CASO DE ÉXITO BANCO DE BOGOTÁ.

Objetivo General

Diseñar e implementar una serie de soluciones tecnológicas que eliminen o mitiguen las problemáticas que limitan la eficacia de los sistemas de seguridad existentes en las oficinas del Banco de Bogotá, que ocasionan ineficiencias y repercuten en costos operativos o financieros.

Objetivos Específicos

1. Analizar las problemáticas de los sistemas de seguridad existentes.

2. Identificar, diseñar e implementar los sistemas de seguridad con tecnologías que permitan realizar pruebas de concepto, bajo el marco de una actualización de los sistemas existentes o de una renovación tecnológica.

3. Evaluar los resultados de las pruebas de concepto de las nuevas tecnologías, en adaptarse a los protocolos de seguridad de la entidad y su eficacia en la eliminación y reducción de las problemáticas analizadas.

4. Incluir dentro de las soluciones de seguridad propuestas, la posibilidad de obtener datos que sean relevantes para mejorar la respuesta ante posibles eventualidades que expongan la seguridad y la administración de la operación bancaria.

Glosario

Analíticas y Gestión de Video (CCTV IP - IA): son plataformas que emplean las cámaras, equipos grabadores o servidores que centralizan el video o el conjunto de estos, para generar datos, métricas, alertas, identificación, entre otros tipos de información, sobre las personas y los comportamientos de estas dentro de la oficina.

Esta información se emplea para la gestión de la seguridad, administración de la operación, entre otros usos. Para nuestro caso empleamos TYCO

Audio doble vía: Es un sistema por medio del cual se puede interactuar desde la central de monitoreo (central de seguridad), con las personas que se encuentran en

alguna de las áreas del Banco, permitiendo conocer el estatus y responder algún tipo de situación que exponga la seguridad de la oficina. Para nuestro caso empleamos TYCO

Cerrajería Mecatrónica: elementos que tienen similitud en funcionamiento a la cerrajería convencional, pero que pueden almacenar información y transferirse datos entre ellos y con una plataforma de gestión, para controlar el acceso a diferentes lugares. Se componen de cilindros mecatrónicos y llaves inteligentes. Para nuestro caso empleamos ISEO

Control de Acceso (biometría): Los controles de acceso son sistemas que al parametrizaren (horarios, calendarios, tipos de usuario, áreas internas, entre otras), controlan el acceso a una infraestructura y sus diferentes áreas internas, asignando al personal privilegios y permisos de ingreso. Estos sistemas emplean dispositivos que son llamados lectoras, que realizan la función de autenticar la identidad de las personas que solicitan el acceso. La autenticación a través de biometría se realiza por algún tipo de rasgo propio de la persona (huellas, voz, rostro, y demás); proporcionando el mejor método de comprobación de seguridad, al comparase con otros, como los códigos numéricos o alfanuméricos, tags y tarjetas de identificación ya que son fácilmente transferibles. Los equipos empleamos para nuestro caso MORPHO - IDEMIA

Plataforma Integrada de Seguridad y Gestión Unificada: Es una metodología de operación, basada en hardware y software que permite gestionar la seguridad por medio de la integración de la información proporcionada por diferentes sistemas de seguridad (señales de alarma, datos, imágenes o videos entre otros), a través de tecnologías que sean abiertas, adaptables a los protocolos de seguridad de la entidad, escalables y perdurables en el tiempo. Para nuestro caso la fábrica PACOM.

Sistema de Alarma: Sistema que por medio de sensores custodia de forma electrónica un o varias áreas de un inmueble y al estar en estado de seguridad (armado) y activarse alguno de sus sensores envía señales de alerta informado la presencia de un intruso. Para nuestro caso la fábrica PACOM.

Sistemas Anti vandalismo: Los cambios ocurridos en las modalidades del accionar delictivo contra las entidades financieras ha generado la necesidad de una serie de complementos a los sistemas de seguridad actuales

- Barrera de niebla.
- Barrera de sonido.
- Barrea de luz.

