UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS

IMPLEMENTACION DE SEGURIDAD ELECTRONICA PARA EL CONTROL DE RIESGO DE ROBO EN UNA ENTIDAD FINANCIERA

Autor**:**

Bach. RAMOS CORONEL ELIO

Línea de Investigación Institucional:

NUEVAS TECNOLOGÍAS Y PROCESOS

PARA OBTENER EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACION

HUANCAYO – PERU

2020

_____

DR. HENRY GEORGE MAQUERA QUISPE

ASESOR METODOLÓGICO

_____

DR. JOHN FREDY ROJAS BUJAICO

ASESOR TEMÁTICO

DEDICATORIA

Dedico esta Tesis a Dios, a mis queridos padres por su apoyo incondicional en toda mi existencia, a mis hermanas, sobrinas y cuñado por su compañía.

Bach. Elio Ramos Coronel

HOJA DE CONFORMIDAD DE JURADOS

_____

Dr. CASIO AURELIO TORRES LOPEZ
PRESIDENTE

_____

Mg. JORGE VLADIMIR PACHAS HUAYTAN
JURADO 01

_____

Dr. EDWARD EDDIE BUSTINZA ZUASNABAR
JURADO 02

_____

Ing. RAFAEL EDWIN GORDILLO FLORES
JURADO 03

_____

Mg. MIGUEL ANGEL CARLOS CANALES
SECRETARIO

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La presente tesis titulada “Implementación de Seguridad Electrónica para el Control de Riesgo de Robo en una Entidad Financiera”. La problemática de la tesis se ha basado en la influencia que tuvo implementar un sistema de CCTV, Alarmas y Control de Acceso en las “Incidencias de Robo”.

El objetivo de la tesis es “Implementar un Sistema de Seguridad Electrónica” y sus implicancias en base a la mejora continua.

Esta tesis realizó un análisis, diseño e implementación de un sistema de seguridad electrónica mediante la Metodología Top Down Design, apoyado por el enfoque de Mejora Continua, la ISO 31000 y la ISO 22301; permitiéndonos retroalimentar y optimizar el sistema, con base formal a las Normas Internas, recomendaciones de la Póliza de Seguro y Normas de Proyectos de Ley. Los incidentes siempre existirán en toda organización, la finalidad es reducirlos.

Palabras clave: seguridad electrónica, control de riesgo, metodología top down, entidad financiera.

ABSTRACT

The present thesis entitled "Implementation of Electronic Security for the Control of Theft Risk in a Financial Institution". The problem of the thesis has been based on the influence that the implementation of a CCTV, Alarms and Access Control system had on the “Theft Incidents”.

The objective of the thesis is "Implement an Electronic Security System" and its implications based on continuous improvement.

This thesis carried out an analysis, design and implementation of an electronic security system using the Top Down Design Methodology, supported by the Continuous Improvement approach, ISO 31000 and ISO 22301; allowing us to provide feedback and optimize the system, formally based on the Internal Rules, recommendations of the Insurance Policy and Rules for Bills. Incidents will always exist in every organization, the purpose is to reduce them.

Keywords: electronic security, risk control, top down methodology, financial institution.

INTRODUCCION

La Investigación surge de la necesidad de demostrar a Gerencia una reducción de los Incidentes de Riesgo de Robo en la Implementación de la Seguridad Electrónica en una Entidad Financiera, de 16 agencias en el lapso de 52 semanas dividido en 26 semanas sin Seguridad Electrónica y 26 semanas de incremento paulatino de Seguridad Electrónica, todo bajo el enfoque de la Metodología Top Down Design apoyado por la herramienta de gestión de Mejora Continua de Deming y usando muchas recomendaciones de la ISO 31000 de Gestión de Riesgos, también de la ISO 22301 de Continuidad del Negocio; que juntos nos orientan a las mejores prácticas específicamente para este tipo de trabajos donde la razón de ser es la optimización del Sistema, por ejemplo mejorando la calidad de sensores, o aumentando los sensores en lugares nuevos o puntos ciegos.

En el Capítulo I, nos orientamos en hacer una mirada total de la problemática y donde se ubica la Organización, para lo cual hay una formulación de problemas, los cuales se justifican tanto Social, Científica y Metodológica, en base a ello definimos los objetivos del presente trabajo.

En el Capítulo II, Marco Teórico que tiene como partes los antecedentes tanto nacionales como internacionales, los que aportan un complemento.

En el capítulo III, Hipótesis, aquí realizamos la definición de nuestra Hipótesis General y las 3 Hipótesis Especificas con su respectiva Operacionalización de las variables de investigación.

En el capítulo IV, que se denomina Metodología, se describe el método, tipo de investigación, nivel de Investigación y Diseño de la Investigación, además de definir la población a trabajar, la técnica aplicada es la entrevista y los instrumentos son las fichas de entrevista para las 26 semanas posteriores y para las 26 semanas previas, se tiene un informe de incidencias semanal de las 16 agencias. Usando como base la metodología Top Down Design.

En el Capítulo V, denominado Resultados, se presenta los resultados de las 52 semanas visto en dos partes, también se adiciona para un mejor entendimiento un gráfico por cada indicador que incluye los incidentes y los incidentes resueltos, dando una mejor visión grafica para la comprensión respectiva.
Análisis y discusión de resultados, que en base a la cantidad de muestras se demuestra si nuestra Hipótesis es Nula o Alternativa.
Finalmente se presentan las conclusiones y recomendaciones.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Planteamiento de problema

La seguridad es una de las principales necesidades de la población peruana, siendo un fenómeno social, multidimensional y multicausal, lo que conlleva a tomar medidas muy diversas porque requiere soluciones eficaces y efectivas.

Según Indicadores de la Encuesta Nacional de Programas Presupuestales 2017 a julio 2019 – INEI, hay indicadores para medir la situación de inseguridad, violencia y delito a nivel Nacional.

Tabla 1. Población Víctima de algún hecho delictivo 2019

	Ene17 - Jun17	Feb17 - Jul17	Mar17 - Ago17	Abr17 - Sep17	May17 - Oct17	Jun17 - Nov17	Jul17 - Dic17	Ago17 - Ene18	Sep17 - Feb18	Oct17 - Mar18	Nov17 - Abr18	Dic17 - May18
Nacional Urbano	26.9%	27.1%	27.3%	27.4%	27.3%	26.6%	25.5%	25.3%	25.3%	25.6%	25.5%	26.1%
Ciudades de 20 mil habitantes	29.7%	30.2%	30.2%	30.4%	30.2%	29.3%	27.8%	27.3%	27.4%	27.5%	27.3%	28.2%
Lima Metropolitana	30.2%	30.9%	31.0%	30.8%	30.8%	29.7%	27.8%	27.0%	27.3%	27.7%	27.2%	28.2%
Centros Poblados Urbanos entre 2 mil y menos de 20 mil habitantes	19.5%	19.0%	19.8%	19.5%	19.4%	19.3%	19.4%	20.0%	19.5%	20.3%	20.4%	20.6%

Ene18 - Jun18	Feb18 - Jul18	Mar18 - Ago18	Abr18 - Sep18	May18 - Oct18	Jun18 - Nov18	Jul18 - Dic18	Ago18 - Ene19	Sep18 - Feb19	Oct18 - Mar19	Nov18 - Abr19	Dic18 - May19	Ene19 - Jun19	Feb19 - Jul19
25.9%	26.1%	26.2%	26.0%	26.4%	25.9%	26.1%	26.2%	26.3%	26.5%	26.0%	26.2%	26.4%	25.9%
28.0%	28.5%	28.6%	28.5%	29.0%	28.4%	28.8%	28.9%	29.0%	29.0%	28.5%	28.7%	28.9%	28.2%
27.8%	28.8%	29.2%	29.1%	29.6%	29.0%	29.6%	29.8%	29.5%	29.7%	29.5%	29.5%	29.7%	29.0%
20.5%	19.7%	19.6%	19.0%	19.5%	19.1%	18.7%	18.9%	19.3%	19.8%	19.3%	19.4%	19.7%	19.9%

	Ene - Jun 19		Feb - Jul 19	
	No fue víctima	Fue víctima	No fue víctima	Fue víctima
Nacional Urbano	73.6	26.4	74.1	25.9
Ciudades de 20 mil habitantes	71.1	28.9	71.8	28.2
Lima Metropolitana	70.3	29.7	71.0	29.0
Centros Poblados Urbanos entre 2	80.3	19.7	80.1	19.9

Fuente: Encuesta Nacional de Programas Presupuestales, 2017-julio 2019 INEI

Además hubo un aumento el Riesgo de Robo, Estafa, Fraude en la administración, Falsificación, Delitos Informáticos según muestra las estadísticas del INEI 2008-2018.

Tabla 2. Personas detenidas por cometer delito, según tipo de delito

DELITOS

PERSONAS DETENIDAS POR COMETER DELITO, SEGÚN TIPO DE DELITO, 2008 - 2017

(Casos registrados)

Tipo de delito	2008	2009	2010	2011	2012	2013	2014
Total	**60 053**	**66 331**	**75 412**	**74 597**	**92 868**	**91 698**	**95 265**
Contra el patrimonio	**24 695**	**29 133**	**29 942**	**29 187**	**30 804**	**30 622**	**29 373**
Hurto	9 665	10 475	10 350	10 878	12 136	11 825	12 207
Robo	12 517	16 329	16 143	15 227	15 857	15 925	13 449
Apropiación ilícita	353	297	375	280	186	218	227
Estafas y otras defraudaciones	775	707	735	776	600	117	102
Abigeato	518	503	783	590	299	509	574
Fraude en la Administración	17	31	43	19	18	17	17
Daños simples y agravados	148	145	209	103	178	8	-
Delitos informáticos	-	-	-	-	7	201	181
Otros 3/	702	646	1 304	1 314	1 523	1 800	2 616
Contra la fe pública	**574**	**525**	**676**	**699**	**1 142**	**1 089**	**952**
Falsificación de documentos en general	442	376	482	480	877	924	711
Falsificación sellos, timbres-marcas oficina	-	-	-	23	64	13	15
Otros 5/	132	149	194	196	201	152	225

Fuente: INEI 2008-2018.

Existe un alto porcentaje de riesgo de robo según estadísticas, tenemos Delitos contra el Orden Financiero y Monetario, y Delitos contra la Confianza y la Buena Fe en los Negocios.

Tabla 3. Denuncias por Comisión de Delitos, según delito genérico.

DELITOS							
DENUNCIAS POR COMISIÓN DE DELITOS, SEGÚN DELITO GENÉRICO, 2011- 2017							
Delito Genérico(Casos registrados)	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Total	**240,438**	**271,813**	**299,474**	**326,578**	**349,323**	**355,876**	**399,869**
Delitos contra el Patrimonio	168,618	185,357	204,935	224,753	242,697	242,653	265,219
Delito contra la confianza y la buena fe en los negocios	100	226	145	211	42	55	47
Delitos contra los derechos intelectuales	162	158	80	175	98	93	156

Delitos contra el orden económico	123	154	58	207	37	58	74
Delitos contra el orden financiero y monetario	926	1,119	1,284	1,402	914	687	663
Delitos tributarios	309	275	211	371	109	181	142
Nota 1: El total comprende a las denuncias por comisión de delitos registrados en Comisarías y Unidades Especializadas en Investigación Criminal.							
Nota 2 : Información 2008-2010 corresponde a datos proporcionados por Ministerio del Interior MININTER							

Fuente: INEI, Censo Nacional de Comisarias 2013-2014, Registro Nacional de Delitos 2014, Registro Nacional de Denuncias de Delitos y Faltas 2015-2016 y Sistemas de Denuncias Policiales 2015-2016.

El último año en el Perú el 67% de los bancos sufrieron fraudes internos, siendo los empleados de la propia entidad quienes cometen gran parte de estos delitos, reveló un estudio elaborado por Deloitte.

Según informó el diario Gestión, esta tasa es la segunda más alta de Latinoamérica, solo detrás de Colombia donde el 100% de los bancos sufrió ataques internos en el último año.,

El documento precisa que los fraudes con empleados o terceros desde dentro de organizaciones, son el origen de las brechas de seguridad internas.

Existen dos tipos de vulnerabilidades, una es el robo externo con delincuentes que vulneran los controles perimetrales y el segundo es el robo interno efectuado por el propio personal de la entidad.

Para ambas modalidades se plantea la Implementación de Seguridad Electrónica para el Control de Riesgo de Robo, lo cual conlleva a Instalar un Sistema CCTV, Alarmas y Control de Acceso. En base a un marco Legal y Técnico:

Decreto Legislativo Nº 1213 para Alarmas y Control de acceso.

Decreto legislativo Nº 1218 para Cámaras de Seguridad.

Normas Internas.

Requisitos de póliza de seguro ED La Positiva (adecuado a la Ley 29946)

Todo bajo el enfoque de la Metodología Top Down Design, y teniendo como base las buenas prácticas del enfoque de Mejora continua de Deming, la Gestión de Riesgos y la Continuidad del Negocio.

1.2. Delimitación del Problema

La Implementación se efectuará en las 16 agencias de la Coopac, y contará con la instalación de:

CCTV, con cámaras externas e internas orientadas en las áreas comunes y también en las áreas críticas de seguridad como bóveda, tratando en lo posible de cubrir todas las áreas vitales de ingreso y salida sin dejar áreas oscuras, las cuales servirán para el control de personal externo e interno.

Alarmas, de grado 3, el grado es el nivel de seguridad y se clasifican según las normas UNE-EN 50131-1:2008/A2:2017 (UNE Normalización Española), se instalara alarmas de detección fuera de horario de trabajo, para la seguridad del local en horas sin resguardo de vigilancia, se tendrá como requisitos: tener doble instalación en caso que algún elemento no funcione, el cableado será configurado para sabotaje, la señal de aviso en caso de alguna ocurrencia será doble con teléfono y señal de internet en caso uno no funcione.

Control de Acceso; en horario de oficina se contara con control de acceso para limitar el acceso del personal interno y externo a áreas no autorizadas.

Por ahora se consideran los 3: CCTV, alarmas y control de acceso, posteriormente se implementara cercos eléctricos para la seguridad perimetral, también protocolos de seguridad, se incluirá la seguridad de la información, y se probará nuevas tecnologías como el uso de radares de calor para detectar la presencia humana y drones para un patrullaje y verificación en caso ocurra un incidente fuera del horario de trabajo.

1.3. Formulación del Problema

1.3.1. Problema General

¿De qué manera mejorar la seguridad para reducir el riesgo de robo en una entidad financiera?

1.3.2. Problemas Específicos

1.3.2.1 ¿Cómo supervisar las incidencias de robo dentro y fuera del horario de trabajo?

1.3.2.2 ¿Podemos reducir y reportar las incidencias fuera del horario de trabajo?

1.3.2.3 ¿Se puede controlar el ingreso y salida del personal a espacios comunes o restringidos en horario de trabajo?

1.4. Justificación

1.4.1. Social o Práctica

Esta investigación se debe de hacer cuando el desarrollo de la investigación ayuda a resolver un problema o por lo menos, propone estrategias que al aplicarse contribuirían a resolverlo. (Bernal, Cesar, Metodología de la investigación. 3º edición Colombia, 2010.).

Con la instalación de cámaras en caso ocurran incidentes de robo o pérdida de bienes, se podrá recurrir al video para revisar el motivo del percance; con la instalación de alarmas fuera del horario de oficina, se protege de manera activa la seguridad de los bienes; con la instalación de Control de Acceso se controla el tránsito de personal a áreas comunes o de restricción; esta investigación se realiza por que existe la necesidad de controlar los bienes y dejar al personal concentrarse en sus labores dejando el trabajo de control a la solución instalada,

1.4.2. Metodológica

Esta investigación se da cuando el proyecto que se va a realizar propone un nuevo método o una nueva estrategia para generar conocimiento válido y confiable. (Bernal Cesar, Metodología de la investigación. 3º edición Colombia, 2010).

La Implantación de la Seguridad Electrónica usando la Metodología Top Down en la reducción de Incidentes de Robo en una Entidad Financiera, propone una solución de acuerdo al presupuesto, al personal que labora y sus condiciones laborales, a las políticas del negocio, a las normas y estatutos regidos, los cuales son únicos y difíciles de replicar.

1.5. Objetivos

1.5.1. Objetivo General

Implementar la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una Entidad Financiera

1.5.2. Objetivos Específicos

1.5.2.1 Instalar un sistema CCTV para supervisar las incidencias dentro y fuera del horario de trabajo.

1.5.2.2 Disponer un sistema de Alarmas Centralizadas para reducir y reportar las incidencias fuera del horario de trabajo.

1.5.2.3 Establecer un sistema de Control de Acceso para controlar el ingreso y salida del personal a espacios comunes y restringidos.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes

2.1.1. Nacionales

- (Lima Ortega 2015) (1) en la tesis “Diseño e Implementación de un Sistema Integral de Seguridad, controlado y monitoreado en forma local y remota mediante las redes de comunicación para las agencias de Caja Rural Los Andes S.A.”. Su trabajo consiste en un sistema que utiliza técnicas de electrónica acordes a los conocimientos adquiridos en la carrera universitaria e ideas innovadoras que convierten al sistema de seguridad en un sistema autónomo, que integra diferentes elementos para que trabajen conjuntamente con las redes de comunicación públicas. La primera parte del proyecto consistió en la revisión de la documentación básica necesaria para poder comprender el funcionamiento de este tipo de sistemas, se realizó un estudio de los aspectos geográficos y ambientales a considerar y de la normativa pertinente. Considerando que el ámbito de trabajo de la empresa es el sector Rural, y el factor tecnológico es una limitante muy seria. Por último, se plantea un diseño aplicando los automatismos que permita la máxima eficiencia en el aprovechamiento de los medios geográficos y ambientales para los respectivos sistemas de alarmas.

- (Hernández Malca 2017) (2) En la tesis “Estudio de la Implementación de un sistemas de Video vigilancia basada en Tecnología IP para la Empresa Cobra Perú S.A. – Zonal Chiclayo 2017”. Su investigación tuvo como objetivo estudiar la implementación de un sistema de video vigilancia basada en tecnología IP para la empresa Cobra Perú – Zonal Chiclayo, de la ciudad de Chiclayo. La investigación fue cuantitativa desarrollada bajo el diseño no experimental, descriptivo. La población fueron los empleados de la empresa y la muestra se delimito a 41 de ellos; para la recolección de datos se utilizó el instrumento del cuestionario mediante la técnica de la encuesta, los cuales arrojaron los siguientes resultados: en la dimensión de Nivel de satisfacción de la seguridad actual

se observó que el 100% NO se siente satisfecho con la seguridad actual, con respecto a segunda dimensión de Nivel de impacto de la implementación de los sistemas de video vigilancia basada en tecnología IP, se observó la satisfacción del 100%, en caso exista impacto con respecto a la instalación de los sistemas de video vigilancia basada en tecnología IP. Estos resultados, coinciden con las hipótesis específicas y en consecuencia confirma la hipótesis general, quedando así demostrada y justificada la investigación de mejorar la administración en plataformas Cloud Computing en la empresa Cobra Perú S.A, Zonal Chiclayo.

- (Sierra García 2017) (3) en la tesis “Propuesta del Sistema de Video Vigilancia en la seguridad Ciudadana distrito de pueblo libre 2016-2020”. La tesis tuvo como objetivo general el implementar y articular el sistema de video vigilancia para solucionar una parte importante del problema de la seguridad ciudadana en el distrito de Pueblo Libre entre el 2016 y 2020, la que tiene a cargo la Gerencia de Seguridad Ciudadana de la Municipalidad, que cuenta con un aproximado de 200 trabajadores, y una cantidad aproximada de 189 equipos de video vigilancia, habiendo concluido y recomendado la cantidad y tipos de equipos de video vigilancia que faltan, los puntos sensibles donde se requieren las cámaras, la descentralización del centro de control y la articulación con la Policía Nacional, Serenazgo y los Comités de Juntas vecinales del distrito de Pueblo Libre.

El método utilizado en la investigación es el deductivo, de enfoque cualitativo, el diseño es de estudio de casos, hermenéutico Interpretativo, cuya información es de un período específico, que se desarrolló al aplicar las preguntas de acuerdo al problema del tema en investigación y el cuestionario de entrevista no estructurada, que brindaron información sobre cámaras de video, del incremento, la descentralización, los puntos sensibles. La investigación recomienda que para proponer una buena seguridad en el distrito de Pueblo Libre, se requiere de seis (06) centrales de control de Video Vigilancia descentralizados, aparte del centro de control principal, la instalación de sesenta (60) equipos de cámaras de

video vigilancia, en los lugares recomendados y la coordinación con Serenazgo, PNP y Juntas Vecinales .

2.1.2. Internacionales

- (Avilés – Coveña 2015) (4) en la tesis “Diseño e Implementación de un Sistema de seguridad a través de cámaras, sensores y alarmas, monitorizado y controlado telemétricamente para el Centro de Acogida “Patio Mi Pana” perteneciente a la fundación proyecto Salesiano”. Está basado en la integración de los distintos estudios aprendidos en el transcurso de la carrera, teniendo como propósito solucionar la problemática de Seguridad.

Su finalidad es el diseño e implementación de un sistema de seguridad que ayude al personal que habita y labora en las Instalaciones de la fundación. Comenzó con la elaboración de diagramas de conexiones físicas de todos los equipos que integran el sistema de seguridad, el paso siguiente fue la simulación y programación de la tarjeta electrónica de la central de alarmas haciendo uso del Software Proteus, Pic C, Pickit 2, entre otros, luego se efectuó la instalación y programación de las cámaras IP, sensores, alarmas. De esa manera se entregó un sistema de seguridad que tiene como objetivo la protección de los habitantes y trabajadores.

- (Álvarez franco 2017) (5) En la tesis “Sistema de Seguridad Electrónica de respaldo para las agencias del Banco del Pacifico basado en arduino y SMS”. El sistema de respaldo de alarmas se probó en dos sectores de la ciudad de Guayaquil, el panel con el sistema arduino se ubicó en el sector noroeste “Cdra. Valle de los Geranios Mz. 59B villa: 06 y los teléfonos celulares en la matriz del Banco del Pacifico, ubicado en Pedro Carbo 220 y P. Icaza octavo piso; existiendo una distancia aproximada de 20Km entre ambos puntos. La duración de las pruebas han sido de 90 días, dentro de los cuales se transmitieron señales de alarmas vía SMS. Para la comprobación del funcionamiento general del sistema; en estas pruebas, han participado varias personas las cuales incluyen a los operadores de consola del Banco del Pacifico, quienes monitorearon el sistema por medio de los teléfonos móviles. El propósito del proyecto es usarlo como un sistema redundante dentro de las agencias, ventanillas y

cajeros automáticos en la institución, cuando falle el panel de alarma principal el cual se comunica por vía IP, que actualmente es el único sistema con el que cuenta la institución para su control y vigilancia de alarmas, una vez que sea instalado el sistema de respaldo, entrara a operar y se comunicara por vía celular. Dando de esta manera continuidad al sistema de monitoreo.

-(Laura Guangasi 2011) (6) En la tesis “Red de Vigilancia mediante cámaras IP para el mejoramiento de la seguridad en el supermercado Express de la Ciudad de Ambato”. El proyecto se encuentra dividido en varios capítulos que comprende los aspectos más relevantes acerca de los métodos de vigilancia electrónica por medio de la tecnología IP.

El primer capítulo contiene el Planteamiento del Problema que enfoca la necesidad de establecer una verdadera investigación científica sobre nuevos sistemas de vigilancia; en base a esto, se realiza el planteamiento del problema, se justifica el proyecto enmarcando las delimitaciones y definiendo así los objetivos de la investigación.

El segundo capítulo trata sobre los principios teóricos, en el que se fundamenta el diseño del sistema propuesto, tomando en cuenta la evolución de los métodos de seguridad se realiza una breve descripción de conceptos fundamentales como: Video, Estándares, principios de funcionamiento.

El capítulo seis trata sobre la propuesta del sistema de vigilancia, donde se realiza un estudio previo de la red y los equipos existentes dentro de la empresa, además un análisis de factores que se deben tomar a consideración para poder determinar el tipo de cámara IP a utilizarse en los diferentes puntos estratégicos a ser monitoreadas, estableciendo tanto hardware como software necesario para el funcionamiento del sistema de seguridad, realizado el estudio se determinó así las respectivas conclusiones y recomendaciones del proyecto.

