UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado**:**

"Diseño e Implementación de una arquitectura de comunicaciones seguras de radio y celular para una empresa confidencial basada en el estándar ISO 27000"

Realizado por:

IVAN VINICIO FREIRE VIERA

Director del proyecto:

ING. JUAN GRIJALVA

Como requisito para la obtención del título de:

INGENIERO EN REDES DE LA INFORMACIÓN Y TELECOMUNICACIONES

Quito, Julio del 2014

DECLARACION JURAMENTADA

Yo, IVÁN VINICIO FREIRE VIERA, con cédula de identidad # 050248631-9, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Iván Vinicio Freire Viera

C.C.: 050248631-9

DECLARATORIA

El presente trabajo de investigación titulado:

"DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE COMUNICACIONES SEGURAS DE RADIO Y CELULAR PARA UNA EMPRESA CONFIDENCIAL BASADA EN EL ESTÁNDAR ISO 27000"

Realizado por:

IVAN VINICIO FREIRE VIERA

como requisito para la obtención del Título de:

INGENIERO DE SISTEMAS EN INFORMÁTICA Y REDES DE LA INFORMACIÓN

Ha sido dirigido por el profesor

ING. JUAN SEBASTIÁN GRIJALVA

quien considera que constituye un trabajo original de su autor

ING. JUAN SEBASTIÁN GRIJALVA

DIRECTOR

PROFESOR INFORMANTE

ING. VERÓNICA RODRIGUEZ, MBA

Después de revisar el trabajo presentado,

lo he calificado como apto para su defensa oral ante

el tribunal examinador

Ing. Verónica Rodríguez, MBA

Quito, 30 de junio de 2015

DEDICATORIA

.

Dedico el presente trabajo de investigación a mis padres y mi familia quienes son pilar fundamental en el desarrollo de mi vida.

A cada persona que de una u otra manera colaboró para que este trabajo sea una realidad.

AGRADECIMIENTO

Al profesor Juan Grijalva por su acertada dirección de la tesis. Su profesionalismo y entrega fueron determinantes a la hora de conformar este documento.

A la profesora Verónica Rodríguez, quienes con sus lecturas aportaron una visión diferente e integradora de mi investigación.

A la Universidad Internacional SEK,

Índice General de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

En la actualidad las comunicaciones son primordiales para todo modelo de negocio, permiten acortar distancias y tiempo, por lo cual la información que se transmite se convierte en el activo más importante de cada empresa, más aún si esta se dedica al transporte de valores, la cual lleva a cabo sus operaciones con todas los tipos de comunicaciones disponibles como son radio y celulares incluyendo rastreo GPS para geolocalización del automotor. En meses anteriores se suscitaron varios robos de vehículos blindadados con altos indicios de intercepción de sus comunicaciones. Esta es la premisa y punto de partida del presente trabajo de investigación, en el cual el autor planteó como objetivo el diseño de una arquitectura de comunicaciones seguras, la cual está fundamentada en la norma ISO/IEC 27002:2005, en su dominio Gestión de las Comunicaciones y Operaciones. Específicamente se describió el estado actual de las empresas de transporte de valores en su sección de comunicaciones, analizar la seguridad en las transmisiones de radiofrecuencia y telefonía móvil utilizando un equipo de intercepción para finalmente sugerir controles que le permitan a las empresas de transporte de valores mitigar el riesgo operativo. Este último punto se desarrolló con la redacción de una política de comunicaciones en la cual se demostró que con normas y software se puede prevenir la intercepción de la información sensible de una empresa de trasporte de valores. Para el estudio se inició con un flujo de procesos describiendo la metodología de un transporte de valores del punto A o un punto B, enfatizando en a las comunicaciones que cada proceso utiliza. El complemento de este estudio previo y posterior fue análisis de riesgos que permitió tener una visión clara del estado actual de las comunicaciones tanto de radio y celular y el riesgo residual posterior a la aplicación de las políticas planteadas. A continuación se realizó una práctica de intercepción en la cual se encontró debilidades en una comunicación de radio al interceptar la misma con un escáner de frecuencias, para mitigar este riesgo se aplicó criptografía simple al mensaje que se transmitió y se evidenció que funciona al demostrar que el interceptor no supo el verdadero mensaje que se ocultó. Para finalizar se implementó lo desarrollado en una empresa de transporte de valores, evidenciando su situación actual de las comunicaciones vía radio, los procesos y riesgos iniciales, para posteriormente se aplicar la política desarrollada, con recomendaciones y soluciones a los problemas encontrados, y concluye con el informe del riesgo residual que permite posteriores actualizaciones a la solución planteada.

Palabras claves: Comunicaciones inalámbricas, dispositivo, seguridad, análisis, política, estándar

Abstract

Currently communications are essential for all business model, allow to shorten distances and time, which transmits the information becomes the most important asset of any company, even if it is dedicated to the transport of values, which conducts its operations with all types of communications are available as radio and cellular including GPS tracking for automotive. In previous months to several indications armored robberies with high percentage interception of their communications. This is the premise and starting point of this research, which settled the objective design of a communications architecture based on the points associated with the standard ISO / IEC 27002: 2005 in the domain of communications and operations management. Specifically the current state of the transport companies in the securities described communications section, analyze safety and radio frequency transmissions using a mobile phone interception equipment to finally suggest controls that allow transport companies mitigate securities operational risk. This latter point was developed with the drafting of a communications policy which showed that standards and software can prevent interception of sensitive information in a transport company securities. For the study began with a process flow describing the methodology of a transport of valuables from point A or point B, communications emphasizing that each process uses. The complement of this study was to pre- and post-risk analysis that allowed a clear view of the current state of both radio communications and cellular and subsequent residual risk to the implementation of the policies proposed. Following a practice interception in which weaknesses found in radio communication by intercepting it with a frequency scanner to mitigate this risk was made simpler cryptography applied to the message being conveyed and evidenced that works to prove that the interceptor did not know the true message was hidden. Finally we implemented all it developed into an enterprise x dedicated to the transport of values and their present status of their communications, processes and initial risks, as well as the implementation of the policy developed with recommendations for solutions to the problems encountered was evident and the presentation of the residual risk allowing subsequent updates to the proposed solution.

Keywords: Wireless, device, security analysis, policy, standard

CAPÍTULO I

INTRODUCCIÓN

Proteger la información valiosa y sensible en una sociedad tecnológica, es una prioridad dado que cada vez la tecnología forma parte de las actividades tanto personales como empresariales. El desconocimiento de las vulnerabilidades del manejo de la información, afecta directamente a la rentabilidad y ocasiona disminución en las actividades comerciales como otros tipos de fraudes en el ámbito personal.

Bajo esta premisa, toda persona o empresa debe tomar las debidas consideraciones en el manejo seguro de sus datos, previniendo un futuro o pérdida de información con métodos actualizados de protección, manejo seguro de comunicaciones y respaldo de información.

En el Ecuador, la explotación de las vulnerabilidades de seguridad por parte de los delincuentes ha evolucionado con la elección de objetivos puntuales como vehículos blindados que transportan valores de un punto a otro generando pérdidas millonarias, como lo informan varios reportes de seguridad e incidentes de las empresas de transporte de valores y aseguradoras que las cubren.

