información.
b) Identificar posibles personas no autorizadas que puedan deambular en la instalación.
c) Marcar los puntos de control de rondas de la instalación.
d) Cumplir con el acompañamiento de visitantes a áreas de mayor criticidad como: Oficinas de Dignatarios, cuartos de suministros, data center o alguna otra área que en ese momento se considere como crítica.
e) Cumplir funciones de acompañamiento a visitantes, con el propósito de custodiar y dirigirle hasta el sitio autorizado de ingreso o persona de contacto.
f) Apoyar a sus compañeros de vigilancia fija en cualquiera de los puestos que requieran apoyo por cualquier motivo.
g) Realizar coordinaciones con el centro de control y monitoreo para identificar las áreas que requieren de mayor atención.

h) Abastecer logísticamente los otros puestos de trabajo.

Puesto de vigilancia Fija: Monitoreo y Comunicaciones.

a) Realizar el monitoreo de las diferentes áreas a través de cámaras de video vigilancia.
b) Coordinar con el personal de vigilancia, para indicar sobre situaciones que puedan representar amenazas para las instalaciones, bienes, personas o información. Para que el personal de vigilancia del área tome procedimiento.
c) Monitorear eventos o actividades que reviertan riesgo para funcionarios, visitantes, y usuarios.
d) Coordinar con las autoridades policiales asignadas a las instalaciones para situaciones que reviertan cierto riesgo o amenaza existente.
e) Dar seguimiento a eventos o actividades críticas.
f) Apoyar al personal de vigilancia de las diferentes áreas, comunicando oportunamente amenazas del sector por el monitoreo de las cámaras exteriores que podrán detectar: manifestaciones, vigilancia de personas, vehículos sospechosos, etc.
g) Realizar las comunicaciones a la fuerza de respuesta (patrullas privadas de seguridad y personal policial asignado), en caso de requerir el apoyo de las mismas.
h) Reportar el estado de funcionamiento del sistema de cámaras, control de acceso, incendios, etc.
i) Garantizar que se evidencien situaciones que amerite su grabación permanente.
j) Monitorear el acceso del personal verificando con el registro de control de acceso.
k) Receptar todos los reportes de comunicaciones y escritos de los diferentes puestos de vigilancia.
l) Registra ingreso y salida de ejecutivos principales.
m) Cumplir con los procedimientos de emergencia en los diferentes eventos disruptivos que pudieran presentarse.

Puesto de vigilancia Fija: Recepción, Revisión y Control de Correspondencia

a) Revisar si hay datos incompletos del remitente, si hay advertencias de abrir solo el destinatario, confidencial, urgente, sellos que no correspondan, protuberancias y

cinta protegiendo bordes o manchas, serán justificaciones para que el sobre sea revisado minuciosamente.

b) Revisar si llegan paquetes que alojen varillas, demasiado empaquetados, remitentes o dirección inexistentes o incompletos, protuberancias, olores no identificados. Estos serán justificativos para someter a una revisión minuciosa al paquete.
c) Retener discretamente en el sitio a la persona que deja el paquete hasta que se complete la revisión.
d) Verificar los siguientes datos en la correspondencia:
    - Nombre del destinatario.
    - Nombre del Remitente.
    - Forma como está escrito (observar faltas ortográficas)
e) Estampar el sello de revisado por y firma del vigilante en caso de satisfacer la revisión.
f) Utilizar el SCANER si considera necesario de acuerdo a inspección física.
g) Realizar el registro y firma de persona que deja la correspondencia o paquetería.
h) En caso de que la inspección de positivo, coordinar con personal policial.
i) En caso negativo proceder a estampar el sello y despachar al destinatario.
j) Todo paquete que de positivo, no debe ser manipulado.

5.7.3. Medidas de protección de instalaciones informáticas

5.7.3.1. Objeto

Establecer las medidas necesarias para proteger la información y las instalaciones de accesos no autorizados, impidiendo daños o interferencias y evitando, de este modo, la interrupción de las actividades por incidentes disruptivos así como de riesgos propios de las instalaciones del Consejo Nacional Electoral.