2.2. Base Teórica o Científica

2.2.1. Reduciendo Riesgos

Lambert (2013) (7) Sistemas de seguridad o vigilancia son diseñados para reducir riesgos. Los dueños de estos sistemas de vigilancia o seguridad invierten dinero por esa razón.

2.2.2. Seguridad Electrónica

Un Sistema de Seguridad Electrónico es la interconexión de recursos, redes y dispositivos cuyo objetivo es proteger la integridad de las personas y su entorno, previniéndolas de posibles peligros y presiones externas.

Las principales funciones de un Sistema de Seguridad Electrónico son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, etc.), la vigilancia remota mediante circuito cerrado de televisión (CCTV), detección/extinción de incendio. Asimismo, los sistemas de seguridad no sólo sirven para proteger a los bienes, inmuebles y las personas, sino que además ahorran tiempo y dinero en los procesos domésticos e industriales, al gestionar el funcionamiento y prevención de fallas en los mismos. (2017) *SISTEMA SEGURIDAD ELECTRONICA* - Cámara Nacional de Comercio y Servicios del Uruguay (8).

2.2.3. Tipos de Seguridad Electrónica

2.2.3.1 CCTV

Definición:

Este sistema es un instrumento visual de seguridad, evaluación y documentación.

Se utiliza por una o más de las siguientes razones:

-Vigilancia en forma directa.

-Reconstrucción luego de un incidente (forense).

-Disuasión.

-Evaluación de cualquier alarma activada para determinar la causa e iniciar una respuesta apropiada.

Elementos a tener en cuenta:

-Pase lo que pase, el sistema con el tiempo se volverá obsoleto (la tecnología avanza muy rápido).
-Si el sistema es muy antiguo, pero cumple con el objetivo para el que fue instalado, no es necesario su cambio.
No todos los tipos de cámaras sirven para todas las funciones: identificar personas a través de sus rostros (normalmente frente a una caja, mostrador o puerta de entrada), identificar escena general – acción de las personas (hall o similar para ver qué hace una persona o hacia dónde se dirige). (9) (2017) *SISTEMA SEGURIDAD ELECTRONICA* - Cámara Nacional de Comercio y Servicios del Uruguay.

Características de las cámaras:

Cantidad

La forma tradicional de comenzar y saber cuántas cámaras colocar es mediante el Teorema de la Galería de Arte y según necesidades de la Organización.

Calidad

Las cámaras se evalúan en función de factores como, si están a la intemperie, si están con una fuente de luz muy fuerte, cobertura que se desea abarcar, distancia de reconocimiento, calidad de luz en la oscuridad, cálculo de cobertura de cámaras (pixeles y resolución), etc.

Posición

Es importante definir qué objetivos tiene la instalación de cámaras y hacia qué objetivos se desea mirar, el problema común aquí son los puntos ciegos, cuando se concluye el trabajo por cambios o modificación de la estructura de los locales se generan puntos ciegos.

Primer Paso "Teorema de la Galería de Arte"

El problema de la vigilancia de la galería de arte es uno de esos problemas bonitos de las matemáticas. Se puede enunciar de forma sencilla, utilizando además elementos reales de la vida cotidiana. Todo el mundo puede analizar ejemplos concretos de "galerías de arte" que les permitirán entender mejor, con

más profundidad, el problema. Tiene una demostración bella, con una parte visual muy atractiva y que puede entender cualquier persona. Los resultados matemáticos relacionados tienen aplicaciones reales. Y existen interesantes generalizaciones del problema, lo que hace que sea un problema vivo.

En 1973 el matemático norteamericano Víctor Klee le propuso a su colega Václav Chvátal el conocido como problema de la galería de arte, que pertenece al área de las matemáticas que recibe el nombre de “Geometría Combinatoria”:

¿Cuál es el mínimo número de guardas, o cámaras de vigilancia, que se necesitan para vigilar una galería de arte?

(10) Aigner y Ziegler, El libro de las demostraciones, 2005

El “Teorema de la Galería de Arte” consiste en plasmar el plano del local a una figura geométrica y dibujar y proyectar triángulos la mayor posible, evitando solaparse, luego se ubica en cada vértice un punto el cual es llenado con la cantidad de cámaras o alarmas.

Ejemplo un local que tiene la forma de un rectángulo, se le podrá inscribir 2 triángulos y cada triangulo tiene 2 vértices por lo tanto el mínimo seria 2 cámaras o 2 sensores que abarcan el local de forma de un rectángulo.

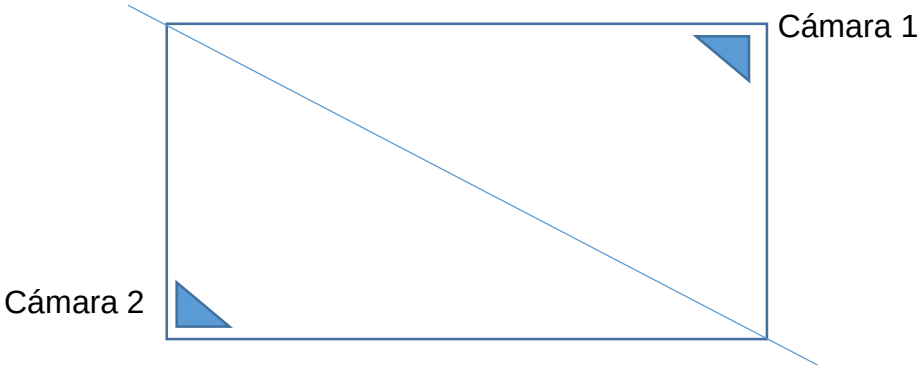


Figura 1. Teorema de la Galería de Arte
Fuente: Elaboración propia.

CCTV (Circuito Cerrado de TV)

Elementos que lo integran

Los elementos que lo integran son:

El equipo que almacena y procesa las imágenes **DVR o NVR**, tiene como función principal digitalizar la señal de video que ingresa de una cámara analógica o ip y

posteriormente la transmisión a una red de datos. El protocolo de digitalización es un algoritmo usado por Dahua el H.264, H.265 y con mejoras el H.264 plus, H.265 plus. La resolución o tamaño de fotogramas que componen el streaming de video consiste a mayor tamaño de imagen más detalles se pueden observar pero en contraposición tendremos una mayor tasa de bits para la transmisión.

Los FPS es la cantidad de fotogramas por segundo cuantos más fotogramas tenemos mejora la sensación de fluidez pero en contraparte aumenta la tasa de bits.

La tasa de bits o bit rate, tiene razón directa en la calidad de imagen de los fotogramas.

Figura 2. DVR Dahua.
Fuente: Elaboración propia.

Cámaras, dependiendo pueden ser de tipo domo, tubular, ptz, etc.; según la resolución hay de 760MP, 1080MP, 2K, 4K, etc.; analógicas o digitales, etc. Algunas características que se usan son en el caso de Dahua, la característica Starlight que tiene sensibilidad alta a la luz, ya que ofrece imágenes más nítidas y brillantes en lugares oscuros.

Esa característica se usa en bóvedas o lugares de almacenamiento donde no necesariamente existe iluminación constante. Material plástico o metálico, resistencia a tipos de entornos, conformidad ONVIF, que es un protocolo que asegura la interoperabilidad entre fabricantes independientes.

Figura 3. Cámara Dahua
Fuente: Elaboración propia.

Conexión, ya sea inalámbrico como cableado, en nuestro caso se recurrirá a un cableado cat 6a, STP, marca Dixon código 9067. Lo más importante en el entornos que se usara cable Ethernet es considerar la distancia recomendada y para evitar interferencia electromagnética un cable STP apantallado.

Figura 4. Cable Dixon
Fuente: Elaboración propia.

Balun, es un dispositivo conductor que convierte líneas de transmisión desequilibradas en líneas equilibradas que permite usar cable de red en lugar de cable coaxial para conectar una cámara de vigilancia el grabador.

Figura 5. Balun Dahua
Fuente: Elaboración propia.

Disco duro, para almacenar el video por los días necesarios, algunos equipos que se instaló tienen la capacidad de soportar 2 discos de 6 terabytes Purple WD, la característica de estos discos es el uso por 24 horas al día los 7 días a la semana y los 365 días del año, se configura según el trabajo, por lo tanto a mayor movimiento se almacena y si no existe movimiento se reduce el almacenamiento, estos discos funcionan en elevadas temperaturas, escritura continua, incrementa la densidad en las áreas de formato en la mayoría de locales tenemos un total de 12 terabytes de almacenamiento.

Figura 6. Disco duro de 6 TB WD
Fuente: Elaboración propia.

2.2.3.2 Alarmas

Definición:

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

Por ejemplo:

- La intrusión de personas.
- Inicio de fuego.
- El desbordamiento de un tanque.

Cualquier situación que sea anormal para la agencia.

Son capaces de reducir el tiempo de ejecución de las acciones a tomar en función del problema presentado, reduciendo así las pérdidas.

Partes

Un sistema se compone de varios dispositivos conectados a una central.

Central procesadora o panel de control: es la CPU del sistema. En ella se albergan la placa base, la fuente, la memoria central, dispositivos de comunicación al exterior. Esta parte del sistema es la que recibe las diferentes señales que los diferentes sensores pueden emitir, y actúa en consecuencia, disparando la alarma, comunicándose con "el servicio de monitoreo" por medio de un módem, comunicador incorporado, por TCP/IP, GPRS o Transmisor de radio. Se alimenta a través de corriente alterna y de una batería de respaldo, que en caso de corte de la energía, le proporcionaría una autonomía al sistema de entre 24 horas y 4 días (dependiendo de la capacidad de la batería).

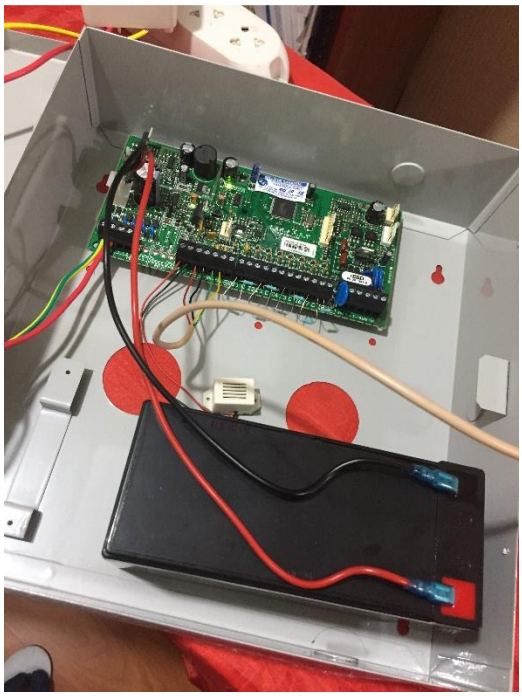


Figura 7: Placa Paradox SP6000 conectado a la batería
Fuente: Elaboración propia.

Sensor PIR: se activa por un movimiento, como indica el piloto LED rojo encendido.

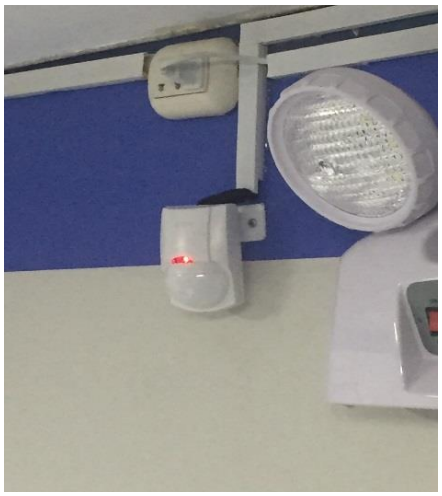


Figura 8. Sensor de movimiento o PIR
Fuente: Elaboración propia

Teclado: es el elemento más común y fácil de identificar en una alarma. Se trata de un teclado numérico del tipo telefónico. Su función principal es la de permitir a los usuarios autorizados (usualmente mediante códigos prestablecidos) armar (activar) y desarmar (desactivar) el sistema. Además de esta función básica, el

teclado puede tener botones de funciones como: Emergencia Médica, Intrusión, Fuego, etc. Por otro lado, el teclado es el medio más común mediante el cual se configura el panel de control.

Figura 9. Teclado Paradox led
Fuente: Elaboración propia.

Sirena exterior: es el elemento más visible desde el exterior del inmueble protegido. Se trata de una sirena con autonomía propia (puede funcionar aun si se le corta el suministro de corriente alterna o si se pierde la comunicación con la central procesadora) colocada dentro de un gabinete protector (de metal, policarbonato, etc.). Puede tener además diferentes sistemas luminosos que funcionan en conjunto con la disuasión sonora. La sirena exterior es opcional y en algunos sitios desaconsejada, en cambio la sirena interior resulta obligatoria de acuerdo con las normas europeas y americanas.

Figura 10. Sirena
Fuente: Elaboración propia.

Contactos magnéticos: se trata de un sensor que forma un circuito cerrado por un imán y un contacto muy sensible que al separarse, cambia el estado (se puede programar como NC (Normalmente Cerrado) o NA (Normalmente Abierto)) provocando un salto de alarma. Se utiliza en puertas y ventanas, colocando una parte del sensor en el marco y otra en la puerta o ventana misma.

Figura 11. Contacto Magnético
Fuente: Elaboración propia.

Detectores de rotura de cristales: son detectores microfónicos, activados al detectar la frecuencia aguda del sonido de una rotura de cristal.

Módulo de Internet: Específicamente el IP150, es un módulo de comunicación por Internet, para controlar y monitorizar la central.

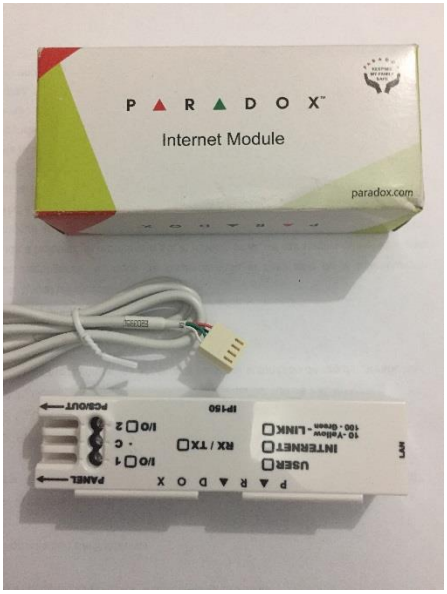


Figura 12. Módulo de Internet IP150
Fuente: Elaboración propia.

Expansor de Zonas: se usará el 8-Zone Expansion Modules, sirve para extender el alcance del cableado y ampliar la cantidad de dispositivos a instalar.

Figura 13. 8-Zone Modulo de Expansión
Fuente: Elaboración propia.

2.2.3.3 Control de Acceso

Un control de accesos es una solución que tiene por objeto impedir el libre acceso del público en general a diversas áreas que denominaremos protegidas. Por lo tanto lo primero que se debe identificar, para justificar la instalación de un control de accesos, es la existencia de activos que se desean proteger. En una empresa o comercio estos elementos a proteger pueden ser fácilmente identificables, como las zonas donde se manipula dinero, donde se guardan los registros de socios, planos de ubicación de bóvedas, entre otras, y algunas no tan obvias, como los sectores donde se resguarda los objetos de valor personal de los empleados. En otras ocasiones es necesario proteger áreas donde solo puede haber personal técnicamente capacitado como salas de energía, desechos peligrosos, etc. O, simplemente, el control de accesos también puede ser utilizado para contener a los empleados en las áreas donde realizan sus tareas, evitando así personas deambulando por sectores donde no deberían estar para no perturbar el normal funcionamiento de una empresa.

Luis Cosentino.

Figura 14. Control de Acceso por huellas digitales
Fuente: Hikvision.

2.3 Definición de Términos

1. Alarma: señal que avisa de un peligro.

2. Amenaza: circunstancia que tiene el potencial de causar daños o pérdidas, puede ser en forma de robos, destrucción, divulgación, modificación de datos o negación de servicios (DOS).

3. AC: Corriente Alterna

4. Actuador: Se denominan actuadores aquellos elementos que pueden provocar un efecto sobre un proceso automatizado, el actuador recibe la orden de un

controlador y da una salida necesaria para activar a un elemento final de control como lo son motores, lámparas o válvulas.

5. Control: Es tener bajo supervisión una variable de un determinado proceso, la cual al final arroja un resultado, dicho resultado llega a un controlador y compara el resultado obtenido al final del proceso con un valor predeterminado y así lograr corregir el margen de error al final del proceso.

6. DC: Corriente Continua.

7. EMI: Interferencia Electromagnética.

8. Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

9. Frame: una imagen de Video Completa

10. Gestión tecnológica: Es conocimiento y es una práctica. Es un sistema de conocimientos y prácticas relacionados con los procesos de creación, desarrollo, transferencia y uso de la tecnología.

11. GSM: (Global System for Mobiles) Estándar paneuropeo para la constitución de redes telefónicas móviles celulares, creado por la CEPT y que utiliza el estándar ETSI en la banda 900 MHz.

12. GPRS: General Packet Radio Service. Tecnología de transmisión de voz y datos en terminales móviles. Algo más avanzado que el GSM y que funciona mediante la conmutación de paquetes entre el terminal (móvil) y la antena.

13. Homologar: Registrar y autorizar, oficial o privadamente, una determinada técnica o producto, un aparato, etc.

14. Incidente: Cosa que se produce en el transcurso de un asunto, un relato, etc., y que repercute en él alterándolo o interrumpiéndolo.

15. Lux: Unidad de medida de intensidad de luz.

16. Monitoreo: Es la supervisión y control permanente de eventos anómalos ocasionados en los sistemas de alarmas y que son realizados a través de medios técnicos y humanos.

17. PGM: Son terminales de salida programables del panel de alarmas que permiten automatizar procesos, tales como: Encender la luz en el área donde se produjo una alarma, activar o desactivar el aire acondicionado, controlar una puerta eléctrica, etc.

18. Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

19. Seguridad Electrónica: Es un conjunto de equipos y dispositivos electrónicos que instalados en un establecimiento, sea residencial, comercial o industrial, controlan y advierten a través del censado de parámetros eléctricos, los riesgos para la vida y los bienes de las personas que allí residen, trabajan o atienden.

20. Sensor: Es un dispositivo capaz de medir magnitudes físicas o químicas, llamadas variables de instrumentación, y transformarlas en variables eléctricas. Las variables de instrumentación pueden ser por ejemplo: temperatura, intensidad, luminosa, distancia, aceleración, inclinación, desplazamiento, presión, fuerza, torsión, humedad, pH, etc.

21. Sistema de Seguridad: Es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas.

22. Sistema de prevención de intrusiones (IPS): Encargados de detectar y bloquear cualquier intento de intrusión, transmisión de código malicioso, o amenazas a través de la red.

23. Vulnerabilidad: Debilidad del Sistema informático que puede ser usada para causar algún tipo de daño.

24. Varifocal: Tipo de objetivo, lente que permite la regulación manual entre dos puntos focales para obtener el campo de visión deseado.

CAPITULO III

HIPOTESIS

3.1. Hipótesis General

La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una entidad Financiera

3.2. Hipótesis Específica

3.2.1. La puesta en funcionamiento de un Sistema CCTV posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.

3.2.2. La Implementación de un Sistema de Alarmas Centralizada Reducirá y Reportará las Incidencias fuera del horario de trabajo.

3.2.3. La puesta en marcha de un Sistema de Control de Acceso proporcionará controlar el ingreso y salida del personal a espacios comunes o restringidos.

3.3. VARIABLES

3.3.1. Definición conceptual de la variable

a) Variable Independiente

La Seguridad Electrónica.

El Sistema de Seguridad Electrónico se refiere a cualquier equipo electrónico que pueda realizar operaciones de seguridad como vigilancia, control de acceso, alarma o control de intrusión a una instalación o área que utiliza una fuente de alimentación de la red eléctrica y también un respaldo de energía como batería, etc.

b) Variable Dependiente

El Riesgo de Robo.

Riesgo es la posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufran perjuicio o daño.

Robo es un delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos de otras personas.

Riesgo de Robo es la posibilidad de que se produzca el apoderamiento de bienes ajenos.

3.3.2. Definición Operacional de la Variable

a) Variable Independiente (V.I.) (Seguridad Electrónica)

La Implementación de Seguridad Electrónica con los tres pilares iniciales; instalación de un sistema CCTV, instalación de alarmas centralizada y la instalación de control de acceso, permitirá reducir el riesgo de robos en una Entidad Financiera.

b) Variable Dependiente (V.D.) (Riesgo de Robo)

La reducción del Riesgo de Robo es el objetivo de toda organización y en especial de la Entidad Financiera y se conseguirá incorporando la Seguridad Electrónica a las medidas propias de la organización.

3.3.3 Operacionalización de las Variable

Tabla 4. Operacionalización de las Variables

VARIABLE Y TIPO DE VARIABLE	DIMENSION	INDICADOR	DESCRIPCION	ITEMS
VARIABLE DEPENDIENTE **RIESGO DE ROBO**	ROBO DE DINERO	CANTIDAD DE INCIDENTES DE ROBO DE DINERO	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron
	PERDIDA DE OBJETOS	CANTIDAD DE INCIDENTES DE PERDIDA DE OBJETOS	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron
	SABOTAJE	CANTIDAD DE INCIDENTES DE SABOTAJE	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron

	ARQUEO DESCUADRADO	CANTIDAD DE INCIDENTES DE ARQUEO DESCUADRADO	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron
	INTENTO DE INTRUSION A UNA AGENCIA FUERA DEL HORARIO DE TRABAJO	CANTIDAD DE INCIDENTES DE INTRUSION FUERA DEL HORARIO DE TRABAJO	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron
	INTRUSION DE PERSONAS AJENAS A LA COOPERATIVA EN AREAS RESTRINGIDAS	CANTIDAD DE INCIDENTES DE INTRUSION DENTRO DEL HORARIO DE TRABAJO	Semanalmente los días miércoles, se hace entrevistas entre el responsable de la implementación de Seguridad y el administrador de la agencia, para recabar información de la cantidad de incidentes en ese lapso de tiempo.	-Cantidad de incidentes semanal -Cantidad de incidentes semanal que se evitaron
VARIABLE INDEPENDIENTE	CCTV		La primera fase en la instalación de cámaras consiste en definir la cantidad de cámaras, para lo cual se recurre al “Problema de la galería”, y en base a los requerimientos de la empresa aseguradora y a los requerimientos de	Se hace una entrevista consultando si la cantidad sirvió para solucionar el incidente, si la

SEGURIDAD ELECTRONICA	(CENTRAL DE CAMARAS DE TV)	CANTIDAD DE CAMARAS	la Cooperativa, con lo que se determina la cantidad mínima de cámaras que se requiere, y luego se adiciona según prioridades, llegando a la cantidad a instalar. En base al resultado de las entrevistas y necesidad de la Coopac se adicionan algunas para llegar a un punto óptimo.	respuesta es negativa se hace la sub pregunta del ¿Por qué?
		CALIDAD DE CAMARAS	Se llega a la calidad de cada cámara según necesidades iniciales, técnicas y económicas, es el punto inicial, Pero en base a los requerimientos de la empresa aseguradora y a los requerimientos de la Cooperativa se llega a mejorar la calidad para cada área y puntos, llegando a un punto óptimo.	Se hace una entrevista consultando si la calidad sirvió para solucionar el incidente, si la respuesta es negativa se hace la sub pregunta del ¿Por qué?
		POSICION DE CAMARAS	Este indicador comienza con un punto de comienzo según necesidades iniciales y técnicas para luego en base al resultado de las entrevistas y necesidad de la Coopac se llega a un punto óptimo, también depende del mantenimiento preventivo.	Se hace una entrevista consultando si la posición sirvió para solucionar el incidente, si la respuesta es negativa se hace la sub pregunta del ¿Por qué?
			El factor más importante es llegar al tiempo de respuesta óptimo que está en	Se hace una entrevista

	ALARMAS	TIEMPO DE RESPUESTA OPTIMO DE LA ALARMA	relación al sonido de la sirena, la señal de llamada, y el tiempo que demora la persona encargada (administrador de agencia) de desactivar la alarma.	consultando el tiempo óptimo de respuesta de la alarma y el ¿Por qué?
		CANTIDAD DE SENSORES	Es muy importante tener la cantidad optima de sensores, muchas veces se efectúan cambios en la infraestructura de las agencias lo que crea zonas ciegas para los sensores	Se hace una entrevista consultando si existen cambios estructurales o movimientos de mobiliario y la zona.
		MANTENIMIENTO OPTIMO DE LA ALARMA	El mantenimiento es un tema vital, no es igual el tiempo de duración de una batería de respaldo en Lima y una por ejemplo en San Cristóbal (mina), en San Cristóbal hay muchos cortes de fluido y ahí funciona la batería y su tiempo útil es menor. O una agencia como Cobriza donde la humedad es muy alta y se deteriora con mayor facilidad.	Se hace una entrevista consultando el funcionamiento óptimo de algunos componentes de la alarma. Y el ¿Por qué?
	CONTROL DE ACCESO(C.A.)	OPERATIVIDAD OPTIMA	Para lograr un funcionamiento óptimo del control de acceso, se hace entrevistas a todo trabajador desde el encargado de limpieza hasta los administradores y cada uno tiene	-Se efectúa una entrevista a todo el personal, sobre el ingreso a áreas restringidas a personal externo,

			necesidades diferentes en el uso de espacios.	¿Por qué? - Se efectúa una entrevista a todo el personal si el Control de Acceso ocasiona interferencia en actividades laborales, ¿Por qué? - Se efectúa una entrevista a todo el personal si el Control de Acceso ocasiona interferencia de actividades personales, ¿Por qué?

