



**USMP**  
UNIVERSIDAD DE  
SAN MARTÍN DE PORRES

**FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA**

**SISTEMA DE DUALIDAD REMOTA**

**INFORME POR EXPERIENCIA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO  
ELECTRÓNICO**

**PRESENTADO POR**

**JUAN CARLOS PORTILLA GÓMEZ**

**LIMA - PERÚ**

**2013**



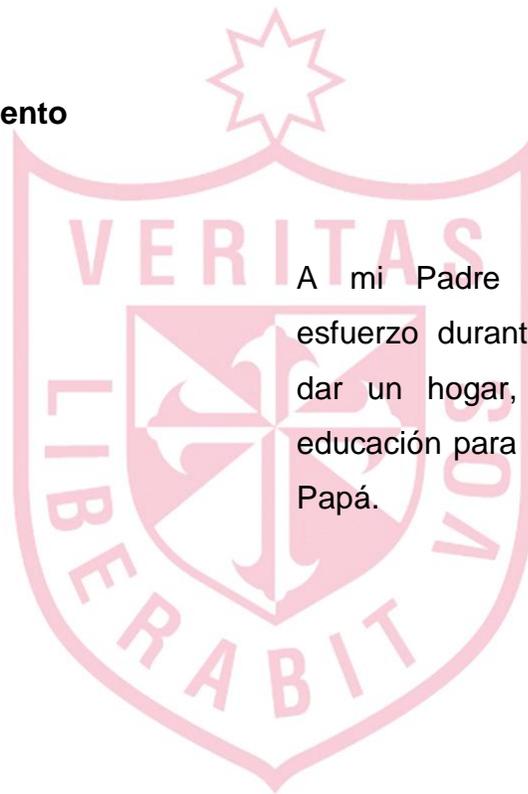
**SISTEMA DE DUALIDAD REMOTA**

## Dedicatoria



El presente trabajo está dedicado a mi Madre por su constante apoyo y compañía en los buenos y malos momentos. A mis hermanas y sobrinos por todo su amor y cariño.

## Agradecimiento



A mi Padre por su invaluable esfuerzo durante su compañía, por dar un hogar, una familia y una educación para sus hijos. Mil gracias Papá.



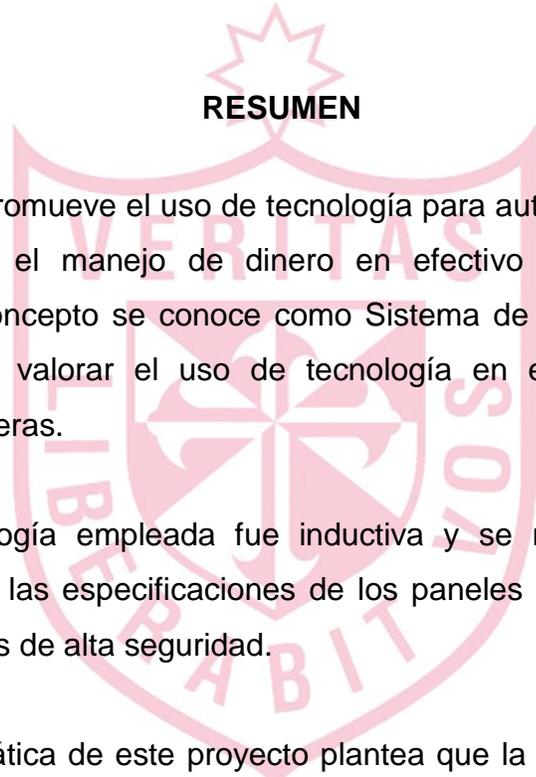
## ÍNDICE

	Pág.
Índice	v
Resumen	viii
Abstract	ix
Introducción	x
<b>Capítulo I TRAYECTORIA PROFESIONAL</b>	<b>1</b>
1.1 Centro de Control del Banco Interbank	1
1.2 Jefatura de Seguridad Electrónica	2
1.3 Logros en Seguridad Electrónica	2
<b>Capítulo II CONTEXTO EN QUE SE DESARROLLO LA EXPERIENCIA</b>	<b>4</b>
2.1 La Empresa	4
2.2 La Organización	7
2.3 Política de la Empresa	8
2.4 Actividades de la Empresa	10
2.5 Ubicación y acceso	10

<b>Capítulo III ACTIVIDADES DESARROLLADAS</b>	<b>11</b>
3.1 Antecedentes	11
3.2 El Sistema Financiero	11
3.3 Las Instituciones	12
3.4 Los entes reguladores	13
3.5 La Seguridad Bancaria	15
3.6 La Base Legal	17
3.7 El Departamento de Seguridad	24
3.8 Los Sistemas de Seguridad Electrónica	25
3.9 El Centro de Control	28
3.10 Situación problemática	29
3.11 La metodología	30
3.12 El proyecto para lograr la solución	32
3.13 Análisis Costo - Beneficio	37
3.14 Aporte Ingenieril	38
3.15 Duración	39
3.16 Tecnologías utilizadas	45
3.17 Medios de atesoramiento de efectivo	52
<b>Capítulo IV REFLEXIÓN CRÍTICA DE LA EXPERIENCIA EVALUACIÓN Y DETERMINACIÓN DE ACIERTOS, ERRORES Y RESULTADOS</b>	<b>57</b>
4.1 Aporte en el área de desarrollo predominante	58
4.2 La Cadena de valor	60
4.3 Aportes y responsabilidades	61
4.4 Desarrollo profesional	62
4.5 Necesidades atendidas	64
4.6 Metas alcanzadas	64
4.7 Indicadores	66

CONCLUSIONES	67
RECOMENDACIONES	68
FUENTES DE INFORMACIÓN	69
GLOSARIO	70
ANEXOS	72



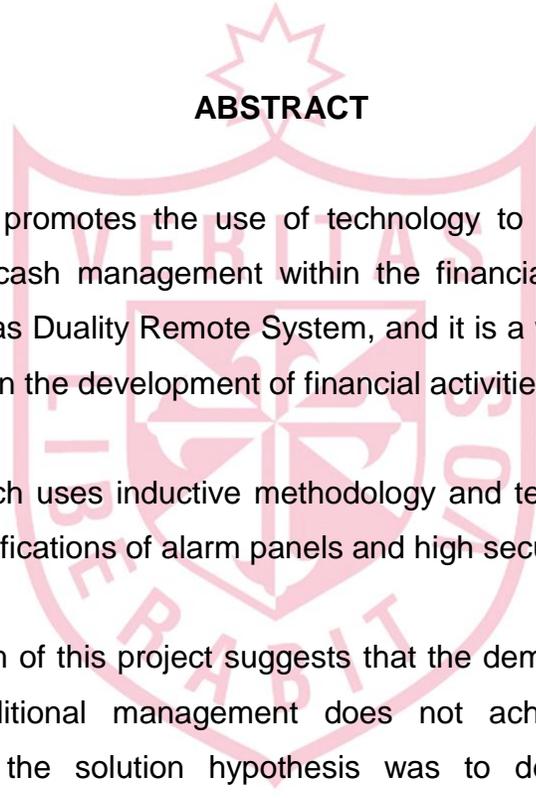


## RESUMEN

Esta tesis promueve el uso de tecnología para automatizar un proceso manual como es el manejo de dinero en efectivo dentro del entorno financiero. Este concepto se conoce como Sistema de Dualidad Remota, y es una forma de valorar el uso de tecnología en el desarrollo de las actividades financieras.

La metodología empleada fue inductiva y se realizó investigación técnica en base a las especificaciones de los paneles de alarmas y de las cerraduras digitales de alta seguridad.

La problemática de este proyecto plantea que la demanda de horas / hombres para el manejo tradicional de dinero en efectivo no permite lograr una ventaja competitiva, por lo tanto, se planteó como hipótesis de solución diseñar, desarrollar e implementar el Sistema de Dualidad Remota para que la necesidad del recurso humano disminuya en esta área y se enfoque en otros campos del negocio. La hipótesis planteada se corroboró.

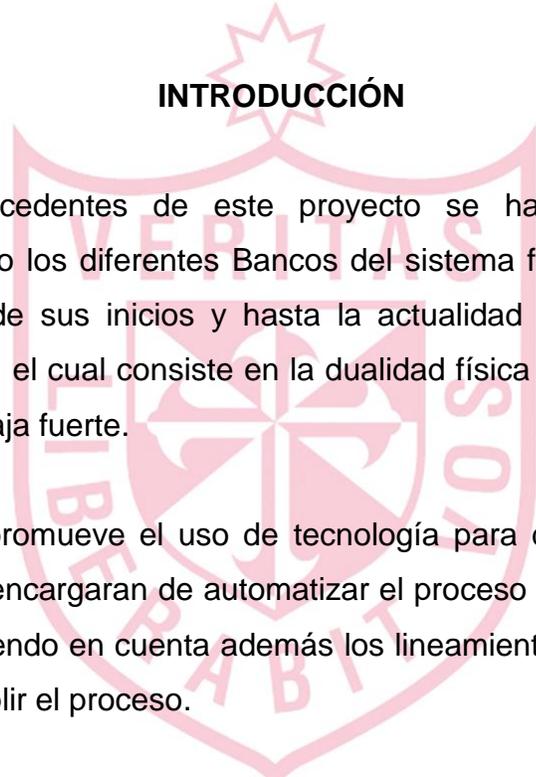


## **ABSTRACT**

This thesis promotes the use of technology to automate a manual process such as cash management within the financial environment. This concept is known as Duality Remote System, and it is a way to recognize the use of technology in the development of financial activities.

This research uses inductive methodology and technical investigation based on the specifications of alarm panels and high security digital locks.

The problem of this project suggests that the demand for man / hours to the cash traditional management does not achieve a competitive advantage, thus, the solution hypothesis was to design, develop and implement the Duality Remote System, so that, the need for human resource decreases in this area and it focus on other business fields. The hypothesis was confirmed.



## INTRODUCCIÓN

Como antecedentes de este proyecto se ha investigado como manejan el efectivo los diferentes Bancos del sistema financiero del país, y se tiene que desde sus inicios y hasta la actualidad aún se mantiene el manejo tradicional, el cual consiste en la dualidad física (dos personas) para la apertura de la caja fuerte.

Esta tesis promueve el uso de tecnología para diseñar y desarrollar interfaces que se encargaran de automatizar el proceso de apertura física de la caja fuerte, teniendo en cuenta además los lineamientos de seguridad con los que debe cumplir el proceso.

La problemática de este proyecto plantea que la demanda de horas/hombres para el manejo tradicional del efectivo no permitirá lograr una ventaja competitiva; por lo tanto, se justifica diseñar, desarrollar e implementar el Sistema de Dualidad Remota para que el recurso humano liberado se enfoque directamente al “core” del negocio.

Asimismo, es oportuno mencionar que el objetivo general de este proyecto consiste en dar a conocer que con técnicas de integración de software y hardware de alarmas se pueden automatizar procesos en el manejo de efectivo. Mientras que, entre los objetivos específicos se encuentran: módulo de interfase de bloqueo, desarrollar la interfase grafica de usuario y realizar la integración del DLS con el SDR.

En lo referente a la hipótesis se plantea el uso del Sistema de Dualidad Remota, lo que se propone conseguir es romper un paradigma en el sistema financiero de que para abrir una caja fuerte necesariamente deben estar presentes físicamente dos personas.

Por otro lado, este proyecto tuvo como limitaciones las siguientes: el tiempo de implementación, abrir el código fuente del software DLS para la integración con la interfase del operador. Un alcance acerca de esta investigación está en el hecho que su uso es para todo manejo de efectivo en las Tiendas financieras ubicadas a nivel nacional, convirtiéndose en un estándar de seguridad.

Finalmente, la estructura de la tesis denominada “Sistema de Dualidad Remota”, se presenta a continuación: en el Capítulo I se plasma la trayectoria profesional del tesista, mientras que en el Capítulo II se presenta el contexto en que se desarrollo la experiencia.

Asimismo, el Capítulo III muestra las actividades desarrolladas, y el Capítulo IV la reflexión crítica de la experiencia, evaluación y determinación de aciertos, errores y resultados.



## **CAPÍTULO I**

### **TRAYECTORIA PROFESIONAL**

#### **1.1 Centro de Control del Banco Interbank**

Inicialmente, en junio de 1999, tuve a cargo la operación del Centro de Control de Seguridad del Banco Interbank, siendo trabajador de la Cooperativa Santo Domingo destacado en Interbank, dedicado a la gestión de las señales de alarmas provenientes de los sistemas de seguridad instalados a nivel nacional. El entorno era crítico e importante, las labores duraban las 24 horas del día, se laboraba en tres turnos de manera rotativa, incluso fines de semana y feriados.

En noviembre de ese mismo año por la coyuntura presentada y debido a la eficiencia de las funciones encargadas, fui invitado junto a un grupo de operadores a formar parte de la planilla del Banco Interbank. Conforme se acercaba el año 2000, se hablaba de los problemas o posibles catástrofes que se originarían por un eventual colapso de los sistemas basados en computadoras. La corrección del problema costó miles

de millones de dólares en el mundo entero, sin contar otros costes relacionados. Con creatividad y esfuerzo en nuestro país se logró la adaptación de las máquinas y programas. Para la fecha límite, un equipo de profesionales a tiempo completo, permanecían en el Centro de Control monitoreando las señales de alarmas de la red de tiendas siendo apoyados por personal experto de sistemas para cualquier contingencia.

### **1.2 Jefatura de Seguridad Electrónica**

A partir de octubre del 2001 apoyé a la Jefatura de Seguridad en la realización de labores de revisión y reprogramación de los paneles de alarmas, elaboración de credenciales de identificación y programaciones de niveles de acceso en el sistema de control de acceso, así como también la captura de imágenes de video para detectar posibles estafas y fraudes en contra de los clientes.

Posteriormente, a finales de octubre del 2001, estuve a cargo de la realización de la ingeniería de seguridad de los nuevos proyectos y remodelaciones que se ejecutaban dentro de la institución. Para ese entonces la Seguridad Electrónica Financiera no se impartía, ni se encontraba escrita en libros, ni mucho menos dictada en ninguna institución del país; de esta manera desde el 1 de noviembre del 2004 fui promovido a la Jefatura de Seguridad Electrónica del Banco, labor que cumplo hasta la fecha.

### **1.3 Logros en Seguridad Electrónica**

A cargo del puesto antes citado, se lograron desarrollar e implementar muchas mejoras tecnológicas en la institución, tales como:

- Migración de los sistemas de alarmas de línea telefonía a IP
- Desarrollo de un prototipo antifraude para cajeros automáticos

- Implementación del primer sistema de dualidad remota para cajas fuertes
- Mejoramiento de seguridad electrónica en cajeros automáticos
- Uso de estándares de seguridad para las instalaciones
- Implementación del Centro de Control Alterno
- Diseño e implementación de seguridad en locales remotos
- Implementación del primer sistema de video digital para Interbank

Esto conllevó a obtener varios reconocimientos por la contribución hecha a la institución.





## **CAPÍTULO II**

### **CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA**

#### **2.1 La Empresa**

El Banco Interbank se fundó el 1 de mayo de 1897, e inició sus operaciones el 17 del mismo mes con un Directorio presidido por el Sr. Elías Mujica. El primer local estuvo ubicado en la calle Espaderos, hoy Jirón de la Unión. En 1934 comenzó el proceso de descentralización administrativa, siendo Chiclayo y Arequipa las primeras agencias en abrirse, seguidas un año después por las de Piura y Sullana.

La política de expansión se intensificó de manera notable en 1942, cuando se adquiere una propiedad en la Plazuela de la Merced y otra en la calle Lescano, donde se construyó el edificio "Sede La Merced", cuyos bellos acabados han llevado al Instituto Nacional de Cultura a catalogarlo como Monumento Histórico.

En el pasado, el accionariado del banco incluyó capitales vinculados a la agroindustria, como la Fabril S.A. y W.R. Grace Co. En la década de los setenta, el Chemical Bank de Nueva York participó en el accionariado y fue responsable de la gerencia del banco. En 1970, el Banco de la Nación adquiere el mayor porcentaje de las acciones, convirtiéndose de esta forma en miembro de la Banca Asociada del país. En 1980 el banco pasó a llamarse Interbanc.



Fig. 2 Local La Merced

Fuente: Interbank

El 20 de julio de 1994 un grupo financiero liderado por el Dr. Carlos Rodríguez-Pastor Mendoza, e integrado por grandes inversionistas como Nicholas Brady (ex Secretario del Tesoro de los EEUU),

entre otros, se convirtió en el principal accionista del banco al adquirir el 91% de las acciones disponibles.

En 1996 decidieron cambiar el nombre a Interbank, y convertir cada agencia en una auténtica tienda financiera en la que con sólo ingresar, los clientes sintieran que accedían a un banco confiable y sólido, donde podían encontrar productos y servicios financieros brindados con asesoría necesaria y un trato especial.



Fig. 3 La nueva Sede Torre Interbank

Fuente: Interbank

## 2.2 La Organización

A continuación se presenta el organigrama del Banco Internacional del Perú – Interbank.