Estos ataques se describen como emboscadas, con conocimiento de la localización y de rutas de recorrido por el automotor, utilizando sistemas de intercepción de comunicación móvil afectando a los dispositivos celulares del personal de seguridad, identificando la ubicación de los automotores que transportan valores y consumando el robo.

1.1 EL PROBLEMA DE INVESTIGACIÓN

1.1.1 Planteamiento del Problema

En el año 2014 se suscitaron varios robos a vehículos blindados según lo reportaron las entidades policiales y el Ministerio del Interior, los estudios forenses de dichos atentados han revelado que algunos de ellos se han producido debido a la intercepción en las comunicaciones y sistemas de geo posicionamiento de los mismos.

1.1.2 Objetivos

1.1.2.1 Objetivo General

Diseñar una arquitectura de comunicación segura, basada en los puntos asociados al dominio 10 Gestión de comunicaciones y operaciones, del estándar ISO/IEC 27002:2005.

1.1.2.2 Objetivos Específicos

- Describir el estado actual de las comunicaciones de las empresas de transporte de valores en la ciudad de Quito.

- Analizar la seguridad en las transmisiones de radiofrecuencia, utilizando un equipo de intercepción contando con los debidos permisos a nivel legal.

- Sugerir controles que permitan mitigar el riesgo operativo previniendo la intercepción de información sensible en las empresas de transporte de valores.

1.1.3 Justificación

El estándar ISO/IEC 27002:2005, en su dominio 10, Gestión de comunicaciones y operaciones está compuesto por un conjunto de normas para la gestión informática. Al aplicar éstas recomendaciones, las empresas podrán garantizar la fiabilidad de sus operaciones internas.

El presente proyecto tiene como meta principal, el desarrollo de una arquitectura de comunicaciones seguras, con el desarrollo de una o varias políticas de seguridad basadas en el estándar ISO/IEC 27002:2005, en su dominio Gestión de comunicaciones y operaciones, para evitar la intercepción de información sensible de las empresas de transporte de valores.

1.2 MARCO TEÓRICO

1.2.1 Estado actual de conocimiento sobre el tema

1.2.1.1 Comunicaciones Móviles

Las comunicaciones móviles se producen cuando el emisor o el receptor están en movimiento. La movilidad de estos dos elementos que se encuentran en los extremos de la comunicación hace que no sea factible la utilización de hilos (cables) para realizar la comunicación en dichos extremos. Por lo tanto utilizan básicamente la comunicación vía radio. (Nichols & Lekkas, 2003)

1.2.1.2 Redes celulares y tecnologías portadoras

El término *celular* se utiliza ampliamente para describir a los dispositivos de comunicación inalámbrica. Una celda se define como un área o zona geográfica que rodea a un transmisor en un sistema telefónico. Gracias a este esquema y a la tecnología celular de conmutación subyacente, millones de usuarios móviles pueden mantener conversaciones desde una celda a otra. (Nichols & Lekkas, 2003)

El diseño basado en celdas permite reutilizar cada frecuencia que no sean adyacentes, a medida que se reduce el tamaño de las mismas, las ventajas del reciclaje de frecuencias se incrementan significativamente. (Nichols & Lekkas, 2003)

Tabla 1. Tipos de Celdas
Autor: Iván Freire

Tipos de celdas	Número de canales	Conversaciones simultáneas	Cobertura
Macro celdas	12	7	Aproximadamente 15 kilómetros
Micro celdas	128	1536	Varios kilómetros
Pico celdas	514	Miles	Varias manzanas o edificios

Las tecnologías portadoras que trasmiten las comunicaciones inalámbricas están en constante cambio, actualmente se utiliza la tercera generación (3G) y se inició la migración a la cuarta generación (4G).

Tabla 2. Generaciones de tecnologías inalámbricas
Autor: Iván Freire

Generación	Arquitectura	Ejemplos de tecnologías
Primera (1G)	Analógica	AMPS, N-AMPS, NMT, TACS, FDMA, CDMA, TDMA, GSM
Segunda (2G)	Digital	CDMA, TDMA, GSM
Tercera (3G)	Digital de segunda generación	SMS, EDGE GPRS, USSD, WCDMA, WATM
Cuarta (4G)	Digital de tercera generación	HSDPA, HSPA+, HSUPA, LTE

1.2.1.3 Sistema global de comunicaciones móviles (GSM)

Global System for Mobile communications, GSM, es un estándar que solo permite la transmisión digital, y no fue diseñado para que sea compatible con los sistemas analógicos existentes. Está basada en TDMA[1] y utiliza la compartición de tiempo para permitir el acceso simultáneo de varios usuarios, hasta un máximo de ocho sobre una misma banda de 200 kHz. Para operación dúplex se requieren dos bandas de 200 kHz. (Nichols & Lekkas, 2003)

Tabla 3. Espectro de frecuencias de operación de GSM
Autor: Iván Freire

Bandas	Rango	Emparejamiento
GSM 400	450, 4 a 457,6 MHz	460,4 a 467,6 MHz
GSM 900	880 a 915 MHz	925 a 960 MHz
GSM 1800	1710 a 1785 MHz	1805 a 1880 MHz
GSM 1900	1850 a 1919 MHz	1930 a 1990 MHz

El sistema GSM tiene varios tipos de canales para señales de control, que transportan información del sistema y de localización de los móviles, y coordinan el acceso de la misma manera que los canales de control de los sistemas analógicos. A diferencia de los canales analógicos, los de GSM ofrecen funcionalidades como el envío de mensajes de difusión a móviles, modos de inactividad avanzados, entre otros. (Nichols & Lekkas, 2003)

[1] TDMA: (Time Division Multiple Access, Acceso múltiple por división de tiempo) es un método de transmisión digital inalámbrico que permite a varios usuarios acceder, en secuencia, a un canal único de radio frecuencia sin interrupciones, mediante la asignación de periodos de tiempo únicos a cada usuario dentro de cada canal.

GSM fue diseñado para admitir con facilidad cualquier codificador de voz de media velocidad, el cual asigna una franja temporal a una de cada dos tramas, lo que permite potencialmente un máximo de hasta 16 usuarios simultáneos por cada canal.

Durante una conversación de voz en el dispositivo móvil, una franja temporal se emplea para transmisión, otra para recepción y las seis restantes están inactivas. Las franjas temporales inactivas se emplean para medir la intensidad de la señal de las frecuencias portadoras de las celdas vecinas.

GSM ofrece las diversas funcionalidades por medio de un módulo de identificación de abonado (SIM, subscriber identification module), que se inserta en una ranura situada en el aparato telefónico. El módulo SIM contiene datos del perfil de usuario, una descripción de los privilegios de acceso y una identificación del operador de telecomunicaciones móviles en el área doméstica en la que se activó el teléfono. (Nichols & Lekkas, 2003)

El módulo SIM es universal y se puede intercambiar entre teléfonos con tecnología GSM, lo que permite al abonado moverse libremente a través de distintos entornos GSM existentes en el mundo. La información contenida del módulo SIM es confidencial, y se emplean mecanismos criptográficos (aunque débiles) para garantizar su protección.