Fuente: Elaboración propia.

CAPITULO IV

METODOLOGIA

4.1. Método de Investigación

La investigación realizada es Deductivo-Inductivo, usando el análisis documental, principalmente entrevistas, etc.; en el caso deductivo se dedujo conclusiones lógicas a partir de una serie de premisas o principios y en el caso inductivo se sacó conclusiones generales partiendo de hechos particulares.

4.2. Tipo de Investigación

Por el tipo de investigación, el presente estudio reúne las condiciones metodológicas de una investigación Aplicada, Según Murillo (2008), la investigación aplicada recibe el nombre de "investigación práctica o empírica", que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la practica basada en investigación.

4.3. Nivel de Investigación

De acuerdo a la investigación, agrupa por su nivel las características de un estudio Explicativo. Según el autor Sampieri (2019), Los estudios Explicativos van más allá de la descripción de fenómenos, conceptos o variables o del establecimiento de relaciones entre estas, como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta.

4.4. Diseño de Investigación. La investigación es Pre Experimental.

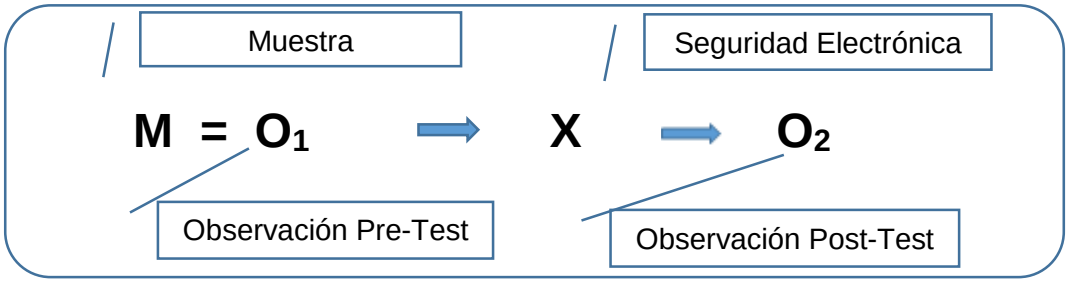


Figura 15. Entrada de datos Diseño de Investigación
Fuente: Elaboración propia.

4.5. Población y Muestra

Población

El presente trabajo fue desarrollado en una COOPAC (Cooperativa de Ahorro y Crédito) con 16 oficinas a nivel Nacional; el estudio e Implementación se efectúa en todas las oficinas, siendo la Población los "**incidentes de la COOPAC**", con una medida semanal durante 26 semanas previas y 26 semanas posteriores.
La medición semanal posterior se realizó los días miércoles, día que no hay mucha carga de trabajo para el personal.

Muestra

Toda la población fue la muestra debido a que la cantidad de incidencias es pequeña y se requiere la mayor fiabilidad en los resultados, por lo que se considera el total de manera representativa.

Muestreo

Debido a que consideramos a la población como muestra, no se realizará muestreo en la investigación.

4.6. Técnicas e Instrumentos de recolección de datos

Para el procesamiento y análisis de los datos recolectados se usara informe de incidentes semanal (anterior) y entrevistas telefónicas los días miércoles de los incidentes por semana con el administrador de cada agencia (posterior), nuestro instrumento principal es la entrevista.

Instrumentos

Variable Dependiente

Entrevistas estructurada y entrevista focalizada, donde se evalúa los incidentes de robo de dinero, perdida de objetos, sabotaje y arqueo de caja, en un determinado lapso de tiempo (semanal).

Variable Independiente

Para el análisis se tomara los resultados del análisis de la entrevista de incidentes, funcionalidad y tiempo de respuesta de los sensores.

Informe de Auditorías Internas de Funcionamiento, donde se evalúa la funcionalidad y tiempos de respuesta de los sensores.
Cronometro, para medir el tiempo de respuesta óptimo de los sensores de la puerta, ya que tiene un tiempo de retraso.

4.7. Técnicas de Procesamiento y Análisis de Datos

La técnica que se usara es la Prueba de rangos con signo de Wilcoxon

4.8. Aspectos Éticos de la Investigación

En el desarrollo del presente trabajo de Investigación se ha considerado de forma estricta el cumplimiento de los principios éticos que permite la originalidad de la Investigación.

4.9. Descripción de la Metodología Seleccionada

MODELO APLICATIVO

4.9.1. Metodología Top Down Design

La metodología elegida es la Top Down Design, diseño que se ajusta muy bien al trabajo efectuado en esta tesis, es una metodología que parte de arriba hacia abajo, desde concebir una idea general y fragmentarlo en módulos más pequeños, bajo una misma plantilla de desarrollo, y lo más importante que verificando y repitiendo este ciclo de verificación hasta obtener un producto óptimo. La implantación de la solución se enfoca en el mantenimiento y si requiere cambiar algo no es necesario cambiar todo, de lo contrario el percance es fácilmente detectable y subsanable, el desarrollo se efectúa con los módulos cada vez más pequeños y que conlleva a tener una forma más simple de trabajarlas todo bajo aportes del enfoque de Mejora Continua de Deming y usando algunos elementos de las mejores prácticas de la Gestión de Riesgos y Continuidad del Negocio.

Fases de la Metodología Top Down Design:

1.- Análisis de los Requerimientos

2.- Diseño Lógico del Sistema

3.- Diseño Físico del Sistema

4.- Probar y Optimizar el Sistema

4.9.1.1 Análisis de Requerimientos

a) Análisis del Objetivo del Negocio

RUBRO DE LA EMPRESA: FINANZAS

FECHA DE CREACION: 20 DE OCTUBRE DE 1963

MISION: Satisfacer las necesidades económicas, financieras y sociales de los socios, brindando servicios de calidad en el marco del desarrollo cooperativo y empresarial.

VISION: Ser una institución con liderazgo nacional que brinde servicios de calidad, mejorando el crecimiento económico, financiero y social de los socios en particular y la comunidad en general.

SERVICIOS: -Ahorros.
-Créditos.
-Convenios Institucionales
-Fondo de Previsión Social
-Tasas de intereses bajas
-Responsabilidad Social de los Socios.

OBJETIVOS EMPRESARIALES:

-Establecer con el socio vínculos cooperativos de largo plazo prestando ayuda económica.
-Mantener tasas de interés a los ahorros que beneficien a los socios.
-Incrementar las agencias a lo largo y ancho del territorio nacional, fortaleciendo así la presencia de la Institución.

b) Análisis de los Objetivos Técnicos

Se logró coincidir en varias reuniones con Gerencia y el área de Sistemas a los siguientes Objetivos técnicos, que se respetaran en todas las etapas ya lo largo del tiempo.

FLEXIBILIDAD.

Capacidad de adaptación a los cambios, tanto físicos, lógicos, tecnológicos y en el tiempo, ejemplo se requiera tener el número de serie de los billetes, se adicionara una cámara especial para dicho fin y no es necesario volver a diseñar todo.

REDUNDANCIA.

El objetivo es darle continuidad a la seguridad en caso ocurra algún intento de sabotaje o daño producido adrede o involuntario. Por ejemplo si la alimentación eléctrica de un panel deja de funcionar se deberá contar con otro medio que reemplace al que acaba de dejar de funcionar, o en caso de corte del hilo telefónico exista otra segunda alternativa que funcionara ni bien la otra está fuera de funcionamiento.

ESCALABILIDAD.

Capacidad de adaptarse a los incrementos, por ejemplo se requiera aumentar la cantidad de cámaras en lugares no definidos inicialmente, la solución debe tener esa capacidad sin requerir grandes modificaciones ni impacto general.

SEGURIDAD.

Capacidad de reducir el riesgo, esta es una de las prioridades fundamentales, tanto lógicas como el resguardo de las claves de acceso y serie de los equipos, y físicas considerando la seguridad perimetral de las centrales de cámaras y alarmas. Dotando de “tamper” o anti sabotaje; a las alarmas y en caso de corte de cable exista una señal de aviso.

DISPONIBILIDAD.

Situación de estar disponible. Se designara a un personal para que monitorice todos los sistemas instalados, con la consigna de que se tenga a disposición oportuna cuando se requiera, un ejemplo es en caso ocurra una señal de alarma dirigida a un número telefónico y esta no da recepción tener una segunda, o en el caso de daño de una central se tenga la reacción inmediata de detectar dicho percance y sustituir inmediatamente.

Bajo esas 5 objetivos técnicos se trabajara todos los módulos, todos en conjunto sin recurrir a prioridades.

c) Requerimientos

El primer paso luego de definir los objetivos técnicos es dejar una constancia de los mismos y definirlos como normas de trabajo. Una vez definidos los objetivos técnicos, se programó reuniones para definir la cantidad y posición de los equipos a instalar y las necesidades que se requiere. Para lo cual se recurrió a los planos estructurales de todas las agencias.

d) Plano de Ubicación Inicial

Se recolecto los 16 planos de cada agencia para hacer un esbozo inicial de la ubicación tanto de las cámaras, alarmas y centrales. Dando como resultado un “entregable de ubicación de cámaras y alarmas”.

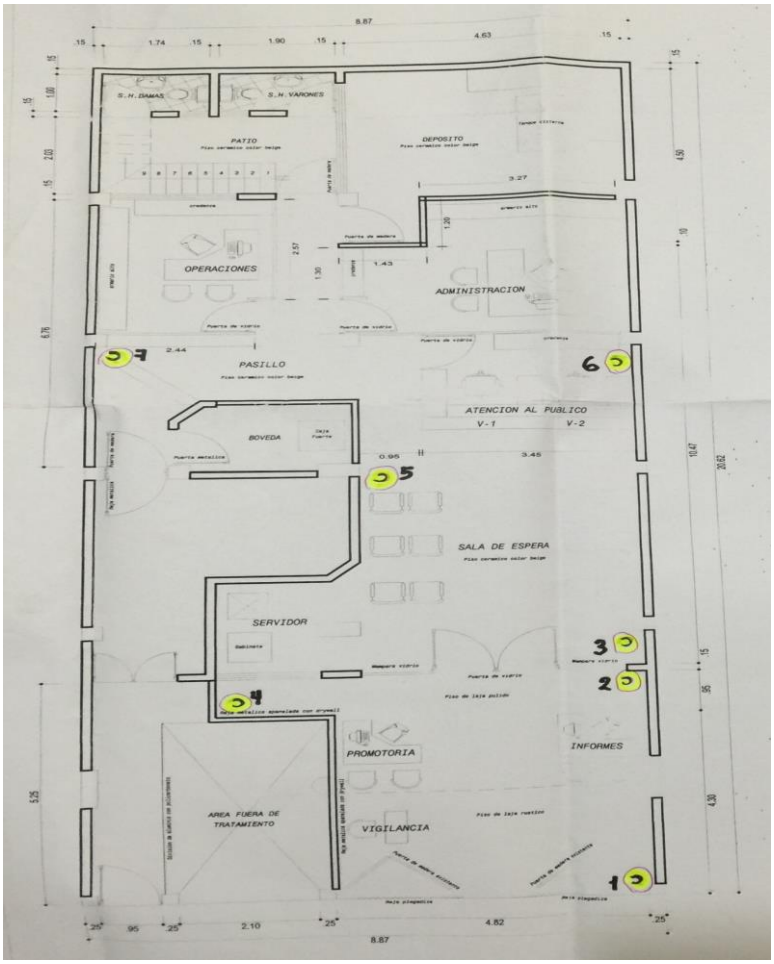


Figura 16. Plano de ubicación inicial
Fuente: Elaboración propia.

e) Ancho de Banda de Internet

Se analizó el ancho de banda inicial en las agencias y se dio informe del ancho de banda por local. Y el requerimiento de las necesidades una vez implementado en las 16 agencias con las recomendaciones por local.

Figura 17. Medición de ancho de banda
Fuente: Elaboración propia.

f) Ubicación de los Paneles y Central

Se revisó y analizo la ubicación más segura para ubicar las centrales y paneles, y se hizo de conocimiento de gerencia. Las características definidas son:

Seguridad, ventilación, orden, alimentación independiente, independiente al sistema de la agencia.

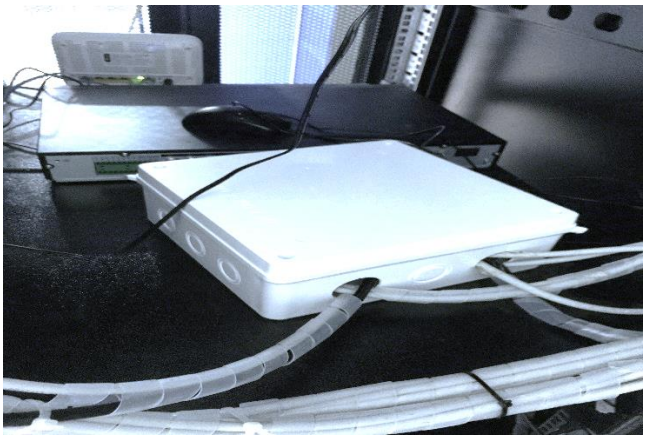


Figura 18. Ubicación de DVR, balun, conectores
Fuente: Elaboración propia.

4.9.1. 2. Diseño Lógico del Sistema

Diseño Topológico

Cámaras

La topología que se desarrollara es de tipo estrella, y estará bajo dos sistemas analogía e IP, se optara primero por la tecnología analógica y se procederá luego a implementar la IP, se definió de ese modo por temas económicos, costo beneficio.

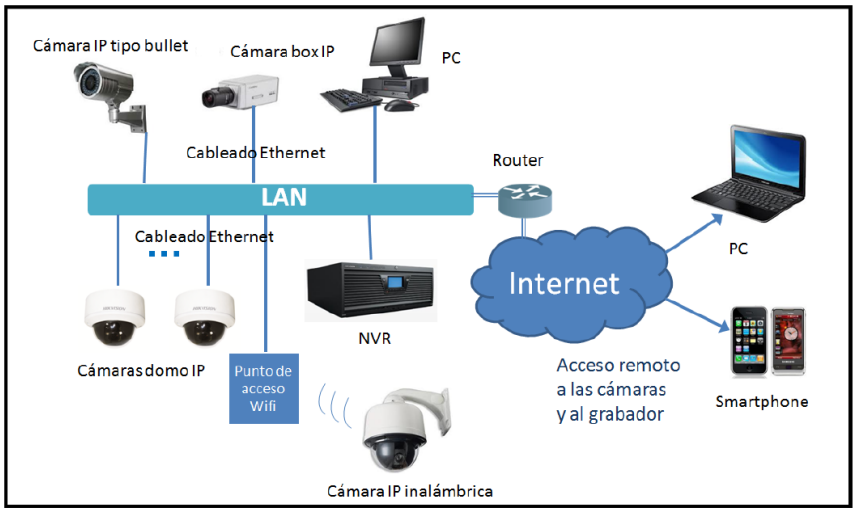


Figura 19. Topología Estrella
Fuente: https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf.

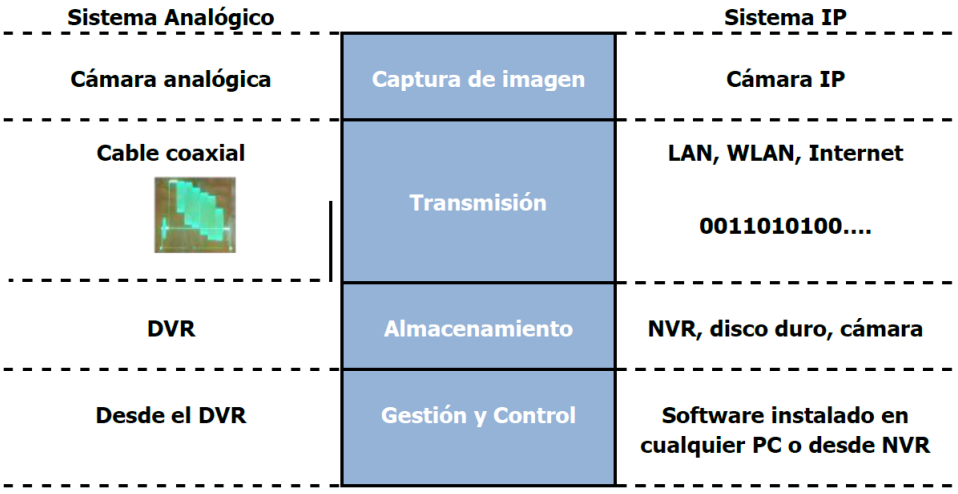


Figura 20. Tecnologías Analógicas e IP
Fuente: https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf.

Alarmas

La topología que se uso es la topología Estrella, siendo el eje principal el Panel Central

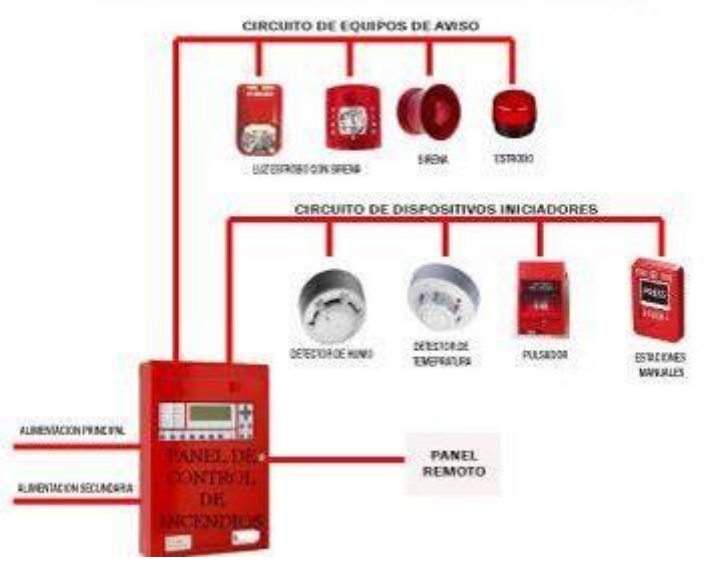


Figura 21. Topología Estrella alarmas
Fuente: http://createcsoft.com/aguascalientes-mexico/servicios/sistemas-de-deteccion-de-incendios.

Diseño del Modelo y Direcciones IP

Tabla 5. Designación de IP de las Agencias

UBICACION	DVR(SERIE PARA CONEXION)	USUARIO ADMINISTRADOR	USUARIO NORMAL			IP DVR
CAJAMARCA						192.127.1.137
TRUJILLO						192.127.2.137
HUARAZ						192.127.3.137
LIMA CENTRO						192.127.4.137
LIMA LOS OLIVOS						192.127.5.137
LIMA ATE						192.127.6.137
LA OROYA						192.127.7.137
HUANCAYO						192.127.8.137
C. DE PASCO						192.127.9.137
CASAPALCA						192.127.10.137
SAN CRISTOBAL						192.127.11.137
COBRIZA						192.127.12.137
CHIMBOTE						192.168.13.137
AREQUIPA						192.168.14.137
HOTEL HUARAZ						192.168.1.137
CHICRIN						192.168.1.137

Fuente: Elaboración propia.

Diseño de Ubicación Física de Cámaras y Sensores

Para lo cual se usó los planos de ubicación inicial.

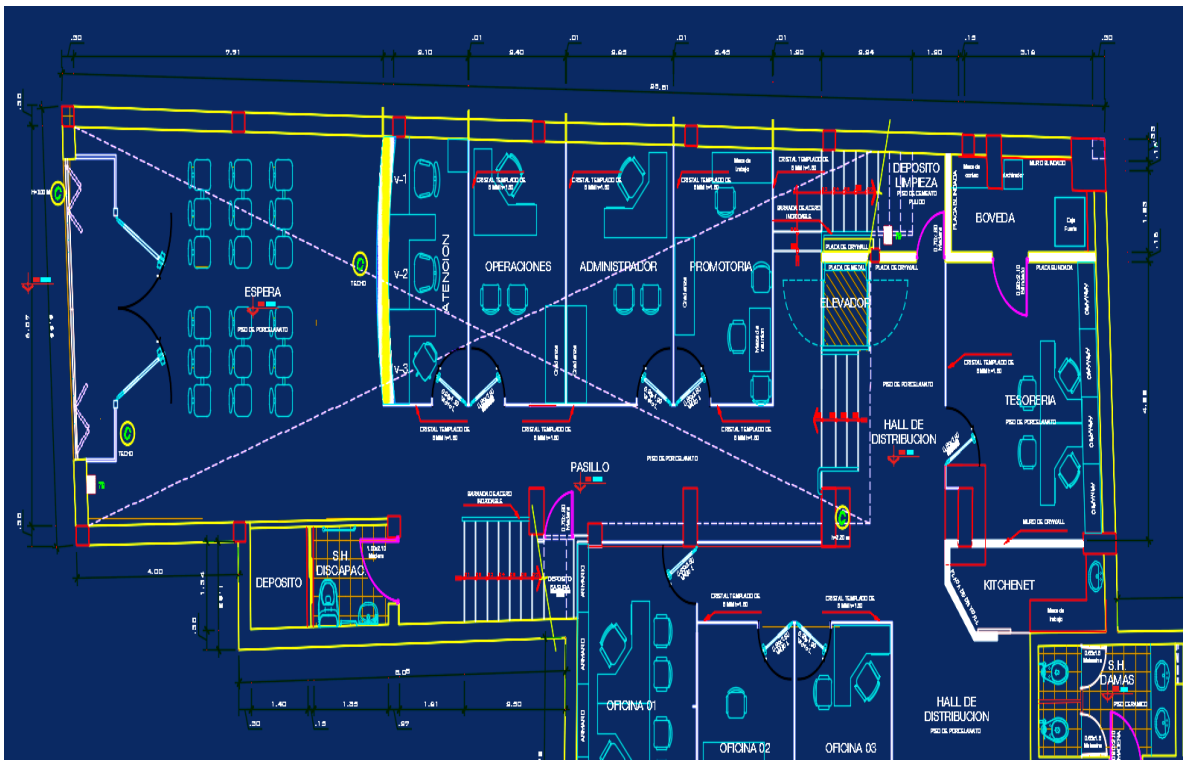


Figura 22. Plano de Ubicación Inicial de cámaras y sensores
Fuente: Elaboración propia.

Desarrollo de Estrategias de Seguridad

Según la metodología Top Down en el tema de seguridad elegimos 9 pasos importantes en el tema de seguridad, y se señala cada uno.

1. **Indique activos**. Los activos en primer lugar es el contenido de la bóveda, los equipos de cómputo, el material inmobiliario y las personas.
2. **Analice Riesgos de seguridad**. Cada local tiene su reporte de riesgos que es elaborado por la Compañía de Seguros la Positiva (Ver Anexos Riesgo de Seguridad).
3. **Analice los requerimientos de seguridad y restricciones**. En base a las reuniones con gerencia se pudo detectar entre muchos las 3 principales requerimientos x zona:

a) Cubrir la bóveda
b) Cubrir las cajas
c) Cubrir los ingresos y salida.

Según RFC 2196, "la Guía de Sitios de Seguridad" Un viejo tema en la seguridad es que el costo de protección contra una amenaza debería ser menos que el costo de recuperación si la amenaza fuera a golpearle. El costo en este contexto debería ser recordado para incluir pérdidas expresadas en verdadero dinero, reputación, honradez, y otras medidas menos obvia.