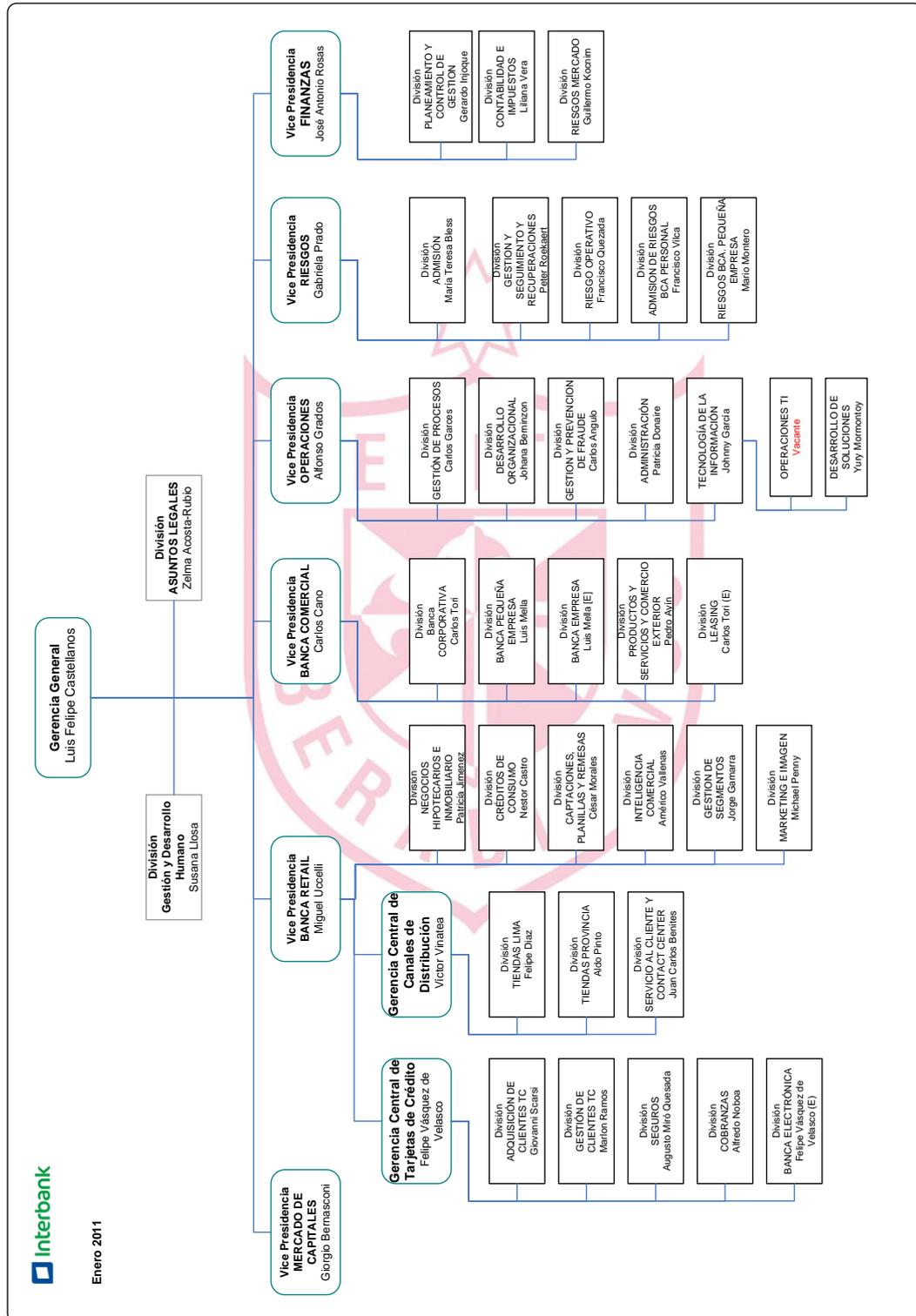


Fig. 4 Organigrama de Interbank

Fuente: Interbank

## 2.3 Política de la Empresa

En junio de 2009, Interbank renovó su imagen después de casi 13 años, el objetivo era reflejar el carácter innovador y dinámico del banco.



Fig. 5 La nueva imagen de Interbank

Fuente: Interbank

Este cambio va de acuerdo con la filosofía “El tiempo vale más que el dinero”, que prioriza la agilidad, conveniencia y buena atención al cliente a través de una actitud de servicio eficiente y amigable.

- a) **Misión:** Mejorar la calidad de vida de nuestros clientes, brindando un excelente servicio en todo momento y en todo lugar.
- b) **Visión:** Ser el mejor banco a partir de las mejores personas.
- c) **Valores:** Los colaboradores de Interbank siguen un riguroso proceso de selección que busca cubrir los requerimientos técnicos para el puesto, pero principalmente busca contar con personas íntegras y profesionales, cuya conducta se encuentre guiada por un conjunto de valores.

Los valores que se buscan en Interbank son los siguientes:

- c.1) **Trabajo en Equipo:** La búsqueda de un ideal común nos une. Con esfuerzo y dedicación buscamos alcanzar nuestras metas.

**c.2) Sentido del Humor:** Aún en tiempos difíciles el sentido del humor ilumina a quienes lo reflejan, contagiando de esperanza y bienestar a los que nos rodean.

**c.3) Vocación de Servicio:** La vocación de servicio refleja la humildad, el interés y la entrega para servir a los demás sin esperar nada a cambio

**c.4) Creatividad e Innovación:** Valor por el que estamos en una constante búsqueda de mejoras para el éxito de nuestra institución

**c.5) Espíritu de Superación:** A quien demuestra su constante lucha y afán por asumir los retos, sin importar los obstáculos que se le presenten en el camino.

**c.6) Transparencia:** Tener la virtud de expresarse con sinceridad siempre, guiado por sólidos principios que defenderemos ante cualquier circunstancia.



Fig. 6 Los valores de Interbank

Fuente: Interbank

## **2.4 Actividades de la empresa**

La empresa Interbank además de ser un banco, cuenta con Tiendas Financieras, mediante las cuales, son las primeras en acercarse al cliente a través de un Horario Extendido, una iniciativa sin precedentes en el sistema financiero nacional, que ha logrado llevar la banca al supermercado. Han continuado progresando significativamente desarrollándose hacia un banco moderno.

Es una entidad financiera presta los servicios de banca y finanzas, así como también brinda servicios adicionales a los que decidan abrir cuentas.

## **2.5 Ubicación y acceso**

La sede principal, denominada Torre Interbank, está ubicada entre las avenidas Javier Prado y Paseo de la República, esta sede marca el inicio de una nueva era, con mejores servicios integrados, tecnología de avanzada y con los mismos valores, filosofía y compromiso que garantizan que se brinde un excelente servicio a sus clientes.

## **CAPÍTULO III ACTIVIDADES DESARROLLADAS**

### **3.1 Antecedentes**

No se cuestiona la importancia que tiene el sistema financiero en el que convergen experiencia, profesionalidad y medios, pero también una diversidad de riesgos, y en algunas ocasiones poca consideración hacia las inversiones en materia de seguridad. Seguridad es lo que para la mayoría de las personas, representa este tipo de entidades. Cuando un cliente ofrece su dinero o sus bienes a una entidad bancaria para su custodia, espera de ella los máximos valores de seguridad. Tanto es así que el asalto a bancos es uno de los delitos que mayor repercusión tiene sobre la opinión pública.

La seguridad que representan las entidades financieras está sustentada tanto en tecnologías de seguridad, software y hardware, así como políticas y procedimientos internos.

### **3.2 El Sistema Financiero**

El sistema financiero está conformado por el conjunto de Instituciones Bancarias, financieras y demás empresas e instituciones de derecho público o privado, debidamente autorizadas por la Superintendencia de Banca y Seguro, que operan en la intermediación

financiera (actividad habitual desarrollada por empresas e instituciones autorizada a captar fondos del público y colocarlos en forma de créditos e inversiones).

Es el conjunto de instituciones encargadas de la circulación del flujo monetario y cuya tarea principal es canalizar el dinero de los ahorristas hacia quienes desean hacer inversiones productivas. Las instituciones que cumplen con este papel se llaman “Intermediarios Financieros” o “Mercados Financieros”.



Fig. 7 El Sistema Financiero Peruano

Fuente: Banca y Seguros

### 3.3 Las instituciones

Las siguientes son las instituciones que conforman el Sistema financiero Peruano y que están encargadas de la circulación del flujo monetario, cuya finalidad es la de canalizar el ahorro, hacia quienes desean hacer inversiones productivas:

- Bancos
- Financieras
- Compañía de Seguros
- AFP
- Banco de la Nación
- COFIDE
- Bolsa de Valores
- Bancos de Inversiones
- Sociedad Nacional de Agentes de Bolsa

### 3.4 Los entes reguladores

Las entidades que regulan y controlan las operaciones del sistema financiero son:

**a) Banco Central de Reserva del Perú.-** Encargado de regular la moneda y el crédito del sistema financiero. Sus funciones principales son:

- Propiciar que las tasa de interés de las operaciones del sistema financiero, sean determinadas por la libre competencia, regulando el mercado.
- La regulación de la oferta monetaria
- La administración de las reservas internacionales (RIN)
- La emisión de billetes y monedas.

**b) Superintendencia de Banca y Seguro (SBS).-** Organismo de control del sistema financiero nacional, controla en representación del estado a las empresas bancarias, financieras, de seguros y a las demás personas naturales y jurídicas que operan con fondos públicos.

La Superintendencia de Banca y Seguros es un órgano autónomo, cuyo objetivo es fiscalizar al Banco Central de Reserva del Perú, Banco de la Nación e instituciones financieras de cualquier naturaleza. La función

fiscalizadora de la superintendencia puede ser ejercida en forma amplia sobre cualquier operación o negocio.

- c) Comisión Nacional Supervisora de Empresas y Valores (CONASEV).**- Institución Pública del sector Economía y Finanzas, cuya finalidad es promover el mercado de valores, velar por el adecuado manejo de las empresas y normar la contabilidad de las mismas. Tiene personería jurídica de derecho público y goza de autonomía funcional administrativa y económica.
- d) Superintendencia de Administración de Fondos de Pensiones (SAFP).**- Al igual que la SBS, es el organismo de Control del Sistema Nacional de AFP.

El actual mercado financiero esta caracterizado hoy en día por:

- Una elevada complejidad originada por el incremento de la competencia de Entidades Financieras y No Financieras
- Mayor cultura financiera de la clientela
- Reducción de márgenes de ganancia
- Nuevos segmentos de población, nuevos productos y servicios
- Nuevos canales de información y venta, etc.

Este entorno dinámico obliga a todas las Entidades Financieras a adoptar nuevos modelos de actuación con el cliente que, en resumen, tratan de superar la simple venta de productos.

Los bancos son usuarios muy importantes de tecnologías modernas, las inversiones en tecnología representan un porcentaje importante del presupuesto de las instituciones, estas aplicaciones han generado cambios importantes en la industria de la

seguridad. La enorme revolución de la informática y de la comunicación conduce a la rápida transmisión de datos desde los distintos lugares remotos.

Ahora bien, se puede concluir que el negocio bancario se ha desarrollado conforme al avance tecnológico, y lo que antiguamente significaba un negocio de manejo de dinero, se ha convertido en los últimos tiempos en un negocio de gestión y proceso de información.

### **3.5 La Seguridad Bancaria**

Dentro del ámbito mundial, para cualquier país, la seguridad bancaria es una prioridad de los bancos como forma de brindar un servicio completo de satisfacción al cliente.

Una persona particular, una corporación o una pequeña empresa, relaciona a los Bancos con la seguridad. Todos ellos depositan su dinero, confiando en que estos lugares emplean y disponen de los más altos estándares de protección para la custodia de sus posesiones. Custodiar elevadas sumas de dinero y bienes los sitúa también en la mira de las bandas organizadas.

Las reglamentaciones Gubernamentales establecen una serie de medidas de seguridad obligatoria para los Bancos. Con respecto a los medios electrónicos de protección, todos los bancos deben contar con sistemas de protección con capacidad para detectar el ataque a cualquier elemento de seguridad física donde se custodien efectivo y valores.

El Sistema Financiero Peruano está regido por los Requisitos Mínimos Obligatorios de Seguridad, establecido por el Ministerio del Interior y que son aquellos de carácter preventivo, disuasivo, auxilio inmediato e identificatorio, orientados a proteger la vida y la integridad física de las personas, así como el patrimonio público y privado, siendo estos de

observancia obligatoria para las empresas cuyo control ejerce la Superintendencia de Banca y Seguros, las que en adelante se denominarán OFICINAS.

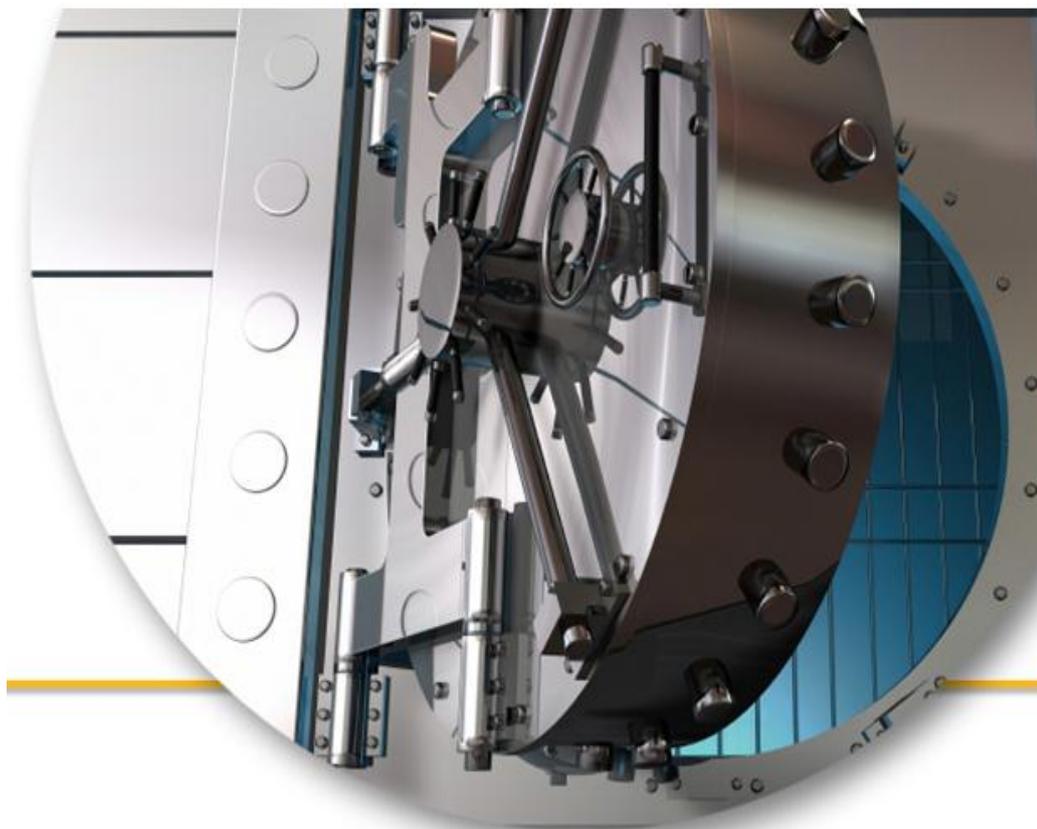


Fig. 8 Protección de los ambientes de efectivo  
Fuente: March Network

### 3.5.1 Concepto de seguridad

La palabra seguridad proviene del Latín SECURITATES y se refiere a la percepción de tranquilidad y ausencia de riesgo que caracteriza un entorno, un procedimiento o una acción.



Fig. 9 Logo de seguridad Interbank

Fuente: Interbank

Es oportuno mencionar que, Interbank define la palabra seguridad como: **Protección, Prevención y Control**; entonces, cuando alguno de estos elementos no se encuentra presente falla la seguridad.

### 3.6 La Base Legal

El Reglamento de Requisitos Mínimos Obligatorios de Seguridad 02/06/2000 - R.M. N° 0689-2000-IN/1701- **Modifica el Reglamento de Requisitos Mínimos Obligatorios de Seguridad que deben adoptar las instituciones cuyo control ejerce la SBS. (11/06/2000) RESOLUCION MINISTERIAL N° 0689-2000-IN/1701** en sus artículos con respecto al control que deben ejercerse especifica lo siguiente:

***REGLAMENTO DE REQUISITOS MINIMOS OBLIGATORIOS DE SEGURIDAD QUE DEBEN ADOPTAR LAS INSTITUCIONES CUYO***

## **CONTROL EJERCE LA SUPERINTENDENCIA DE BANCA Y SEGUROS**

### **CAPITULO I GENERALIDADES**

**Artículo 1º.-** Establézcase que los requisitos mínimos obligatorios de seguridad son aquellos de carácter preventivo, disuasivo, auxilio inmediato e identificatorio orientados a proteger la vida y la integridad física de las personas, así como el patrimonio público y privado, siendo estos de observancia obligatoria para las empresas cuyo control ejerce la Superintendencia de Banca y Seguros, las que en adelante se denominarán OFICINAS.