1.2.1.4 SMS

Actualmente, todos los operadores de telecomunicaciones móviles del mundo proporcionan el servicio SMS acrónimo de Short Message Service, servicio de mensajes cortos. Este servicio permite a los abonados de telefonía celular recibir mensajes cortos de texto de varios tamaños, de entre 160 y 180 caracteres. (Nichols & Lekkas, 2003)

Aunque se aplican mecanismos de seguridad a los datos SMS, los entornos inalámbricos constituyen un desafío muy particular, en el sentido de que, si se dispone de los equipos adecuados, puede interceptarse la señal inalámbrica (y modificarla) más fácilmente que con una línea telefónica convencional. Para comprobar que el tráfico SMS no ha sufrido modificaciones durante el tránsito, se emplea un código de redundancia cíclica (CRC).

Un problema potencial de seguridad y/o intimidad es el relacionado con las aplicaciones de banca móvil representan uno de los usos potenciales de SMS. La banca móvil se está convirtiendo rápidamente en una de las aplicaciones inalámbricas principales, al permitir a los abonados acceder a información sobre sus cuentas, pagar facturas y realizar transferencias, lo que las convierte en un objetivo potencialmente lucrativo para alguien que disponga de las herramientas adecuadas.

1.2.1.5 Entornos inalámbricos de cuarta generación (4G)

Tabla 4. Resumen de la Tecnología 4G
Autor: Iván Freire

Razones para disponer de tecnologías 4G	Novedades en la tecnología 4G
Soporte para servicios multimedia interactivos: teleconferencia, Internet inalámbrica, etc.	Redes de conmutación de paquetes puras.
Mayores anchos de banda y velocidades de bit más altas.	Todos los elementos de red son digitales.
Movilidad global y portabilidad de servicios.	Mayores anchos de banda para proporcionar servicios multimedia a un menor coste.
Bajo coste.	Seguridad de red más estricta.
Escalabilidad de las redes móviles.	

A continuación se compara las dos tecnologías utilizadas en la actualidad.

Tabla 5. Comparación de tecnologías 3G y 4G
Autor: Iván Freire

3G	4G
Compatible con la tecnología 2G.	Amplía la capacidad de la tecnología 3G en un orden de magnitud.
Redes de conmutación de circuitos y de Paquetes.	Redes completamente basadas en conmutación de paquetes.
Combinación de equipos existentes y equipos evolucionados.	Todos los elementos de red son digitales. Mayor ancho de banda (hasta 100 Mbps).
Velocidad de datos (hasta 2 Mbps)	

1.2.1.6 Clasificación de la movilidad en las redes de comunicación inalámbricas

A continuación se detalla las características de la comunicación inalámbrica fija, transportable y completamente móvil.

Tabla 6. Tipos de movilidad en las redes de comunicación inalámbricas
Autor: Iván Freire

Tipos	**Conexiones cableadas**	**Conexión inalámbrica restringida**	**Completamente móvil**
Fija	Teléfono convencional	Teléfonos inalámbricos domésticos	Teléfonos celulares
Transportable	Estaciones base móviles con usuarios conectados por cable	Estaciones base móviles con terminales de abonado inalámbricos (no satelitales)	Sistemas celulares militares con estación base
Completamente móvil	Red radio de conmutación de paquetes	Infraestructura terrestre más repetidores situados en aeronaves no tripuladas	Red de radio con satélites de baja órbita

1.2.1.7 Seguridad móvil

La infraestructura, como tal, siempre ha sido vulnerable. Desde ese punto de vista, los entornos inalámbricos no son diferentes al resto de ambientes (a menos que se resistan a nuestros esfuerzos para dotarlos de seguridad). Los medios inalámbricos tienen, de hecho, menos activos físicos que proteger, pero, al mismo tiempo, no existe ninguna puerta con llave alrededor de las ondas de radio, por lo que resulta mucho más fácil acceder a ellas. (Nichols & Lekkas, 2003)

1.2.1.8 Grados razonables de seguridad

El nivel de riesgo, en su forma más simple, es igual al producto de las Amenazas y las Vulnerabilidades, dividido por el producto de las Contramedidas aplicadas y el Impacto.

Aunque resulta absurdo, en sentido estricto, tratar de conseguir una cierta precisión a la hora de cuantificar los niveles de seguridad inalámbrica, o cualquier otro nivel de seguridad de un sistema de información, sí que es mucho lo que puede hacerse para reducir el nivel de riesgo hasta un nivel de seguridad aceptable. (Nichols & Lekkas, 2003)

1.2.1.9 Vulnerabilidades en los sistemas telefónicos

La interconexión e interdependencia de la infraestructura nacional de comunicaciones de los países presenta un objetivo valioso y vulnerable a los ataques terroristas. Las torres de telefonía celular son fácilmente reconocibles. Estas torres están normalmente colocadas en áreas de fácil acceso que, debido a su necesaria proximidad a las autopistas, son áreas a las que resulta fácil acercarse sin ser detectado. Si hay algún tipo de sistema de seguridad instalado, puede que no sea suficiente para detener a un terrorista armado con una bomba. (Nichols & Lekkas, 2003)

Pirateo Telefónico

La Red Telefónica General de Conmutación (RTGC), al igual que cualquier otra red informática, constituye un objetivo de los piratas informáticos y es vulnerable al pirateo. Los piratas informáticos (hackers) que atacan las redes telefónicas se denominan phreakers y su versión de ataque informático se denomina phreaking, que consiste, básicamente, en realizar sus actividades con un teléfono en lugar de con una computadora, y así acceder de manera gratuita a las líneas de larga distancia. (Nichols & Lekkas, 2003)

Aspectos legales

Una serie de gobiernos de distintos países han aprobado varias leyes relativas a los teléfonos inalámbricos y a las escuchas de conversaciones ajenas. Sin embargo, el hecho de que una ley exista no garantiza que vaya a ser obedecida ni que pueda ser puesta en práctica. Este problema afecta a todos los países. (Nichols & Lekkas, 2003)

1.2.1.10 Identificación del atacante

Según (Nichols & Lekkas, 2003), lo primordial es identificar qué información es importante y de qué modo puede ser útil pero, en cualquier caso, sigue siendo fundamental restringir la información puesta a disposición de atacantes. A continuación se enlista los dispositivos que pueden ser vulnerables.

- Teléfonos inalámbricos
- Teléfonos celulares
- Sistemas de Voz

1.2.1.11 Seguridad criptográfica

La criptografía es la ciencia de mantener secretas las comunicaciones, orales, escritas y de otros tipos, así como de proporcionar un medio de autenticar a aquéllos que intervienen en las comunicaciones. Esta metodología se basa en algunas interesantes y complejas estructuras matemáticas. (Nichols & Lekkas, 2003)

1.2.1.12 Ocultación

Una de las formas más seguras de preservar el secreto de la información consiste en ocultarla de forma tan efectiva que aquéllos que deseen obtenerla no puedan reconocer su presencia. La ocultación de un mensaje para evitar que alguien sea consciente de su existencia genera lo que se conoce como clave de ocultación o clave nula. (Nichols & Lekkas, 2003)

Puesto que los mensajes se pueden reducir a una secuencia de bits[2] 1 y 0, cualquier patrón en el que estén presentes dos diferentes valores puede utilizarse como vehículo para ocultar la información.

[2] Bit: es el acrónimo Binary digit (dígito binario) .1 Un bit es un dígito del sistema de numeración binario.