5.7.3.2. Ámbito de aplicación

Esta Norma será de aplicación en todos los organismos del CNE

5.7.3.3. Normativa Marco (Normativa Superior de Referencia)

ISO 27001:2005.

5.7.3.4. Normativa derogada

Ninguna.

5.7.3.5. Vigencia

Esta norma entrara en vigor a 30 días laborables posteriores a la fecha de su aprobación definitiva.

5.7.3.6. Disposiciones generales y transitorias

Los criterios y directrices emitidos en cualquier otra norma al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente.

5.7.3.7. Contenido

5.7.3.8. Aéreas seguras

La Dirección Nacional de Seguridad Integral en coordinación con la Dirección Nacional de Informática, a través de las distintas áreas de soporte y apoyo, definirá:

- Cuáles son las áreas protegidas de acuerdo al nivel de criticidad de los equipos e información que contienen.
- Los parámetros de seguridad para proteger dichas áreas.
- Los permisos de acceso del personal a dichas áreas.

Todas las personas que accedan a las áreas protegidas deberán exhibir alguna forma de identificación visible, poseer la autorización de acceso al área y registrarse manual o electrónicamente.

El CNE alienta a todo su personal a cuestionar la presencia de desconocidos, no acompañados por personal debidamente autorizado o que no exhiban una identificación.

La Unidad de Tecnología, a través de las distintas áreas de la Dirección de Soporte, revisara y actualizara periódicamente los derechos de acceso a las áreas protegidas.

La unidad de tecnología, a través de las distintas áreas de la Dirección de Soporte, delimitara el acceso del personal externo a las áreas protegidas.

5.7.3.9. Seguridad del equipamiento

Todos los equipos de procesamiento del CNE, contaran con los adecuados niveles de Seguridad Física.

Los usuarios serán responsables de la Seguridad Física de los equipos que estén a su cargo.

La unidad de tecnología, a través de las distintas áreas de la Dirección de Soporte, determinara cuales son los niveles adecuados de Seguridad Física, teniendo en cuenta las especificaciones de los proveedores del hardware y criticidad de la información según la definición de sus Propietarios.

El equipamiento del CNE, estará protegido, con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas, en función de su criticidad.

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

El mantenimiento de los equipos será llevado a cabo por personal debidamente autorizado y de acuerdo a las recomendaciones del proveedor.

Los fallos, reales o supuestos y el mantenimiento, preventivo o correctivo, de los equipos serán registrados adecuadamente.

Se borrara la información del equipamiento destinado a ser dado de baja del CNE.

5.7.3.10. Controles generales

Los protectores de pantalla de los diferentes equipos se activaran auténticamente luego de un periodo predeterminado de inactividad.

Los protectores de pantalla se desactivaran mediante autenticación de contraseña.

Los usuarios, cuando terminen su horario laboral y se retiren de su lugar de trabajo, dejaran toda la información que estuvieron utilizando en lugar seguro y los equipos bajo su responsabilidad apagados.

El retiro de equipamiento, información o software de las instalaciones del CNE requeriría de autorización previa del propietario correspondiente.

El ingreso a las instalaciones del CNE de equipamiento, información o software ajeno al grupo del Consejo Nacional Electoral, requerirá de su autorización previa de la unidad de tecnología a través de la Dirección Nacional de Informática.

En caso de existir equipos en ubicaciones de alto riesgo, los mismos se apagaran después de un periodo definido de inactividad.

BIBLIOGRAFÍA

(s.f.). Obtenido de http://aceproject.org/ace-es/focus/fo_elections-and-security/onePage

(s.f.). Obtenido de http://portal.cne.gob.ec/index.php/Mision-Institucional/Autoridades/mision-institucional-institucional.html

ACE Project Red de Conocimientos Electorales,. (s.f.). Obtenido de http://aceproject.org/ace-es/focus/fo_elections-and-security/onePage

Alfonsin, R. (1990). *Agenda para la consolidación de la Democracia en Ámerica Latina* (Primera Edición ed.). Costa Rica: IIDH-CAPEL.