### **CAPITULO II**

#### **DE LOS ORGANOS COMPETENTES**

**Artículo 2º.-** El Ministerio del Interior por intermedio de la Dirección General de Control de Servicios de Seguridad, Control de Armas, Munición y Explosivos de Uso Civil (DICSCAMEC), en coordinación con la Superintendencia de Banca y Seguros y el Banco Central de Reserva del Perú, *dispondrá la verificación del cumplimiento de las medidas de seguridad por parte de las OFICINAS, para cuyo efecto se conformará el Comité de Verificación que estará integrado por:*

- a) Dos (2) representantes de la DICSCAMEC.
- b) Un (1) representante del Banco Central de Reserva del Perú.
- c) Un (1) representante de la Superintendencia de Banca y Seguros.

**Artículo 3º.-** La Superintendencia de Banca y Seguros y el Banco Central de Reserva del Perú, comunicarán a la DICSCAMEC el nombre

del representante titular de la entidad correspondiente y de un alterno autorizado para conformar el Comité de Verificación.

### ***CAPITULO III***

#### ***DE LOS REQUISITOS MINIMOS OBLIGATORIOS DE SEGURIDAD***

**Artículo 4º.-** El local que ocupan las OFICINAS deberán contar con sistema de alarma y protección contra asaltos, robos e intrusión, debidamente publicitados.

El sistema de alarma contra asalto será silente (desde el ingreso del personal de la entidad hasta el cierre del local) pudiendo ser sonoro cuando en el local ya no se encuentre este personal. Los Recibidores/Pagadores deberán disponer de un pulsador de alarma.

**Artículo 5º.-** Todas las OFICINAS que efectúen transacciones en efectivo deberán estar protegidas por un servicio de vigilancia armada dotado con chaleco antibalas, con capacidad de efectuar el procedimiento de seguridad establecido por cada oficina así como de hacer funcionar la alarma a distancia con un pulsador inalámbrico bajo su control, durante las horas de operación, debiendo encontrarse instalados desde el horario de ingreso del personal de la entidad hasta el cierre del local.

**Artículo 6º.-** El personal de vigilancia deberá contar con adiestramiento permanente y especializado. Dicho personal estará sujeto a las normas del Reglamento de Servicios de Seguridad Privada de la DICSCAMEC o a las normas reglamentarias específicas de la Policía Nacional, según corresponda.

**Artículo 7º.-** Las OFICINAS que cuenten con servicio de ascensores para el personal y uso del público, deberán contar con un procedimiento de operación de emergencia para evitar la paralización de las cabinas por falta de energía eléctrica.

**Artículo 8º.-** En las OFICINAS se deberá ordenar y dirigir el flujo de los clientes hacia las ventanillas de atención de modo que frente a cada una de ellas se encuentre solamente el cliente que por turno le corresponda ser atendido, para lo cual se deberá contar con ordenadores de espera, físicos o electrónicos.

**Artículo 9º.-** El personal de las OFICINAS deberá portar obligatoriamente y en forma visible un distintivo de identificación personal provisto de fotografía, donde se consignen los datos personales correspondientes.

**Artículo 10º.-** Las empresas o entidades del Sistema Financiero deberán contar con una Unidad de Seguridad Interna, encargada de planificar, elaborar y ejecutar las medidas de seguridad en el ámbito de su competencia. Dichas unidades mantendrán una permanente y estrecha coordinación con las autoridades Policiales en los aspectos relativos a su función.

**Artículo 11º.-** La Unidad de Seguridad Interna, previa evaluación, determinará las necesidades de vigilancia, adiestramiento especializado al que se refiere el Art. 6o, sistemas, equipos, dispositivos de seguridad y alarma que requieran las OFICINAS, elaborando a su vez las normas y procedimientos para su mejor operación y mantenimiento.

**Artículo 12º.-** Todas las OFICINAS deberán contar con un sistema de alarma a distancia con capacidad de reportar eventos de asalto e intrusión a una central de alarma de operación continua de propiedad de las Empresas, Asociación o Fundación del Sistema Financiero o de terceros.

Esta central deberá contar con los medios de comunicación necesarios para transmitir la información de manera eficiente e inmediata a los órganos de auxilio de la Policía Nacional.

**Artículo 13º.-** Las OFICINAS deberán contar con un sistema de energía de respaldo para permitir la continuidad en el funcionamiento de sus sistemas operativos de seguridad.

**Artículo 14º .-** Las OFICINAS que cuentan con sistemas informáticos para el desarrollo de sus actividades (servidor/cliente, cajeros automáticos), deberán instalar sistemas de seguridad orientados a bloquear operaciones fraudulentas a través de hardware y software de seguridad.

**Artículo 15º.-** Las OFICINAS que realicen movimientos de efectivo deberán efectuarlos a través de las empresas transportadoras de caudales utilizando, preferentemente, el sistema de "fardo cerrado", debiendo dar prioridad al personal de las unidades blindadas para la recepción y/o entrega de remesas, facilitando un acceso directo con el fin de reducir al máximo los tiempos de espera de acuerdo a los procedimientos establecidos por cada entidad y coordinando debidamente con la empresa transportadora de caudales.

En aquellos lugares donde no existieran empresas transportadoras de caudales, las OFICINAS establecerán sus procedimientos para realizar las remesas entre ellas, contando para los efectos con el concurso de uno o más efectivos policiales que garantice la seguridad de la operación.

**Artículo 16º.-** Las OFICINAS que cuenten con ambientes especiales para el manipuleo de dinero, efectuarán las operaciones de recepción y/o entrega de dinero fuera de la visión del público.

En las OFICINAS que no se cuente con ambientes especiales o acceso directo, las operaciones de entrega y/o recepción de remesas deberán ser realizadas en la ventanilla más próxima al ambiente de la bóveda o

caja fuerte de seguridad; debiendo ser atendidas prioritariamente por el empleado responsable.

**Artículo 17º.-** Todas las puertas de bóveda y caja fuerte de seguridad de las OFICINAS deberán estar dotadas de cerraduras especiales de llave, clave, retardo (corto y largo plazo).

**Artículo 18º.-** Para la apertura y cierre de la puerta de bóveda y/o caja fuerte de seguridad, la OFICINA deberá contar con un plan dual en los mecanismos de seguridad, claves o llaves y sus combinaciones, debiendo efectuarse los cambios de claves cada vez que se reemplace a la persona responsable. La llave duplicada deberá guardarse en custodia en otro local.

**Artículo 19º.-** Las OFICINAS con bóvedas de concreto armado y/o acero y caja fuerte de seguridad deberán contar con niveles de seguridad susceptible de reducir el riesgo de incendio y de violación por elementos mecánicos o equipo de oxicorte.

**Artículo 20º.-** En el caso de OFICINAS que se encuentren equipadas con caja fuerte de seguridad, estas deberán instalarse en un recinto cerrado, opaco, de material resistente a prueba de intrusión violenta, protegido con seguridad electrónica y fuera de la vista del público.

Cuando la caja fuerte de seguridad pese menos de mil (1,000) kilos deberá contar con un anclaje fijo en estructura de concreto armado al suelo o al muro.

**Artículo 21º.-** Todos los ambientes de bóvedas u otros dedicados a la custodia de dinero, deberán ser equipados con dispositivos electrónicos de seguridad con capacidad de ser particionados, destinados a contrarrestar riesgo de accesos no autorizados, en forma independiente del área del local ubicadas fuera de la vista del público.

**Artículo 22º.-** Las OFICINAS que cuenten con bóvedas o cajas fuertes de seguridad, deberán observar las siguientes normas:

- a) Guardar en el interior de la bóveda o caja fuerte de seguridad sólo dinero y valorados.
- b) Contar con un registro de ingreso de personas ajenas a la organización a la bóveda o ambiente de caja fuerte de seguridad, que por necesidad de mantenimiento, auditoría, seguridad u otros, deban ingresar.
- c) Contar con un sistema de extinción de fuego acorde con el material de combustible a combatir.
- d) Las bóvedas deberán contar con iluminación suministrada por un sistema de alimentación externa.
- e) El recinto de las cajas fuertes de seguridad deberán contar con un sistema de detección contra incendios.
- f) Contar con el aviso de restricción de acceso "sólo a personal autorizado", según el formato del Anexo 02.

**Artículo 23º.-** Los Cajeros Automáticos ubicados en las OFICINAS así como en Lobbys y aislados, deberán observar las siguientes normas:

- a) Las paredes donde se encuentra ubicado el frontis del Cajero debe ser reforzada y sus recintos interiores protegidos con medios electrónicos de seguridad.
- b) El ambiente y los cubículos de atención, deberán estar protegidos con sistemas de seguridad electrónica.
- c) Deberá encontrarse anclado y dotado o implementado de medios de seguridad electrónica.
- d) Para el abastecimiento de cajeros automáticos por las empresas de transporte de dinero y valores, deberá reducirse al máximo el tiempo de espera para la operación.

Realmente es interesante considerar este marco regulatorio, ausente o prácticamente ausente en otras actividades propias de la seguridad electrónica, que indefectiblemente deben converger a una legislación

que establezca un marco de referencia para la actividad. Un ejemplo de la ausencia de marco regulatorio es la video vigilancia en la vía pública.

### **3.7 Departamento de Seguridad**

Es el encargado de planificar, organizar, dirigir y controlar las actividades de seguridad, preservando el patrimonio del Banco a nivel nacional, así como resguardar el recurso humano mediante la ejecución e implementación de medios físicos, electrónicos y medidas de tipo organizativo requeridas para la prevención y/o mitigación de siniestros. Desde el 1 de noviembre de 2004 se me encargó la Jefatura de Seguridad Electrónica del Banco, labor que cumpla hasta la fecha. Esta área es responsable de dirigir, supervisar y controlar las actividades del personal técnico, mantener los sistemas de seguridad electrónica operativos a través de programas de mantenimiento, los cuales brindan la protección necesaria del recurso humano y patrimonio a nivel nacional, proponiendo nuevas propuestas tecnológicas de acuerdo a las necesidades requeridas por el Banco.

La electrónica tiene como herramienta a la tecnología, y esta se puede definir como un mecanismo para convertir las ideas en procesos o servicios, que permitan lograr mejoras o desarrollar mejores procesos. La tecnología hoy en día desempeña un papel crítico en la competitividad de las empresas y la Seguridad Electrónica trabaja para rediseñar y mejorar los sistemas de seguridad tanto en tiendas como en los cajeros automáticos.

Cuando se implementan sistemas de seguridad en el sistema financiero, la seguridad electrónica se convierte en el complemento natural e ideal de la seguridad física y su importancia radica en que se sustenta en la aplicación y uso de la tecnología y soportada en base a diseños adecuados, instalación e interconexión, de manera tal, que permita obtener una alerta temprana de los eventos generados en las

instalaciones, en el momento en que pudieran estar siendo vulneradas por personas extrañas a la organización.

A la seguridad electrónica se debe tomarla como un recurso que existe para ser utilizada siempre que se esté haciendo un programa de aseguramiento de un área específica, ya que sus alternativas son muy variadas.

### 3.8 Los sistemas de seguridad electrónica

Debido a las diversas aplicaciones que ofrecen estos sistemas, sus servicios satisfacen oportunamente las demandas de quienes buscan prevenir riesgos ya sea en sus negocios y en sus hogares.

Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos (interior y exterior), el control de accesos, la detección de incendios y la video vigilancia.



Fig. 10 Los sistemas de seguridad electrónica

Fuente: Tecnología de Seguridad

Los criterios que fundamentan la importancia y necesidad de la implementación de un sistema de seguridad, según la Asociación de Bancos del Perú (ASBANC), son:

**“Siempre existen actividades no previstas:** y si lo están, siempre se presentan imprevistos, desde una remodelación de instalaciones efectuado por personal que no necesariamente conoce de sistemas de seguridad, condiciones climáticas variables o extremas que pueden alterar el correcto funcionamiento de los equipos y dispositivos, hasta sabotajes e intentos de intrusión.

**Son nuestros ojos y oídos las 24 horas del día, los 7 días de la semana:** La tecnología ha logrado un gran desarrollo, permitiendo contar en la actualidad con equipos y dispositivos de seguridad confiables, facilitando la tarea de control y supervisión, manteniéndonos informados de lo que ocurre en las instalaciones aun cuando el usuario no esté presente.

**Un diseño adecuado es indispensable:** Toda la tecnología disponible no sirve por más sofisticada que sea, si el diseño del sistema de seguridad que ha de ser implementado en sus instalaciones, no cuenta con un respaldo de conocimientos y experiencia probada y comprobada; esto solo puede ser ofrecido por empresas especializadas que demuestren que cuenta con el personal calificado y la experticia necesaria, para garantizar el correcto funcionamiento del diseño ofrecido.

**Debe existir una periodicidad para ejecutar el mantenimiento preventivo:** Recuerde que es como un seguro, ya que si le falla cuando usted más lo necesita de nada valdrá haber invertido en instalarlo para asegurar sus instalaciones, determinándose su periodicidad en función al tipo de sistema de alarma instalado, y otras condiciones particulares que se determinen para cada sistema.

**Familiarícese con su sistema de alarma:** Recuerde que cuanto mayor sea el conocimiento de sus sistemas de alarma por parte de los funcionarios y empleados a cargo de la seguridad interna de su entidad, mayor será el provecho que puede obtener del

mismo, adoptando actitudes pro activas en beneficio de la seguridad de sus instalaciones.

- **Confianza y Seguridad:** Son los dos principales pilares que sustentan el normal desarrollo y la continuidad del negocio financiero en nuestro país, por tal motivo, se debe considerar que el mantenimiento de los sistemas de seguridad electrónica debe ser efectuado por una entidad que contribuya a cumplir con estos objetivos.”

Así mismo se puede apreciar que actualmente se viene incrementando la utilización de sistemas de Circuito Cerrado de Televisión (CCTV) como complemento a los sistemas de seguridad, nuestra reglamentación aún no contempla su uso, pero se estima que en un futuro cercano y tomando como ejemplo algunos países de la región como Colombia se convertirá en una exigencia que todo el sistema financiero deberá cumplir, por el bienestar de los clientes y de las operaciones que se realicen.

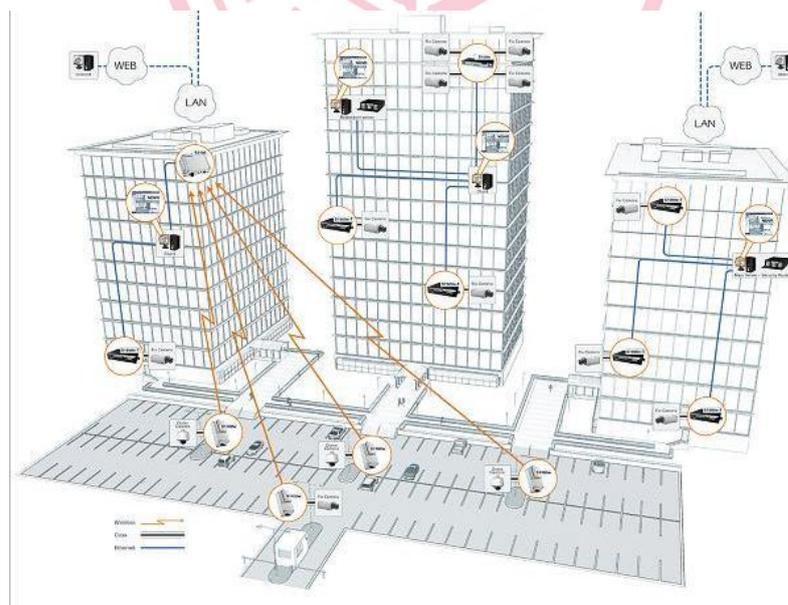


Fig. 11 Los sistemas de CCTV

Fuente: Novenca

### 3.9 El Centro de Control

Los centros de control son salas especialmente equipadas para monitorear y controlar las operaciones de seguridad en las sucursales bancarias. En este ambiente se centralizan y gobiernan los diferentes sistemas (Alarmas, accesos, incendios, videos, etc).

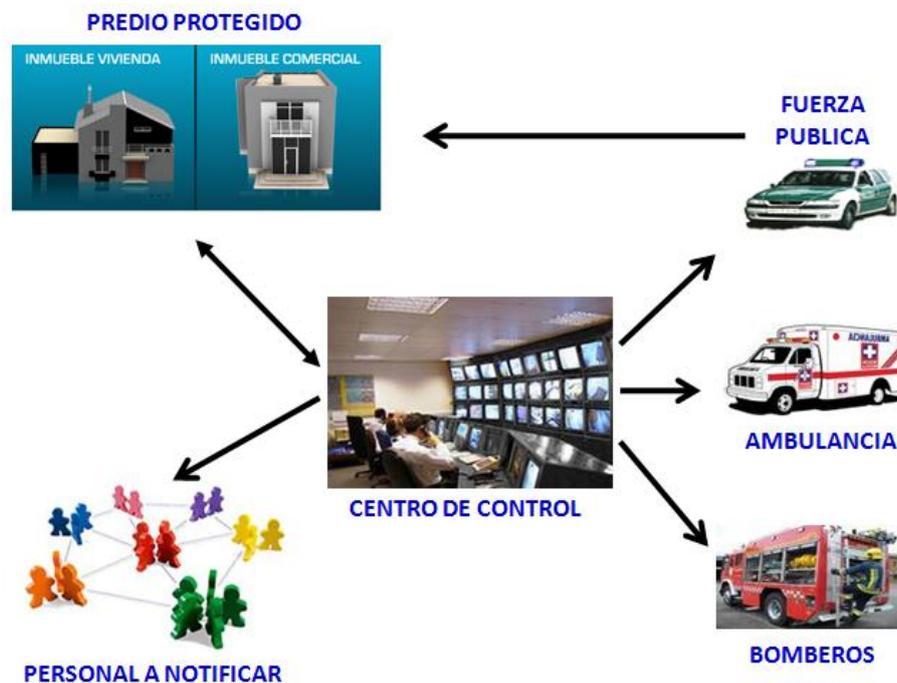


Fig. 12 El Centro de Control

Elaborada por el autor

Debido al desarrollo tecnológico (Internet, telefonía móvil, redes LAN/WAN), desde el centro de control es posible la gestión de los diferentes sistemas desde cualquier lugar del mundo y a cualquiera hora mediante un programa informático navegador o el teléfono móvil.