1.2.1.13 Criptografía digital

La criptografía[3] moderna se dedica casi exclusivamente a la protección de información en forma digital, es decir, de secuencias de valores 1 y 0. Puede utilizarse alguno de los métodos vistos, transposición y sustitución, o pueden combinarse ambos para forman un algoritmo complejo y aplicar dicho algoritmo con una clave, que será también una secuencia de valores 1 y 0, obteniendo así los mensajes cifrados a partir de los mensajes en claro originales. (Nichols & Lekkas, 2003)

Transposición

Considerando la Tabla 7 de Alfabeto en lenguaje Binario:

Tabla 7. Alfabeto Binario
Autor: Iván Freire

A	01000001	**N**	01001110
B	01000010	**O**	01001111
C	01000011	**P**	01010000
D	01000100	**Q**	01010001
E	01000101	**R**	01010010
F	01000110	**S**	01010011
G	01000111	**T**	01010100
H	01001000	**U**	01010101
I	01001001	**V**	01010110
J	01001010	**W**	01010111
K	01001011	**X**	01011000
L	01001100	**Y**	01011001
M	01001101	**Z**	01011010

[3] Criptografía: Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Se escribe la palabra “Hola” de la siguiente manera:

01001000010011110100110001000001

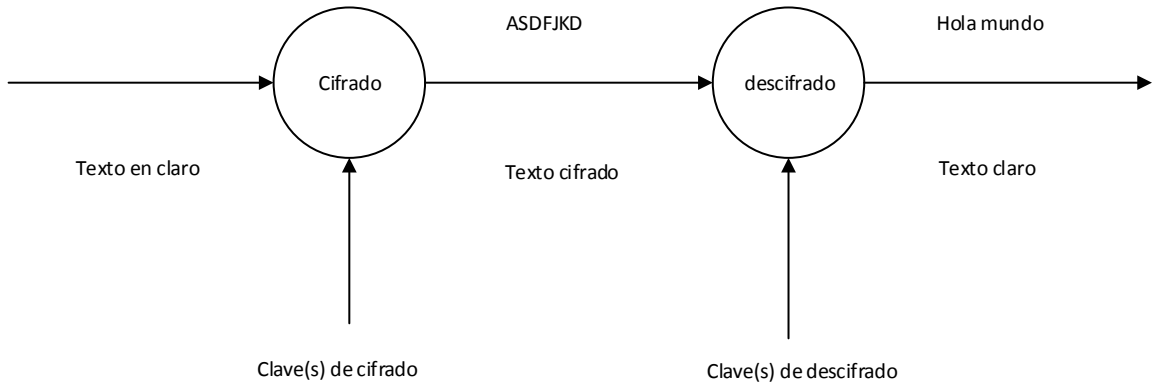
Al modificar el mensaje, por ejemplo leyendo cada byte de derecha a izquierda, obtenemos:

00010010111100100011001010000010

Sustitución

Los códigos de sustitución utilizan una clave y un algoritmo para sustituir los caracteres del mensaje por otros caracteres que no parezcan tener sentido para el receptor. En los modernos sistemas de comunicaciones, los circuitos para llevar a cabo la sustitución utilizan circuitos denominados puertas lógicas, que aceptan dos o más bits como entrada y proporcionan un bit como salida que depende del tipo de puerta lógica. (Nichols & Lekkas, 2003)

Figura 1. Criptografía de sustitución con clave determinista
Fuente: Nichols & Lekkas, 2003



Adición binaria

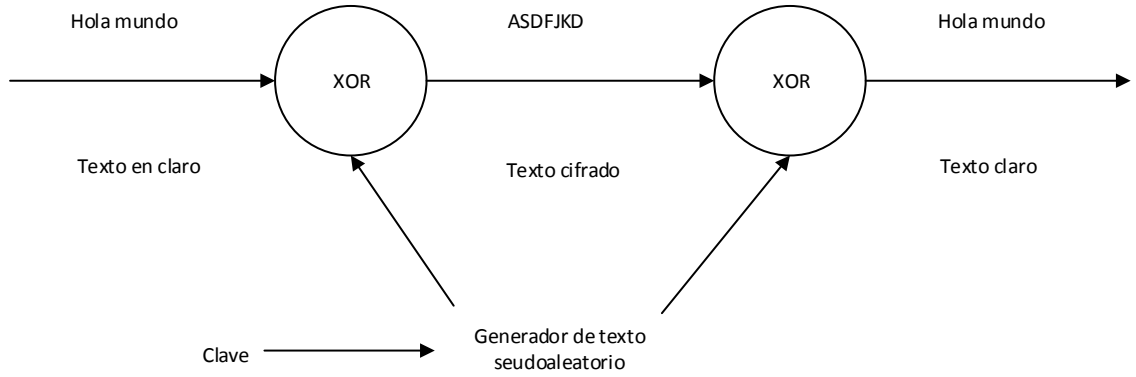
Si tomamos el texto en claro como un flujo de bits y la clave como otro flujo de bits, las claves de cifrado y descifrado son idénticas, y los algoritmos de cifrado y descifrado también lo son: de hecho, se trataría meramente de una operación XOR[4], que puede implementarse fácilmente mediante circuitos electrónicos. (Nichols & Lekkas, 2003)

Para crear el flujo de bits de clave, podemos emplear cualquier generador de números seudoaleatorio suficientemente robusto. Los generadores de números seudoaleatorios son funciones matemáticas que producen una secuencia de números que son aparentemente aleatorios, aun cuando se los genera de manera determinista.

[4] XOR: El operador lógico Disyunción exclusiva también llamado o exclusivo, simbolizado como XOR, EOR, EXOR, ⊻ o ⊕ es un tipo de disyunción lógica de dos operandos que es verdad si solo un operando es verdad pero no ambos.

Es decir, la secuencia de números producida por el generador de números seudoaleatorio es capaz de pasar algunas pruebas diseñadas para detectar la presencia de patrones que pudieran utilizarse, por un criptoanalista, para duplicar el flujo de números y romper así el sistema de cifrado.

Figura 2. Cifrado mediante adición binaria
Fuente: Nichols & Lekkas



1.2.1.14 Tipos de Ataques

Ataques por fuerza bruta

Este tipo de ataque se limita a probar todas las posibles claves, una de tras de otra. El tiempo para averiguar el texto claro correspondiente a un determinado texto cifrado, depende directamente del número de bits de la clave. (Nichols & Lekkas, 2003)

Ataques estándar

Si se conoce parte del texto en claro, esta información puede aprovecharse en lo que se denomina un ataque de texto claro conocido. Todavía resulta mejor si se puede averiguar el texto cifrado correspondiente a un texto en claro suministrado por el propio criptoanalista y cifrado con la clave que se está buscando; este ataque todavía más potente se denomina ataque de texto en claro seleccionado. (Nichols & Lekkas, 2003)

Ataques Avanzados

Aunque la longitud de la clave tiene una gran importancia para el nivel de un sistema de cifrado, las debilidades permiten descifrar la clave por métodos distintos, como son el criptoanálisis diferencial y el criptoanálisis lineal. (Nichols & Lekkas, 2003)