Alfonsin, R. (1990). *Agenda para la Cosolidación de la Democracia en América Latina* (Primera Edición ed.). Costa Rica: IIDH-CAPEL.

ASIS. (2012). Obtenido de VGHGVHcfvh

ASIS, I. (2009-2013). Estándar ANSI - SPC1.

Broder, J. (1999). *"Risk Analysis and the Security Survey".*

CEAS, E. (s.f.). *"Sistemas Técnicos de Seguridad.* (C. Internacional, Ed.) Madrid, España.

Chavez , F. (2013). ASIS Capitulo Nº 231. *Analisis de riesgos.* Quito.

Dr. Manunta, G. (s.f.). *Presentación del libro "Seguridad: una Introducción" Revista Seguridad Corporativa.*

HORA, L. (s.f.). Obtenido de http://www.lahora.com.ec/index.php/noticias/show/1101414559#.UTv7drtWSls

Hurtado, O. (2006). *El Poder Politico en el Ecuador* (DECIMO SEXTA ed.). Quito, Ecuador: Planeta del Ecuador.

La Rotta, L. (2005). "Consultor Didáctico Diccionario de Seguridad METIS.

Mallet, A. (1983). *La búsqueda de la seguridad social.* Buenos Aires, Argentina.

Momboisse, R. (1968). *"Industrial Security for Strikes, Riots and Disasters".* Springfield: Springfield, III. Chas. C. Thomas.

POA , P. (s.f.). *"Análisis de la Amenaza (DBT) Amenaza base del Diseño de Protección.*

Sanchez, M. (1998). *"Seguridad en Entidades Bancarias"* (1998 ed.). Madrid, España.

GLOSARIO DE TÉRMINOS

Amenaza

Técnicamente la amenaza es la probabilidad de ocurrencia de un evento con una cierta intensidad, en un sitio específico y en un período de tiempo determinado.

Candidato político.

Se denomina candidato a la persona que se postula a ser elegida para algún cargo público electo en unas elecciones, normalmente incluido en unas listas electorales.

Ciudadano

La calidad de ciudadano es condición jurídico político básica para el hombre dentro del Estado, el ciudadano siempre es una persona y el hecho de que el orden jurídico constitucional le reconozca y atribuya esta calidad, deviene condición necesaria para que a tal individuo se le concedan para ejercerlos, por extensión legal, todos los derechos, prerrogativas y obligaciones de la ciudadanía.

Corrupción electoral

Entiéndase por corrupción electoral todo acto o procedimiento que atente contra el legítimo y libre ejercicio del derecho de sufragio, que por lo general se traduce en una alteración y adulteración de la auténtica voluntad de los electores y/o en un falseamiento de los resultados electorales.

Daño

Resultado de una calamidad o de la agresión de un agente perturbador.

Delincuencia común

García Máynez, la define como delincuencia callejera: asalto a transeúntes, carterismo, violación, robo de bienes y artículos menores, robo a casa habitación, robo de vehículos, vandalismo, grafitos y pinta de muros y monumentos

Delincuencia organizada

Grupos o redes con una dirección estructurada, dedicados a las actividades ilegales encubiertas.

Elecciones

Es un proceso de toma de decisiones usado en las democracias modernas donde los ciudadanos votan por sus candidatos o partidos políticos preferidos para que actúen como representantes en el gobierno.

Estudio de seguridad

Conjunto de procedimientos que permiten la recolección análisis, formulación y evaluación de la información relevante sobre los hechos reales y potenciales relacionados con la Seguridad de un ámbito específico, seguida de un diagnóstico, pronóstico y formulación para determinar las fuentes de riesgo y vulnerabilidad en cada recurso de incidencia, en un espacio y tiempo determinados.

Extorsión

Usurpación o despojo, por la fuerza, de una cosa perteneciente a otra. (Todo daño o perjuicio.

Gestión de riesgos

Proceso social complejo que conduce al planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar los

efectos adversos de fenómenos peligrosos sobre la población, los bienes y servicios y el ambiente.