Su misión principal es cumplir con el triángulo crítico de emergencias: detección del riesgo, comunicación oportuna y respuesta inmediata. Así mismo como parte de sus funciones están

encargados de: dar aviso técnico de fallas en los sistemas y el control de alarmas por omisión o error de procedimientos.

En los entornos de control, los operadores deben consultar información relativa a una situación en tiempo real en el mismo momento en que esta sucede. En consecuencia, necesitan disponer de varias pantallas para visualizar los eventos y mejorar el flujo comunicativo, ya que así podrán gestionar la situación desde lejos o bien proporcionar a las personas allí presentes toda la información necesaria para actuar.

### **3.10 Situación problemática**

Debido al creciente dinamismo del sector financiero los Bancos se encuentran en una permanente búsqueda de cómo lograr una ventaja competitiva frente al resto de sus competidores.

Según refiere el gerente general de Master Card para Perú y Bolivia, Juan Antonio Cabañas: “la competencia se acentúa cuando se está saliendo de una etapa de restricciones del crédito, lo que deriva en mejores ofertas, productos y servicios al consumidor final. Nadie quiere perderse ni un trocito de lo que puede ganar en el actual contexto de recuperación, ya que se está saliendo de una crisis global donde se registraron algunas restricciones de crédito”.

En ese sentido se evaluó el proceso del manejo del efectivo en donde a los funcionarios que tengan bajo su responsabilidad el manejo de cajas fuertes o bóvedas, se les asignará la clave respectiva y deben ser los únicos que la conocen. Estas claves son asignadas por los departamentos de seguridad a dos personas, siendo estas personales e intransferibles, por lo que cada vez que se requiera la apertura de la caja fuerte o bóveda estas dos personas deben encontrarse presentes físicamente. Esta forma de operar demanda el uso horas - hombre para la apertura de la caja fuerte, dejando de atender a los clientes por un lapso de 10 minutos, que es el tiempo que debe transcurrir como retardo de apertura.

Por lo que optimizar este proceso era el reto a desarrollar.

### **3.11 La Metodología**

Entonces para lograr el objetivo de agilizar el proceso para la apertura de la caja fuerte por parte del personal de las agencias y enfocarlo en la atención al público se establecieron en primer lugar algunos criterios que deben cumplir las alternativas planteadas.

#### **a) Los criterios**

Con la finalidad de que el sistema funcione dentro de los parámetros establecidos se debieron cumplir ciertos criterios:

- Seguridad en el proceso
- Monitoreo desde del centro de control.
- Recuperación de la inversión menor a 2 años
- Optimizar el proceso de apertura de las cajas fuertes.

#### **b) Selección de alternativas**

Para la selección de las alternativas se usó la matriz de rango de actuación. Esta consiste en un arreglo de dos matrices, que busca seleccionar un conjunto de alternativas en dos etapas, en la primera se analiza cada una de las alternativas de acuerdo a los resultados obligados (lo mínimo) que han sido previamente determinados.

En la segunda etapa, las alternativas que fueron aceptadas son nuevamente valoradas, de acuerdo al grado con el que se aproximen más a los resultados deseables (lo máximo). Para ello se le asigna a cada alternativa una calificación entre 1 a 5 para cada uno de los resultados deseables, y se multiplican por sus correspondientes pesos específicos que previamente se definieron.

Finalmente, se jerarquizan las alternativas aceptadas de acuerdo a las calificaciones resultantes.

### c) Evaluación de las alternativas

Se evaluaron las siguientes alternativas:

- **Alternativa A:** que se mantenga la dualidad física para la apertura.
- **Alternativa B:** que cada usuario pueda realizar independientemente la apertura.
- **Alternativa C:** establecer en la programación de la cerradura la creación de grupos de usuarios.
- **Alternativa D:** que no exista retardo de apertura.
- **Alternativa E:** sistema de dualidad que gestione remotamente las cerraduras de las cajas fuertes.

Análisis y cumplimiento de los resultados obligados (SI/NO)	ALTERNATIVAS A CONSIDERAR				
	A	B	C	D	E
Que sea ejecutable	SI	SI	SI	SI	SI
Que sea un proceso seguro	SI	NO	NO	NO	SI
Que se pueda monitorear	NO	NO	NO	NO	SI
Que no demande demasiado tiempo la implementación	SI	SI	SI	SI	NO
Que cumpla el objetivo	NO	SI	NO	SI	SI

Fig. 13 - Matriz del nivel mínimo de actuación

Elaborada por el autor

Como resultado del proceso de selección de alternativas se aprobaron en el primer análisis las alternativas A, B, D y E.

### d) Valoración de alternativas

En la siguiente matriz se evaluaron las alternativas en relación con los objetivos deseados por el proyecto, usando la siguiente escala de valoración:

PESO	IMPACTO
5	MUY FAVORABLE
4	FAVORABLE
3	INDIFERENTE
2	POCO FAVORABLE
1	DESFAVORABLE

Análisis y cumplimiento de los objetivos deseables (B x C)	CALIFICACION C (1-5) DE LAS ALTERNATIVAS CONSIDERADAS										
	PESO (B)	A	A'	B	B'	C	C'	D	D'	E	E'
Proceso de apertura seguro	4	5	20	1	4	1	4	1	4	5	20
Monitoreado por el Centro de Control	2	1	2	1	2	1	2	1	2	5	10
Tiempo de implementación	3	4	12	4	12	4	12	4	12	2	6
Costo de la implementación	1	4	4	4	4	4	4	4	4	2	2
Libera tiempo para los clientes	5	1	5	5	25	5	25	5	25	5	25
<b>TOTAL B x C</b>			<b>43</b>		<b>47</b>		<b>47</b>		<b>47</b>		<b>63</b>

Fig. 14 Matriz del nivel máximo esperado

Elaborado por el autor

En consecuencia, se eligió la realización de la ALTERNATIVA D, el sistema de dualidad remota.

### 3.12 El proyecto para logra la solución

Interbank con su cultura de innovación, y mediante la aplicación de tecnología encontró una oportunidad de mejora en donde el objetivo es optimizar la operación de las aperturas de las cajas fuertes en la red de Tiendas, de manera tal que se libere más recurso humano a favor del negocio, que es una mejor atención al cliente y la venta de productos, pero basados en los lineamientos de prevención, protección y control del proceso. En el cuadro inferior se resume la cantidad de horas que se liberan al aplicar el sistema de dualidad remota en la red de Tiendas.

TIPO	#Tdas	# Aperturas CF	Tiempo apert. (Min)	Diario (Min)	Mensual (Min)	Hrs/Mes	TOTAL (Hrs)	HORARIO
TL	117	5	10	5850	140400	2340	2574	L-V
	117	3	10	3510	14040	234		S
TP	64	5	10	3200	76800	1280	1408	L-V
	64	3	10	1920	7680	128		S
TM	48	5	10	2400	72000	1200	1200	L-D
<b>Total de Horas mensuales</b>							<b>5182,00</b>	
<b>Equivalentes a posiciones de RFs</b>							<b>648</b>	

Fig. 16 Cuadro de horas liberadas

Elaborado por el autor

Considerando que cada tienda realiza un número de cinco (5) aperturas de caja fuerte de lunes a viernes y tres (3) los fines de semana, siendo que esta operación de apertura les toma diez minutos (10'); entonces, al mes en toda la red de Tiendas se liberarían más de 5,182 horas mensuales lo que equivale a decir 648 posiciones de Representantes Financieros (se considera que un representante financiero - RF- trabaja una jornada laboral de 8 horas). Así, el proyecto contendrá lo siguiente:

**a) Sistema de Dualidad Remota (SDR)**

En los permanentes procesos de innovación como parte de los valores de la Cultura Interbank se planteó, desarrolló e implementó el Proyecto de Sistema de Dualidad Remota o también conocido como SDR, en la red de Tiendas financieras.

Este proyecto conllevó a la inclusión de tecnología electrónica para desarrollar soluciones tanto de hardware y software, para que funcionen de manera combinada y permitan agilizar el proceso de apertura de los elementos de atesoramiento de efectivo, maximizando el uso del recurso humano, cambiando la presencia física de apertura (dualidad) a solo una persona en interacción dual con el Centro de Control mediante de una gestión remota.

Si bien es cierto que este desarrollo de gestión remota de apertura de los medios de atesoramiento de efectivo, es una innovación en el sector financiero, los elementos utilizados no están homologados.

El ciclo operativo de la gestión remota de cerraduras empieza cuando el usuario solicitante realiza la comunicación para la programación del retardo de desbloqueo, esta acción se origina en la ventana horaria de 08:30 a 09:00 am, el operador registra la solicitud en su sistema y culmina cuando el sistema de dualidad remota – SDR - ejecuta en automático el pulso de desbloqueo (luego de haber transcurrido los 10 minutos de retardo establecido).

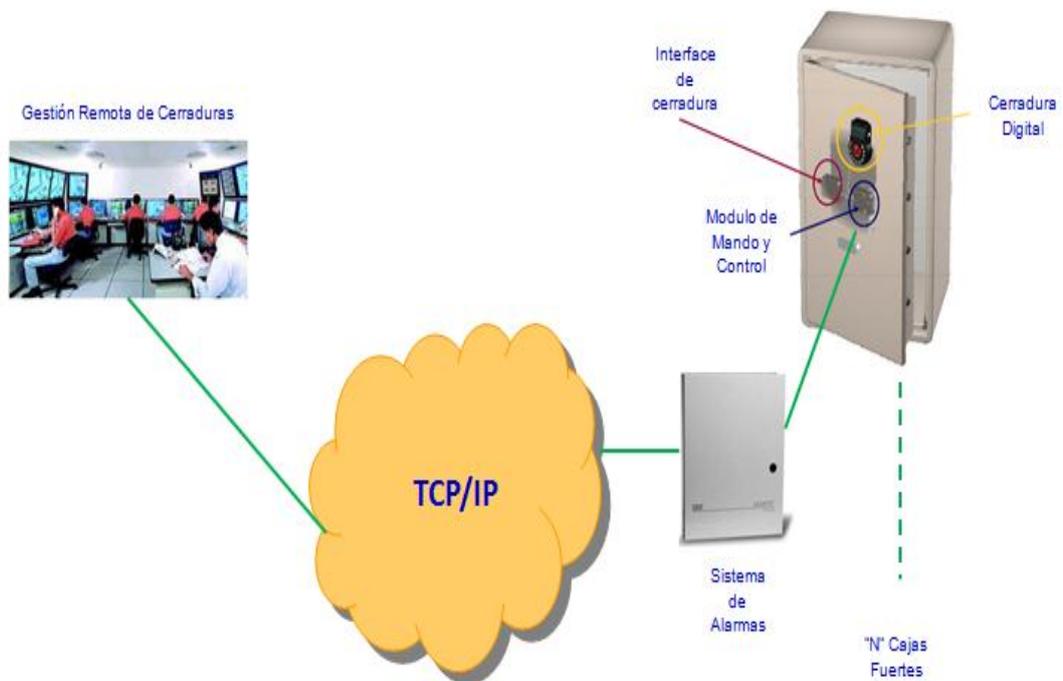


Fig. 17 Proyecto SDR  
Elaborada por el autor

## b) La gestión de apertura remota

La gestión de aperturas remotas de cajas fuerte es un sistema de seguridad diseñado para el control, apertura y cierre de las cajas fuertes, se trata de un sistema que permite realizar las tareas de gestión de la forma más sencilla posible.

Al desarrollar un sistema de gestión remota de Bloqueo/Desbloqueo de las cerraduras, se cuenta con un monitoreo, seguridad y un mejor control del parque cajas fuertes instalado, sin importar donde está instalada la cerradura. De esta forma, la combinación de tecnología de hardware y software se pone al servicio del departamento de seguridad.

Con la gestión remota se planifica, organiza, supervisa y controla los elementos de atesoramiento de efectivo para garantizar un nivel de servicio de acuerdo a la solución planteada.

El sistema de gestión remota tiene los siguientes objetivos: Maximizar el aprovechamiento de los recursos, mejorar el servicio, reducir costes / inversiones y garantizar su disponibilidad.



Fig. 18 Gestión remota de Cerraduras

Fuente: Lagard Iberica

Los operadores responsables de la operativa de control pueden disponer del estado de las cerraduras y reaccionar ante cualquier evento anómalo o no reportado.

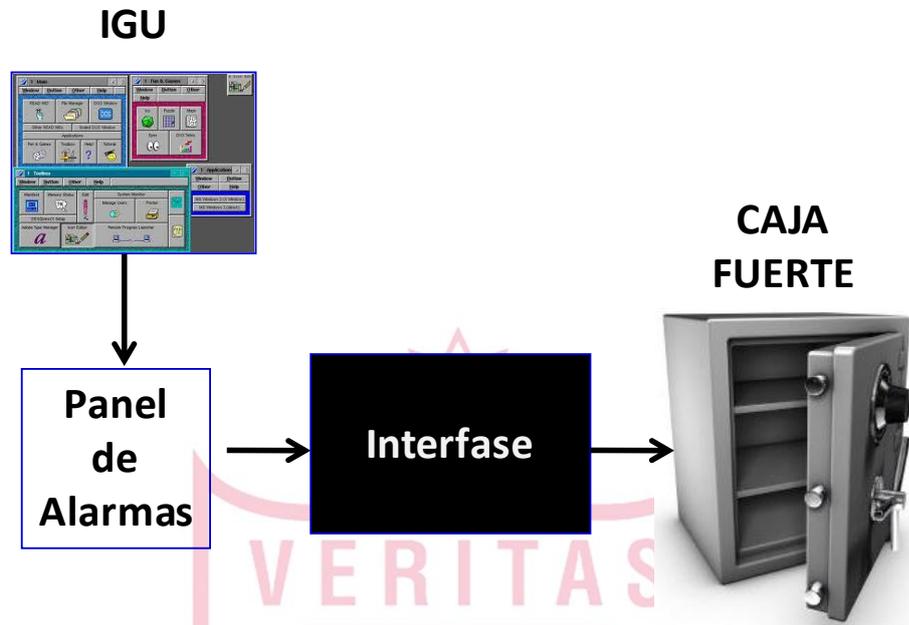


Fig. 19 Hardware de bloqueo proyecto SDR

Elaborado por el autor

Este sistema de gestión remota integra el software de monitoreo denominado Control Central y el desarrollo de la interfaz gráfica de usuario denominada SDR (Software especial desarrollado para el Banco). Mediante esta interfaz gráfica se tiene en pantalla a todas las sucursales con dualidad remota al mismo tiempo y mostrando el estatus en línea de cada caja fuerte. Entre las ventajas que ofrece el sistema de dualidad remota se tiene:

- Desbloqueo automático luego de programado
- Tiempos de retardo programable.
- Monitoreo en línea del estatus de la caja fuerte
- Tiempo excedido de caja fuerte abierta en línea

### 3.13 Análisis Costo - Beneficio

Durante los últimos años la visión que se tenía con respecto al área de seguridad ha cambiado, ya no es vista solo como un área que ocasiona gasto sino como parte de un engranaje principal que aporta valor a las instituciones y a los clientes.

Por ello, los Bancos cuidan mucho los recursos sobre los que invierte, no siempre toda implementación tecnológica tiene un costo cero, en este caso es evidente que existe un beneficio permanente, ya que la seguridad de los fondos y el patrimonio de los clientes, es el objetivo principal de las instituciones de este tipo.

En consecuencia con la implementación de este proyecto y considerando que las 648 posiciones de RF's liberados realicen en promedio de 6480 transacciones, las cuales reportarán un ingreso de US\$57,600.00, por lo que se tendrá un periodo de recuperación de un año, aplicando la fórmula del punto de equilibrio, lo que se muestra a continuación:

$$\text{P.E.} = \frac{\text{COSTO DE INVERSIÓN}}{\text{INGRESO X TRANSACC.}} \times 12$$

$$\text{P.E.} = \frac{59,625.40}{57,600.00} \times 12 = 12.42 \text{ meses}$$

Fig. 15 Análisis Costo/Beneficio

Elaborado por el autor

El resultado muestra que la inversión en el sistema SDR se recuperará en poco más de 1 año (12.42 meses).

### 3.14 Aporte Ingenieril

Desde la llegada a la Jefatura de Seguridad Electrónica se realizaron investigaciones sobre los detalles técnicos de todos los elementos que conforman los diversos sistemas de seguridad, profundizando en su estructura y operación. La experiencia adquirida permitió que se pudiera evaluar soluciones tecnológicas y alternativas de mejoras a los problemas presentados.