Problemática a Resolver

Dentro de los análisis realizados para el planteamiento de nuestro proyecto Tomorrow Office para el Banco de Bogotá se identificaron, las siguientes problemáticas:

1. Existe un bajo control y administración de llaves codificadas de apertura de la oficina.
2. Existen costos asociados al mantenimiento por cambios de guardas de cerraduras codificadas por pérdida, robo de llaves, traslado o reemplazo de funcionarios.
3. Los tiempos en dar acceso al interior de la oficina a personal de emergencias, por situaciones que exponen la seguridad, dependen de la disponibilidad y los tiempos de respuesta de los funcionarios.
4. Las lectoras que permiten actualmente el acceso a áreas exclusivas para funcionarios, no garantizan que la persona que solicita el acceso, sea un funcionario, ni tienen la capacidad de identificarlo, adicionalmente no proporciona un registro que se pueda consultar o transferir para ser almacenado.
5. Los elementos actuales para el cumplimiento de los protocolos de seguridad por parte de los funcionarios se encuentran al borde de la obsolescencia tecnológica.
6. Los procedimientos y/o sistemas actuales con los que cuenta la oficina no permiten un control de las variables de consumo energético.
7. La entidad no cuenta con elementos o sistemas que permitan proporcionar un mayor retardo frente a las nuevas modalidades del accionar delictivo generado por los estallidos sociales.
8. Los sistemas de seguridad actuales no son compatibles con los elementos de disuasión activa, que permita tomar acciones que mitiguen las nuevas modalidades del accionar delictivo.
9. los comunicadores que transmiten las señales de alarma de los sistemas de seguridad a través de internet no son nativos y presentan intermitencia en la comunicación.
10. La respuesta a novedades de seguridad reportada por los paneles de alarma no Integra de forma automática los sistemas de video vigilancia.
11. Los sistemas de video vigilancia actuales no permiten generar alertas preventivas ante situaciones que expongan la seguridad de la oficina.

12. Los sistemas de video vigilancia no proporcionan datos que permitan realizar un análisis de la operación bancaria y el desarrollo de la atención a clientes.

Investigación.

Al definir las necesidades de seguridad, control y administración necesarios, se aplicó una metodología de análisis de riesgos basados en la norma ISO 31000, a la búsqueda de equipos y/o sistemas de seguridad que ofrecieran la solución a estas situaciones descritas como problemáticas, encontrando varias fábricas.

Establecidos los marcos de evaluación para las tecnologías de las fábricas seleccionadas; inicialmente se analizaron bajo los aspectos de cumplimiento de protocolos de seguridad ya implementados por la entidad y la compatibilidad con la tecnología de seguridad existente. El resultado del análisis en la etapa de evaluación técnica y operativa, identificó que las tecnologías de seguridad existentes no pueden ser actualizadas para acoplar nuevos equipos que ejecuten las funcionalidades que eliminan o mitigan las problemáticas encontradas. Por tal motivo, se decidió continuar la búsqueda de tecnologías retomando un enfoque de renovación del binomio hardware – software o Panel de Alarma – Software de Monitoreo, y que permitieran integración con los sistemas de video durante la aplicación de los protocolos de respuesta ante la activación de los sistemas de alarmas (detección de intrusos).

El segundo marco de búsqueda contempla la capacidad de una plataforma tecnológica diseñada para el monitoreo de señales de alarmas de diferentes puntos o múltiples sitios, planteando una integración con los sistemas de video existentes.

Se encontró la tecnología que cumple con el marco de evaluación; adicional a los requerimientos, presenta una metodología más eficiente de efectuar el monitoreo de alarmas, el cual es mediante un sistema gráfico de atención de eventos, el

hardware cuenta con funcionalidades para efectuar el rol de sistema de alarma y control de acceso, un comunicador ethernet embebido (en la misma tarjeta) con redundancia, y permite programar rutinas, que de forma autónoma responden a diferentes eventualidades que controlarían la aplicación de los protocolos de seguridad que deben ejecutar los funcionarios durante sus actividades.

Análisis con el cual se concluye las tecnologías que se presentan e instalan

Una vez superada la evaluación técnico – operativa, se analizó la aplicación de la tecnología frente a las problemáticas y se evaluaron sus resultados, los cuales se describen a continuación.