4. **Desarrolle un Plan de Seguridad**. Hay un plan de seguridad y está a cargo de una empresa de resguardo especializado y legalmente constituido compuesto por vigilantes armados. Pero adicionalmente se está desarrollando un Plan de Seguridad de Protección de la Seguridad Electrónica y un Protocolo de Procedimientos una vez ocurrido el incidente, para la protección de la tecnología y los activos, una política de seguridad es un documento vivo, la Organización siempre está en cambios constantes por lo mismo las políticas deberían seguir el mismo derrotero.
5. **Defina Políticas de Seguridad**. Existen algunos Protocolos de procedimientos en diferentes áreas: como Protocolo de transporte de Dinero, Protocolos de Seguridad de la Información, etc. Para nuestro caso estamos en proceso de terminar los Protocolos en base a las Políticas definidas, pero algunos como el caso de Protocolos de almacenamiento de Videos ya se tiene elaborado y funcionando:

	DIAS						
	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
Nivel de Backup	BT 1:10 p.m.	BI 1:10 p.m.	BI 1:10 p.m.	BT 1:10 p.m.	BI 1:10 p.m.	BI 11:30 a.m.	
	BI 4:00 p.m.			BI 4:30 p.m.			

Figura 23. Horarios para Protocolo de Seguridad de copia de videos
Fuente: Elaboración propia.

6. **Entrene a usuarios, gerentes y personal técnico**. El entrenamiento se efectúa entre el personal encargado de Seguridad Electrónica, el encargado de TI, y el Gerente General. (Ver Anexo Manual de usuario grabador Dahua)).

   En el equipo de grabación se tiene un Historial de Registro de Uso, donde indica, que usuario apago, que usuario reinicio, que usuario efectuó una copia; indicando usuario, fecha y hora.

Figura 24. Historial de Uso grabador Dahua
Fuente: Elaboración propia.

7. **Ponga en práctica la estrategia técnica y procedimientos de seguridad**, Se está desarrollando paulatinamente y prueba de eso son los resultados obtenidos.

   Uno de los pilares es la comunicación constante con los administradores por ejemplo cuando hacen modificaciones de los ambientes de la agencia a su cargo.

8. **Pruebe la seguridad y actualícelo si algún problema es encontrado**, La característica principal es probar y optimizar nuestro Sistema de Seguridad electrónica.

   Para el tema de Alarmas, por un periodo de varios meses auditoria interna efectúa revisiones de funcionamiento del sistema de Alarmas, el cual es resultado de las recomendaciones por la Compañía de Seguros. En base a eso retroalimentamos nuestro sistema.

   La prueba se efectúa del siguiente modo:

   a) Prueba de sabotaje, se efectúa un corte de un cable en cualquier parte de la red de alarmas, para esta prueba están presentes, un encargado de Seguridad Electrónica y el auditor interno.
   b) Prueba del temporizador de activación de la alarma en el área de bóveda, se activa la alarma y se prueba los sensores de la bóveda.
   c) Prueba de sincronización ingreso a la puerta principal, con la sirena y la salida de señal de aviso a un celular. Con esta prueba llegamos a encontrar el tiempo óptimo para activación y desarmado el sistema, y verificar el tiempo óptimo de la salida de señal de aviso. Para el tema de Cámaras, se efectúa una actualización ni bien exista un nuevo parche, y en base a las entrevistas con los administradores se llega a mejorar los tres indicadores de cámaras la cantidad, la posición y calidad.

9. **Mantenga la seguridad** programando auditorias periódicas, leyendo los log de auditoria, respondiendo a incidentes, leyendo y documentándose de la parte técnica de los equipos electrónicos, probando el Sistema y entrenarse, y actualizando el plan de Seguridad y Políticas.

FIREWALL

Las centrales de Cámaras DVR NVR, y la Central de Alarma y la Central de Control de Acceso, están en una red independiente, en un segmento de red independiente, y protegido por un Firewall en Linux en una distro Centos, con eso tenemos una capa de protección.

IDS

También se tiene un Sistema de Detección de intrusos por Host, que está analizando el tráfico en un servidor de almacenamiento de videos y log de la seguridad electrónica, se tiene un SNORT y un SURICATA en producción.

Seguridad de Claves

La clave tanta de Cámaras, Alarmas y Control de Acceso, sola es manejada por 2 personas, y esta resguardado, la característica es que las claves deben tener por lo menos 12 caracteres combinando números signos y letras,

4.9.1.3 Diseño Físico del Sistema

Informe Técnico de la Elección de la Tecnología para Cámaras, Alarmas y Control de Acceso.

PROYECTO:	INFORME TECNICO DE LAS CAMARAS, ALARMAS Y CONTROL DE ACCESO
OBJETIVO GENERAL:	Mejorar los niveles de Seguridad de la Institución.
OBJETIVOS ESPECIFICOS:	▪ Cumplir los requisitos en seguridad de la Institución. ▪ Lograr un avance tecnológico en la centralización de monitoreo de todas las sedes. ▪ Aumentar los niveles de satisfacción, confianza y seguridad de los clientes. ▪ Contribuir para la prevención de posibles riesgos o amenazas.

METAS:

- Lograr la satisfacción de los productos elegidos, tanto técnica, tecnológica y de garantía, y elegir la marca con la cual trabajar y los atributos técnicos de las cámaras y alarmas y del equipo de almacenamiento a elegir.
- Proponer la marca a trabajar, proponer los modelos que más se adecuan en cuanto a costo beneficios, y se presentara las recomendaciones a Gerencia.

BENEFICIOS: La de **supervisión, control** y **disuasión** en casos delictivos, **evidencia** en acciones delictivos, mejoramiento de la **efectividad y calidad de servicios** a los clientes.

Tipos de Cámaras y Elección de la Marca a Trabajar

Desde un punto de vista de marcas podemos considerar 3 tipos

a.- Las de mayor garantía y soporte pero el tema es el costo muy elevado, entre las cuales podemos citar algunas marcas: **Panasonic, Pelco, Lilin o JVC.**

El inconveniente es que los proveedores no tienen toda la gama de cámaras y solo importan algunos modelos pero de tipos muy básicos y el problema siempre radica en el costo muy elevado

b.- Las más cómodas o mal llamadas las chinas, son en realidad imitaciones a las cámaras originales y tienen un abanico grande de características y de precio bajísimo, pero su punto débil es la garantía, el tiempo de vida por el material que usan es muy reducido por lo que el tiempo de vida es una gran falencia.

c.- Las marcas originales y que combina la calidad garantía y el costo, por la masificación del mismo en el mercado peruano, entre las que decidimos trabajar con 2 marcas **DAHUA y HIKVISION,** garantía, tecnología propia y tiempo de vida es aceptable y tienen un gran abanico de modelos para diferentes necesidades.

Comparación entre las Marcas DAHUA Y HIKVISION

Esta comparativa ha sido hecha por nosotros. Toda la información y resultados responden a sus análisis. Se tomó esta base para elegir una de esas en la agencia de Trujillo. Las cámaras IP de 4 MP son las más comerciales, ofreciendo no sólo una mayor resolución sino también un WDR real a precios de cámaras con resolución “sólo” 1080p. Sin embargo, estos modelos iniciales salieron especialmente en gamas baja de productos, con lentes fijas y opciones limitadas.

Figura 25. Dahua Hikvision Comparativa
Fuente: Elaboración propia.

Ahora, Dahua y Hikvision han lanzado nuevos modelos de domos con características de gama alta, como el zoom y enfoque remoto, audio de dos vías a precios muy por debajo de los mínimos históricos.

Hemos comprado y puesto a prueba estos modelos de Dahua y Hikvision (Dahua IPC-HDBW2431R-Z y Hikvision HK-DS2CD1743G0-IZ) para ver sus diferencias con cámaras de 4 MPX de bajo coste, así como cámaras de 1080p de alto rendimiento.

Principales Ventajas

Los modelos Dahua y Hikvision probados aquí son opciones sólidas para aquellos que buscan un mayor rendimiento a 1080p, y que requieren zoom y enfoque remotos.

Campo de Visión y WDR

El rendimiento en escenas donde se necesita un mayor ángulo de visión y en escenas WDR fue mejorado ligeramente respecto a los modelos de bajo coste,

aunque ambas cámaras estudiadas aportan mejoras significativas en situaciones con poca luz la cámara Dahua le lleva de encuentro a la otra.

La Dahua superó a la Hikvision en nuestras pruebas, con una cobertura más uniforme de IR lo que resulta en un mejor rendimiento con poca luz y un enfoque más fácil debido de los botones de enfoque automático / remoto (ambas características le falta el modelo Hikvision).

Sin embargo, el consumo de ancho de banda del Hikvision era inferior al modelo Dahua 4MP en nuestras pruebas debido a su inclusión del CODEC H.264 plus inteligente. El espacio de almacenamiento puede ser ligeramente más bajo debido a esto al utilizar la cámara de Hikvision.

Resultados Claves

Aquí están las principales conclusiones de este ensayo:

- En amplios campos de visión (~ 60 '), el zoom de la cámara 4 MP Dahua tuvo un desempeño ligeramente mejor que el equivalente de 4 MP con zoom motorizado de Hikvision , con más incluso la exposición y una mejor legibilidad del gráfico.
- Ambas cámaras con zoom Dahua y Hikvision siempre ligeramente más detalles de la carta sujeto / prueba de que sus respectivos homólogos de bala lente fija en FOV ancho.
- A la luz baja, el zoom de la cámara Dahua 4 MP se comportó mejor que el equivalente Hikvision, que tenía un centro muy brillante punto de acceso IR, mucho más oscuro en los bordes del campo de visión.
- El Dahua incluye zoom motorizado, así como una salida de vídeo compuesto, lo que hizo que el objetivo y el enfoque más fácil. Hikvision incluye la salida de vídeo compuesto, pero no hay controles físicos en la cámara.
- El Hikvision incluye zoom lógico, pero no incluye el enfoque automático. modelo motorizado 4 MP de Dahua.

Focus / Características de Zoom

Aunque ambos modelos 4 MP probadas incluyen lentes con zoom, hay algunas diferencias clave entre los dos:

- Hikvision: No tiene enfoque automático y debe ajustarse a través de la interfaz web. El botón “Focus auxiliar” que se encuentra en la vista en vivo no activa el enfoque automático como lo hace en otros modelos.

Imagen Diurna – Comparación de Calidad

Comenzamos las pruebas en un campo de unos 58º.

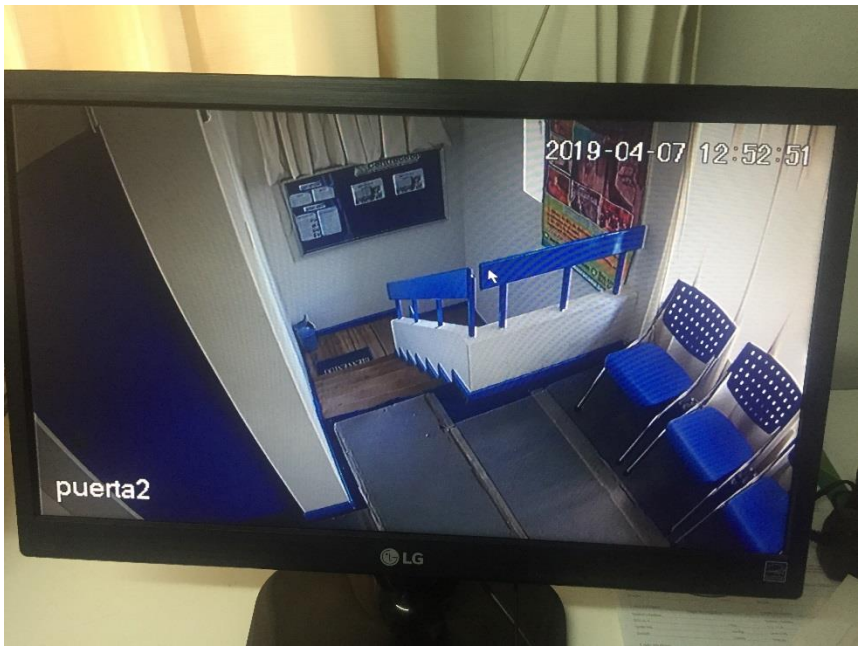


Figura 26. Prueba en el día
Fuente: Elaboración propia.

Los resultados son similares, con una ligera ventaja para Dahua debido a la sobre exposición en los modelos Hikvision.

Rendimiento de los infrarrojos

El patrón IR del Dahua fue ocupó el campo de visión completo, mientras que el Hikvision tuvo un fuerte punto caliente central, pero sobreexponía moderadamente los objetos, estando muy oscuro hacia los bordes del campo de visión. Aquí se ve el resultado de la cámara Dahua a 5 metros con zoom.

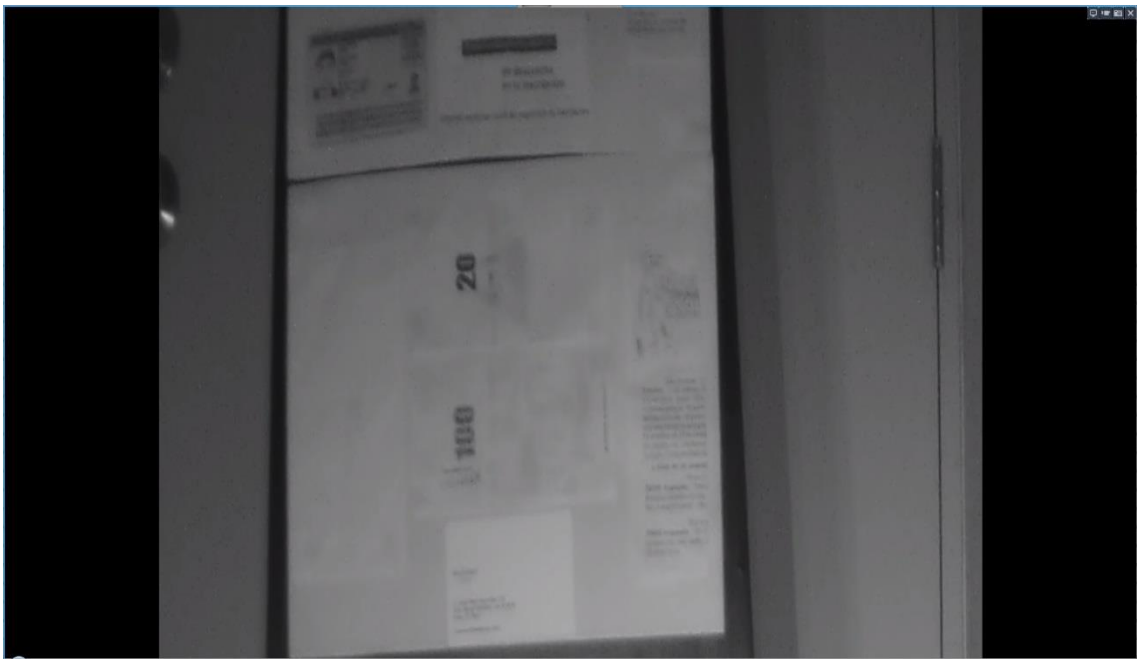


Figura 27. Prueba de noche
Fuente: Elaboración propia

Con el IR encendido, ambos modelos con zoom producen datos de menos calidad que sus equivalentes bullet de bajo costo debido a un ligero emborronamiento de la imagen. Hay que tener en cuenta que ambas cámaras se centraron de forma remota antes y después de cambiar a modo nocturno.

Comparación WDR

Se ha probado WDR en una escena de almacén, un contraluz intenso:

El modelo de zoom Dahua produjo los detalles más fuertes en esta escena, tanto en las zonas claras y oscuras de la escena, con una ligera ventaja sobre el rendimiento de Hikvision. WDR Los dos modelos de zoom dieron unos resultados ligeramente mejores que las bullet de bajo coste similar.

CONCLUSION

Dicho eso se eligió trabajar con el modelo **DAHUA**, pero están muy a la par en sus productos, por las características físicas del local, el clima, Dahua tiene muchos modelos de sensor para cámaras similares siendo las mejores de 1/3 costo beneficio, la característica WDR es mejor en Dahua, la tecnología de compresión con su algoritmo SMART H.265+, por la grabación nocturna, mejoras

significativas en sus DVR y NVR , con reducción de tamaño y ruido, reducción y optimización de los materiales y que soporta grandes temperaturas sin que se recaliente.

4.9.1.4. Probar y Optimizar el Sistema

Una vez efectuado la instalación se procedió a efectuar la parte medular, esta cuarta fase PROBAR Y OPTIMIZAR, usando como instrumento: entrevistas, a los administradores de las agencias de forma semanal, los días miércoles y se tiene una base de datos de 6 meses los que alimentan información del comportamiento de los sistemas y en base a eso se corrigen, modifican, cambian y mejoran los elementos instalados.

CAPITULO V

RESULTADOS

5.1 Contrastación de Hipótesis

5.1.1 Prueba de Normalidad

Como primer paso se efectuó la prueba de Normalidad a los valores cuantitativos, usando el método de Kolmogorov – Smirnov, porque la muestra maneja más de 50 valores, empleando el programa estadístico SPSS, con grado de confianza de 95%.

Para nuestro análisis se observará la Significancia (Sig.)

Si:

Sig. ≥ 0,05 → Es una Distribución Normal

Sig. < 0,05 → Es una Distribución no Normal

Tabla 6. Incidentes antes y después de la Instalación de la Seguridad Electrónica

ITEM	SEGURIDAD ELECTRONICA	INDICADOR	INCICENTES ANTES	INCIDENTES DESPUES
1	CAMARAS	ROBO DE DINERO	2	0
2	CAMARAS	ROBO DE DINERO	3	0
3	CAMARAS	ROBO DE DINERO	1	1
4	CAMARAS	ROBO DE DINERO	1	0
5	CAMARAS	ROBO DE DINERO	2	0
6	CAMARAS	ROBO DE DINERO	1	1
7	CAMARAS	ROBO DE DINERO	0	0
8	CAMARAS	ROBO DE DINERO	1	0
9	CAMARAS	ROBO DE DINERO	0	0
10	CAMARAS	ROBO DE DINERO	2	0
11	CAMARAS	ROBO DE DINERO	0	2
12	CAMARAS	ROBO DE DINERO	0	0
13	CAMARAS	ROBO DE DINERO	2	0
14	CAMARAS	ROBO DE DINERO	0	0
15	CAMARAS	ROBO DE DINERO	0	0
16	CAMARAS	ROBO DE DINERO	2	1
17	CAMARAS	ROBO DE DINERO	0	0
18	CAMARAS	ROBO DE DINERO	3	0
19	CAMARAS	ROBO DE DINERO	0	0
20	CAMARAS	ROBO DE DINERO	0	0
21	CAMARAS	ROBO DE DINERO	0	0

22	CAMARAS	ROBO DE DINERO	1	0
23	CAMARAS	ROBO DE DINERO	1	1
24	CAMARAS	ROBO DE DINERO	0	0
25	CAMARAS	ROBO DE DINERO	1	0
26	CAMARAS	ROBO DE DINERO	0	0
27	CAMARAS	PERDIDA DE OBJETOS	1	1
28	CAMARAS	PERDIDA DE OBJETOS	4	0
29	CAMARAS	PERDIDA DE OBJETOS	3	3
30	CAMARAS	PERDIDA DE OBJETOS	2	0
31	CAMARAS	PERDIDA DE OBJETOS	1	1
32	CAMARAS	PERDIDA DE OBJETOS	0	0
33	CAMARAS	PERDIDA DE OBJETOS	2	1
34	CAMARAS	PERDIDA DE OBJETOS	1	0
35	CAMARAS	PERDIDA DE OBJETOS	1	0
36	CAMARAS	PERDIDA DE OBJETOS	2	2
37	CAMARAS	PERDIDA DE OBJETOS	0	0
38	CAMARAS	PERDIDA DE OBJETOS	3	1
39	CAMARAS	PERDIDA DE OBJETOS	2	0
40	CAMARAS	PERDIDA DE OBJETOS	1	1
41	CAMARAS	PERDIDA DE OBJETOS	2	0
42	CAMARAS	PERDIDA DE OBJETOS	1	0
43	CAMARAS	PERDIDA DE OBJETOS	1	1
44	CAMARAS	PERDIDA DE OBJETOS	2	0
45	CAMARAS	PERDIDA DE OBJETOS	1	0
46	CAMARAS	PERDIDA DE OBJETOS	1	1
47	CAMARAS	PERDIDA DE OBJETOS	2	0
48	CAMARAS	PERDIDA DE OBJETOS	1	0
49	CAMARAS	PERDIDA DE OBJETOS	3	0
50	CAMARAS	PERDIDA DE OBJETOS	2	1
51	CAMARAS	PERDIDA DE OBJETOS	1	0
52	CAMARAS	PERDIDA DE OBJETOS	2	0
53	CAMARAS	SABOTAJE	0	0
54	CAMARAS	SABOTAJE	0	0
55	CAMARAS	SABOTAJE	2	0
56	CAMARAS	SABOTAJE	1	0
57	CAMARAS	SABOTAJE	0	1
58	CAMARAS	SABOTAJE	1	0
59	CAMARAS	SABOTAJE	0	0
60	CAMARAS	SABOTAJE	0	2
61	CAMARAS	SABOTAJE	1	0
62	CAMARAS	SABOTAJE	0	0
63	CAMARAS	SABOTAJE	2	0
64	CAMARAS	SABOTAJE	0	0
65	CAMARAS	SABOTAJE	0	0

66	CAMARAS	SABOTAJE	0	0
67	CAMARAS	SABOTAJE	0	0
68	CAMARAS	SABOTAJE	1	0
69	CAMARAS	SABOTAJE	0	0
70	CAMARAS	SABOTAJE	0	0
71	CAMARAS	SABOTAJE	2	1
72	CAMARAS	SABOTAJE	1	0
73	CAMARAS	SABOTAJE	0	0
74	CAMARAS	SABOTAJE	0	0
75	CAMARAS	SABOTAJE	0	0
76	CAMARAS	SABOTAJE	0	0
77	CAMARAS	SABOTAJE	1	0
78	CAMARAS	SABOTAJE	0	0
79	CAMARAS	ARQUEO DESCUADRADO	1	0
80	CAMARAS	ARQUEO DESCUADRADO	2	1
81	CAMARAS	ARQUEO DESCUADRADO	1	0
82	CAMARAS	ARQUEO DESCUADRADO	2	1
83	CAMARAS	ARQUEO DESCUADRADO	0	1
84	CAMARAS	ARQUEO DESCUADRADO	1	0
85	CAMARAS	ARQUEO DESCUADRADO	1	1
86	CAMARAS	ARQUEO DESCUADRADO	2	1
87	CAMARAS	ARQUEO DESCUADRADO	2	1
88	CAMARAS	ARQUEO DESCUADRADO	1	0
89	CAMARAS	ARQUEO DESCUADRADO	1	0
90	CAMARAS	ARQUEO DESCUADRADO	0	1
91	CAMARAS	ARQUEO DESCUADRADO	2	0
92	CAMARAS	ARQUEO DESCUADRADO	1	1
93	CAMARAS	ARQUEO DESCUADRADO	1	1
94	CAMARAS	ARQUEO DESCUADRADO	2	0
95	CAMARAS	ARQUEO DESCUADRADO	1	0
96	CAMARAS	ARQUEO DESCUADRADO	2	1
97	CAMARAS	ARQUEO DESCUADRADO	2	1
98	CAMARAS	ARQUEO DESCUADRADO	1	0

99	CAMARAS	ARQUEO DESCUADRADO	0	1
100	CAMARAS	ARQUEO DESCUADRADO	2	1
101	CAMARAS	ARQUEO DESCUADRADO	1	0
102	CAMARAS	ARQUEO DESCUADRADO	0	0
103	CAMARAS	ARQUEO DESCUADRADO	2	1
104	CAMARAS	ARQUEO DESCUADRADO	0	0
105	ALARMAS	ALARMAS INCIDENTES	0	0
106	ALARMAS	ALARMAS INCIDENTES	0	0
107	ALARMAS	ALARMAS INCIDENTES	1	0
108	ALARMAS	ALARMAS INCIDENTES	0	0
109	ALARMAS	ALARMAS INCIDENTES	0	1
110	ALARMAS	ALARMAS INCIDENTES	1	0
111	ALARMAS	ALARMAS INCIDENTES	0	0
112	ALARMAS	ALARMAS INCIDENTES	0	0
113	ALARMAS	ALARMAS INCIDENTES	1	0
114	ALARMAS	ALARMAS INCIDENTES	0	0
115	ALARMAS	ALARMAS INCIDENTES	0	0
116	ALARMAS	ALARMAS INCIDENTES	1	0
117	ALARMAS	ALARMAS INCIDENTES	0	0
118	ALARMAS	ALARMAS INCIDENTES	0	0
119	ALARMAS	ALARMAS INCIDENTES	1	1
120	ALARMAS	ALARMAS INCIDENTES	0	0
121	ALARMAS	ALARMAS INCIDENTES	0	0
122	ALARMAS	ALARMAS INCIDENTES	0	0
123	ALARMAS	ALARMAS INCIDENTES	2	0
124	ALARMAS	ALARMAS INCIDENTES	0	0
125	ALARMAS	ALARMAS INCIDENTES	0	0
126	ALARMAS	ALARMAS INCIDENTES	0	0
127	ALARMAS	ALARMAS INCIDENTES	1	0
128	ALARMAS	ALARMAS INCIDENTES	2	0
129	ALARMAS	ALARMAS INCIDENTES	1	0
130	ALARMAS	ALARMAS INCIDENTES	0	0
131	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
132	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	3	0
133	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
134	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
135	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
136	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	0

137	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
138	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
139	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
140	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	1	0
141	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	3	2
142	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
143	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
144	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
145	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	0
146	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
147	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
148	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	0
149	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
150	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
151	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	3	0
152	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	1
153	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	0	0
154	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	0
155	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	1	0
156	CONTROL DE ACCESO	CONTROL DE ACCEO INCIDENTES	2	0

Fuente: Elaboración propia.