Sin embargo, dado que la ocupación principal se enfoca primordialmente en la gestión de la seguridad electrónica, y por la importancia y envergadura del reto, debido a la demanda de horas/hombre que ello implica, se convocó a diversos proveedores del Banco para llevar a cabo el proyecto en mención. En ese sentido se lideró todo el proyecto, y como gestores de la solución se asesoró y supervisó cada uno de los elementos que constituirían el sistema SDR.

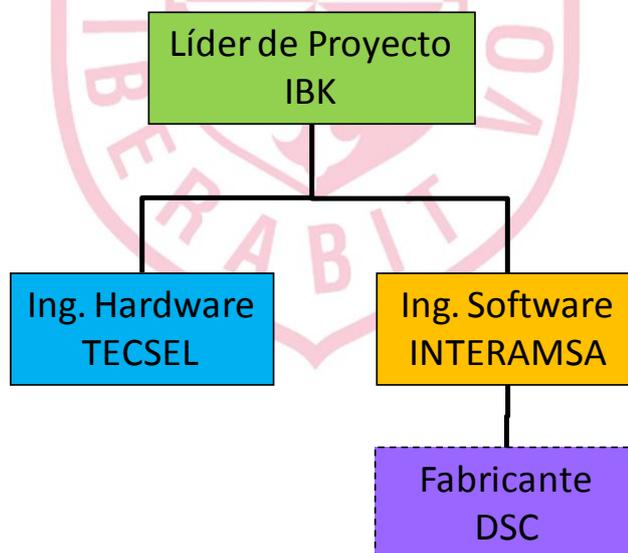


Fig. 20 Estructura del equipo de trabajo

Elaborado por el autor

La solución consistió en desarrollar un sistema que permita pasar de la dualidad de apertura física (dos personas), a solo una, reemplazando la segunda por la acción remota. Las etapas de esta solución conllevan a lo siguiente:

- Desarrollar el interfaz de control electrónico MIB
- Desarrollar la interfaz gráfica de usuario
- Integrar el software DLS con el sistema SDR

### 3.15 Duración

Para lograr este proyecto se estableció las tareas y actividades que deben ejecutarse en los diferentes módulos integrantes del sistema SDR, a partir de ello se estableció el Gantt del proyecto:

- Durante tres meses se desarrollaría la interfase de bloqueo MIB, desde el diseño del circuito, la simulación del modelo, la implementación del PCB pasando por el montaje respectivo y realizando las pruebas en vacío.
- En forma paralela y por cuatro meses se trabaja el desarrollo de la interfase gráfica del usuario, desarrollado el análisis y modelado de usuarios, tarea y entornos, el diseño e implementación de la interfase.
- Los siguientes cuatro meses se realiza la integración de los módulos, analizando en primer lugar los códigos fuentes del DLS para luego insertar las rutinas del SDR y puedan ejecutarse los comandos de control.
- La validación se hará en un mes comprobando que el sistema cumpla con la ejecución de tareas designadas, facilidad de utilización, aceptación de la interfase.
- La última etapa de tres meses corresponde a pruebas pilotos dentro de un ambiente real de funcionamiento evaluando el rendimiento del sistema.



### a) Módulo de Interfase de bloqueo - MIB

Este elemento estuvo bajo el encargo de la empresa TECSEL, especialista en desarrollo de hardware, quien bajo las directivas brindad llevo a cabo el desarrollo y fabricación del modulo de bloqueo denominado MIB - Modulo de Interfase de Bloqueo – el cual se describe en detalle en el anexo 2.

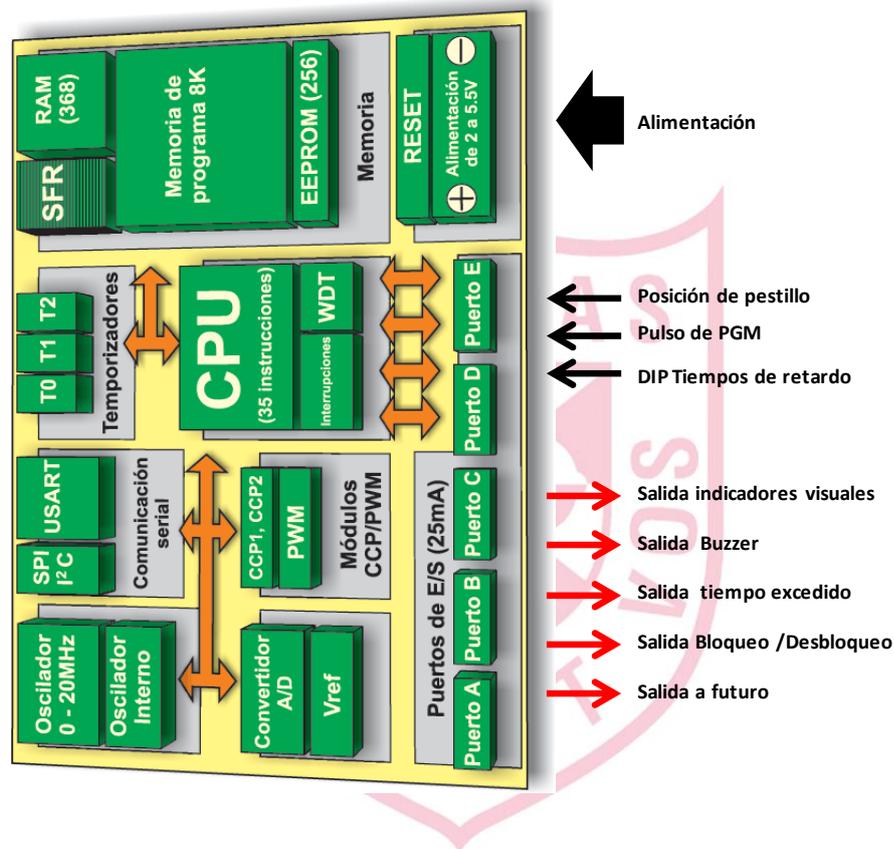


Fig. 22 Esquema en bloques del MIB  
Adaptado por el autor (Mikroelektronika)

Se decidió por hacer el diseño en base a microcontroladores debido a su gran versatilidad, fácil manejo y disponibilidad del recurso.

Por otro lado, se aprovechó una de las tantas funcionalidades que posee el panel principal de alarmas (MAXSYS 4020) como lo es la salida PGM la cual puede generar una señal temporizada (mediante una programación interna) y que envía un voltaje de control (alrededor

de los 12v DC) para que el MIB ejecuta las funciones lógicas previamente programadas (habilitar, deshabilitar, etc.) sobre las cerraduras.

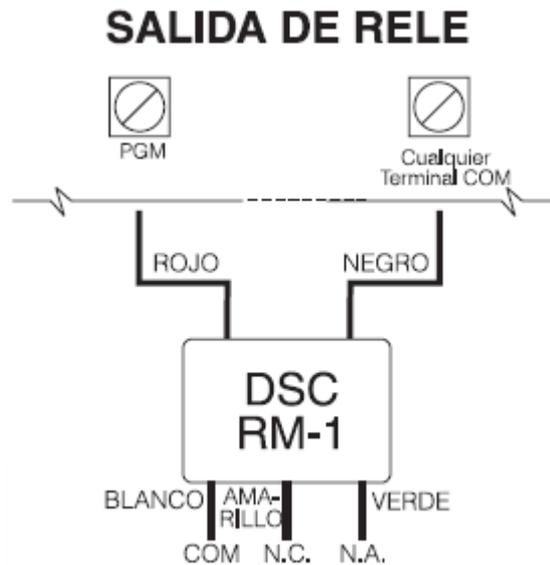


Fig. 23 Salida PGM

Fuente: DSC

## b) La interfase gráfica de usuario

Era indispensable contar con una pantalla gráfica que sirva como medio de comunicación para los operadores, como la interfase de la operativa diaria, esta labor le fue encomendada a la empresa INTERAMSA quien desarrollo el software de acuerdo a las especificaciones recibidas.

Este programa interactúa con el usuario, utilizando un conjunto de imágenes para representar la información y acciones disponibles en la interfaz. Se decidió por una matriz donde se encuentran la totalidad de sucursales a monitorear, donde cada rectángulo representa una sucursal, que muestra los detalles de cada una de ellas como por ejemplo, nombre, número de identificación y la hora.

Su principal uso, consiste en proporcionar un entorno visual sencillo al operador para permitir tomar las acciones correspondientes.



The image shows a software interface for registration. It features a blue background with three white input fields. The first field is labeled 'Cod. Agencia', the second 'Nombre de agencia (alfabetico)', and the third 'Cod. funcionario'. Below the first two fields are small icons: a black circle and a white circle with a black dot. To the right of the third field is a button labeled 'enter'.

Fig. 25 Ventana de registro de solicitudes  
Elaborado por el autor

### c) Integración del software de seguridad (DLS)

Para que las soluciones desarrolladas puedan trabajar coordinadamente se necesitaba la integración del software de gestión remota SDR con el sistema de alarmas principal a través del software de comunicación conocido como DLS.

En coordinación y asesoramiento con la marca DSC, INTERAMSA conjuntamente con un Ingeniero programador se analizó el programa Fuente: del software de seguridad para integrarlo a la interfaz gráfica de usuario SDR.

A través del software de seguridad de alarmas DLS y el sistema SDR se realiza una comunicación remota con el panel de alarmas ejecutando un comando de salida (mediante la salida PGM) que actúa sobre la interfaz de bloqueo MIB.

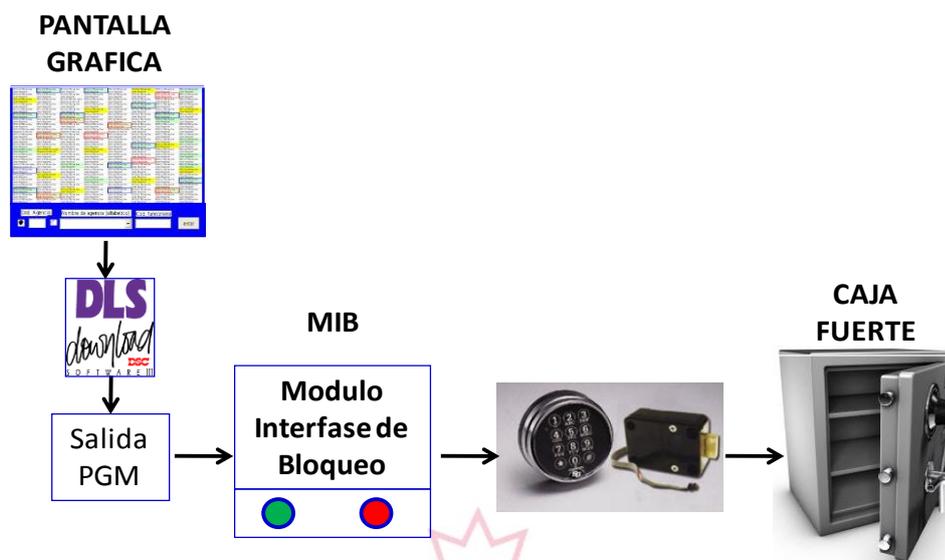


Fig. 26 Esquema final del proyecto

Elaborado por el autor.

### 3.16 Tecnologías utilizadas

El ingenio de la delincuencia para apropiarse de lo ajeno ha provocado que los fabricantes de sistemas de seguridad respondan a este problema con dispositivos grandemente mejorados en la detección, incluso con procesamiento digital de las señales, muchos detectores hoy en día son más eficaces, más confiables y menos costosos que antes.

Así también las plataformas de comunicaciones han mejorado grandemente, ya es una realidad la transmisión de señales de alarma vía una red LAN/WAN, manteniendo a la línea telefónica como un medio alternativo y teniendo a la red celular como una tercera alternativa de comunicación.

#### 3.16.1 La tecnología IP aplicada a la seguridad

Cuando se aplican las tecnologías de información y comunicación (TIC) al ámbito de la seguridad, esta mejora enormemente, este desarrollo tecnológico en las comunicaciones por IP y su

inclusión en los sistemas de seguridad ha posibilitado la apertura de un nuevo campo para la gestión remota de la seguridad y la máxima fiabilidad en todos los dispositivos.

La comunicación continua, mediante tecnología IP, de los dispositivos anti-intrusión de cualquier sucursal bancaria con la Central de Monitoreo, donde los operadores vigilan todos los sistemas, permite que la entidad bancaria se encuentre siempre protegida.

Con esta tecnología las desventajas de la línea telefónica convencional – corte de línea – desaparecen, dado que los sistemas de alarmas además monitorean el estatus de la línea telefónica, que solo es usada como medio alternativo de comunicación, quedando el cliente conectado al Central Receptora permanentemente y, en consecuencia, protegido.

### 3.16.2 Los sistemas de seguridad

Un sistema de seguridad electrónica consiste en la instalación de una serie de dispositivos electrónicos estratégicamente ubicados dentro del predio a proteger e interconectados hacia una Central Receptora localizada en un Centro de Control.

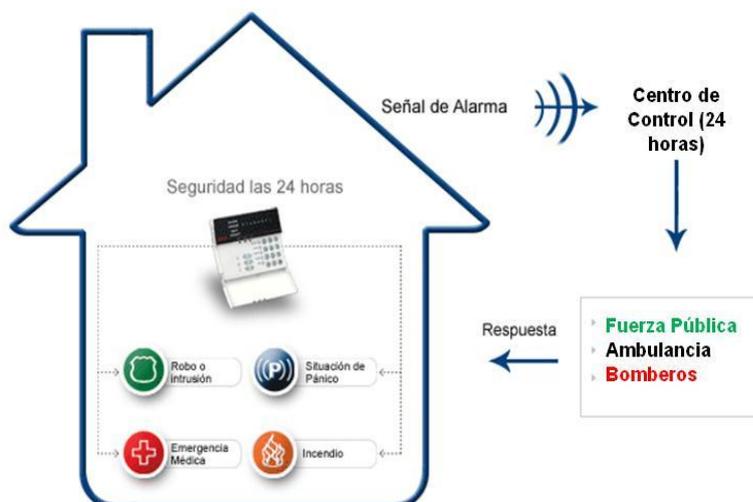


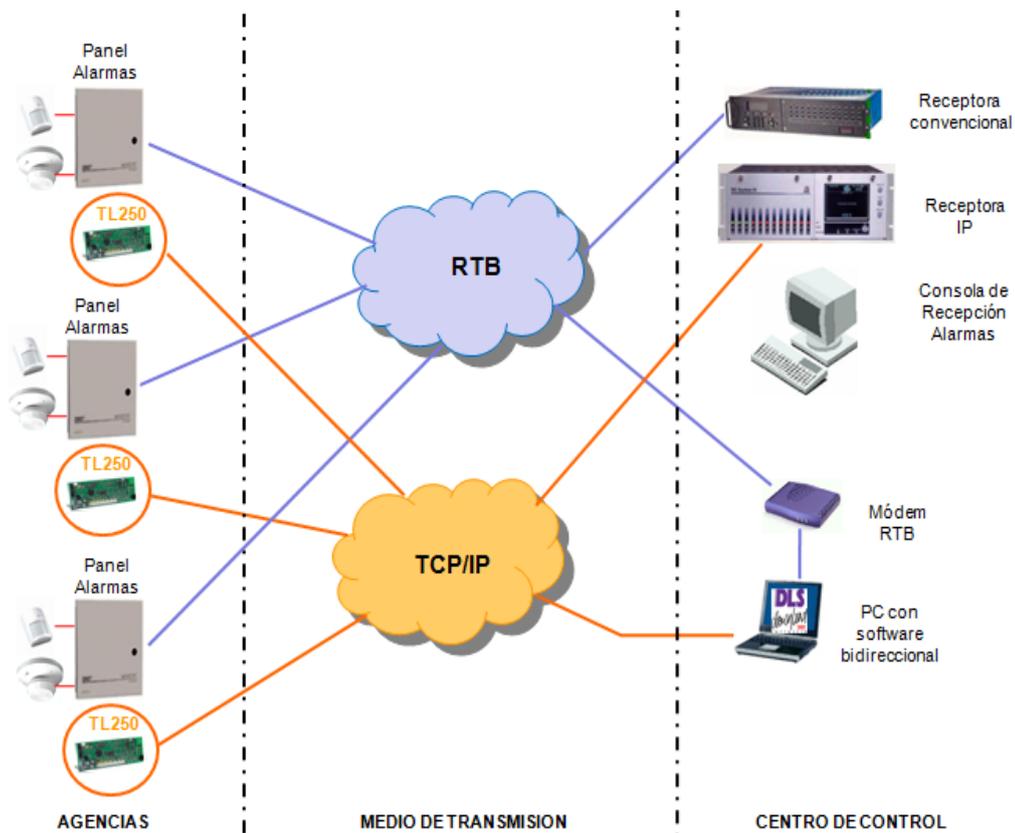
Fig. 27 El Sistema de Seguridad  
Adaptado por el autor (ADT)

Existen una gran variedad de dispositivos de protección electrónica y que son monitoreados durante las 24 horas del día, dentro de los cuales se tienen:

- Sensores de movimiento
- Sensores de impacto
- Sensores de aniego
- Sensores de vibración estructural
- Contactos magnéticos
- Detectores de temperatura
- Detectores de humo
- Botón de pánico
- Discriminadores de audio
- Barreras fotoeléctricas

a) **Arquitectura de un sistema de seguridad**

Los elementos que conforman en forma general los sistemas de seguridad, aunque físicamente se encuentran dispersos, están unidos de una manera lógica de tal manera que se proporciona la comunicación entre cualquier panel de control existente en cada lugar (Sucursal, local, etc.) y el Centro de Control donde se ubica la Central Receptora de alarmas.