Tabla 8. Tipos de Ataques avanzados
Autor: Iván Freire

Criptoanálisis	Método	A Favor	En Contra
Diferencial	Toma parejas de cadenas de texto cuya combinación mediante operaciones XOR (diferencia) tenga ciertas características.	Puede llegar a obtenerse la clave sin probar todas las combinaciones.	Sólo funciona contra determinados algoritmos de cifrado.
Lineal	Encuentra aproximaciones simples de la función compleja utilizada en cada ronda de un sistema de cifrado	Requiere unos 10 billones de bloques de texto en claro conocido.	No es una amenaza práctica para DES[5]

[5] DES: Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos

1.2.1.15 Firmas digitales

Un mensaje puede ser cifrado utilizando una clave privada y descifrada utilizando la clave pública correspondiente. Tal esquema nos proporciona confidencialidad, dado que todo el mundo tiene acceso a la clave pública y puede, por tanto, leer el mensaje. Pero sólo el propietario de la clave privada puede haber escrito el mensaje, suponiendo que la clave privada haya sido mantenida a buen recaudo. (Nichols & Lekkas, 2003)

Esta forma robusta de autenticación, que garantiza que el mensaje recibido sólo puede haber sido enviado por el propietario de la clave privada correspondiente a la clave pública utilizada para cifrar el mensaje, es suficiente para probar (delante de un juez, si fuera necesario, en aquellos lugares donde dicho método de autenticación esté reconocido como válido) que el mensaje provenía, ciertamente, del supuesto emisor.

El emisor no puede repudiar el mensaje, lo que hace que este esquema de cifrado sea tan válido como una firma en un documento en papel, lo cual es la razón por la que se denomina a este mecanismo firma digital.

1.2.1.16 Inversores de frecuencia

El inversor de frecuencia simplemente invierte el espectro, de modo que las frecuencias más bajas se mueven a la parte alta de la banda, mientras que las frecuencias más altas se mueven a la parte más baja. Las dos bandas situadas por encima y por debajo de la frecuencia

portadora se denominan bandas laterales superior e inferior, respectivamente. Las bandas laterales son simplemente imágenes especulares una de otra, con las frecuencias más bajas y más altas intercambiadas. (Nichols & Lekkas, 2003)

1.2.1.17 ISO/IEC

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. (Merino Bada & Cañizares Sales, 2011)

1.2.1.18 Serie 27000

La serie 27000 es un conjunto de estándares que proporcionan el marco de trabajo para que cualquier organización pública o privada, independientemente de su tamaño, área o actividad, pueda adoptar las mejores prácticas recomendadas para desarrollar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información. (Merino Bada & Cañizares Sales, 2011)

1.2.1.19 ISO/IEC 27002:2005

Es una guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables en cuanto a seguridad de la información publicada en el 2005. Esta norma no es certificable dado que es una guía para la implementación de controles y forma parte de la ISO 27001 como su anexo.

Contiene 39 objetivos de control y 133 controles, divididos en 11 dominios de seguridad. Esta norma no se centra solamente en las tecnologías de la información; también incluye aspectos sobre asuntos organizacionales, gestión de recursos humanos, seguridad física, normativa legal, etc. Para el presente trabajo nos centraremos en el dominio de Gestión de comunicaciones y operaciones. (Merino Bada & Cañizares Sales, 2011)

1.2.2 Marco Conceptual

1.2.2.1 Arquitectura de comunicaciones

La comunicación entre dispositivos es posible por el establecimiento de estándares comunes, llamados protocolos, es decir, un conjunto de reglas para iniciar y mantener la comunicación entre los emisores y receptores. Estos protocolos, junto a su implementación física en hardware y software y su organización, se la nombran arquitectura de comunicaciones. (Carmen de Pablos Heredero, 2004)

1.2.2.2 Seguridad de la información

La meta primordial de la seguridad de la información es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las tecnologías de la información y comunicación de la empresa, a sus socios comerciales, clientes, administración pública, suministradores, etc. (Areitio Bertolín, 2008)

1.2.2.3 Estándar ISO

Los estándares internacionales son producidos y publicamos por la ISO (International Organization for Standardization, Organización de Estándares Internacionales), una organización voluntaria no surgida de un acuerdo, fundada en 1946. Sus miembros son las organizaciones de estándares nacionales de los 89 países miembros entre ellos se encuentran Estados Unidos, Gran Bretaña, Francia, Alemania, etc. La ISO emite normas sobre una gran cantidad de temas, desde los más básicos, como tuercas y pernos, hasta el revestimiento de postes telefónicos. (Tanenbaum, 2003)

CAPÍTULO II

MÉTODO

2.1 ANÁLISIS

2.1.1 Estudio preliminar

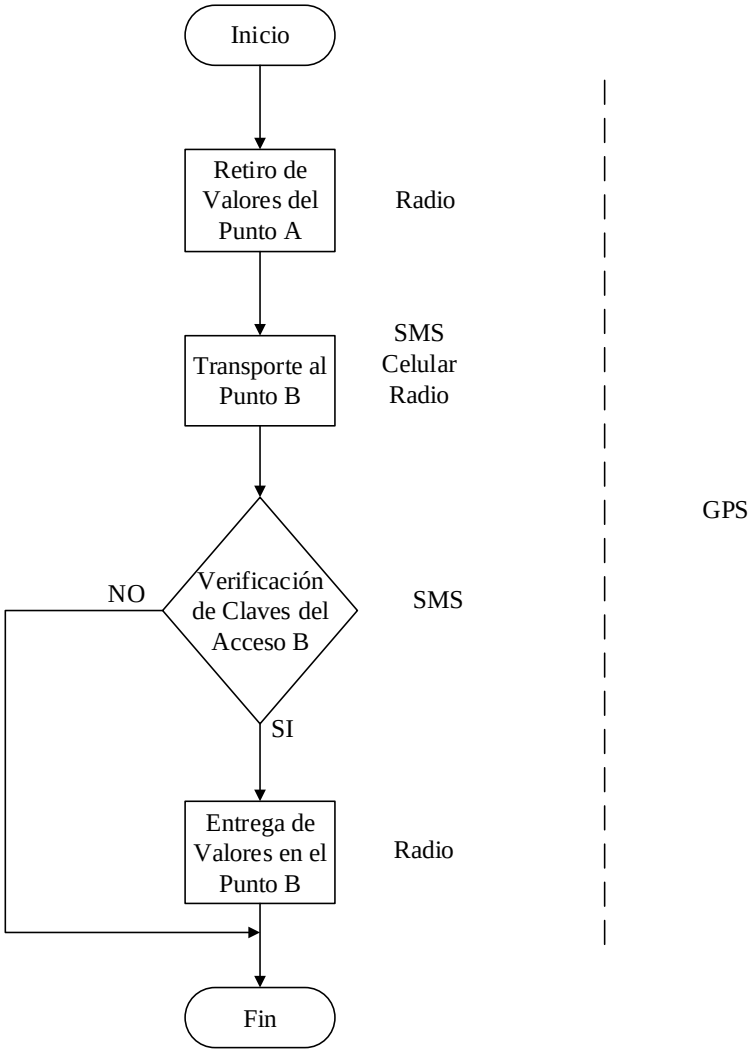
En la actualidad las empresas de transporte de valores, utilizan comunicaciones de radio o celulares para determinar su posición, administración de incidentes, claves, etc. En estas comunicaciones no se aplican controles o estándares de seguridad de la información.