Grupos sociales o agrupaciones políticas adversos

Grupos aislados independientes o como parte de partidos políticos adversos, cuyo objetivo sea la organización y coordinación de actividades que afecten el desarrollo de los eventos electorales para su interés particular.

Hurto

Son reos de hurto los que, sin violencias ni amenazas contra las personas, ni fuerza en las cosas, sustrajeren fraudulentamente una cosa ajena, con ánimo de apropiarse.

Movimientos insurgentes

Estos movimientos surgen al margen de las instituciones establecidas, se hacen visibles y miden su poder en contraposición al poder hegemónico, en los acontecimientos políticos y masivos.

Peligro

Situación donde los elementos de ataque están menos definidos que en la amenaza donde existe un blanco potencial de daño.

Plagio (secuestro)

El delito de plagio se comete apoderándose de otra persona por medio de violencias, amenazas, seducción o engaño, sea para venderla o ponerla contra su voluntad al servicio de otro, o para obligarla a pagar rescate, o entregar una cosa mueble, o extender, entregar o firmar un documento que surta o pueda surtir efectos jurídicos, o para obligar a un tercero a que ejecute uno de los actos indicados, tendientes a la liberación del secuestrado.

Protección activa

Denominamos como seguridad activa a todos los mecanismos, medios y elementos que mediante su uso y/o actividad, permiten mantener o ampliar el nivel de protección y seguridad.

Protección pasiva

Se considera como seguridad pasiva todos los medios o elementos inherentes e inertes, que permiten ampliar el nivel de protección sólo con su presencia.

Riesgo

Es la relación entre un sistema de protección y la amenaza producto de la vulnerabilidad.

Robo

El que, mediante violencias o amenazas contra las personas o fuerza en las cosas, sustrajere fraudulentamente una cosa ajena, con ánimo de apropiarse, es culpado de robo, sea que la violencia tenga lugar antes del acto para facilitarlo, en el momento de cometerlo, o después de cometido para procurar su impunidad

Robo calificado

La pena será de reclusión menor de tres a seis años, si concurre alguna de las circunstancias siguientes:

1. Si las violencias han producido heridas que no dejen lesión permanente;
2. Si el robo se ha ejecutado con armas, o por la noche, o en despoblado, o en pandilla, o en caminos o vías públicas;
3. Si se perpetrare el robo con perforación o fractura de pared, cercado, techo o piso, puerta o ventana de un lugar habitado o sus dependencias inmediatas”

Seguridad

La seguridad es una necesidad básica y ancestral de las persona, que figura entre instintos primarios, como un componente muy importante del instituto de conservación.

La seguridad es la enseñanza de un sistema coherente de creencias donde la regla prescribe las acciones que constituyen la alternativa para sobrevivir. Su meta es crear un contexto de tranquilidad para su desarrollo.

Seguridad ciudadana

Práctica racional cuya misión es la fraternidad, la buena voluntad y la colaboración que acompaña el espíritu solidario de los ciudadanos.

Seguridad de la información

Protección y preservación de la información confidencial y salvaguarda contra la vergüenza o las implicaciones legales por usar indebidamente las redes de una empresa o el acceso a ellas.

Seguridad física

Organización de elementos tangibles, diseñados con el objeto de detectar, resistir y disuadir los posibles ataques.

Seguridad integral

Fusión de un método (conocimiento más experiencia) con la actitud tanto del protector como la del protegido, de percibir, prevenir, proteger y preservar, generando un ambiente de orden, tranquilidad y paz en aspectos humanos, legales, sociales, económicos y técnicos.

Seguridad personal

Reúne las actividades de la protección inteligente y elegante de personas, con elementos técnicos y teóricos conjugados creativamente para brindar el cuidado de la vida e integridad de las personas como un derecho inalienable, así como la vigilancia del entorno más íntimo de los protegidos, por parte del personal afín y de confianza.

Seguridad privada

Practica racional de medidas pasivas que por propia iniciativa toman los particulares con el fin de neutralizar la amenaza que pesa individualmente sobre ellos.

Votante

Persona que emite un voto en una elección o consulta

Vulnerabilidad

Incapacidad de respuesta a un riesgo.