LEYENDA	
Línea Telefónica	

Fig. 28 Arquitectura de un Sistema de Seguridad  
Elaborado por el autor

Los sistemas de seguridad se componen de:

- Dispositivos de protección
- Panel de Control
- Medio de Transmisión (Red TCP/IP, Línea Telefónica, etc.)
- Centro de Control (Central Receptora de alarmas, MODEM).

Los paneles de control hoy en día pueden automatizar procesos, como por ejemplo el control de encendido de luces, control de encendido de aire acondicionado o simplemente encender una luz de cortesía, con lo cual puede ahorrarle al usuario dinero y hacer las tareas manuales de un operador algo más fácil.

Usando las salidas programables (PGM) al instalar un panel de alarma llevará más allá al sistema de seguridad y lo convertirá en un sistema de seguridad y automatización.

El PGM es un terminal programable y será conectado a +12V cuando sea activa en función de las opciones de programación que han sido seleccionada. Este terminal puede suministrar un máximo de corriente de 50mA. Si la corriente necesaria es mayor que 50mA, deberá usarse un relé.

Otra de las particularidades de los paneles de control es que pueden determinar áreas o particiones que pueden ser manejadas independientemente por los usuarios, esto es útil cuando dentro de un mismo local se tiene un determinado ambiente el cual es bastante restringido y que debe ser controlado.

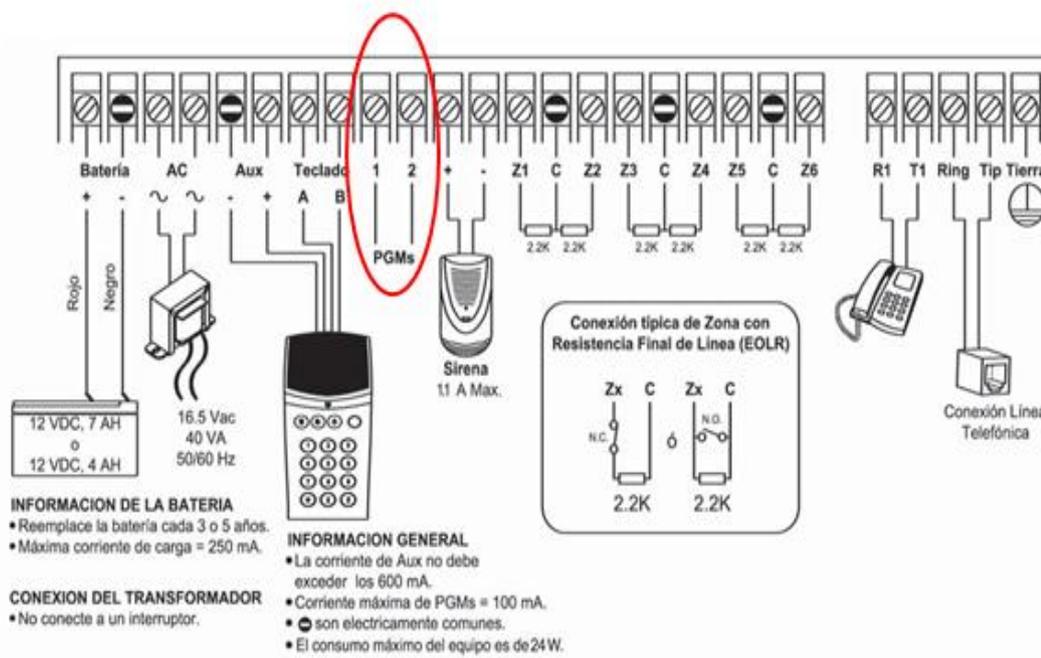


Fig. 29 Panel de control típico

Fuente: Alonso A2K4

## b) Software de seguridad (DLS)

El DLS es un paquete de software para la gestión remota de paneles de control, es una herramienta de diagnóstico muy versátil que incluye características tales como: Detección automática de tipo panel y la versión, asistente de actualización y comprobación de errores.

El DLS ayuda a simplificar las instalaciones, reduciendo los tiempos de programación y reducir las llamadas de servicio, a su vez permite tener la capacidad para realizar cambios en el sistema remotamente en cuestión de minutos, sin tener que visitar el predio.

El DLS resulta fácil de usar y ofrece a los usuarios la capacidad de ver y de cambiar los códigos, las tarjetas de acceso y los horarios, así como la capacidad de ver la condición del sistema, armar/desarmar particiones y ver, clasificar e imprimir la zona intermedia de eventos.

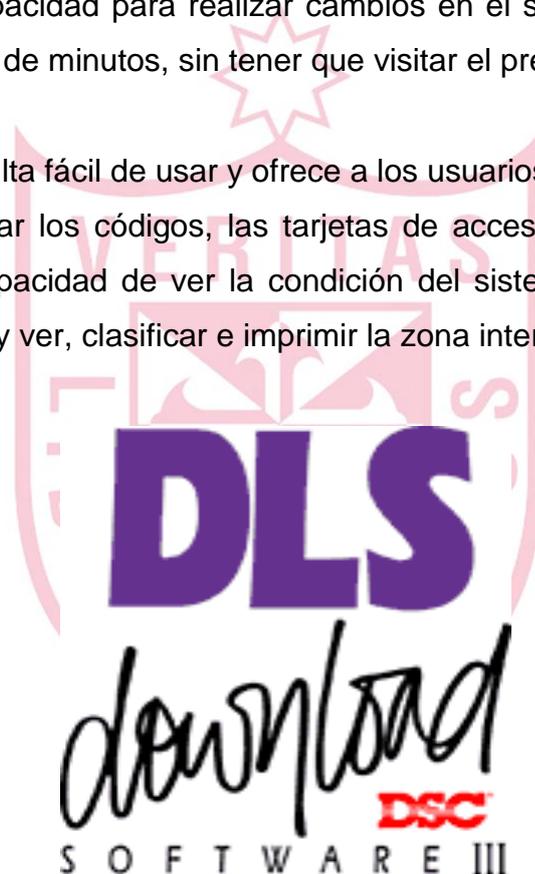


Fig. 30 Software de seguridad DLS

Fuente: DSC

Las pantallas de programación son de fácil entendimiento, con una breve explicación el operador estará en condiciones de realizar las programaciones básicas para poder realizar el primer intento de comunicación con el panel de alarmas y descargar el resto de campos que el personal técnico instalador haya realizado previamente.

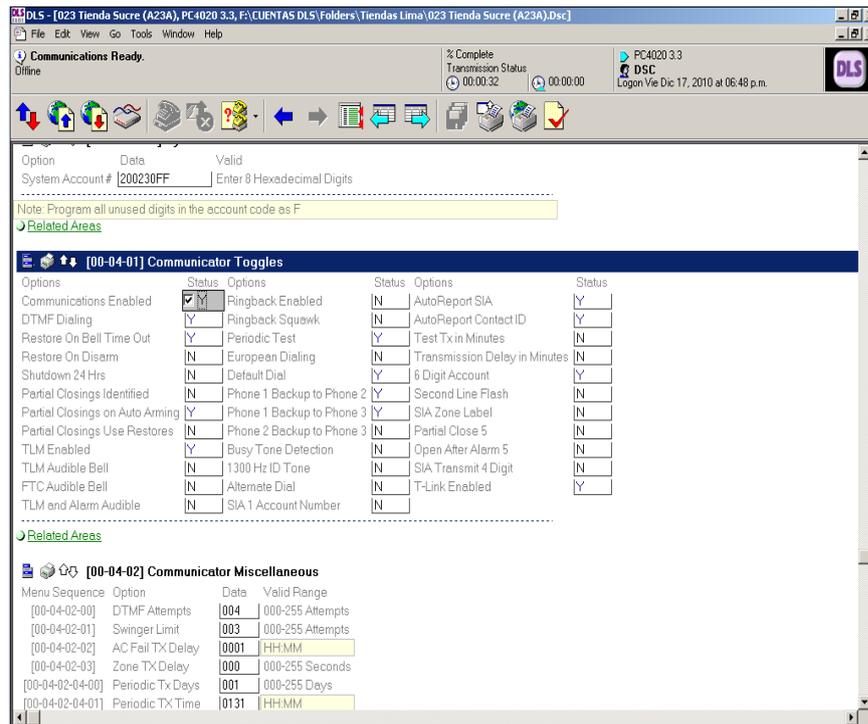


Fig. 31 Pantalla de programación del DLS

Fuente: DSC

El software de comunicación de DLS tiene las siguientes características:

- Interfaz de uso intuitivo
- Detección automática del tablero y de la versión
- Corrección automática de la versión del tablero
- Corrección automática de la versión del módulo
- Asistente de actualización
- Verificación de errores
- Programación en lotes

### 3.17 Medios de atesoramiento de efectivo

En estos tiempos actuales y a pesar de la diversidad del establecimiento de medios de pago electrónico, el dinero en efectivo sigue siendo muy común. Los sectores financiero, no financiero así como los de transporte de valores, venta al por menor y el sector del transporte, por mencionar algunos gestionan y procesan volúmenes considerables de monedas y billetes diariamente, los cuales siguen siendo el medio de pago más utilizado hoy en día para las transacciones monetarias.

Debido a que el efectivo es y seguirá siendo una parte importante de la economía, se necesitan sistemas y soluciones que ofrezcan, ante todo, seguridad. Una de las preocupaciones del sector financiero es la protección de objetos de valor frente a robos, es en ese sentido que las cajas fuertes (o las bóvedas) se han constituido en los elementos tradicionales de custodia.

#### a) **Bóvedas**

Las bóvedas son cámaras acorazadas que se construyen para la actividad de depósito, custodia, y tratamiento de monedas, billetes y valores, debiendo reunir las siguientes características:

- Delimitadas por una construcción de muros acorazados con materiales de alta resistencia (concreto armado) en paredes, piso y techo, con acceso a su interior a través de una puerta y mecanismos de cierre igualmente acorazados.
- La puerta de la cámara acorazada contará con un dispositivo de bloqueo y sistema de apertura retardada de al menos diez minutos.

- Idealmente debería estar circundado en todo el perímetro lateral por un pasillo de ronda con una anchura de 40 a 60 centímetros, pero se sabe que en la actualidad los espacios están siendo utilizados al máximo a favor del negocio financiero.

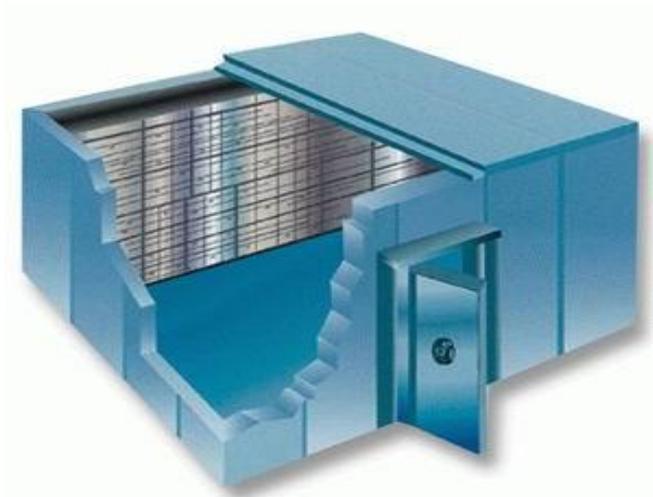


Fig. 32 Ambiente de bóveda

Fuente: LMP

## b) Cajas Fuertes

Las Cajas fuertes o también llamadas cajas de seguridad son uno de los servicios más rentables que ofrecen los bancos. El depósito no es seguro en sí mismo, sino que se almacena en una caja fuerte segura.

El concepto de cajas de seguridad y la invención de cerraduras es tan antiguo como la humanidad.

Una caja fuerte es un compartimento de seguridad que ha sido inventado para que su apertura sea muy difícil para personas no autorizadas y así poder guardar elementos de valor. Por lo general son fabricadas en un metal extremadamente duro, por lo que son muy pesadas y constan de un sistema de cierre que solo se puede abrir mediante claves secretas, y que estas claves pueden cambiarse para preservar más aún la seguridad.



Fig. 33 Caja Fuerte

Fuente: LMP

### c) Cerraduras de alta seguridad

Uno de los dispositivos de seguridad más comúnmente utilizados como medio de protección y seguridad son las cerraduras. Estos elementos de cierre basan su efectividad en su diseño, construcción y su instalación. Pero la característica más importante es el control que la entidad financiera debe ejercer sobre la posesión de las llaves (llaves de cerraduras y llaves de combinación) y claves, que viabilizan la apertura.

Estos dispositivos combinan las características de las cerraduras mecánicas clásicas con un medio electrónico para incrementar el nivel de protección de todo tipo de cajas fuertes y puertas de bóveda. Para su apertura admite la utilización de uno u otro o la combinación de ambas claves asignadas.

Las cerraduras digitales consisten en un motor eléctrico que acciona un pasador. Hay una batería que alimenta la energía del motor que acciona el pasador y esto se complementa con un chip que almacena en su memoria un número (clave) que permite el acceso.

Estas cerraduras brindan las siguientes prestaciones:

- Accionamiento motorizado
- Programación sencilla
- Penalidad por ingreso de clave errónea
- Memoria de eventos
- Retardo programable
- Emite señales de alarmas
- Indicador de posición de pestillo
- Posibilidad de conexión con otros sistemas de seguridad
- Memoria de eventos y operaciones realizadas
- Gestión centralizada local y/o remotamente
- Acceso a uso y programación por código, a los autorizados
- Incluir display indicador de estado y funciones.
- Supervisión continua del estado de la cerradura.

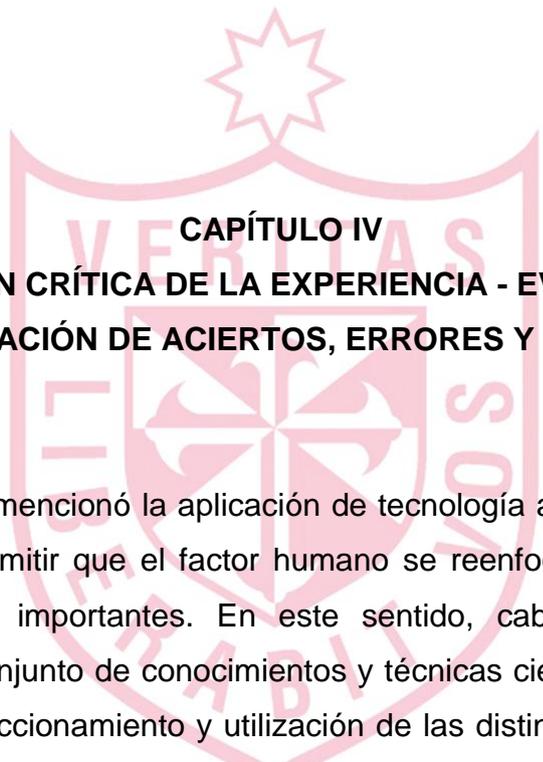
Las aplicaciones más corrientes son para acoplar en las cajas fuertes y puertas de bóveda utilizadas en la protección bancaria, joyerías, despachos de lotería y casinos, etc.



Fig. 34 Cerradura de alta seguridad  
Fuente: SARGENT & GREENLEAF

En el concepto de “proteger y resguardar los valores que se encuentran en su interior o bajo su resguardo” no ha cambiado con el transcurrir de los años, sus materiales de producción y normas de precisión sí, se han perfeccionado hasta transformarlos en mecanismos altamente seguros.

Otro de los aspectos que destacan a estos dispositivos de seguridad es que, provee la posibilidad de que posibilitan la interconexión a cualquier sistema de alarma. De esta manera, pueden ser monitoreadas a distancia por un Centro de Control para optimizar la seguridad y el resguardo de los valores que protegen.



**CAPÍTULO IV**  
**REFLEXIÓN CRÍTICA DE LA EXPERIENCIA - EVALUACIÓN**  
**Y DETERMINACIÓN DE ACIERTOS, ERRORES Y RESULTADOS**

Como ya se mencionó la aplicación de tecnología ayuda a automatizar procesos para permitir que el factor humano se reenfoque a otras labores que también son importantes. En este sentido, cabe recordar que la ingeniería es el conjunto de conocimientos y técnicas científicas aplicadas a la invención, perfeccionamiento y utilización de las distintas técnicas en sus diversos aspectos incluyendo la resolución u optimización de problemas que afectan directamente a los seres humanos en su actividad cotidiana.

Los ingenieros electrónicos por medio de las áreas tecnológicas como la computación, los sistemas de información, las telecomunicaciones, la automatización y control, serán capaces de manejar, adoptar, implementar y diseñar aplicaciones y servicios de hardware en diversas industrias y empresas, de esa forma, podrán formar parte activa en procesos de reingeniería y ocupar posiciones administrativas desde las que influirán en la toma de importantes decisiones. Se advierte que al momento de graduarse, los ingenieros electrónicos tienen un conocimiento fortalecido en todas las

áreas técnicas, sin embargo, este saber debe ser complementado con el dominio de áreas de gestión, que siempre serán necesarias para su desempeño eficiente, puesto que permiten la aplicación de los nuevos avances de la ciencia y la tecnología a la luz del enfoque económico, el mismo que hace viable la utilización de materiales, recursos humanos y capital dinerario de la manera más eficiente posible.