Cerrajería Mecatrónica

Se realizó a instalación de la tecnología de cerradura mecatrónica en 3 puertas de la oficina centro comercial Nuestro Bogotá del Banco de Bogotá, estas puertas fueron, la puerta de ingreso a la oficina, puerta de ingreso al área de la caja fuerte que contiene el dinero en efectivo con otros documentos de valor, y puerta de ingreso al cuarto técnico en el que se encuentran los tableros de control eléctricos, el rack de comunicaciones y los sistemas de seguridad (detección de intrusos y video)

Cilindro Mecatrónico

Llave Inteligente

Puerta Ingreso Oficina

Puerta Ingreso área de caja fuerte

Puerta Cuarto Técnico

Los funcionarios, realizaban la solicitud de permisos ante el sistema generando un registro de quien, hora y fecha de la apertura de alguna de estas puertas, lo que proporciona un control de sus actividades.

En los casos en que un funcionario con llave inteligente no asistía a la oficina, el otro funcionario podía solicitar que los permisos le fueran transferidos temporalmente, evitando un impacto negativo en la operación bancaria.

Se simplificó el uso de llaves pasando de un aproximado de 10 llaves a solo 2.

Se comprobó la pérdida de acceso al deshabilitar una de las llaves evidenciando una administración total de este insumo de seguridad, evitando el cambio de guardas de cerraduras codificadas.

Control de Acceso (biometría)

Se implementaron lectores biométricos dactilares para las puertas de acceso exclusivo a funcionarios, los Lectores son administrados, sus registros almacenados y transferidos desde el sistema de alarmas a una base de datos implementada para la prueba de concepto.

Los registros obtenidos permiten identificar a las personas que realizan la autenticación y se pudieron parametrizar horarios, calendarios y privilegios a los usuarios del sistema, de esta forma tener un control de acceso según los protocolos de seguridad establecidos por la entidad.

Plataforma Integrada de Seguridad y Gestión Unificada:

Se consideraron los objetivos estratégicos establecidos por la entidad para determinar el modelo de seguridad a implementar y en función de estos y las limitaciones encontradas se diseñó, implementó y evaluó la capacidad de los equipos y el software ofrecido por la fábrica PACOM, obteniendo los siguientes resultados:

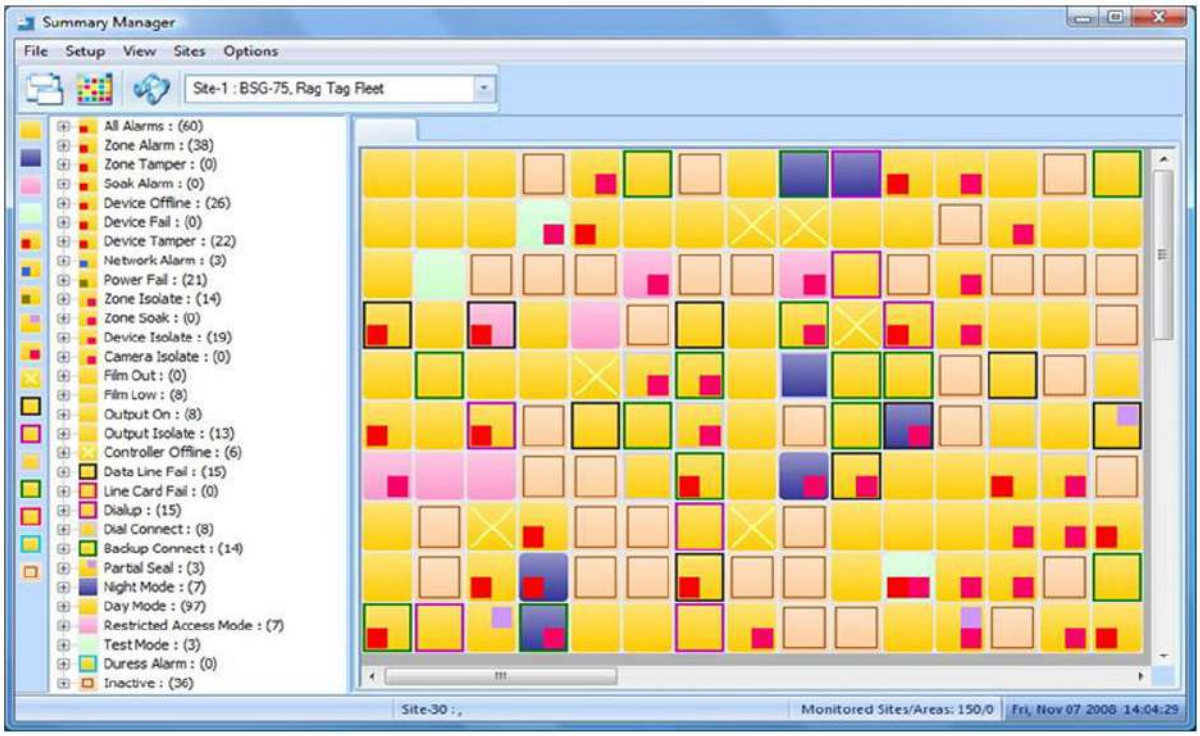
1. Reemplazar las diferentes tarjetas que efectúan los controles sobre el cumplimiento de los protocolos de seguridad, frente a las actividades de la operación bancaria. Adicionalmente proporcionando herramientas de seguimiento, alerta y adaptación a posibles cambios requeridos en los protocolos de seguridad y minimizó los posibles puntos de falla, reduciendo los costos por visitas de mantenimiento.
2. Permitió el control de una variable de consumo eléctrico, iluminación, y se confirmó la capacidad de controlar otros sistemas como aire acondicionado.