Tabla 7. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Cámaras, Alarmas y Control de Acceso.

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	156	100.0%	0	0.0%	156	100.0%
después	156	100.0%	0	0.0%	156	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 8. Medida descriptiva antes y después de la instalación de la Seguridad Electrónica

Descriptivos				
			Estadístico	Error estándar
Incidentes antes	Media		0.91	0.077
	95% de intervalo de confianza para la media	Límite inferior	0.76	
		Límite superior	1.06	
	Media recortada al 5%		0.84	
	Mediana		1.00	
	Varianza		0.921	
	Desviación estándar		0.960	
	Mínimo		0	
	Máximo		4	
	Rango		4	
	Rango intercuartil		2	
	Asimetría		0.714	0.194
	Curtosis		-0.372	0.386
Incidentes después	Media		0.27	0.043
	95% de intervalo de confianza para la media	Límite inferior	0.18	
		Límite superior	0.35	
	Media recortada al 5%		0.20	
	Mediana		0.00	
	Varianza		0.288	
	Desviación estándar		0.537	
	Mínimo		0	
	Máximo		3	
	Rango		3	
	Rango intercuartil		0	
	Asimetría		2.147	0.194
	Curtosis		5.086	0.386

Fuente: SPSS
Elaboración propia.

Tabla 9. Prueba de Normalidad de la muestra de 156 valores

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
incidentes antes	0.264	156	0.000
incidentes después	0.461	156	0.000

a. Corrección de significación de Lilliefors

Fuente: SPSS
Elaboración propia.

Por los datos obtenidos estamos en el caso de:

Sig. < 0,05

Por lo tanto es una **Distribución no Normal o No Paramétrica**.

5.1.2 Prueba de Hipótesis

Usando la prueba de normalidad las variables que tenemos muestran una Distribución no Normal, lo que nos ubica en la Prueba no Paramétrica de estudio Longitudinal con dos medidas en momentos diferentes (antes de la Instalación y después de la Instalación de la Seguridad Electrónica) con lo que vamos a usar el Método de **Wilcoxon**.

Hipótesis General (HG)

La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una entidad Financiera

Hipótesis Específicas (HE)

(HE1) La puesta en funcionamiento de un Sistema CCTV posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.

(HE2) La Implementación de un Sistema de Alarmas Centralizada Reducirá y Reportará las Incidencias fuera del horario de trabajo.

(HE3) La puesta en marcha de un Sistema de Control de Acceso proporcionará controlar el ingreso y salida del personal a espacios comunes o restringidos.

5.1.2.1. Hipótesis General

HG: La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una entidad Financiera.

Definición de Variables

- IRRsse: Incidentes de riesgo de robo sin Seguridad Electrónica.
- IRRcse: Incidentes de riesgo de robo con Seguridad Electrónica.
- H0: Hipótesis Nula
- HA: Hipótesis Alternativa.
- HG: Hipótesis General
- HEn: Hipótesis Especifica, donde n es el número de hipótesis.

H0: La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down NO permitirá reducir el riesgo de robo en una entidad Financiera.

Si: IRRsse ≤ IRRcse → H0

Los Incidentes de Riesgo de Robo sin la Seguridad Electrónica son menores e iguales que con la Seguridad Electrónica.

HA: La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una entidad Financiera.

Si: IRRsse > IRRcse → HA

Los Incidentes de Riesgo de Robo con la Seguridad Electrónica son menores que sin la Seguridad electrónica.

Tabla 10. Prueba de Signo de Wilcoxon

Prueba de rangos con signo de Wilcoxon				
Rangos				
		N	Rango promedio	Suma de rangos
IRRcse - IRRsse	Rangos negativos	74[a]	41.41	3064.00
	Rangos positivos	7[b]	36.71	257.00

	Empates	75[c]		
	Total	156		

a. IRRcse < IRRsse
b. IRRcse > IRRsse
c. IRRcse = IRRsse

Fuente: SPSS
Elaboración propia.

Tabla 11. Estadísticos de Prueba

Estadísticos de prueba[a]	
	IRRcse - IRRsse
Z	-6,844[b]
Sig. asintótica(bilateral)	0.000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Fuente: SPSS
Elaboración propia

Podemos decir que, como el valor de la Sig. Asintótica (bilateral) es menor que 0.05, entonces se rechaza la Hipótesis Nula, además existe un valor alto de rangos negativos que apoyan inequívocamente los resultados. Y se concluye que hay evidencia suficiente para plantear que hay una Reducción de Incidentes de riesgo de Robo al Implementar la Seguridad Electrónica con un nivel de significación del 5%.

5.1.2.2. Hipótesis Específica

HE1: La puesta en funcionamiento de un Sistema CCTV posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.

Definición de Variables

- IRsse: Incidentes de Robo sin Seguridad Electrónica.
- IRcse: Incidentes de Robo con Seguridad Electrónica.

H0: La puesta en funcionamiento de un Sistema CCTV NO posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.

Si: IRsse ≤ IRcse → H0

Los Incidentes de Robo sin Seguridad Electrónica son menores e iguales que los Incidentes de Robo con Seguridad Electrónica.

HA: La puesta en funcionamiento de un Sistema CCTV posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.

Si: IRsse > IRcse → HA

Los Incidentes de Robo con la Seguridad Electrónica son menores que los Incidentes de robo sin la Seguridad Electrónica.

Tabla 12. Prueba de Rangos con signo de Wilcoxon

Prueba de rangos con signo de Wilcoxon				
Rangos				
		N	**Rango promedio**	**Suma de rangos**
IRcse - IRsse	Rangos negativos	11[a]	6.36	70.00
	Rangos positivos	1[b]	8.00	8.00
	Empates	14[c]		
	Total	26		
a. IRcse < IRsse				
b. IRcse > IRsse				
c. IRcse = IRsse				

Fuente: SPSS
Elaboración propia.

Tabla 13. Estadísticos de prueba

Estadísticos de prueba[a]	
	IRcse - IRsse
Z	-2,471[b]
Sig. asintótica(bilateral)	0.013
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Fuente: SPSS
Elaboración propia.

Podemos decir que, como el valor de la Sig. Asintótica (bilateral) es de 0.013 y siendo menor que 0.05, entonces se rechaza la Hipótesis Nula. Y se concluye que hay evidencia suficiente para plantear que hay una Reducción de Incidentes de Robo al Implementar la Seguridad Electrónica con un nivel de significación del 5%.

HE2: La Implementación de un Sistema de Alarmas Centralizada Reducirá y Reportará las Incidencias fuera del horario de trabajo.

Definición de Variables

- IAsse: Incidentes de Alarma sin Seguridad Electrónica.
- IAcse: Incidentes de Alarma con Seguridad Electrónica.

H0: La Implementación de un Sistema de Alarmas Centralizada NO Reducirá ni Reportará las Incidencias fuera del horario de trabajo.

$$\text{Si:} \quad IAsse \leq IAcse \quad \rightarrow \quad H0$$

Los Incidentes de Alarma sin Seguridad Electrónica son menores e iguales que los Incidentes de Alarma con Seguridad Electrónica.

HA: La Implementación de un Sistema de Alarmas Centralizada Reducirá y Reportará las Incidencias fuera del horario de trabajo.

$$\text{Si:} \quad IAsse > IAcse \quad \rightarrow \quad HA$$

Los Incidentes de Alarma con la Seguridad Electrónica son menores que los Incidentes de Alarma sin la Seguridad Electrónica.

Tabla 14. Rangos

Rangos				
		N	Rango promedio	Suma de rangos
IAcse - IAsse	Rangos negativos	8[a]	5.13	41.00
	Rangos positivos	1[b]	4.00	4.00
	Empates	17[c]		
	Total	26		
a. IAcse < IAsse				
b. IAcse > IAsse				
c. IAcse = IAsse				

Fuente: SPSS
Elaboración propia.

Tabla 15. Estadísticos de prueba

Estadísticos de prueba[a]	
	IAcse - IAsse
Z	-2,310[b]
Sig. asintótica(bilateral)	0.021
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Fuente: SPSS
Elaboración propia.

Podemos decir que, como el valor de la Sig. Asintótica (bilateral) es de 0.021 y siendo menor que 0.05, entonces se rechaza la Hipótesis Nula. Y se concluye que hay evidencia suficiente para plantear que hay una Reducción de Incidentes de Alarma al Implementar la Seguridad Electrónica con un nivel de significación del 5%.

HE3: La puesta en marcha de un Sistema de Control de Acceso proporcionará controlar el ingreso y salida del personal a espacios comunes o restringidos.

Definición de Variables

- ICAsse: Incidentes de Control de Acceso sin Seguridad Electrónica.
- ICAcse: Incidentes de Control de Acceso con Seguridad Electrónica.

H0: La puesta en marcha de un Sistema de Control de Acceso NO proporcionará controlar el ingreso y salida del personal a espacios comunes o restringidos.

$$\text{Si:} \quad ICAsse \leq ICAcse \quad \rightarrow \quad H0$$

Los Incidentes de Control de Acceso sin Seguridad Electrónica son menores e iguales que los Incidentes de Control de Acceso con Seguridad Electrónica.

HA: La puesta en marcha de un Sistema de Control de Acceso proporcionará controlar el ingreso y salida del personal a espacios comunes o restringidos.

Si: ICAsse > ICAcse → HA

Los Incidentes de Control de Acceso con la Seguridad Electrónica son menores que los Incidentes de Control de Acceso sin la Seguridad Electrónica.

Tabla 16. Prueba de Rangos con signo de Wilcoxon

Prueba de rangos con signo de Wilcoxon				
Rangos				
		N	Rango promedio	Suma de rangos
ICAcse - ICAsse	Rangos negativos	11[a]	6.00	66.00
	Rangos positivos	0[b]	0.00	0.00
	Empates	15[c]		
	Total	26		
a. ICAcse < ICAsse				
b. ICAcse > ICAsse				
c. ICAcse = ICAsse				

Fuente: SPSS
Elaboración propia.

Tabla 17. Estadísticos de prueba

Estadísticos de prueba[a]	
	ICAcse - ICAsse
Z	-2,980[b]
Sig. asintótica(bilateral)	0.003
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Fuente: SPSS
Elaboración propia.

Podemos decir que, como el valor de la Sig. Asintótica (bilateral) es de 0.003 y siendo menor que 0.05, entonces se rechaza la Hipótesis Nula. Y se concluye que hay evidencia suficiente para plantear que hay una Reducción de Incidentes de Control de Acceso al Implementar la Seguridad Electrónica con un nivel de significación del 5%.

5.2 Descripción de Resultados:

Los resultados obtenidos de la siguiente investigación está centrado en los “incidentes” ocurridos antes y después de la instalación de la Seguridad Electrónica, cuyo objetivo primordial es la influencia de la Instalación progresiva; un primer paso está focalizado en ese análisis de 26 semanas previas sin instalación y 26 semanas posteriores luego de la instalación progresiva de la Seguridad Electrónica, lo que nos permitirá obtener proyecciones e indicadores; posteriormente se efectuará un análisis en base a 26 semanas posteriores a la instalación progresiva, usando la Metodología Top Down se retroalimentó la Seguridad Electrónica, obteniendo cambios que serán analizados cada vez que se retroalimentó, en esta segunda parte nuestro análisis está centrado en los “incidentes” e “incidentes resueltos”.

5.2.1. INDICADOR: INCIDENTES DE ROBO DE DINERO (CAMARAS)

Vamos a detallar los casos que ocurren:

- Perdida de dinero de bóveda.
- Perdida de dinero de caja.
- Robo de dinero a la agencia en el día.
- Robo de dinero a personal de la agencia.
- Robo de dinero a personal externo de la agencia a socios en las instalaciones.

Tabla 18. Incidentes antes de la instalación – Robo de Dinero

16 AGENCIAS - Antes de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	2	1
2	0	0	0	3	1
3	0	0	0	1	0
4	0	0	0	1	0
5	0	0	0	2	1
6	0	0	0	1	0
7	0	0	0	0	0
8	0	0	0	1	0
9	0	0	0	0	0
10	0	0	0	2	0
11	0	0	0	0	0

12	0	0	0	0	0
13	0	0	0	2	1
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	2	0
17	0	0	0	0	0
18	0	0	0	3	1
19	0	0	0	0	0
20	0	0	0	0	0
21	0	0	0	0	0
22	0	0	0	1	0
23	0	0	0	1	0
24	0	0	0	0	0
25	0	0	0	1	1
26	0	0	0	0	0

Fuente: Elaboración propia.

Tabla 19. Incidentes después de la instalación – Robo de Dinero

16 AGENCIAS – Después de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	0	0
2	4	0	4	0	0
3	7	0	4	1	1
4	7	0	8	0	0
5	10	0	12	0	0
6	12	0	15	1	0
7	13	0	17	0	0
8	17	0	17	0	0
9	17	0	18	0	0
10	19	0	19	0	0
11	19	0	21	2	1
12	21	0	24	0	0
13	24	0	24	0	0
14	24	2	24	0	0
15	24	4	26	0	0
16	26	8	27	1	1
17	29	8	28	0	0
18	35	12	31	0	0
19	35	12	31	0	0
20	37	14	31	0	0
21	39	14	36	0	0
22	40	16	37	0	0
23	40	16	37	1	1
24	42	20	41	0	0

25	42	24	41	0	0
26	43	24	41	0	0

Fuente: Elaboración propia.

La Cantidad y Calidad son acumulativos y excluyentes y hasta la fecha de semana 26 se tenían 67 cámaras instaladas.

Tabla 20. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Robo de Dinero

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia

Tabla 21. Medida descriptiva antes y después de la instalación de cámaras- Robo de Dinero

Descriptivos				
			Estadístico	Error estándar
antes	Media		0.88	0.195
	95% de intervalo de confianza para la media	Límite inferior	0.48	
		Límite superior	1.29	
	Media recortada al 5%		0.82	
	Mediana		1.00	
	Varianza		0.986	
	Desviación estándar		0.993	
	Mínimo		0	
	Máximo		3	
	Rango		3	
	Rango intercuartil		2	
	Asimetría		0.778	0.456
	Curtosis		-0.513	0.887
después	Media		0.23	0.101
	95% de intervalo de confianza para la media	Límite inferior	0.02	
		Límite superior	0.44	
	Media recortada al 5%		0.16	
	Mediana		0.00	
	Varianza		0.265	

	Desviación estándar	0.514	
	Mínimo	0	
	Máximo	2	
	Rango	2	
	Rango intercuartil	0	
	Asimetría	2.260	0.456
	Curtosis	4.782	0.887

Fuente: SPSS
Elaboración propia

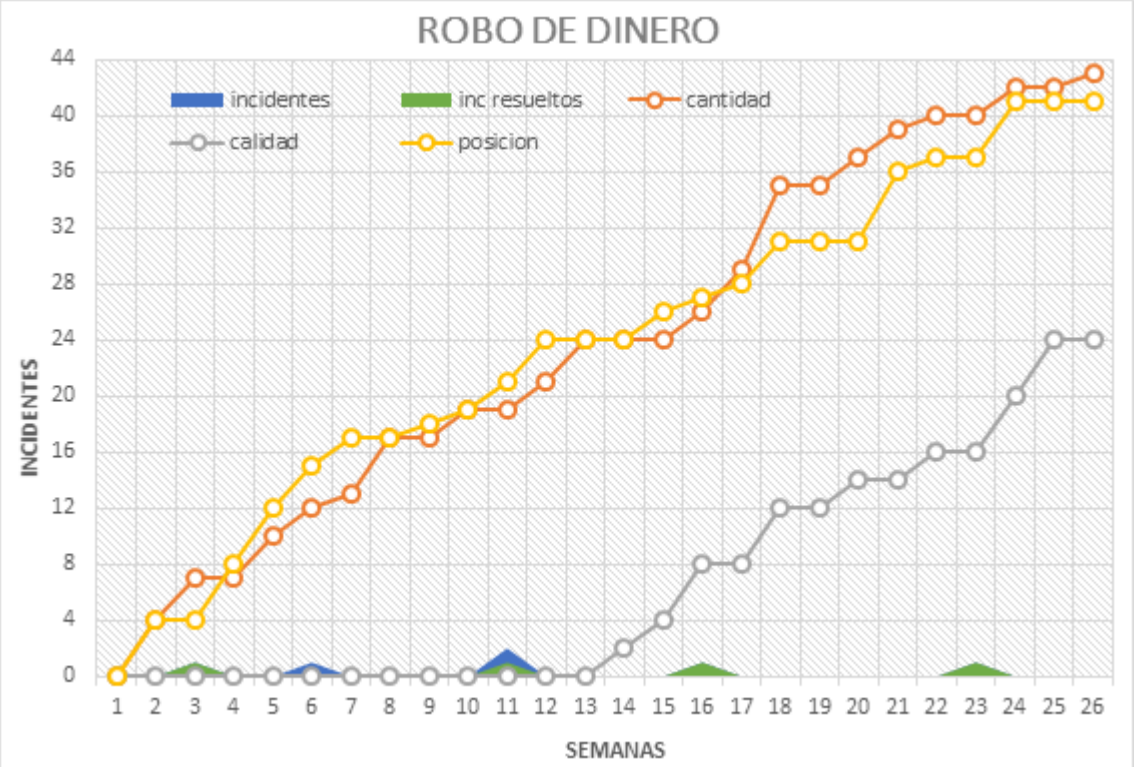


Figura 28. Indicador Robo de Dinero, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.2.2. INDICADOR: INCIDENTES DE PERDIDA DE OBJETOS (CAMARAS)

Vamos a detallar los casos que ocurren:

- Olvidar el DNI o documento del socio.
- Olvidar un objeto del socio.
- Perdida de objetos por parte de los trabajadores de la agencia.
- Supuestas pérdidas por parte de los socios.

Tabla 22. Incidentes antes de la instalación – Perdida de Objetos

16 AGENCIAS - Antes de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	1	1
2	0	0	0	4	2
3	0	0	0	3	2
4	0	0	0	2	1
5	0	0	0	1	1
6	0	0	0	0	0
7	0	0	0	2	1
8	0	0	0	1	0
9	0	0	0	1	0
10	0	0	0	2	1
11	0	0	0	0	0
12	0	0	0	3	1
13	0	0	0	2	0
14	0	0	0	1	1
15	0	0	0	2	1
16	0	0	0	1	0
17	0	0	0	1	0
18	0	0	0	2	1
19	0	0	0	1	0
20	0	0	0	1	1
21	0	0	0	2	1
22	0	0	0	1	0
23	0	0	0	3	1
24	0	0	0	2	1
25	0	0	0	1	0
26	0	0	0	2	1

Fuente: Elaboración propia.

Tabla 23. Incidentes después de la instalación – Perdida de Objetos

16 AGENCIAS – Después de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	1	1
2	4	0	4	0	0
3	7	0	4	3	2
4	7	0	8	0	0
5	10	0	12	1	1
6	12	0	15	0	0
7	13	0	17	1	1
8	17	0	17	0	0
9	17	0	18	0	0
10	19	0	19	2	1

11	19	0	21	0	0
12	21	0	24	1	1
13	24	0	24	0	0
14	24	2	24	1	1
15	24	4	26	0	0
16	26	8	27	0	0
17	29	8	28	1	0
18	35	12	31	0	0
19	35	12	31	0	0
20	37	14	31	1	1
21	39	14	36	0	0
22	40	16	37	0	0
23	40	16	37	0	0
24	42	20	41	1	1
25	42	24	41	0	0
26	43	24	41	0	0

Fuente: Elaboración propia

La cantidad y calidad son acumulativos y excluyentes y hasta la fecha de semana 26 se tenían 67 cámaras instaladas.

Tabla 24. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Perdida de Objetos

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 25. Medida descriptiva antes y después de la instalación de cámaras - Perdida de Objetos.

			Estadístico	Error estándar
antes	Media		1.62	0.185
	95% de intervalo de confianza para la media	Límite inferior	1.24	
		Límite superior	2.00	
	Media recortada al 5%		1.59	
	Mediana		1.50	
	Varianza		0.886	
	Desviación estándar		0.941	

	Mínimo		0	
	Máximo		4	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		0.574	0.456
	Curtosis		0.409	0.887
después	Media		0.50	0.149
	95% de intervalo de confianza para la media	Límite inferior	0.19	
		Límite superior	0.81	
	Media recortada al 5%		0.40	
	Mediana		0.00	
	Varianza		0.580	
	Desviación estándar		0.762	
	Mínimo		0	
	Máximo		3	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		1.766	0.456
	Curtosis		3.503	0.887

Fuente: SPSS
Elaboración propia

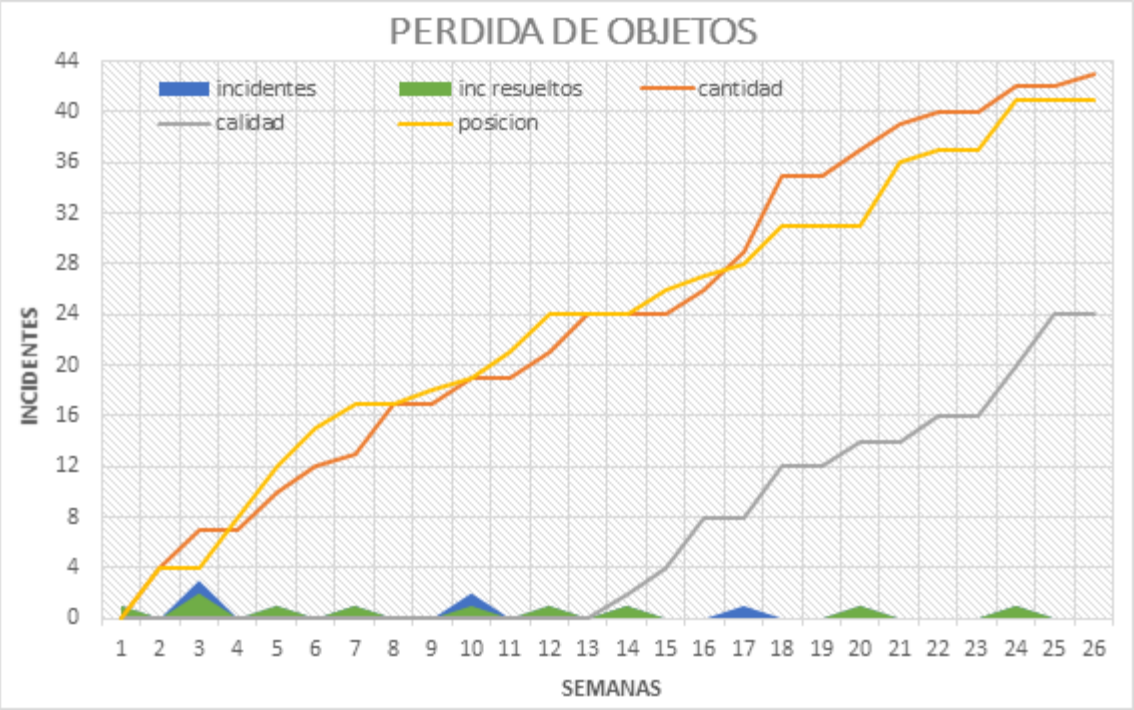


Figura 29. Indicador Pérdida de Objetos, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.2.3. INDICADOR: INCIDENTES DE SABOTAJE (CAMARAS)

Vamos a detallar los casos que ocurren:

- Empleados descontentos con el administrador y malogran equipos.
- Empleados descontentos con el administrador y modifican información de transacciones.
- Empleados descontentos con su centro de labores.