En este punto, es importante destacar que para el desarrollo de proyecto SDR, en cuestión, los cursos de especialidad que se requieren son: Dispositivos y Circuitos Electrónicos, Sistemas de Telecomunicaciones, Sistemas Digitales y Computadoras, y Máquinas Eléctricas. Estos cursos permiten entender los principios de funcionamiento de los sistemas electrónicos que se vayan encontrando durante la trayectoria profesional.

Asimismo, se corroboró que conocer los diversos sensores y sus aplicaciones permite poder adaptarlos y utilizarlos de acuerdo a las necesidades, y en esa secuencia de ideas, se identificó la necesidad de conocimiento específico de las siguientes áreas:

- Automatización y Control Industrial: Sensores
- Microprocesadores: Microelectrónica

Una de las mayores ventajas de los microcontroladores es la posibilidad de realizar modificaciones en el comportamiento del proyecto simplemente actualizando el software que ejecuta el microcontrolador y en pocos minutos se puede tener el nuevo proyecto funcionando.

#### **4.1 Aporte en el área de desarrollo predominante**

Trabajar en el sector financiero brinda la posibilidad de tener permanente contacto con la tecnología. Como es bien conocido, el sector financiero es uno de los que se encuentra en permanente competencia y esto lleva siempre a buscar mejorar sus procesos para ofrecer un mejor servicio a sus clientes.

La principal herramienta con la que cuenta el Ingeniero Electrónico es su creatividad y el dominio de la tecnología, esto ha permitido aportar con:

- a) Profesionalización:** Generalmente la gestión de tecnología (hablando de seguridad electrónica) en el sector financiero está en manos de personal con escasa o ninguna formación en tecnología (administradores, abogados, oficiales, etc.), quienes únicamente se limitan a comprar sistemas de seguridad a precios que se ajusten al presupuesto de la organización, sin tener en cuenta los parámetros técnicos, funcionalidades y condiciones de operación.

El Ingeniero Electrónico con su formación y conocimiento aporta profesionalización al sector de Seguridad Electrónica.

- b) Invención y desarrollo:** La ingeniería electrónica contribuye e incentiva la creatividad e innovación para adaptación, asimilación y desarrollo de la capacidad tecnológica. Este aporte es importante porque gracias a la creatividad e ingenio se desarrollan diferentes sistemas de control que satisfacen las necesidades del cliente interno.

- c) Inclusión y uso de tecnología:** Esto permite desarrollar sistemas con sus propios procesos y dinámicas, en el que las innovaciones son agentes de cambio. Dinámica que se expresa en nuevos o mejores productos o procesos, pero también en nuevas actividades humanas o formas diferentes o mejoradas de hacer las actividades ya establecidas.

El ingeniero electrónico es responsable de encontrar nuevas formas de aplicar la tecnología a fin de mejorar procesos, reducir costos y elevar los estándares de la seguridad electrónica.

## 4.2 La cadena de valor

La cadena de valor es una herramienta de gestión diseñada por Michael Porter que permite realizar un análisis interno de una empresa, a través de la disgregación en sus principales actividades generadoras de valor.



Fig. 35 La cadena de valor de seguridad

Elaborado por el autor

### 4.2.1 Actividades primarias

Para el departamento de seguridad las actividades que están directamente relacionadas con la gestión del área, son:

- Seguridad Física de Tiendas
- Seguridad Canales Electrónicos
- Seguridad Electrónica
- Investigación y Asuntos Especiales
- Mejora Continua

#### **4.2.2 Actividades de apoyo**

Así, dentro de las actividades que agregan valor al producto o servicio ofrecido por el área de seguridad y que sirven de apoyo a las actividades primarias se tiene:

- Gestión de solicitudes de videos
- Atenciones de primer nivel en canales electrónicos
- Verificación y cumplimientos de políticas y estándares de seguridad
- Alertas de seguridad

#### **4.3 Aportes y responsabilidades**

El entorno financiero permanentemente se está focalizando en la revisión de sus procesos con la intención de optimizar y/o realizar acciones de mejoras.

El haber traído en todo el ámbito de la seguridad financiera, estar permanentemente ligado a los procesos de Tiendas y como soporte tecnológico del área, permitió contar con un bagaje intelectual acumulado que determinó liderar la implementación del proyecto.

El carácter investigador del ingeniero hace que se adquieran nuevos conocimientos como las cerraduras de alta seguridad usadas en las cajas fuertes, analizar el mecanismo interno y su funcionamiento permite identificar elementos básicos y comunes como:

- Alimentación a través de baterías alcalinas de 9v,
- Solenoide interno que controla el pestillo de aseguramiento
- Circuito lógico que controla las funciones
- Memoria de almacenamiento de claves.

Así dentro de las principales aportaciones con las que este trabajo contribuye pueden resumirse de la siguiente forma:

- Se define un concepto novedoso acerca de la presencia electrónica en el proceso de manejo de efectivo dentro del entorno bancario. Este concepto ha sido definido con el nombre de Sistema de dualidad remota como una forma de valorar la utilización de tecnología en el desarrollado de las actividades financieras.
- Finalmente, se ha implementado la primera versión de una herramienta software que facilita la gestión remota de las cerraduras de las cajas fuertes, marcando una pauta dentro del entorno de seguridad que desean aplicar este sistema.

#### **4.4 Desarrollo profesional**

Al inicio de esta actividad profesional en el sector de la seguridad implicó un gran esfuerzo por la poca información disponible acerca de los sistemas electrónicos de seguridad, concepto que no se enseñaba en ese entonces dentro de alguna institución especializada.

La interacción con las empresas dedicadas al rubro de seguridad electrónica facilitó el acceso a información y conocimiento lo que permitió comprender los sistemas y su funcionamiento.

Un tema importante en la seguridad electrónica es la integración de los sistemas ya que adaptación a las necesidades de funcionalidad y ergonomía permiten alcanzar niveles de especialización tales que ameritan el expertise de personal capacitado y certificado en el diseño, estructuración e implementación de sistemas complejos y altamente tecnificados.

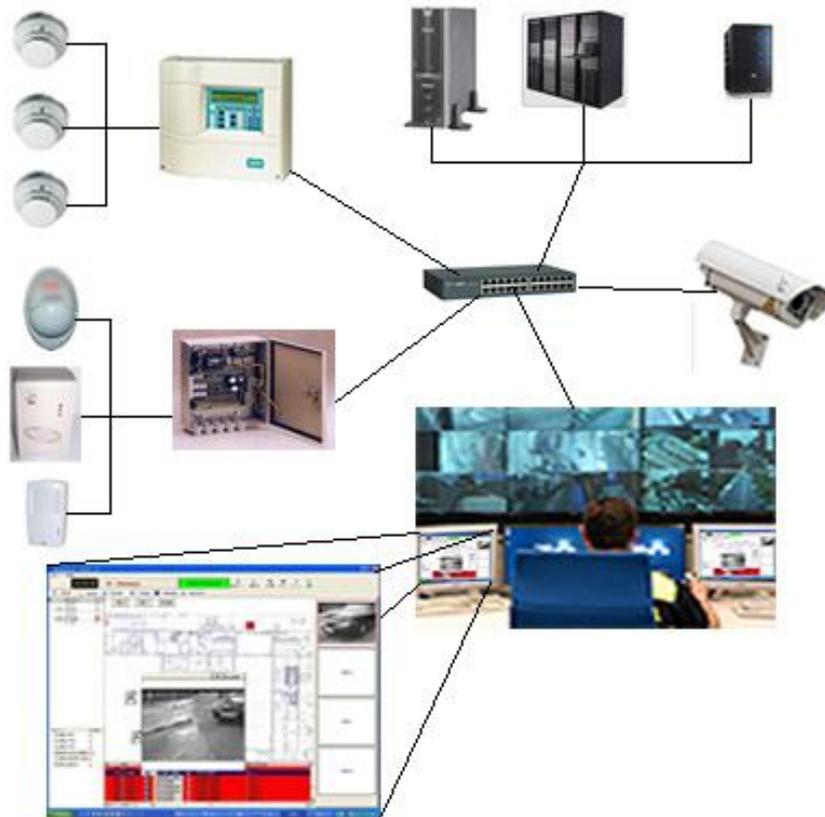


Fig. 36 La seguridad electrónica

Fuente: LESS

Los sistemas de seguridad electrónica se encuentran divididos en cuatro subsistemas:

- Sistemas anti Robo-Hurto
- Sistemas de Video (CCTV)
- Sistemas de detección de Incendio y
- Sistemas de Control de Acceso

Cada uno de estos sistemas se encuentran diseñados para cubrir diferentes necesidades de monitoreo, control y/o supervisión, pero con capacidad de ser interconectados e integrados en un único sistema multifuncional. La utilización de cada uno de ellos depende de las necesidades particulares de cada instalación o edificación, así como de los procedimientos operativos contemplados.

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

#### **4.5 Necesidades atendidas**

Ante la necesidad que tenía la División de Tiendas del Banco Interbank por encontrar una forma creativa de optimizar el proceso de apertura de los medios de atesoramiento de efectivo y enfocar el recurso humano al máximo en favor del negocio, la solución ofrecida por el área de seguridad conocida como Sistema de Dualidad Remota resulto más que útil para tal fin.

Al liberar más recurso humano en favor del negocio se contribuye a mejorar los ratios financieros del Banco.

#### **4.6 Metas alcanzadas**

Los aportes y mejoras realizadas a la institución han hecho que la imagen del Jefe de seguridad electrónica sea valorada y respetada por las diversas áreas con las que interactúa el área de seguridad, esto a su vez ha permitido ser parte de diversos comités internos de la División de Administración como consultor técnico y en la parte estratégica ser integrante del Plan de Continuidad del Negocio (PCN).

Dentro de las importantes mejoras en el área de seguridad se puede destacar:

- Migración de sistemas de alarmas de línea telefónica a IP
- Repotenciación de la seguridad electrónica en cajeros automáticos
- Desarrollo del sistema de bloqueo para ambientes de 24 horas.
- Desarrollo del prototipo de sistema antifraude para cajeros.

- Implementación del primer sistema de video digital para Tiendas.
- Elaboración de un estándar de zonificación de alarmas (no existente hasta ese entonces).

Las mejoras implementadas en el banco ayudaron a que en Marzo de 2008 se obtuviera el premio a la innovación otorgado por la Gerencia de Administración a la cual pertenece mi área.

En el transcurso de la trayectoria profesional no solo en el tema tecnológico, sino también en muchos casos asumir tareas inherentes a la seguridad, como las de realizar labores de reemplazo en el área de seguridad física, constituye un aprendizaje continuo que ha permitido lograr una especialización profesional en el ámbito de la seguridad financiera, sin embargo, esta no es aún muy difundida.

Además de combinar las labores operativas y de gestión, la dedicación de parte del tiempo a la enseñanza interna, ha hecho conseguir ser parte de la cultura del Banco, formando parte de la plana docente de la Universidad Corporativa de Interbank - UCIK, en el Curso de Seguridad Electrónica y Física.



Fig. 37 Universidad Corporativa Interbank

Fuente: Interbank

También se participa en el Programa de Especialización en Gestión de Seguridad Integral en INFES Consultores asociados en el curso de Tecnologías de Seguridad, como expositor.



Fig. 38 INFES Consultores Asociados

Fuente: INFES

La permanencia en Interbank por más de 10 años en el área de seguridad ha permitido estar en contacto con empresas del rubro de seguridad electrónica así como disponer de acceso a la información técnica especializada de los productos y tecnologías existentes y sobre todo conocer desde el interior el tema de la seguridad Financiera.

#### 4.7 Indicadores

Con el fin de gestionar adecuadamente y para determinar el éxito de la implementación física del proyecto SDR, se elaboró un indicador el cual mostraba el avance de la implementación.

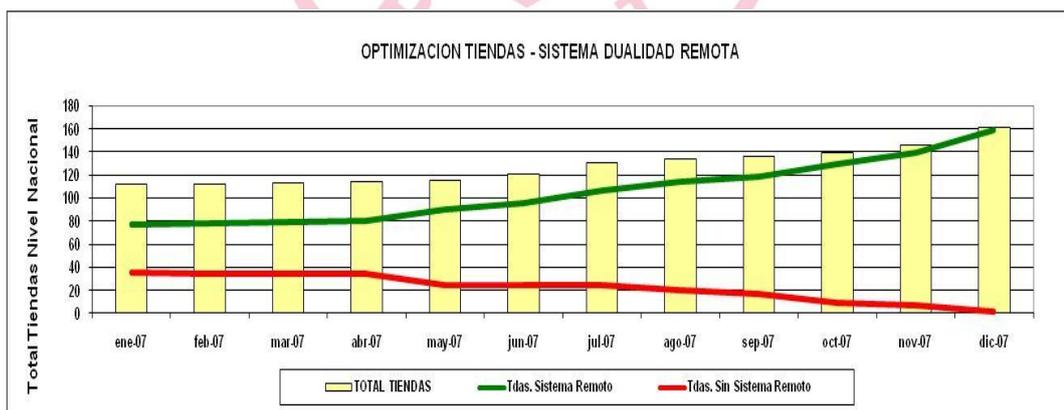


Fig. 39 Implementación del proyecto SDR

Elaborado por el autor

## CONCLUSIONES

Las cuatro conclusiones siguientes se refieren al desarrollo de un sistema para la gestión remota de cerraduras de alta seguridad aplicada a las bóvedas y cajas fuertes y constituyen un aporte importante en el manejo de efectivo en el sistema financiero.

1. Las cerraduras de alta seguridad actualmente utilizadas no están diseñadas para su conexión a la red de datos.
2. Actualmente los fabricantes de cerraduras están incursionando en el mundo IP desarrollando productos de gran flexibilidad y avanzada tecnología y acompañadas del software de gestión.
3. La implementación del sistema de dualidad remota contribuye a que el recurso humano se enfoque en la atención al público y la venta de productos financieros.
4. Es la primera vez que se realiza la integración del sistema de alarmas con un software (de desarrollo local) para el control de a distancia de cerraduras de cajas fuertes.

## RECOMENDACIONES

Después de analizar profundamente las conclusiones a las que se llegó en el presente desarrollo, se procedió a dar las siguientes tres recomendaciones.

1. Homologar el producto desarrollado dado que es una solución in house. Existen en el mercado productos que permiten una acción remota de cerraduras, pero estos no cubren la necesidad del proceso que requiere el Banco.
2. Desarrollar el software a modo multiusuario, esto permitiría que más de un operador pueda operar el sistema en las horas pico.
3. Actualizar el sistema de bloqueo MIB para incorporar mejores prestaciones como por ejemplo: reporte de máximo número de aperturas, indicador de retardo en proceso, bloqueo automático en caso de cortes de energía.



## FUENTES DE INFORMACIÓN

<http://www.dsc.com>

<http://www.sargentandgreenleaf.com/>

<http://www.kaba-mas.com/a.php?page=home>

<http://www.bancafacil.cl/bancafacil/servlet/Contenido?indice=1.0&idCategoria=2>

<http://home.howstuffworks.com/home-improvement/household-safety/security/combination-lock.htm>

[http://bvirtual.indecopi.gob.pe/wcircu/query.exe?cod\\_user=wwwcircu&key\\_user=wwwcircu&base=02&periodo=1&fmt=01&inireg=761&nreg=20&idioma=all&boolexp=REQUISITOS\\$\(76,77\)](http://bvirtual.indecopi.gob.pe/wcircu/query.exe?cod_user=wwwcircu&key_user=wwwcircu&base=02&periodo=1&fmt=01&inireg=761&nreg=20&idioma=all&boolexp=REQUISITOS$(76,77))

[http://www.sbs.gob.pe/0/modulos/JER/JER\\_Interna.aspx?ARE=0&PFL=0&JER=148](http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=148)

<http://www.andina.com.pe/espanol/Noticia.aspx?id=XtE6m6dnCYA=>

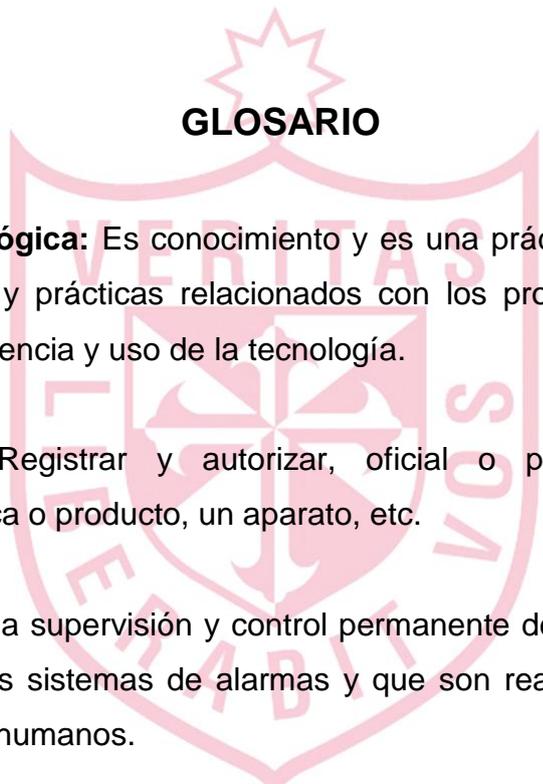
<http://www.interbank.com.pe/>

[http://www.dicscamec.gob.pe/Dispo\\_gen\\_seguridad.html](http://www.dicscamec.gob.pe/Dispo_gen_seguridad.html)

<http://www.seguridadasbanc.com/GOPortal/DesktopDefault.aspx?tabid=719>

[http://www.novenca.com/site/index.php?option=com\\_content&view=article&id=120&Itemid=93](http://www.novenca.com/site/index.php?option=com_content&view=article&id=120&Itemid=93)

<https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-1-definiciones>



## GLOSARIO

- 1. 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.
- 2. Homologar:** Registrar y autorizar, oficial o privadamente, una determinada técnica o producto, un aparato, etc.
- 3. 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.
- 4. Particiones:** Los sistemas de alarmas permiten dividir (o “Particionar”) el recinto a proteger en un máximo de áreas o particiones que se pueden armar o desarmar individualmente. Es recomendable para establecimientos con áreas restringidas, ambientes privados o con artículos valiosos.
- 5. 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.