Para lo cual se investigó la metodología de comunicación utilizada en las mencionadas empresas de transporte de valores. A continuación se muestra en un diagrama de flujo los métodos de comunicación preliminares que se encontraron en primera instancia.

Posteriormente se realiza una matriz de observación preliminar o inicial detallando los procesos de mas importantes y que se repiten a diario. Cada proceso tiene su descripción de los tipos de comunicación que se utilizan.

Finalmente un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) permite obtener una visión clara de la situación inicial de las comunicaciones.

Figura 3. Esquema Inicial de Entrega y Recepción de valores
Autor: Iván Freire



Observaciones Generales:

Tabla 9. Matriz de Observación Inicial
Autor: Iván Freire

Proceso	Detalle
Retiro de Valores Punto A	- Se utiliza comunicación vía radio para las notificaciones de seguridad y ubicación. - Rastreo GPS del blindado
Transporte al Punto B	- Envío de rutas por medio de SMS, celulares o radio - Rastreo GPS del blindado - Cámaras internas de grabación y transmisión de video de vigilancia.
Verificación de Claves Acceso B	- Se recibe claves de ingreso a bóvedas mediante SMS - Rastreo GPS del blindado
Entrega de Valores Punto B	- Confirmación de entrega de valores vía celular o radio - Rastreo GPS del blindado

Tabla 10. Análisis FODA
Autor: Iván Freire

Fortalezas	Oportunidades	Debilidades	Amenazas
Uso de Comunicaciones para agilizar la entrega/recepción	Permite elegir entre varias opciones como radio, celulares, comunicación satelital, etc.	La comunicación no está encriptada en muchos casos	Puede ser interceptada en cualquier punto del proceso
Comunicación vía radio es de bajo costo	Adaptable al tipo de negocio	Pérdida de equipos de mano o daño	Intercepción de frecuencias utilizadas
Telefonía Celular con un número especial o único	Actualización de equipos y tecnología	Pérdida o daño de SIM	Inhibición de señal celular o intercepción
Rastreo GPS en todo el proceso de entrega/recepción	Control de la ubicación del blindado	Daño del equipo	La ubicación puede ser interceptada

A continuación se enumera las herramientas para desarrollar el plan de seguridad que actualmente cumplen las compañías de transporte de valores, enfatizando en la sección de comunicaciones.

2.1.1.1 Medios de protección

Es pertinente establecer los recursos o medios de seguridad a utilizar para minimizar los riesgos. Para lo cual se debe establecer un sistema de seguridad integral.

La seguridad integral está constituida por tres tipos de medios que deben aunarse como partes integrantes de un todo.

- Recursos Humanos: constituidos por el personal de seguridad, tanto Pública, Institucional y/o Privada.
- Recursos Técnicos: pasivos o físicos; activos o electrónicos.
- Recursos Organizativos: planes, normas, estrategias.

Estos tres medios deben ser manejados conjuntamente, para alcanzar una sinergia entre estos elementos, para tener como resultado un sistema de seguridad eficiente y eficaz a servicio de las personas y bienes que engloban las entidades bancarias.

Detalle de los recursos humanos y técnicos:

a. Recurso Humano

- Un Jefe de Operaciones
- Dos conductores
- Un custodio
- Tres vigilantes

b. Recurso Técnico – Sección Comunicaciones

- Tres celulares
- Tres radios bases
- Dos radios portátiles,
- Rastreo satelital,
- Monitoreo GPRS

2.1.1.2 Método de Mósler

Para desarrollar el análisis y evaluación de riesgos se puede utilizar varios métodos existentes, pero se considera que el más adecuado para la actividad de transporte de valores es el Método Mósler, debido a que este método nos da la ventaja de utilizar subcriterios con el fin de cuantificar más objetivamente, y a través de los subcriterios se pueden plasmar los factores de riesgo arriba descritos.

El Método Mósler tiene cuatro fases secuenciales:

1) Definición del riesgo: identifica el riesgo delimitando su contenido y alcance para diferenciarlo de otros riesgos. Para la identificación específica se basa en los elementos característicos que son el bien y el daño.

2) Análisis del riesgo: determina y calcula los criterios de: función (F), sustitución (S), profundidad (P), extensión (E), agresión (A), y vulnerabilidad (V). En esta fase es donde se puede plasmar los factores de riesgo del transporte de valores a través del establecimiento de subcriterios cuya media aritmética del resultado, determina el número que indica la graduación equivalente al criterio. Por ejemplo en la sección de agresión los posibles subcriterios pueden ser:

Tabla 11. Criterios de riesgos
Autor: (Rodriguez Paez, 2013)

Peligrosidad del sector	**Vigilancia en la instalación**	**Circulación vehicular y peatonal**
Peligrosidad alta: 5	Sin vigilantes: 5	Alta circulación: 5
Peligrosidad media alta: 4	Vigilantes alrededor: 4	Media alta circulación: 4
Peligrosidad media: 3	Vigilantes contiguos: 3	Mediana circulación: 3
Peligrosidad media baja: 2	Con vigilante: 2	Media baja circulación: 2
Peligrosidad baja: 1	Con vigilantes dos o más: 1	Baja circulación: 1
Graduación = 4	**Graduación = 2**	**Graduación = 4**

En base a la graduación de cada subcriterio la media aritmética es 3, razón por la cual la graduación del criterio de agresión (A) es 3.

La posibilidad o probabilidad de que el riesgo se manifieste es: (Normal)

Muy Elevada (5)

Elevada (4)

Normal (3)

Reducida (2)

Muy Reducida (1)

3) Evaluación del riesgo: cuantifica el riesgo definido y analizado, para lo cual considera tres cálculos:

- Carácter del riesgo (C): C = I + D donde: I = F x S y D = P x E
- Probabilidad (Pb): Pb = A x V
- Cuantificación del riesgo considerado (ER): ER = C x Pb

4) Cálculo de la clase de riesgo: clasifica el riesgo en base al valor obtenido en la fase de evaluación, dicho resultado siempre estará comprendido entre 2 y 1250, quedando clasificado de la siguiente manera:

VALOR ENTRE	CLASE DE RIESGO
2 y 250	Muy Reducido
251 y 500	Reducido
501 y 750	Normal
751 y 1000	Elevado
1001 y 1250	Muy Elevado

Este análisis y evaluación de riesgo se debe realizar para cada cliente y/o instalación donde se efectuara la entrega recepción de valores para la transportación de los mismos.

Ante esto se recomienda crear la siguiente matriz:

Figura 4. Matriz de análisis y evaluación de riesgos 1
Fuente: Rodríguez Páez, 2013

MATRIZ DE ANALISIS Y EVALUACION DE RIESGOS METODO MOSLER																												
N°	Escenario / Riesgo	ESCENARIO 1							ESCENARIO 2							ESCENARIO 3							ESCENARIO n						
		F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR
1	Asalto																												
2	Robo																												
3	Accidente																												
n	Otros Riesgo																												

En la columna colocamos todos los riesgos definidos en la fase 1 y en la primera fila colocamos los escenarios que para el caso correspondería para cada cliente y/o instalación donde se entregue y reciba valores. En la segunda fila, de bajo de cada escenario colocamos siete columnas para los seis criterios y la cuantificación del riesgo. Para llenar la matriz, colocamos la graduación debajo de cada criterio por cada riesgo y por cada escenario. En la columna del CR aplicamos la fórmula:

$$[[(F \times S) + (P \times E)] \times [A \times V]]$$

Completada la matriz podemos determinar el riesgo global y el escenario más crítico obteniendo la media aritmética de los CRs obtenidos por riesgo y por escenario.