Tabla 26. Incidentes antes de la instalación – Sabotaje

16 AGENCIAS - Antes de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	2	1
4	0	0	0	1	0
5	0	0	0	0	0
6	0	0	0	1	0
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	1	0
10	0	0	0	0	0
11	0	0	0	2	1
12	0	0	0	0	0
13	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	1	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	2	1
20	0	0	0	1	0
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	0	0
24	0	0	0	0	0
25	0	0	0	1	0
26	0	0	0	0	0

Fuente: Elaboración propia.

Tabla 27. Incidentes después de la instalación – Sabotaje

16 AGENCIAS – Después de la Instalación					
semana	**cantidad**	**calidad**	**posición**	**incidentes**	**Inc. resueltos**
1	0	0	0	0	0
2	4	0	4	0	0
3	7	0	4	0	0
4	7	0	8	0	0
5	10	0	12	1	1
6	12	0	15	0	0
7	13	0	17	0	0
8	17	0	17	2	1
9	17	0	18	0	0
10	19	0	19	0	0
11	19	0	21	0	0
12	21	0	24	0	0
13	24	0	24	0	0
14	24	2	24	0	0
15	24	4	26	0	0
16	26	8	27	0	0
17	29	8	28	0	0
18	35	12	31	0	0
19	35	12	31	1	1
20	37	14	31	0	0
21	39	14	36	0	0
22	40	16	37	0	0
23	40	16	37	0	0
24	42	20	41	0	0
25	42	24	41	0	0
26	43	24	41	0	0

Fuente: Elaboración propia.

La cantidad y calidad son acumulativos y excluyentes y hasta la fecha de semana 26 se tenían 67 cámaras instaladas.

Tabla 28. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Sabotaje

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 29. Medida descriptiva antes y después de la instalación de cámaras - Sabotaje.

			Estadístico	Error estándar
antes	Media		0.46	0.138
	95% de intervalo de confianza para la media	Límite inferior	0.18	
		Límite superior	0.75	
	Media recortada al 5%		0.40	
	Mediana		0.00	
	Varianza		0.498	
	Desviación estándar		0.706	
	Mínimo		0	
	Máximo		2	
	Rango		2	
	Rango intercuartil		1	
	Asimetría		1.255	0.456
	Curtosis		0.305	0.887
después	Media		0.15	0.091
	95% de intervalo de confianza para la media	Límite inferior	-0.03	
		Límite superior	0.34	
	Media recortada al 5%		0.07	
	Mediana		0.00	
	Varianza		0.215	
	Desviación estándar		0.464	
	Mínimo		0	
	Máximo		2	
	Rango		2	
	Rango intercuartil		0	
	Asimetría		3.217	0.456
	Curtosis		10.480	0.887

Elaboración propia.

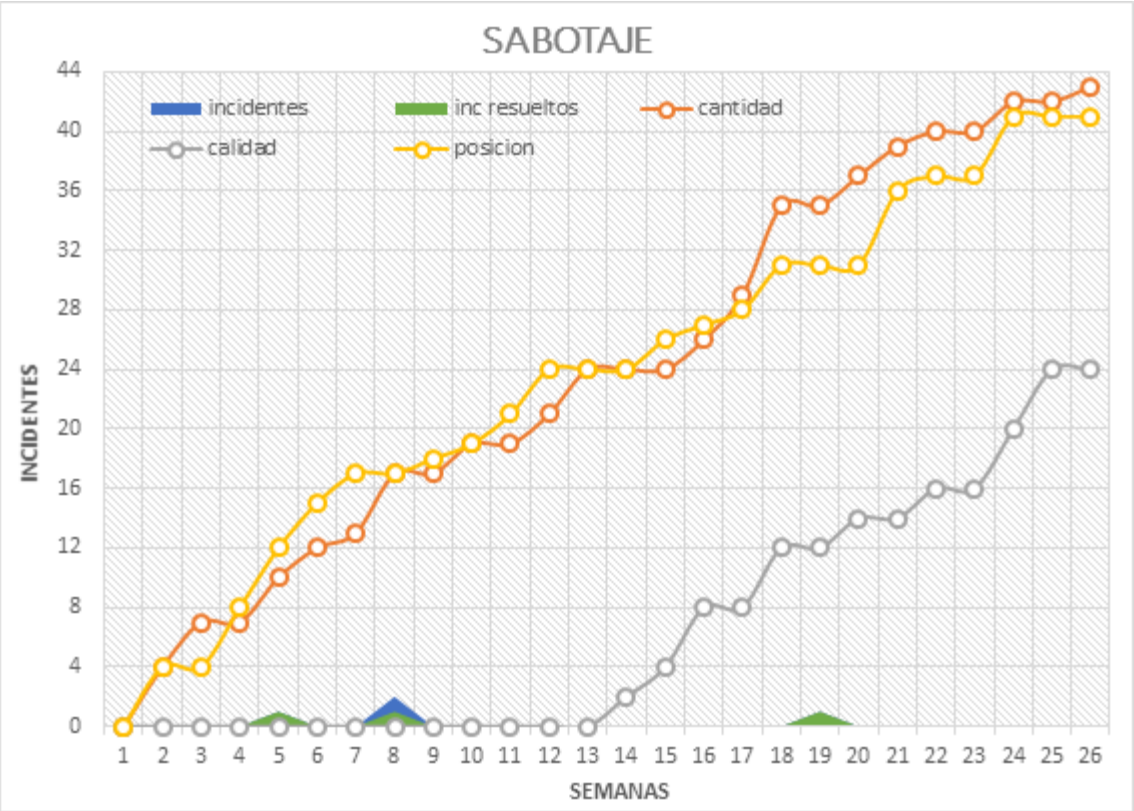


Figura 30. Indicador Sabotaje, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.2.4. INDICADOR: INCIDENTES DE ARQUEO DESCUADRADO (CAMARAS)

Vamos a detallar los casos que ocurren:

- En el transcurso del día en caja se hace un balance del dinero que ingresa y sale y si hay desbalance se efectúa el aviso.

Tabla 30. Incidentes antes de la instalación – Arqueo Descuadrado

16 AGENCIAS - Antes de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	1	1
2	0	0	0	2	1
3	0	0	0	1	1
4	0	0	0	2	1
5	0	0	0	0	0
6	0	0	0	1	1
7	0	0	0	1	0
8	0	0	0	2	1
9	0	0	0	2	0
10	0	0	0	1	1
11	0	0	0	1	0

12	0	0	0	0	0
13	0	0	0	2	1
14	0	0	0	1	0
15	0	0	0	1	1
16	0	0	0	2	1
17	0	0	0	1	1
18	0	0	0	2	1
19	0	0	0	2	1
20	0	0	0	1	0
21	0	0	0	0	0
22	0	0	0	2	1
23	0	0	0	1	0
24	0	0	0	0	0
25	0	0	0	2	1
26	0	0	0	0	0

Fuente: Elaboración propia.

Tabla 31. Incidentes después de la instalación – Arqueo Descuadrado

16 AGENCIAS - Después de la Instalación					
semana	cantidad	calidad	posición	incidentes	Inc. resueltos
1	0	0	0	0	0
2	4	0	4	1	1
3	7	0	4	0	0
4	7	0	8	1	1
5	10	0	12	1	1
6	12	0	15	0	0
7	13	0	17	1	0
8	17	0	17	1	1
9	17	0	18	1	0
10	19	0	19	0	0
11	19	0	21	0	0
12	21	0	24	1	1
13	24	0	24	0	0
14	24	2	24	1	1
15	24	4	26	1	1
16	26	8	27	0	0
17	29	8	28	0	0
18	35	12	31	1	1
19	35	12	31	1	1
20	37	14	31	0	0
21	39	14	36	1	1
22	40	16	37	1	1
23	40	16	37	0	0
24	42	20	41	0	0

25	42	24	41	1	1
26	43	24	41	0	0

Fuente: Elaboración propia.

La cantidad y calidad son acumulativos y excluyentes y hasta la fecha de semana 26 se tenían 67 cámaras instaladas.

Tabla 32. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Arqueo Descuadrado

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 33. Medida descriptiva antes y después de la instalación de cámaras – Arqueo Descuadrado.

Descriptivos				
			Estadístico	Error estándar
antes	Media		1.19	0.147
	95% de intervalo de confianza para la media	Límite inferior	0.89	
		Límite superior	1.49	
	Media recortada al 5%		1.21	
	Mediana		1.00	
	Varianza		0.562	
	Desviación estándar		0.749	
	Mínimo		0	
	Máximo		2	
	Rango		2	
	Rango intercuartil		1	
	Asimetría		-0.338	0.456
	Curtosis		-1.078	0.887
después	Media		0.54	0.100
	95% de intervalo de confianza para la media	Límite inferior	0.33	
		Límite superior	0.74	
	Media recortada al 5%		0.54	
	Mediana		1.00	
	Varianza		0.258	

	Desviación estándar	0.508	
	Mínimo	0	
	Máximo	1	
	Rango	1	
	Rango intercuartil	1	
	Asimetría	-0.164	0.456
	Curtosis	-2.145	0.887

Fuente: SPSS
Fuente: Elaboración propia.

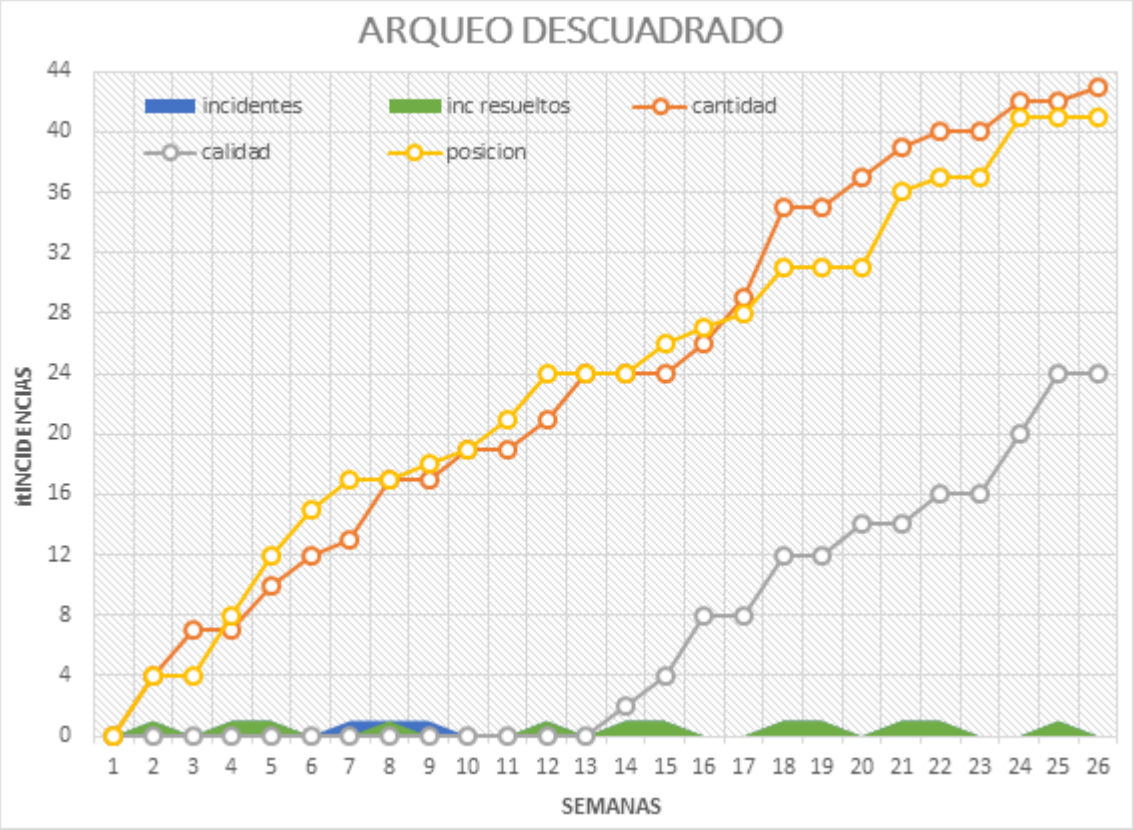


Figura 31. Indicador Arqueo Descuadrado, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.2.5. INDICADOR: INCIDENTES DE INTRUSION FUERA DEL HORARIO DE TRABAJO (ALARMAS)

Vamos a detallar los casos que ocurren:

- Intento de Intrusión a una agencia para robar.

Tabla 34. Incidentes antes de la instalación – Alarmas

16 AGENCIAS - Antes de la Instalación					
SEMANA	**TIEMPO DE RESPUESTA**	**CANTIDAD DE MANTENIMIENTO**	**CANTIDAD DE SENSORES**	**INCIDENTES**	**INCIDENTE QUE SE EVITARON**
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	1	1
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	1	1
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	1	1
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	1	0
13	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	1	1
16	0	0	0	0	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	2	1
20	0	0	0	0	0
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	1	0
24	0	0	0	2	1
25	0	0	0	1	0
26	0	0	0	0	0

Fuente: Elaboración propia.

Tabla 35. Incidentes después de la instalación – Alarmas

16 AGENCIAS - después de la Instalación					
SEMANA	**TIEMPO DE RESPUESTA**	**CANTIDAD DE MANTENIMIENTO**	**CANTIDAD DE SENSORES**	**INCIDENTES**	**INCIDENTE QUE SE EVITARON**
1	10	0	0	0	0
2	10	0	0	0	0
3	10	0	0	0	0
4	8	0	2	0	0
5	8	0	2	1	1
6	8	0	2	0	0
7	8	0	4	0	0
8	8	0	4	0	0
9	8	1	7	0	0

10	8	0	7	0	0
11	8	0	7	0	0
12	8	0	7	0	0
13	8	0	9	0	0
14	8	0	9	0	0
15	8	0	9	1	1
16	8	0	9	0	0
17	7	2	11	0	0
18	7	0	11	0	0
19	7	0	11	0	0
20	7	0	11	0	0
21	7	0	11	0	0
22	7	0	11	0	0
23	6	0	11	0	0
24	6	1	13	0	0
25	6	0	13	0	0
26	6	0	13	0	0

Fuente: Elaboración propia.

- Nota: se tiene 84 sensores instalados.
- Tiempo de respuesta, es el tiempo de retardo en activarse la alarma por acción de un sensor de ingreso.
- Cantidad de Mantenimientos, se orienta a la continuidad ininterrumpida de los dispositivos, generalmente la batería, sensores y placa evitando el sulfatado x humedad.
- Cantidad de Sensores, es el aumento incremental de sensores a los 84 que ya se instalo

Tabla 36. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Alarmas

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 37. Medida descriptiva antes y después de la instalación de Alarmas.

Descriptivos				
			Estadístico	Error estándar
antes	Media		0.42	0.126
	95% de intervalo de confianza para la media	Límite inferior	0.16	
		Límite superior	0.68	
	Media recortada al 5%		0.36	
	Mediana		0.00	
	Varianza		0.414	
	Desviación estándar		0.643	
	Mínimo		0	
	Máximo		2	
	Rango		2	
	Rango intercuartil		1	
	Asimetría		1.286	0.456
	Curtosis		0.669	0.887
después	Media		0.08	0.053
	95% de intervalo de confianza para la media	Límite inferior	-0.03	
		Límite superior	0.19	
	Media recortada al 5%		0.03	
	Mediana		0.00	
	Varianza		0.074	
	Desviación estándar		0.272	
	Mínimo		0	
	Máximo		1	
	Rango		1	
	Rango intercuartil		0	
	Asimetría		3.373	0.456
	Curtosis		10.156	0.887

Fuente: SPSS

Fuente: Elaboración propia.

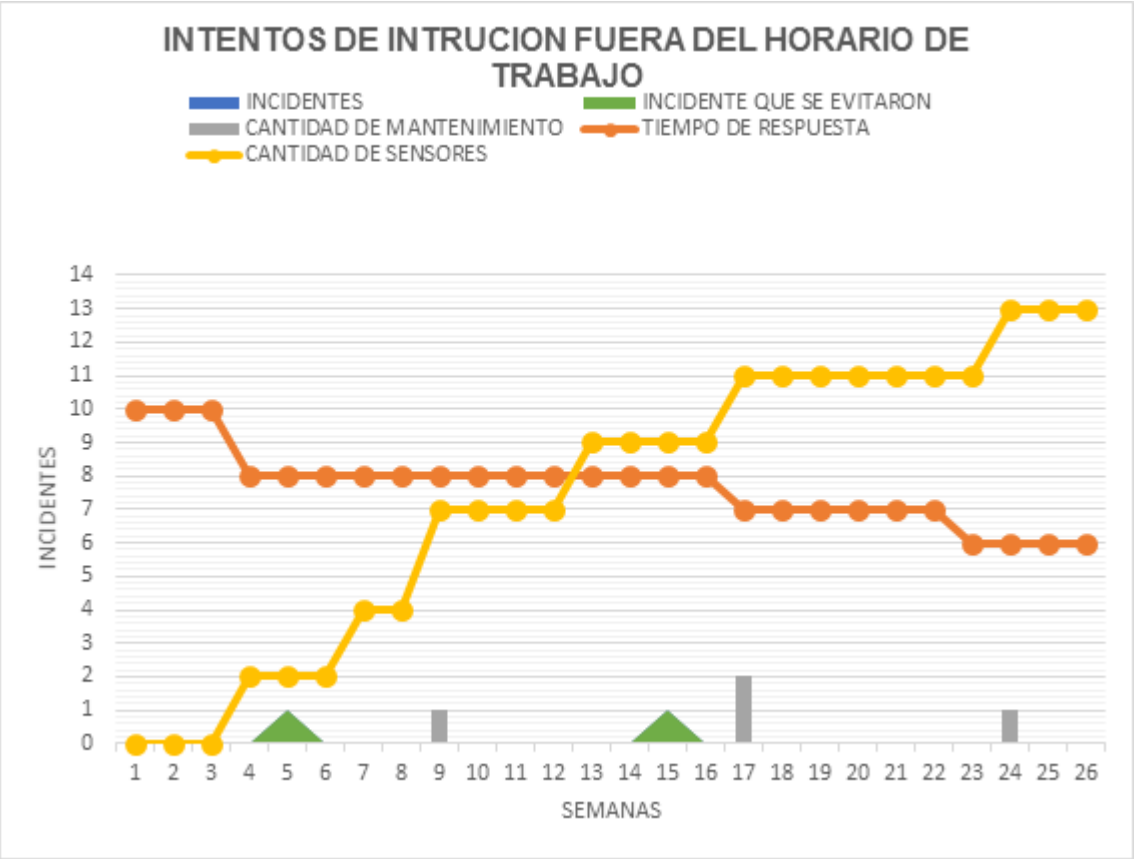


Figura 32. Indicador Intento de Intrusión fuera del horario de trabajo, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.2.6. INDICADOR: INCIDENTES DE INTRUSION DENTRO DEL HORARIO DE TRABAJO (CONTROL DE ACCESO)

Vamos a detallar los casos que ocurren:

-Ingreso de personas externas a las instalaciones de la agencia con intensión de sustraer algo de valor.

-Ingreso de personas externas por desconocimiento de la infraestructura del local de una agencia.

Tabla 38. Incidentes antes de la instalación – Control de Acceso

16 AGENCIAS - antes de la Instalación				
SEMANAS	Nº PERSONAS FORANEAS INGRESO AREAS RESTRINGIDAS	Nº INTERFERENCIAS DE PERSONAL, EN ACTIVIDAD LABORAL	Nº INTERFERENCIAS DE PERSONAL, EN ACTIVIDAD PERSONAL	INCIDENTES PERSONAS FORANEAS INGRESO AREAS RESTRINGIDAS
1	3	0	0	3
2	3	0	0	3

3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	2	0	0	2
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	1	0	0	1
11	3	0	0	3
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	2	0	0	2
16	0	0	0	0
17	0	0	0	0
18	2	0	0	2
19	0	0	0	0
20	0	0	0	0
21	3	0	0	3
22	2	0	0	2
23	0	0	0	0
24	2	0	0	2
25	1	0	0	1
26	2	0	0	2

Fuente: Elaboración propia.

Tabla 39. Incidentes después de la instalación – Control de Acceso

16 AGENCIAS - después de la Instalación						
SEMANA	**Nº PERSONAS FORANEAS INGRESO AREAS RESTRINGIDAS**	**Nº INTERFERENCIAS DE PERSONAL, EN ACTIVIDAD LABORAL**	**Nº INTERFERENCIAS DE PERSONAL, EN ACTIVIDAD PERSONAL**	**INCIDENTES**	**INCIDENTE QUE SE EVITARON**	**INCIDENTES PERSONAS FORANEAS INGRESO AREAS RESTRINGIDAS**
1	0	3	4	7	7	0
2	0	1	3	4	4	0
3	0	1	1	2	2	0
4	0	0	0	0	0	0
5	0	0	0	1	1	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

11	2	1	1	4	4	2
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	1	0	0	1	1	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	1	1	1	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	1	0	0	1	1	1
23	0	0	0	0	0	0
24	0	0	0	0	0	0
25	0	0	0	0	0	0
26	0	0	0	0	0	0

Fuente: Elaboración propia.

Tabla 40. Resumen Casos Válidos antes (26 semanas) y después (26 semanas) – Control de Acceso

Resumen de procesamiento de casos						
	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
antes	26	100.0%	0	0.0%	26	100.0%
después	26	100.0%	0	0.0%	26	100.0%

Fuente: SPSS
Elaboración propia.

Tabla 41. Medida descriptiva antes y después de la instalación del Control de Acceso.

Descriptivos				
			Estadístico	Error estándar
antes incidentes personas foráneas	Media		0.88	0.224
	95% de intervalo de confianza para la media	Límite inferior	0.42	
		Límite superior	1.35	
	Media recortada al 5%		0.82	
	Mediana		0.00	
	Varianza		1.306	
	Desviación estándar		1.143	
	Mínimo		0	
	Máximo		3	

	Rango		3	
	Rango intercuartil		2	
	Asimetría		0.765	0.456
	Curtosis		-1.055	0.887
después incidentes personas foráneas	Media		0.12	0.085
	95% de intervalo de confianza para la media	Límite inferior	-0.06	
		Límite superior	0.29	
	Media recortada al 5%		0.03	
	Mediana		0.00	
	Varianza		0.186	
	Desviación estándar		0.431	
	Mínimo		0	
	Máximo		2	
	Rango		2	
	Rango intercuartil		0	
	Asimetría		3.965	0.456
	Curtosis		16.027	0.887

Fuente: SPSS
Elaboración propia.