El terminal PGM es programable, y se conecta a +12VDC cuando es activada durante el tiempo predeterminado por el instalador.

**6. RFs:** En Interbank los Representantes Financieros son responsables de asesorar a los clientes en sus operaciones con el banco. Se encargan de procesar sus transacciones, así como ofrecerles los productos y servicios, de acuerdo a su perfil y necesidades.

**7. 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 sensado de parámetros eléctricos, los riesgos para la vida y los bienes de las personas que allí residen, trabajan o atienden.

Estos sistemas tienen como objetivo detectar y avisar, por medio de señales de alarmas, a los responsables alguna irregularidad para que sean tomadas las debidas acciones. Es principalmente un sistema netamente preventivo.

**8. 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.

**9. TIC:** Tecnologías de Información y Comunicaciones, son tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de computadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información.

**ANEXOS**



## 1. Arquitectura de un panel de control

Un sistema de seguridad puede hacer un lugar mucho más seguro. Un panel de control es apenas un acoplamiento en la cadena de la seguridad, no elimina la necesidad de otras medidas de seguridad importantes. Un sistema de seguridad es un elemento de seguridad pasiva, esto significa que no evitan una intrusión, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles intrusos.

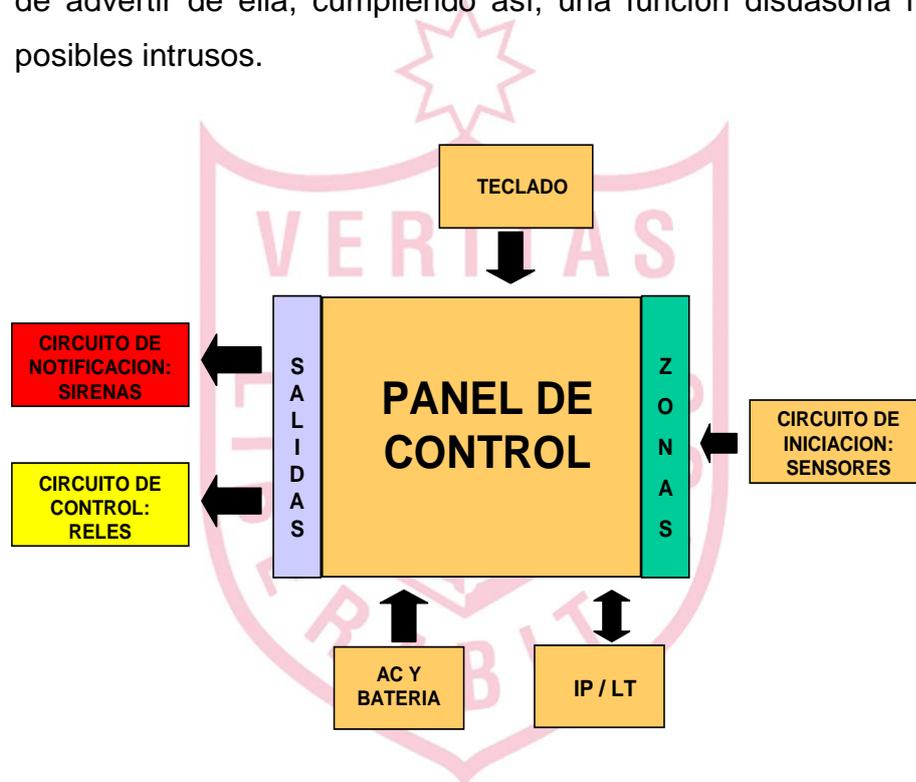


Fig. 40 Diagrama de bloques de un panel de control

Elaborado por el autor

La función principal de un panel de control es advertir el allanamiento en una vivienda o inmueble. Los paneles de control están conectados con una central de monitoreo, también llamada Central receptora, localizada principalmente en una estación central de monitoreo (Centro de Control) a través de la red corporativa (TCP/IP) o por medio de una línea telefónica cumpliendo una función disuasoria

activando un dispositivo sonoro como una sirena. Un sistema de seguridad básico consiste de por lo menos 5 componentes:

**a. Unidad de Control** es el "cerebro" del sistema llamado también panel de control, proporciona la energía adecuada al sistema y monitorea eléctricamente los circuitos. Posee los circuitos lógicos para recibir las señales de los dispositivos de iniciación de alarma y transmitirla a los dispositivos de notificación.

**b. Circuitos de iniciación**, conformado por sensores o "detectores" vienen en una variedad de formas y de tamaños, y se diseñan para detectar el sonido, calor del cuerpo, y otras condiciones que indican que un intruso está presente, existencia de una condición de alarma, o que el tiempo de permanencia esta excedido, etc.

**c. Circuitos de notificación**, permiten saber que se ha activado el sistema de seguridad. Los anunciadores más comunes son sirenas, campanas y luces.

**d. Fuente: de alimentación**, la que permite alimentar todos los dispositivos electrónicos como el panel de control, adicionalmente contar con un sistema alternativo de energía, como puede ser una batería cargada a través de la red eléctrica.

**e. Teclado**, es el elemento más fácil de identificar del sistema; este dispositivo se utiliza para configurar, activar o desactivar el sistema. A veces pueden tener botones con funciones especiales como: Emergencia Médica, Intrusión, Fuego, etc.

**f. Circuitos de control**, que a través de las salidas PGM's pueden controlar dispositivos electrónicos de contacto seco (relés) usados para el encendido y/o apagado de los circuitos de luces, de aire acondicionado, etc.

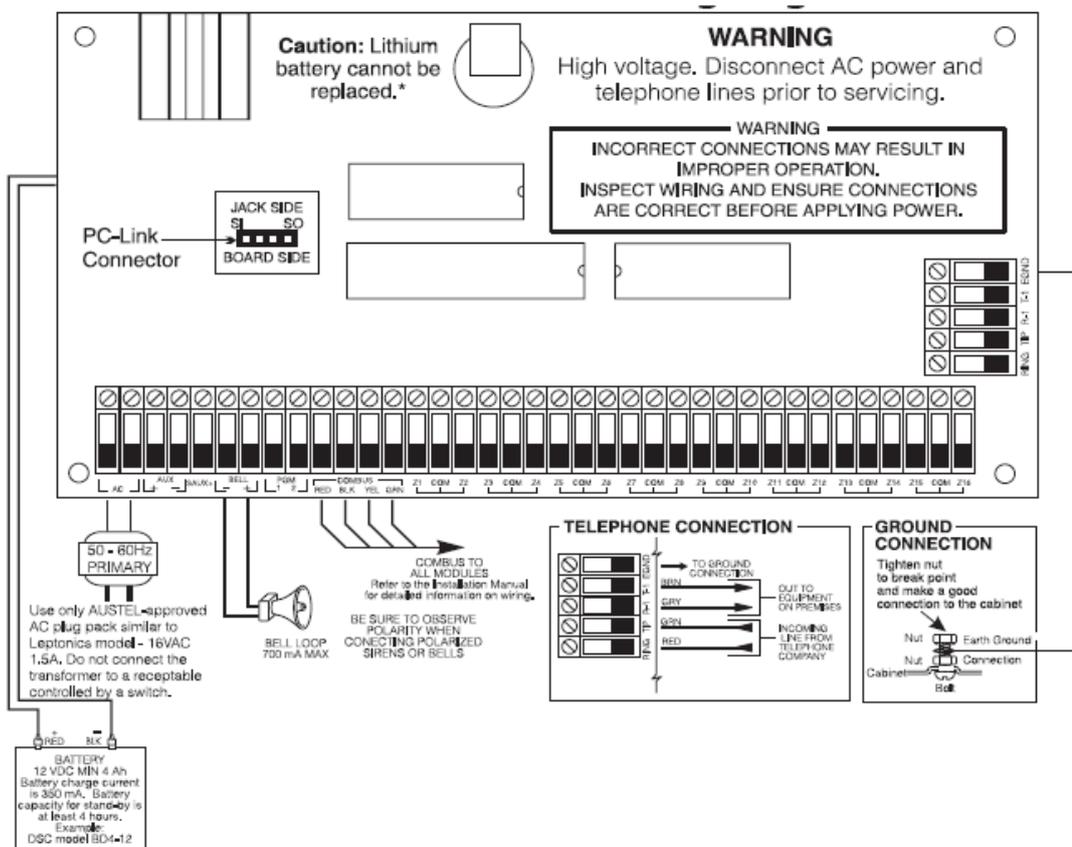


Fig. 41 Panel de control típico y esquemas de conexiones

Fuente: DSC

## Funcionamiento

Los circuitos de iniciación de alarma cuentan con opciones de contactos normalmente cerrados (se conectan en serie) y contactos normalmente abiertos (se conectan en paralelo) para la indicación de una alarma y mediante una resistencia denominada de fin de línea va conectada eléctricamente al panel de control a través de un área denominada "Zona", la cual proporciona la energía del lazo de iniciación, así cuando un sensor se activa pone en derivación la resistencia de fin de línea, esto provoca que aumente la corriente del circuito iniciando una condición de alarma al panel de control y este entonces responde según lo programado, lo cual significa

generalmente accionar los anunciadores y marcar a la central receptora de alarmas.

## 2. Módulo de interfase de bloqueo - MIB

El Modulo Interfase de Bloqueo - MIB es un desarrollo que posibilita la acción de Bloqueo/desbloqueo de una cerradura digital de caja fuerte y a su vez evalúa el estado de la posición de pestillo de esta cerradura.

Otra de las funciones de esta interfase:

- Control de tiempo excedido de caja fuerte abierta
- Bloqueo automático de cerradura
- Supervisión del estado de la cerradura (habilitado/deshabilitado)
- Anunciador sonoro (Buzzer)
- Indicadores visuales del estado del sistema

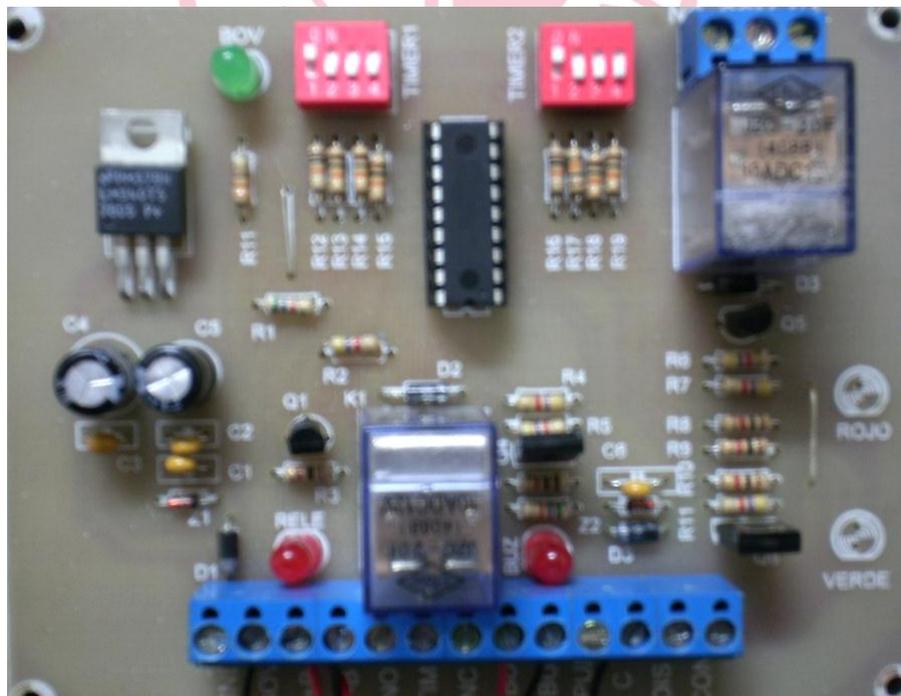


Fig. 42 Modulo de bloqueo MIB

Fuente: TECSEL

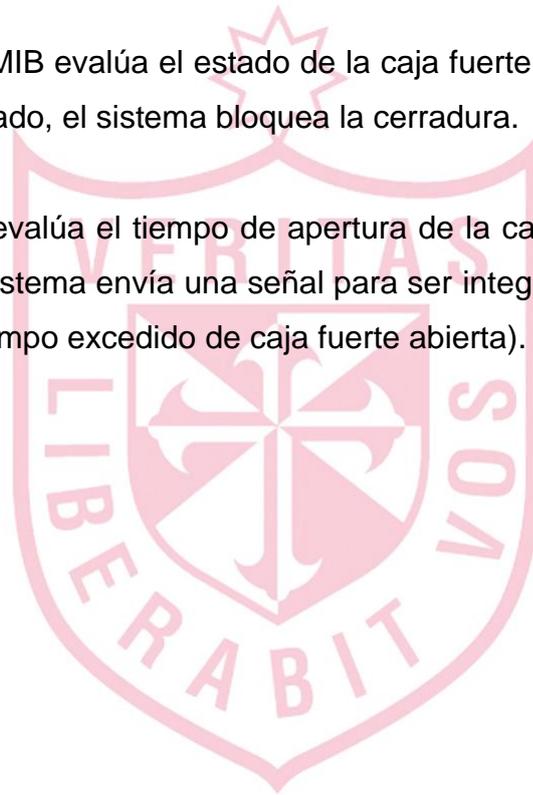
### **Funcionamiento**

Si la posición de pestillo indica la apertura física de la caja fuerte, el sistema bloquea la cerradura hasta el siguiente pulso.

Si la posición indica cerrado, el sistema se pone en modo espera de pulso, para una nueva apertura.

El sistema MIB evalúa el estado de la caja fuerte y si no es abierta en el tiempo fijado, el sistema bloquea la cerradura.

El sistema evalúa el tiempo de apertura de la caja fuerte y si este se excede el sistema envía una señal para ser integrada a un sistema de alarmas (tiempo excedido de caja fuerte abierta).



### 3. Cerraduras de alta seguridad

Las cerraduras SARGENT cuenta con múltiples códigos, un código de restablecimiento, y tiempo de retardo de hasta 99 minutos. Puede funcionar como control simple o control dual.



Fig. 43 Cerradura de alta seguridad  
Fuente: SARGENT AND GREENLEAF

Algunas características de las cerraduras de alta seguridad:

- Retardo de aperturas programable entre 1 y 99 minutos, para ofrecer protección a personas y bienes en caso de asalto.
- Programación de apertura o bloqueo horario semanal programable (168 horas), que imposibilite la apertura durante horas no hábiles, fines de semana, vacaciones o cualquier otra situación donde la institución permanezca cerrada.
- Pestillo con cierre automático.
- Al menos tres niveles de seguridad-Máster-Manager, Usuarios-8, por cada Manager.

- Control de feriados anual programable, 15 períodos de un máximo de 15 días por período.
- Bloqueo de los usuarios seleccionables, por niveles de Máster y Manager.

#### 4. Cuadro de costos

COSTOS TIENDAS MONEY						
TIPO	T TIENDAS	SW	6120	M.O	VIATICOS	SUB
TM	Lima 118	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 119	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 120	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 121	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 122	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 123	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 124	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 125	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 126	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 127	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 128	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 129	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 130	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 131	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 132	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 133	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 134	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 135	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 136	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 137	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 138	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 139	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 140	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 141	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 142	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 143	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 144	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 145	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 146	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 147	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 148	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 149	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 150	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 151	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 152	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 153	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 154	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 155	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 156	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 157	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 158	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 159	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 160	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 161	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 162	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 163	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 164	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
TM	Lima 165	\$8.73	\$130.00	\$40.00	\$0.00	\$178.73
					<b>SUB</b>	\$8,579.21
					<b>IGV</b>	\$1,544.26
					<b>TOTAL</b>	<b>\$10,123.47</b>

Fig. 44 Costos Tiendas Money

Elaborado por el autor





Fig. 46 Costos Tiendas Provincia  
Elaborado por el autor

**Costo total de la inversión**

<b>TIENDAS</b>	<b>COSTO</b>
TIENDAS LIMA	\$24,675.96
TIENDAS MONEY	\$10,123.47
TIENDAS PROVINCIA	\$24,825.96
<b>TOTAL</b>	<b>\$59,625.40</b>

Fig. 47 Resumen de Costos  
Elaborado por el autor