Figura 5. Matriz de análisis y evaluación de riesgos 2
Fuente: Rodríguez Páez, 2013

MATRIZ DE ANALISIS Y EVALUACION DE RIESGOS METODO MOSLER																				
N°	Escenario / Riesgo	ESCENARIO 1							ESCENARIO 2							ESCENARIO 3							RIESGO TOTAL
		F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	
1	Asalto	5	5	5	5	4	4	800	5	5	5	5	5	4	1000	5	5	5	5	3	4	600	800
2	Robo	5	4	4	4	3	3	324	5	4	4	4	4	3	432	5	4	4	4	5	3	540	432
3	Accidente	5	4	4	3	4	4	512	5	4	4	3	5	4	640	5	4	4	3	5	4	640	597
Escenario más crítico								545							691							593	

Con los resultados obtenidos podemos realizar un mejor análisis para gestionar y poder establecer las medidas de prevención y protección de seguridad más adecuadas para minimizar los riesgos de una manera eficiente y eficaz para el transporte de valores.

Fuente: Rodríguez Páez, 2013

2.1.1.3 Manual de Procedimientos – Sección comunicaciones

A continuación se detalla el manual de procedimientos que siguen las empresas de transporte de valores, en su sección de comunicaciones, en las procedimientos de antes, durante y después del proceso normal de entrega de un punto a otro.

a) Antes del servicio

- Jefe de operaciones recepta el pedido de servicio y elabora el recorrido del blindado.
- Jefe de operaciones y tripulantes verifican los medios de comunicación.
- El blindado y seguimiento reportan la salida al recorrido.

b) Durante el Servicio

- El blindado se reportara vía radio a la llegada y salida de cada cliente.
- Jefe de operaciones monitorea y supervisa el cumplimiento del recorrido establecido.

c) Después del servicio

Reportar la llegada a central.

d) En caso de daños mecánicos

- Blindado comunica a Jefe de operaciones ante cualquier daño mecánico para recibir instrucciones.
- Si el daño mecánico no puede ser solucionado se comunicara a Jefe de operaciones para que envié otro vehículo y realizar transbordo.
- Solucionado el problema se comunica a Jefe de operaciones y continúa con el recorrido.

e) En caso de accidente de Transito

- Blindado comunica inmediatamente a jefe de operaciones cuando se presente algún percance y recibe instrucciones.
- Conductor de seguimiento toma contacto con los ocupantes siniestrados y brinda asistencia si amerita. Luego pone en contacto al conductor con jefe de operaciones.

f) En caso de Transbordo

- Jefe de operaciones comunica al blindado los datos del blindado y sus tripulantes con los que realizaran el transbordo.

Fuente: (Rodriguez Paez, 2013)

2.1.1.4 Códigos

Para la comunicación vía radio entre tripulantes y central de monitoreo se utiliza el siguiente Código P:

Tabla 12. Código P
Autor: Rodríguez Páez, 2013

Código P	
PHL Llego a	**PT10-6** Transporte de valores
PHS Salgo de o a	**PT10-7** Ponga guardia en
PHN Alguna novedad	**PT10-8** Funcionario – empleado
PHN0 Sin novedad	**PT10-9** Comisión
PHN1 Con novedad	**PT10-10** Necesito ayuda
PH0 Negativo	**PT10-11** Comunique rol de guardia
PH1 Afirmativo	**PT10-12** Aeropuerto
PHC Casa de la Moneda	**PT10-13** Policía Nacional
PHD Dinero	**PT10-14** Indique su nominativo
PHB Banco Central	**PT10-15** Urgente reportarse
PHG Caja General	**PT10-16** Me encuentro en
PHK Me dirijo a	**PT10-17** Zona Militar
PHX Repita	**PT10-18** Cuál es su rumbo
PHA Diríjase a	**PT10-19** Tiene noticias del Sr.
PHE Espere	**PT10-20** Cambie de ruta
PHO Manténgase en observación	**PT10-21** Chofer
PHM Mensaje	**PT10-22** Esposa
PHU Señal de comunicación	**PT10-23** Ponga distancia de voces
PT10-1 Abro la puerta	**PT10-24** Retire distancia de voces
PT10-2 Cierro la puerta	**PT10-25** Reunión
PT10-3 Vehículo sospechoso	**PT10-26** Custodio
PT10-4 Individuo sospechoso	**PT10-27** No información por este medio
PT10-5 Informe sobre	**PT10-28** Indique la hora

Para referirse a los clientes vía radio se utilizara el siguiente código de comunicación:

Tabla 13. Código Cliente
Autor: Iván Freire

Cliente	Código
Agencia Bancaria X	Alemania
Agencia Bancaria Y	Argentina
Agencia Bancaria Z	Argelia

Finalmente para casos emergentes se tiene establecido la siguiente guía telefónica de emergencia:

Tabla 14. Números de emergencia
Autor: Iván Freire

Institución	Teléfono
Policía	101
Bomberos	102
ECU	911
UPC Mariscal	2456-678
UPC Recreo	2342-122
Clínica Santa María	2913-000

2.1.2 Estudio de factibilidad

2.1.2.1 Factibilidad Técnica

Para el desarrollo de este trabajo investigativo se ha escogido análisis de riesgos, para lo cual en primera instancia se describen los problemas que se encontraron en las comunicaciones del transporte de valores: intercepción de comunicaciones, inhibidor de señales celulares, daño de equipos celulares o de radio, intercepción de GPS.

En el diagrama se representan todos los riesgos a los que se puede encontrar expuesta la empresa de transporte de valores, mostrando su probabilidad de ocurrencia y el impacto o severidad de los mismos, permitiéndonos tener una visión clara y rápida de los riesgos cualitativos de la empresa.

Figura 6. Mapa de Riesgos y Ponderación de valores
Fuente: Marco de gestión de riesgos empresariales, 2004

RIESGO		PROBABILIDAD			
		1 (Poco Frecuente)	2 (Frecuencia normal)	3 (Frecuente)	4 (Muy frecuente)
IMPACTO	5 (Extremo)	0	1	0	2
	4 (Mayor)	0	0	1	0
	3 (Moderado)	1	1	0	0
	2 (Menor)	1	0	0	0
	1 (Insignificante)	1	1	1	1

Riesgo = Probabilidad * Impacto

Riesgo	Puntaje
Bajo	[0 - 4]
Medio	[5 - 8]
Alto	[9 - 14]
Muy alto	[15 - 20]

A continuación se detalla el análisis de riesgos para la empresa de transporte de valores.

Tabla 15. Análisis de riesgo inherente
Autor: Iván Freire

	Problema	Impacto	Probabilidad	Riesgo
1	Intercepción de comunicaciones	5	4	**20**
2	Inhibidor de señales celulares	5	4	**20**
3	Daño de equipos celulares o de radio	4	3	**12**
4	Intercepción de GPS	5	4	**20**

2.1.2.2 Factibilidad Tecnológica

A continuación se detallan los equipos de intercepción que se utilizaron parar los análisis de las comunicaciones empleados en la empresa de transporte de valores.