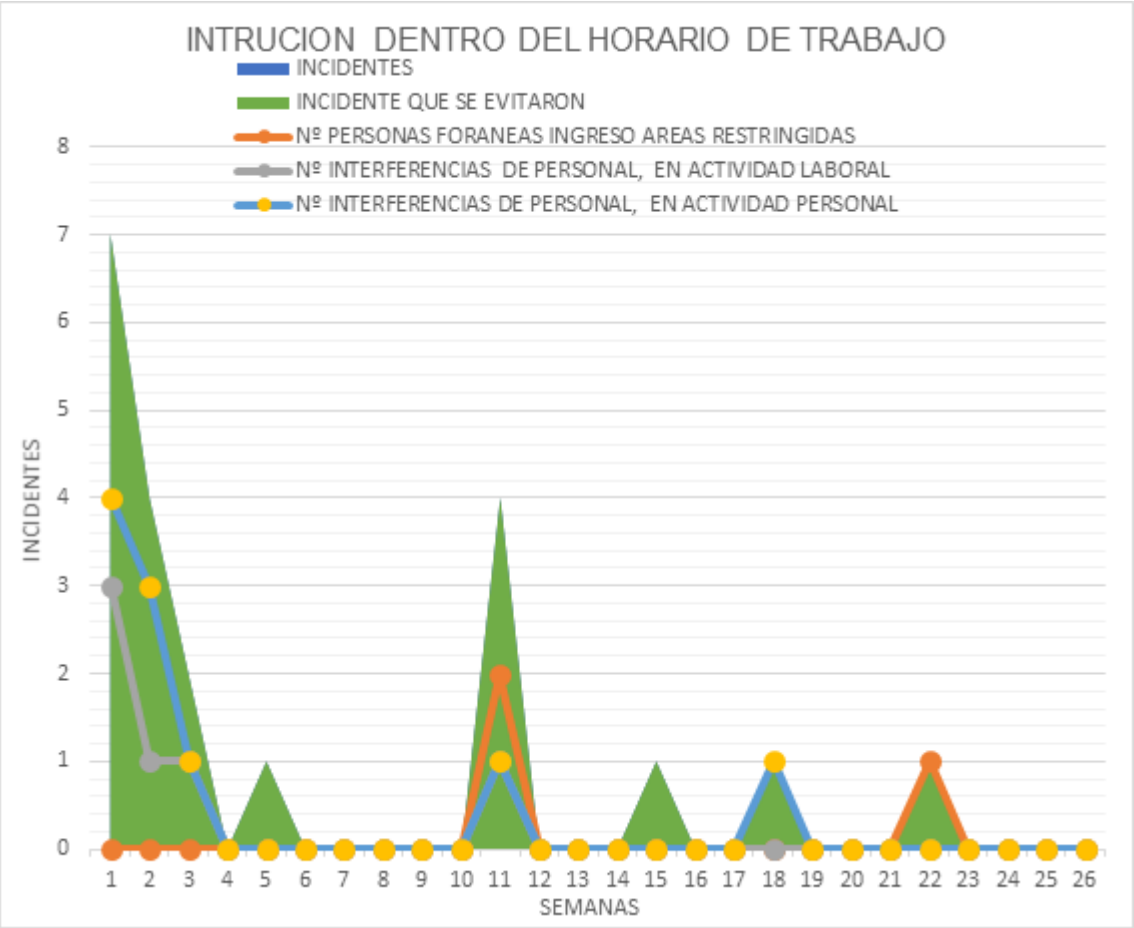


Figura 33. Indicador Intento de Intrusión dentro del horario de trabajo, Incidentes e Incidentes Resueltos después de la instalación de la Seguridad Electrónica
Fuente: Elaboración propia.

5.3 Análisis y Discusión de Resultados

Como resultado de la Implementación progresiva de la Seguridad Electrónica mediante la Metodología Top Down Design se puede observar lo siguiente en cada una de las dimensiones:

a.- DIMENSION ROBO DE DINERO.- Los casos más importantes que se contemplan.

- Perdida de dinero de bóveda.
- Perdida de dinero de caja.
- Robo de dinero a la agencia en el día.
- Robo de dinero a personal de la agencia.
- Robo de dinero a personal externo de la agencia a socios en las instalaciones.

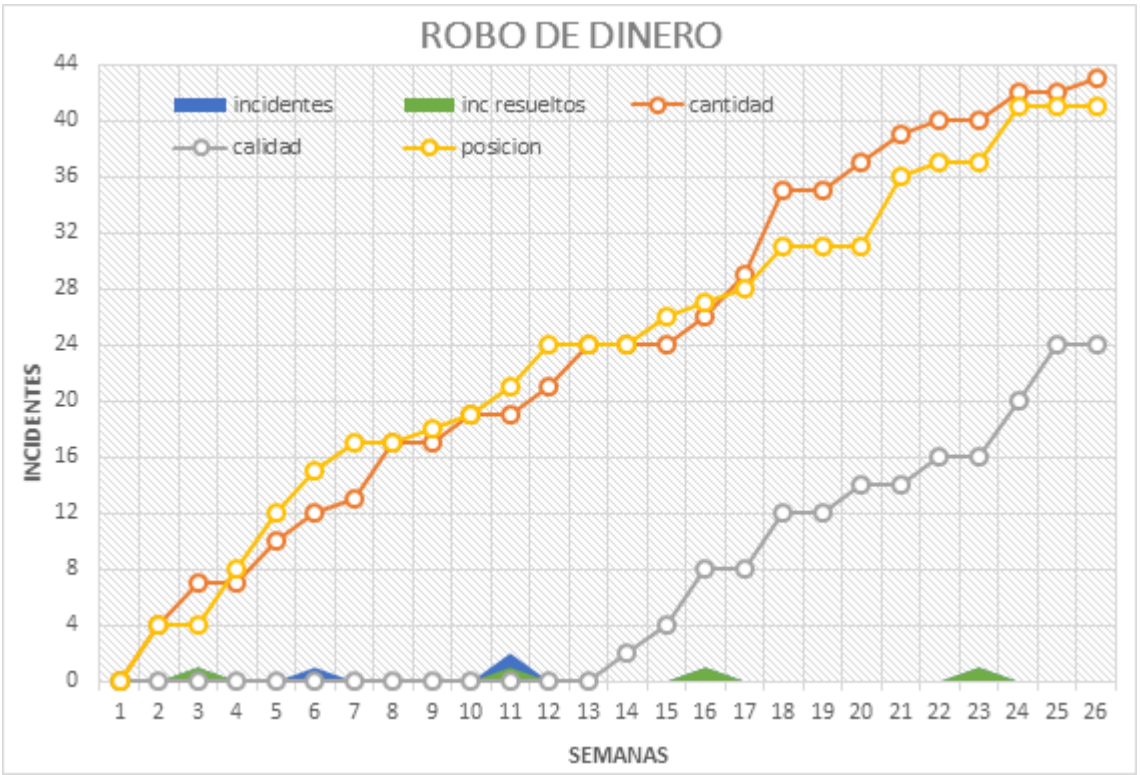


Figura 34. Indicador Robo de Dinero
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes).
b) Los incidentes se reducen en el tiempo, asea los incidentes ocurren en intervalos más largos.
c) Lo ideal es obtener incidentes resueltos (verde), eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.
d) Cada vez que mejoramos la cantidad, calidad y posición de las cámaras se logra el objetivo de tener incidentes resueltos.

b.- DIMENSION PERDIDA DE OBJETOS.- Los casos más importantes que se contemplan.

- Olvidar el DNI o documento del socio.
- Olvidar un objeto del socio.
- Perdida de objetos por parte de los trabajadores de la agencia.
- Supuestas pérdidas por parte de los socios.

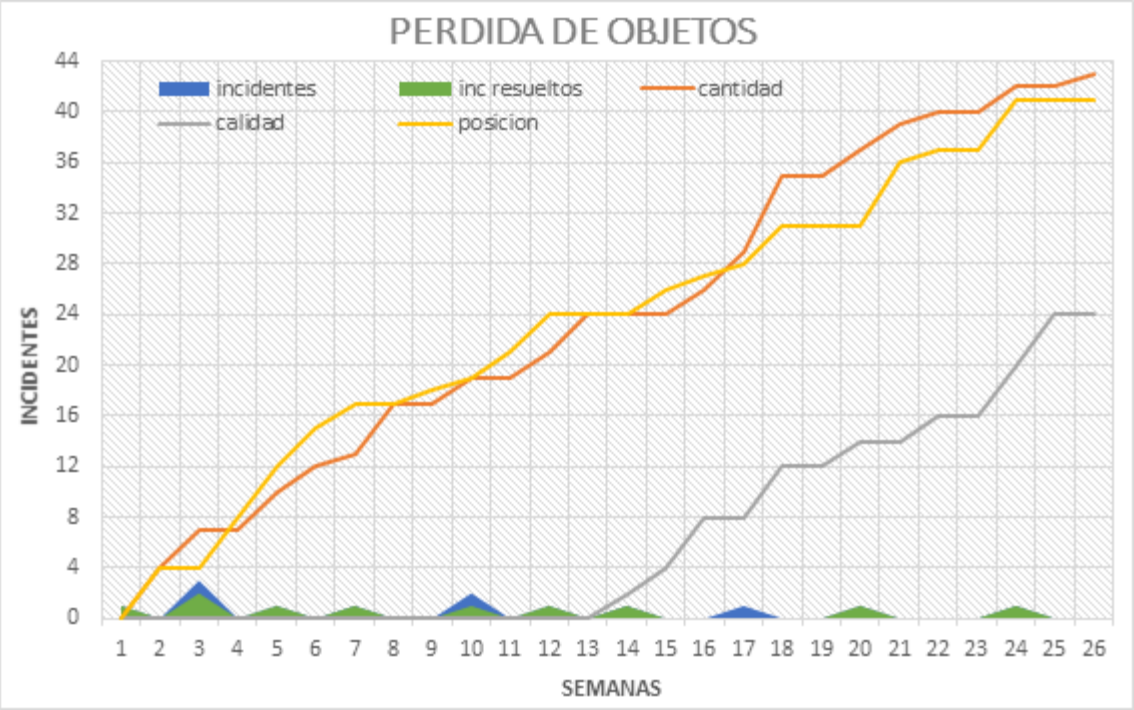


Figura 35. Indicador Pérdida de Objetos
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes), son bastante frecuentes.
b) Los incidentes se reducen en el tiempo, asea los incidentes ocurren en intervalos más largos.
c) Lo ideal es obtener incidentes resueltos, eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.
d) Cada vez que mejoramos la cantidad, calidad y posición de las cámaras se logra el objetivo de tener incidentes resueltos.

c.- DIMENSION SABOTAJE.- Los casos más importantes que se contemplan.

- Empleados descontentos con el administrador y malogran equipos.
- Empleados descontentos con el administrador y modifican información de transacciones.
- Empleados descontentos con su centro de labores.

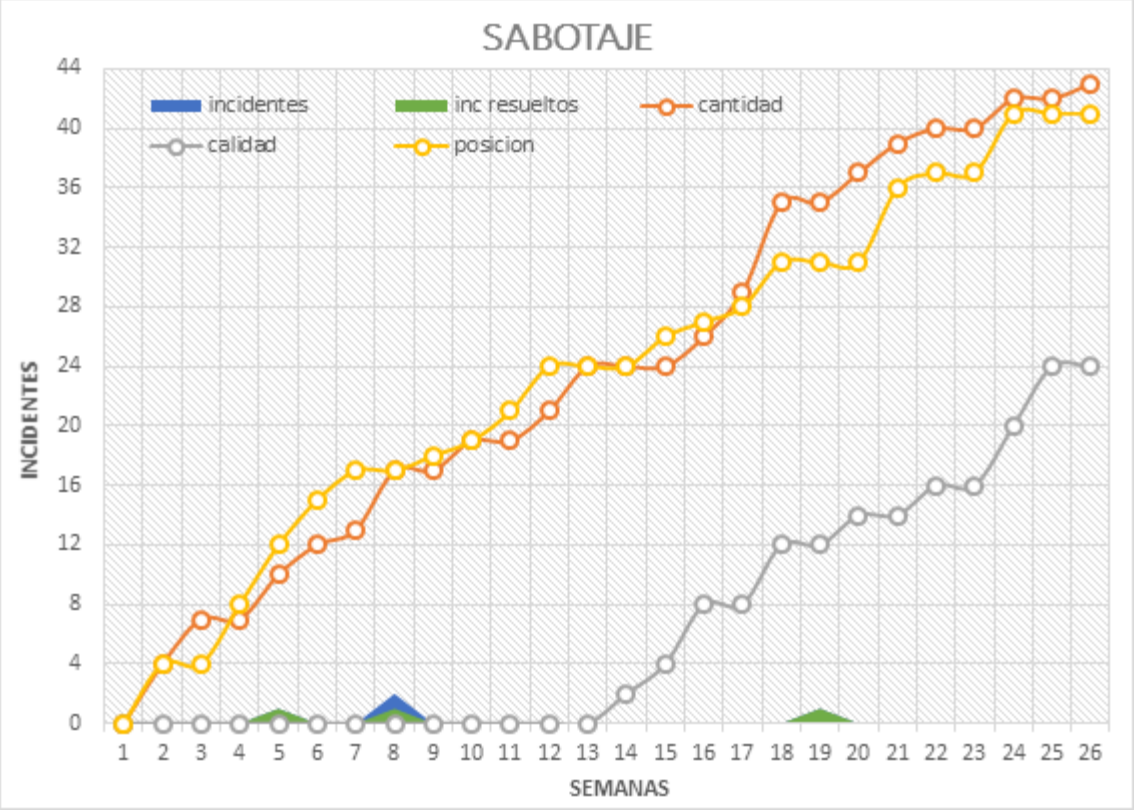


Figura 36. Indicador Sabotaje
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes), son poco frecuentes.

b) Los incidentes se reducen en el tiempo, asea los incidentes ocurren en intervalos más largos.

c) Lo ideal es obtener incidentes resueltos, eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.

d) Cada vez que mejoramos la cantidad, calidad y posición de las cámaras se logra el objetivo de tener incidentes resueltos.

d.- DIMENSION ARQUEO DESCUADRADO.- Los casos más importantes que se contemplan.

- En el transcurso del día en caja se hace un balance del dinero que ingresa y sale y si hay desbalance se efectúa el aviso.

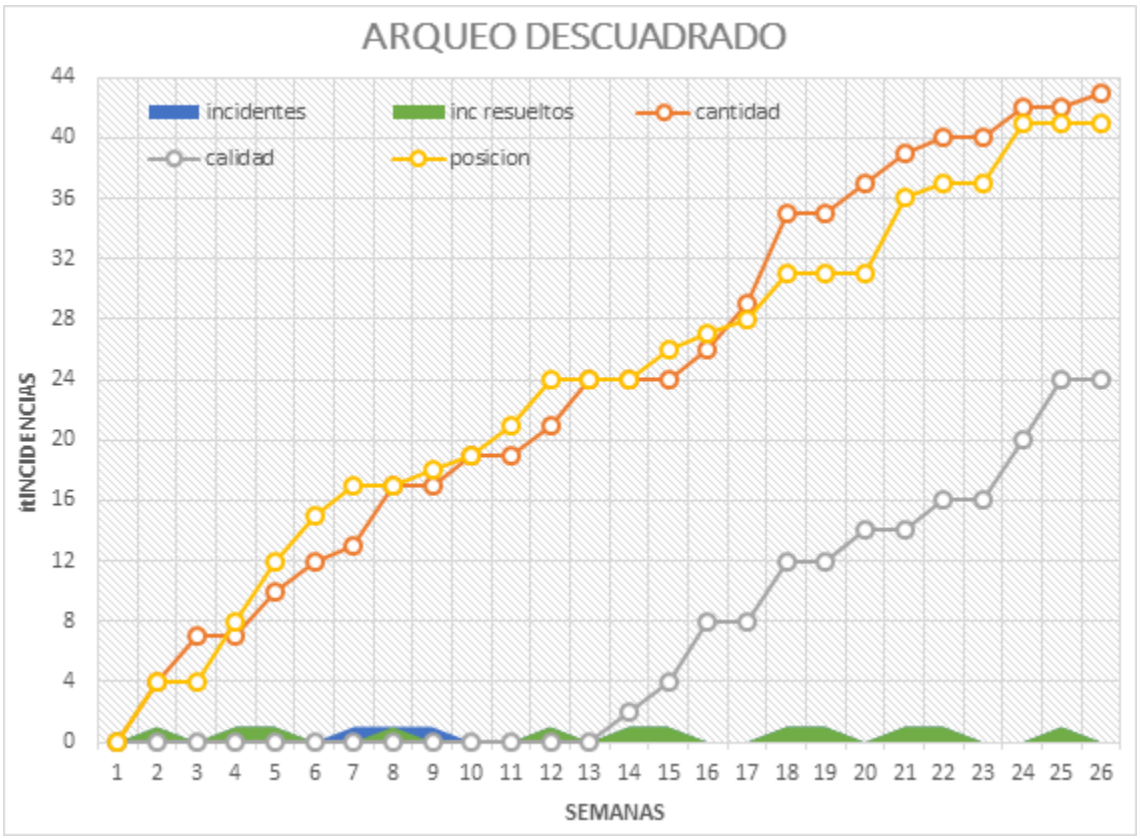


Figura 37. Indicador Arqueo Descuadrado
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes), son muy frecuentes. Contrario a lo que se podría pensar, a medida que un

trabajador tiene más tiempo laborando en caja se va confiando y baja la guardia en cuanto a contar el dinero.

b) Los incidentes no se reducen en el tiempo.

c) Lo ideal es obtener incidentes resueltos, eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.

d) Cada vez que mejoramos la cantidad, calidad y posición de las cámaras se logra el objetivo de tener incidentes resueltos.

e.- DIMENSION INTENTO DE INTRUSION FUERA DEL HORARIO DE TRABAJO.- El caso que se contempla.

- Intento de Intrusión a una agencia para robar.

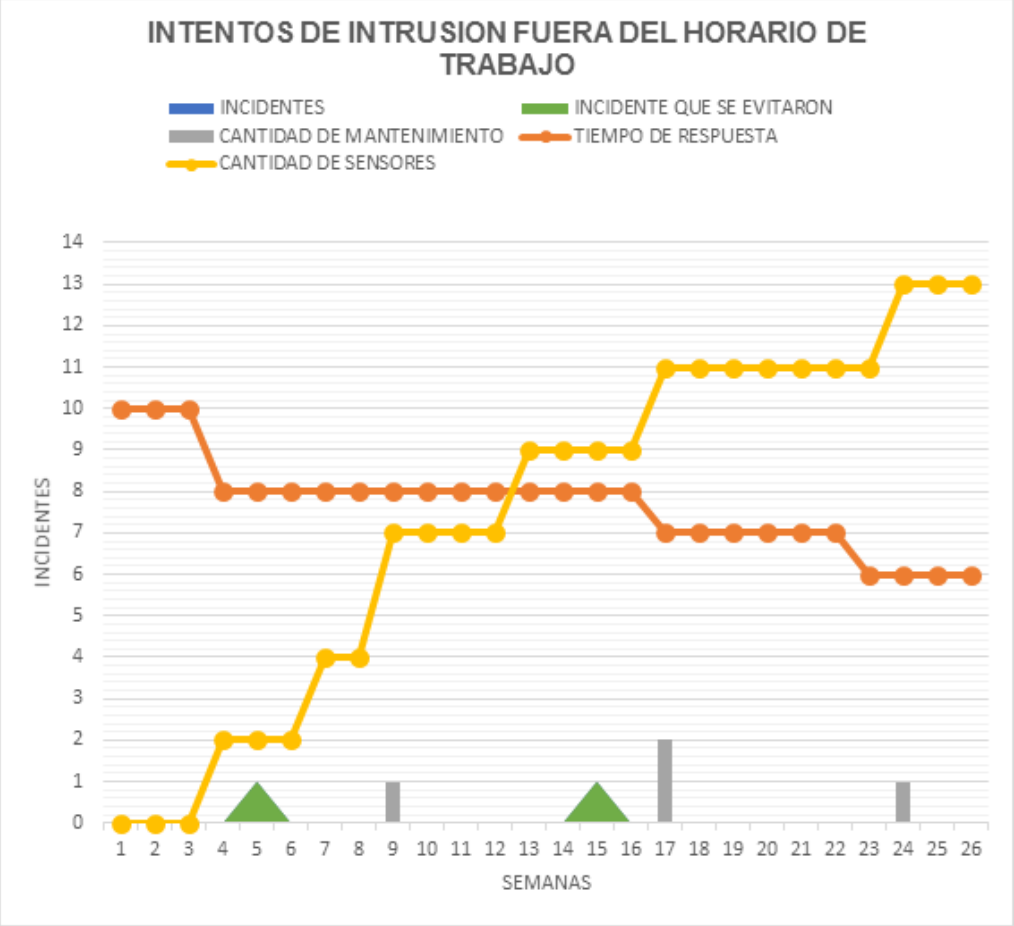


Figura 38. Indicador Intento de Intrusión fuera del horario de trabajo
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes), son poco frecuentes.
b) Los incidentes se reducen en el tiempo.
c) Lo ideal es obtener incidentes resueltos, eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.
d) Cada vez que mejoramos la cantidad de sensores, cantidad de mantenimientos y mejor tiempo de respuesta, se logra el objetivo de tener incidentes resueltos.

f.- DIMENSION INTENTO DE INTRUSION DENTRO DEL HORARIO DE TRABAJO.- El caso que se contempla.

- Ingreso de personas externas a las instalaciones de la agencia con intensión de sustraer algo de valor.
- Ingreso de personas externas por desconocimiento de la infraestructura del local de una agencia

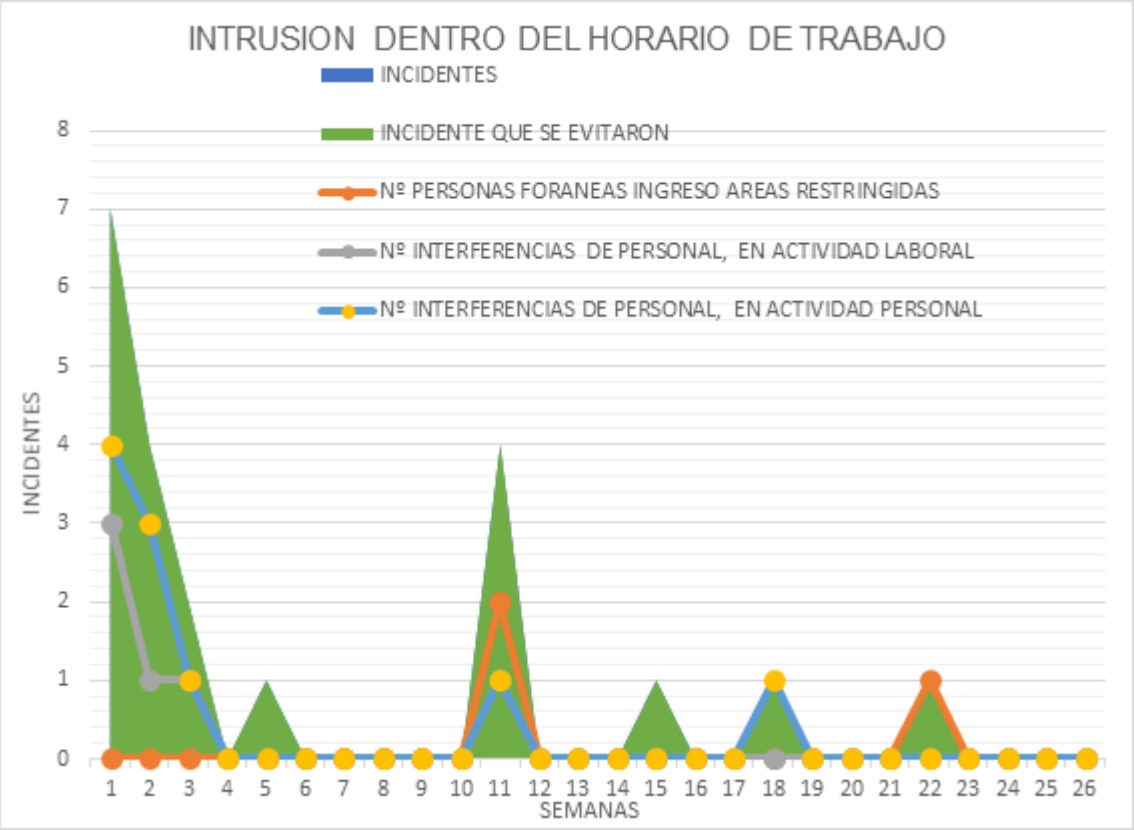


Figura 39. Indicador Intento de Intrusión dentro del horario de trabajo
Fuente: Elaboración propia.

a) Siempre existirán, incidentes (azul) e incidentes resueltos (verdes), son poco frecuentes.
b) Los incidentes se reducen en el tiempo.
c) Lo ideal es obtener incidentes resueltos, eso es el objetivo de todo sistema de seguridad electrónica, resolver todos los incidentes.
d) Cada vez que mejoramos las interferencias de personal, se logra el objetivo de tener incidentes resueltos.

CONCLUSIONES

1. La implementación de la Seguridad Electrónica mediante la Metodología Top Down incidió en la reducción de los incidentes de robo y sobre todo con la mejora progresiva de la Seguridad Electrónica se consiguió obtener incidentes resueltos.
2. Se confirma que con la puesta en marcha del Sistema CCTV, permitió controlar las incidencias de robo dentro y fuera del horario de trabajo.
3. La ejecución de un Sistema de Alarmas Centralizada posibilitó la reducción y reporte de las incidencias fuera del horario de trabajo.
4. La Implementación de un Sistema de Control de Acceso causó un efecto positivo en el control de ingreso y salida del personal a espacios comunes o restringidos.