3. Permitió el control de equipos de disuasión activa como barreras de niebla, barreras de sonido entre otros.

Barrera de Niebla

Barrera de Sonido

4. La implementación permitió la comunicación por red desde la tarjeta principal, enviando la información de todas las transacciones o



eventualidades ocurridas en la oficina (transacciones de control de acceso, aperturas de puertas, registro de funcionarios, control de iluminación, señales de alarma y activación de sistemas de bloqueo por conductas de funcionarios que incumplían los protocolos de seguridad, entre otras).

5. Las eventualidades enviadas fueron reportadas en línea a un software de ambiente gráfico de atención de alarma, en la que se cargó la imagen en 3D de las instalaciones custodiadas electrónicamente.

6. Mediante los dispositivos de video instalados, se alcanzaron los objetivos al extraer información relevante de las imágenes, las analíticas permitieron detectar comportamientos sospechosos, objetos olvidados, entre otros. De manera tal, que generan alertas de forma preventiva al personal de seguridad. Bajo el mismo concepto de análisis de video, se obtuvo información sobre la cantidad de personas en la oficina y otras métricas relevantes sobre la atención prestada por la sucursal y que son de interés para el CORE del negocio.

Por qué es un caso de Éxito

Se considera un caso de éxito la implementación de estas tecnologías, porque se logró demostrar su funcionalidad y adaptación a la operación bancaría, brindado mayores controles y minimizando con mayor eficacia los riesgos de seguridad que en este momento no son atendidos eficientemente. De forma paralela involucra los sistemas de seguridad con inteligencia de negocios, posibilitando determinar cantidad de personas en la oficina, sus movimientos, establecer su tiempo de permanencia antes de ser atendidas, logrando un control administrativo a múltiples niveles. De esta forma la inversión en seguridad es multidimensional obteniendo de ella mayores beneficios.

Sumado a lo anterior, la perdurabilidad de las tecnologías instaladas, sus acuerdos de soporte técnico y garantía, además de las metodologías de atención de fallas, integración con otros sistemas como los de video, transaccionalidad (ATM), audio doble vía, entre otros; generan una reducción apreciable en los costos de mantenimiento, ampliación, u otras adaptaciones requeridas en un futuro.

Se alcanzó mediante la estructuración de este modelo, una filosofía corporativa de la seguridad, enmarcada dentro de un concepto innovador, agradable al usuario, y rentable a largo tiempo.