RECOMENDACIONES

1. Se recomienda la Implementación de Seguridad Electrónica en organizaciones donde el objetivo es el control el riesgo de robo, usando la metodología Top Down, ya que ha sido implantado y verificado durante un tiempo de 2 años, dando resultados óptimos en el tiempo.
2. Se recomienda dar Mantenimiento a todos los equipos, tanto centrales como dispositivos, aproximadamente de 1 año para centrales y dispositivos y de 6 meses a baterías.
3. Se recomienda una inspección cada 3 meses para verificar el funcionamiento óptimo de todos los equipos.
4. Se recomienda efectuar un estudio del tiempo Óptimo para lograr la mejor capacidad de respuesta de la seguridad Electrónica.
5. Se recomienda al administrador de cada agencia reportar cuando se efectúen modificaciones o cambios a la infraestructura del local de la agencia, y sobre cambios o mantenimientos a la red eléctrica.

REFERENCIAS BIBLIOGRAFICAS

1. NFPA (2016). NFPA 72 Código Nacional de alarmas de incendio y señalización.
2. Top Down Network, N.A. (2015) Methodology Top Down Network Design: Tercera Edición. A system analysis approach to enterprise network design.
3. Kurose, R. (2013) Computer Networking a Top-Down approach: Sixth edition. University of Massachusetts.
4. Huerta, M (2015) Metodología Top Down.
5. Vara, A. (2015) 7 pasos para elaborar una tesis: Primera Edición.
6. Paradox (2010-2020). Obtenido de https://www.paradox.com/
7. Dahua (2010-2020). Obtenido de https://www.dahuasecurity.com/la
8. Hickvision (2020). Obtenido de https://www.hikvision.com/es/

ANEXOS 1

MATRIZ DE CONSISTENCIA

PROBLEMA DE LA INVESTIGACION	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSION	INDICADOR	METODOLOGIA
Problema General ¿De qué manera mejorar la seguridad para reducir el riesgo de robo en una entidad financiera?	**Objetivo General** Implementar la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una Entidad Financiera.	**Hipótesis General** La Implementación de la Seguridad Electrónica mediante la Metodología Top-Down permitirá reducir el riesgo de robo en una entidad Financiera.	VARIABLE DEPENDIENTE RIESGO DE ROBO	ROBO DE DINERO PERDIDA DE OBJETOS SABOTAJE ARQUEO DESCUADRADO	CANTIDAD DE INCIDENTES DE ROBO DE DINERO CANTIDAD DE INCIDENTES DE PERDIDA DE OBJETOS. CANTIDAD DE INCIDENTES DE SABOTAJE CANTIDAD DE INCIDENTES DE ARQUEO DESCUADRADO	**Método de Investigación** La investigación realizada es Deductivo-Inductivo. **Tipo de Investigación** Por el tipo de investigación, el presente estudio reúne las condiciones metodológicas de una investigación Aplicada.

Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específica**				**Nivel de Investigación**
¿Cómo supervisar las incidencias de robo dentro y fuera del horario de trabajo?	Instalar un sistema CCTV para supervisar las incidencias dentro y fuera del horario de trabajo.	La puesta en funcionamiento de un Sistema CCTV posibilitará controlar las incidencias de robo dentro y fuera del horario de trabajo.		INTENTO DE INTRUSION A UNA AGENCIA FUERA DEL HORARIO DE TRABAJO INTRUSION DE PERSONAS AJENAS A LA COOPERATIVA EN AREAS RESTRINGIDAS	CANTIDAD DE INCIDENTES DE INTRUSION FUERA DEL HORARIO DE TRABAJO CANTIDAD DE INCIDENTES DE INTRUSION DENTRO DEL HORARIO DE TRABAJO	De acuerdo a la investigación, agrupa por su nivel las características de un estudio Explicativo. **Diseño de Investigación** La investigación es Pre Experimental
¿Podemos reducir y reportar las incidencias fuera del horario de trabajo?	Disponer un sistema de Alarmas Centralizadas para reducir y reportar las incidencias fuera del horario de trabajo.	La Implementación de un Sistema de Alarmas Centralizada Reducirá y Reportará las Incidencias fuera del horario de trabajo.				
¿Se puede controlar el ingreso y salida del personal a espacios comunes o	Establecer un sistema de Control de Acceso para controlar el ingreso y salida del	La puesta en marcha de un Sistema de Control de Acceso proporcionará				

restringidos en horario de trabajo?	personal a espacios comunes y restringidos.	controlar el ingreso y salida del personal a espacios comunes o restringidos.	VARIABLE INDEPENDIENTE SEGURIDAD ELECTRONICA	CCTV ALARMAS CONTROL DE ACCESO(C.A.)	CANTIDAD DE CAMARAS CALIDAD DE CAMARAS POSICION DE CAMARAS TIEMPO DE RESPUESTA OPTIMO DE LA ALARMA CANTIDAD DE SENSORES MANTENIMIENTO OPTIMO DE LA ALARMA OPERATIVIDAD ÓPTIMA.	

ANEXO 2

FICHA DE REGISTRO DE INCIDENTES: MANUAL

	PROCESO	GESTION DE INCIDENTES		
	FORMATO	REPORTE DE INCIDENTE DE SEGURIDAD	**Fecha:**	08/02/2018

REPORTE DE INCIDENTES DE SEGURIDAD	
FECHA Y HORA REPORTE DE INCIDENTE	
LUGAR DEL INCIDENTE	

DETALLES DEL PERSONAL QUE REPORTA/IDENTIFICA INCIDENTE :	

DESCRIPCION DE INCIDENTES DE SEGURIDAD :					
Qué Sucedió?:					
Cómo Sucedió?:					
Porqué Sucedió?:					
Consideraciones Iniciales sobre Activo(s) afectadoss?:					
Impactos adversos para la Entidad?:	SI	☐	NO	☐	Cual?
Se identifica Vulnerabilidad alguna?:	SI	☐	NO	☐	Cual?
Se identifica responsable del Incidente?:	SI	☐	NO	☐	Cual?

ESTADO DEL INCIDENTE	Sucediendo : ☐	Sucedió : ☐	Sucede Nuevamente : ☐

Fuente: Archivos de documentos de la Coopac, años 2017 - 2018

ANEXO 3

ENCUESTA POR TELÉFONO ENTRE EL ENCARGADO DE LA SEGURIDAD Y EL ADMINISTRADOR DE LA AGENCIA - CAMARAS

1.- ¿Hubo incidentes?

NO → Termina la comunicación

SI → Continúa la entrevista, aquí se orienta a qué tipo de seguridad electrónica se orienta.

2.-

a) ¿Las Cámaras sirvieron para resolver el incidente? CANTIDAD

SI → Termina la comunicación

NO → se hace la pregunta ¿Por qué?

b) ¿Las Cámaras sirvieron para resolver el incidente? CALIDAD

SI → Termina la comunicación

NO → se hace la pregunta ¿Por qué?

c) ¿Las Cámaras sirvieron para resolver el incidente? POSICION

SI → Termina la comunicación

NO → se hace la pregunta ¿Por qué?

Fuente: Elaboración propia.

ANEXO 4

ENTREVISTA

Se efectúa una entrevista con el administrador de la agencia sobre el funcionamiento de las alarmas el fin de semana sobre las alarmas

PRUEBAS:

1.- ACTIVAR PUERTAS.- Tiempo de respuesta del sensor de ingreso- tiempo de retardo de ingreso y salida.

2.- SENSOR DE BOVEDA.- Tiempo de respuesta optimo, sonido de sirena y llamada al celular.

Se efectúa las siguientes preguntas:

a).- ¿El tiempo de respuesta de la puerta es el óptimo?

SI → termina la pregunta

NO → se hace la pregunta ¿Por qué?

b).- ¿El tiempo de respuesta de la bóveda es el óptimo?

SI → termina la pregunta

NO → se hace la pregunta ¿Por qué?

c).- ¿El sistema funciona?

SI → termina la pregunta

NO → se hace la pregunta ¿Por qué?

Fuente: Elaboración propia.

ANEXO 5

ENTREVISTA

Se instaló en 3 puertas el Control de Acceso; en la puerta principal, en la puerta de caja, puerta de Gerencia y servidores

Entrevista a todos los trabajadores

1.- ¿El Control de Acceso sirve para que personas extrañas a la Coopac NO INGRESEN a áreas comunes?

SI → Termina la pregunta

NO → Se pregunta ¿Por qué?

2.- ¿El Control de Acceso interfiere en sus actividades laborales?

NO → Termina la pregunta

SI → Se pregunta ¿Por qué?

3.- ¿El Control de Acceso interfiere en sus actividades personales?

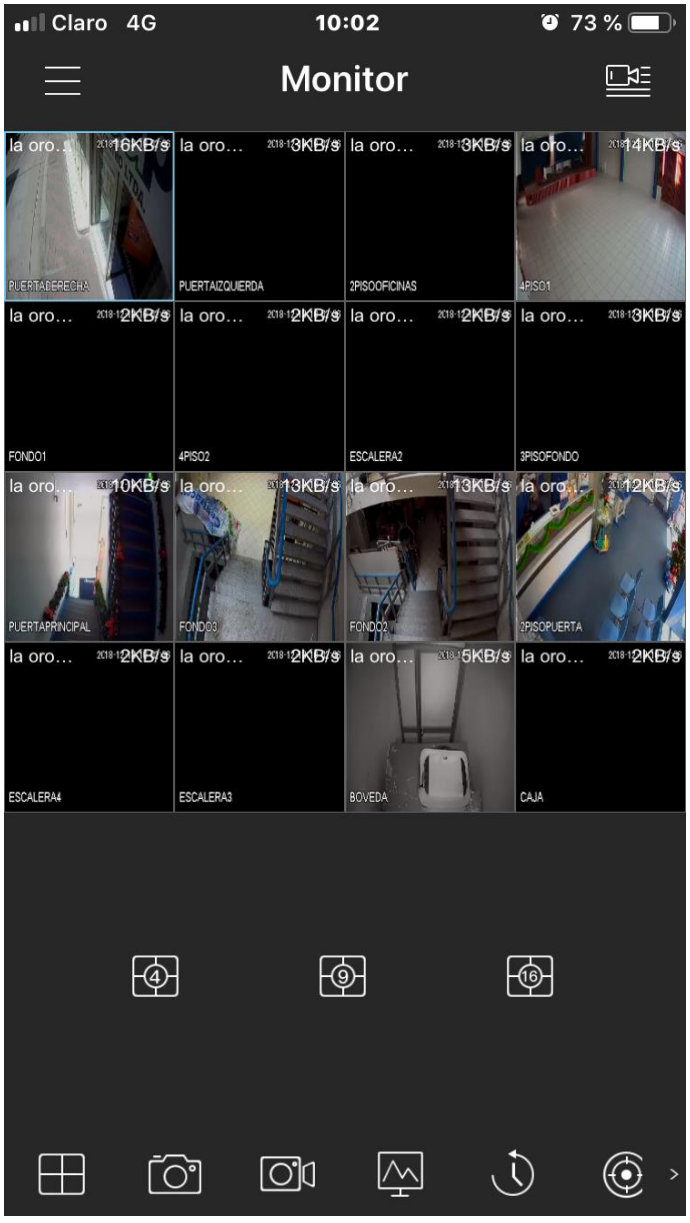
NO → Termina la pregunta

SI → Se pregunta ¿Por qué?

Fuente: Elaboración propia

ANEXO 6

ACCESO A LAS CÁMARAS VÍA CELULAR



Fuente: Elaboración propia

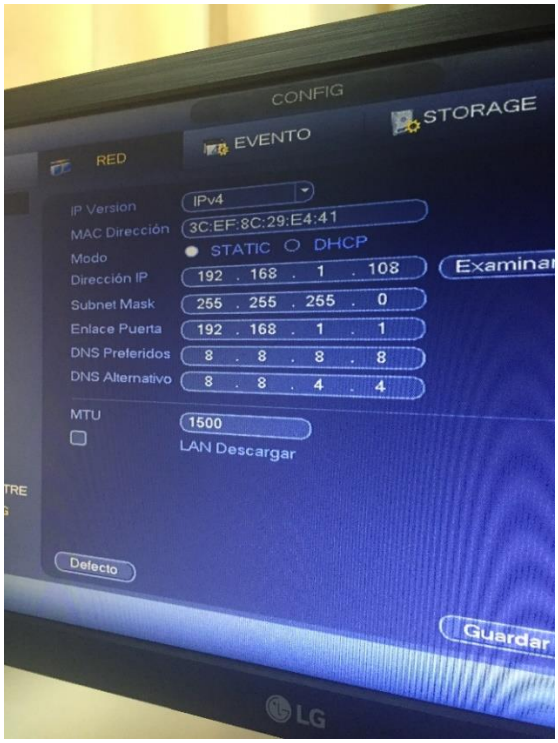
ANEXO 7

CENTRAL DE MONITOREO CAMARAS

Fuente: Elaboración propia

ANEXO 8

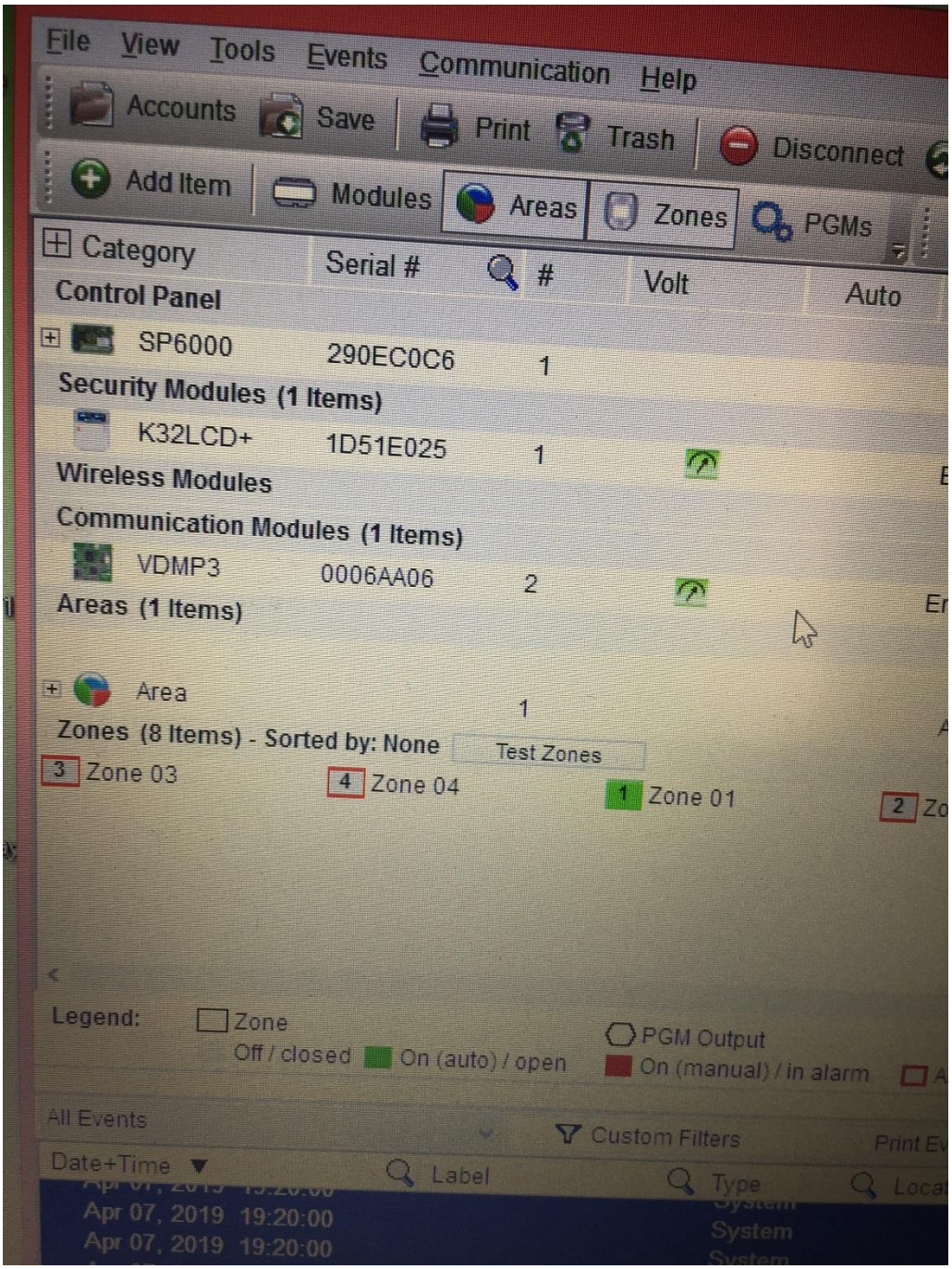
CONFIGURACION DEL EQUIPO DVR CAMARAS



Fuente: Elaboración propia

ANEXO 9

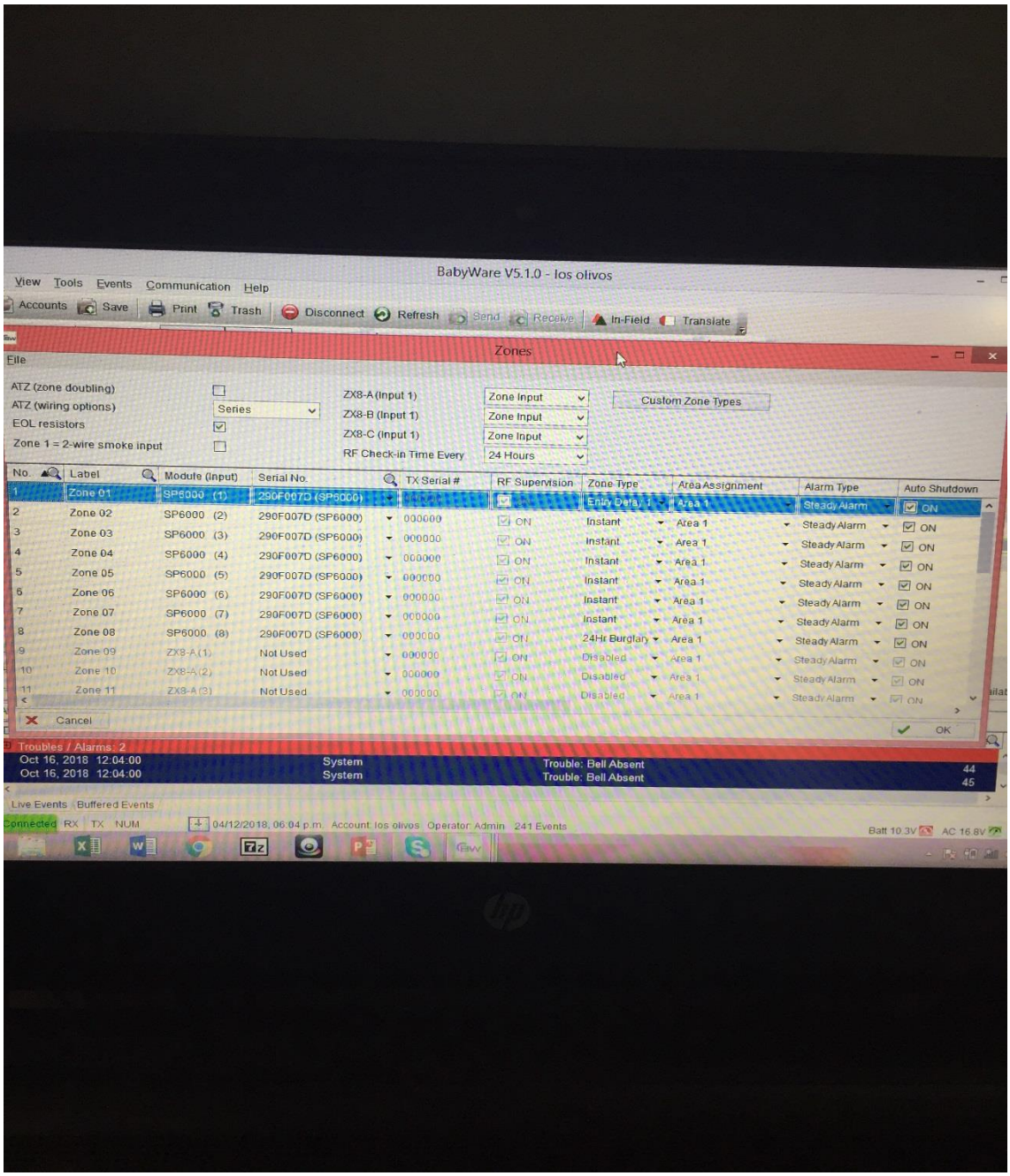
CONFIGURACION DE DISPOSITIVOS DE ALARMA, POR MEDIO DEL PROGRAMA BABYWARE



Fuente: Elaboración propia

ANEXO 10

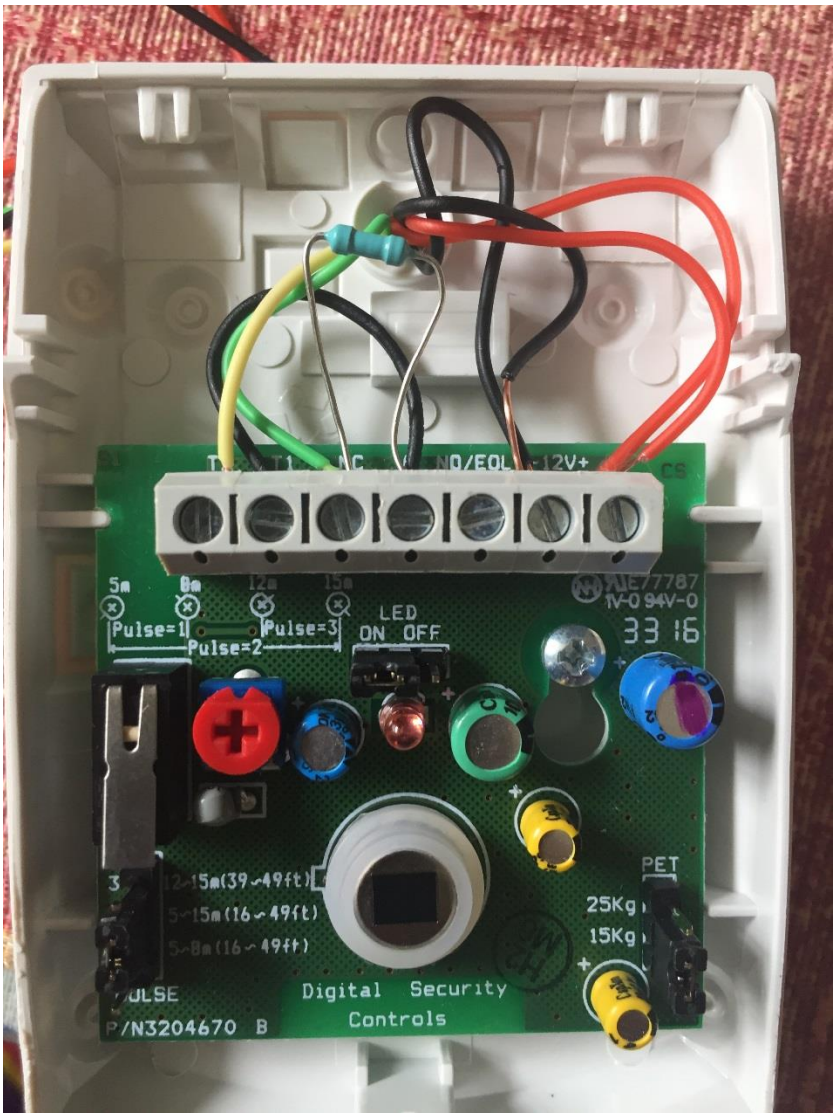
CONFIGURACION DE ZONAS DE ALARMA, POR MEDIO DEL PROGRAMA BABYWARE



Fuente: Elaboración propia

ANEXO 11

CONFIGURACION DE UN SENSOR, PARA LOGRAR QUE TENGA LAS PRESTACIONES DE GRADO 3



Fuente: Elaboración propia

ANEXO 12

CONFIGURACION DE LA CENTRAL DE ALARMAS

Fuente: Elaboración propia

ANEXO 13

CONFIGURACION DEL CABLEADO DE RED TANTO PARA CAMARAS COMO PARA ALARMAS

Fuente: Elaboración propia