Equipo Uniden BC125AT - Escáner de mano con 500 Canales y Etiquetado

El BC125AT incluye una memoria de 500 canales, etiquetado alfa, por lo que se puede nombrar a cada canal, y también incluye la banda de aviones militares. Lo suficientemente práctico para llevar a cualquier parte, su función Close Call incluso puede capturar comunicaciones locales, incluso si no están programadas.

Características:

- 500 Canales con Etiquetas: Le permite nombrar todos los canales para facilitar la identificación de quién habla.
- Modo No molestar: Evita las pausas en el audio mientras sigue la búsqueda de señales cercanas.
- Bandas aéreas civiles y militares: Excelente para las demostraciones de aéreas o sólo escuchar a las aeronaves en vuelo.
- Servicio de búsqueda: Le ayuda a encontrar las frecuencias indocumentadas en su área.
- Modo de banda corta y pasos.

- Pantalla LCD retro iluminada: Hace que sea fácil de ver la selección de canales en la oscuridad.

- Tamaño compacto

- Carga desde el PC mediante USB

Tabla 16. Rango de frecuencias
Fuente: Manual Equipo Uniden BC125AT

Bank No.	Frecuencia (MHz)	Salto
1	25.0000 - 27.9950	5.00
2	28.0000 - 29.6950	5.00
3	29.7000 - 49.9950	5.00
4	50.0000 - 54.0000	5.00
5	108.0000 - 136.9916	8.33
6	137.0000 - 143.9950	5.00
7	144.0000 - 147.9950	5.00
8	225.0000 - 380.000	12.50
9	406.0000 - 449.99375	6.25
10	450.0000 - 469.99375	6.25

Sistemas de intercepción GSM/ 3G / 4G

Este sistema permite la captura de las llamadas entrantes y salientes, tanto de voz como mensajes de texto, de teléfonos objetivo funcionando sobre la red GSM/3G/4G, con la aplicación de inhibición selectivas de canales de control, operando de manera invisible para el objetivo.

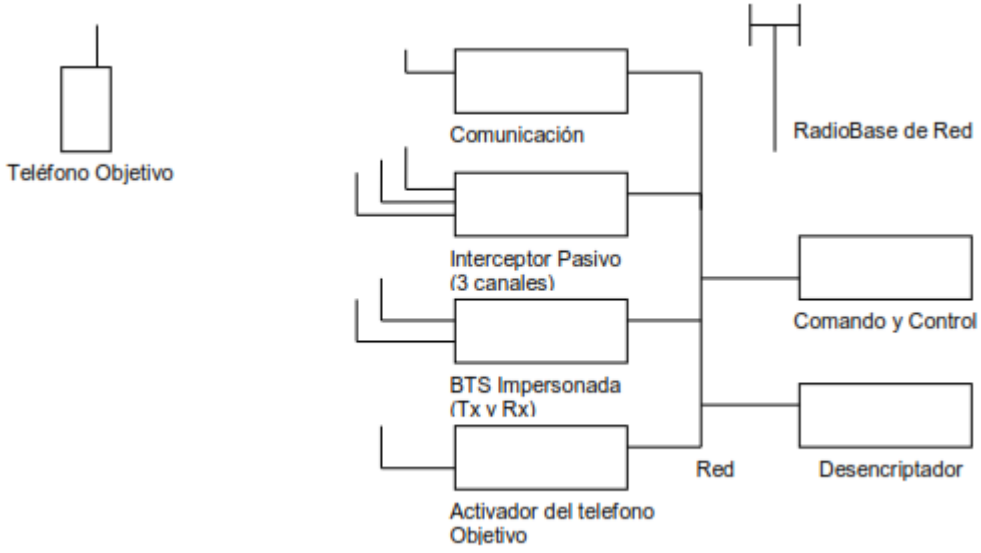
Características generales del sistema:

- Intercepción en tiempo real de llamadas entrantes y salientes, voz y SMS sobre objetivos en redes GSM

- Soporta los algoritmos de cifrado A5/1 y A5/2
- Funcionamiento transparente e indetectable por la prestataria de telefonía celular y el objetivo.
- Trabaja en las 4 bandas GSM (850/900/1800/1900)
- La operación del equipo se realiza totalmente sobre interfaz gráfica en sistema operativo Windows.
- Las llamadas interceptadas se guardan en formato .WAV, permitiendo fácilmente su copia a dispositivos pen-drive y su posterior reproducción en cualquier computadora.

El sistema de intercepción Maxx dispone de distintos modos de funcionamiento, de acuerdo a las necesidades y requerimientos del cliente. En la siguiente figura se muestra la arquitectura completa de un sistema de 3 canales (cantidad mínima para propósitos demostrativos):

Figura 7. Arquitectura del sistema de interceptación celular
Fuente: Cotización de la Empresa Maxx Technology S.A.



2.1.2.3 Factibilidad Económica

Tabla 17. Cuadro detallado de costos
Fuente: Iván Freire

CUADRO DETALLADO DE COSTOS														
TAREA O ACTIVIDAD	TIEMPO DURACIÓN (d)	RECURSOS HUMANOS						OTROS RECURSOS						COSTO POR TAREA O ACTIVID
		Director Proyecto			Analista de Requerimientos			EQUIPOS			MATERIALES			
		% partici-pación	Valor / hora	Valor parcial	% partici-pación	Valor / hora	Valor parcial	% partici-pación	Valor / hora	Valor parcial	Cantidad	Valor unitario	Valor parcial	
Elaboración del plan detallado de trabajo	0.5	1.00	30	120			0			0	1	5	5	125
Especificación de requerimientos	10	0.10	30	240	1	25	2000			0				2240
Reclutamiento	0	0.00	30	0			0			0				0
Investigación documental	2	0.10	30	48			0	2	200	6400	1	10	10	6468
Levantamiento de procesos	8	0.10	30	192			0			0	1	50	50	242
Racionalización	8	0.20	30	384			0			0				384
Elaboración de la Norma de procedimiento	2	0.30	30	144			0			0	1	20	20	164
Validación de la NP.	2	0.30	30	144			0			0				144
Aprobación de la NP.	2	1.00	30	480			0			0				480
Elaboración del plan de implantación de proces	0.5	1.00	30	120			0			0				120
Capacitación	2	0.50	30	240			0			0	1	50	50	300
Implantación de procesos	8	0.20	30	384			0			0	1	100	100	494
Evaluación de la implantación	2	0.50	30	240			0			0	1	20	20	260
Auditoría 1 de precertificación	1	1.00	30	240			0			0				240
Acompañamiento en correcciones	2	0.30	30	144			0			0				144
Auditoría 2 de precertificación	1	1.00	30	240			0			0				240
Acompañamiento en correcciones	2	0.30	30	144			0			0				144
Certificación	1	1.00	30	240			0			0				240
COSTO POR RECURSO	**54**			**3744**			**2000**			**6400**			**255**	**12429**

2.2 DISEÑO

2.2.1 Esquema general de la solución técnica

El presente proyecto se basa en los conceptos de la norma ISO/IEC 27002:2005, la misma que proporciona un conjunto de objetivos de control que refuerza los conceptos de Seguridad de la Información y en específico la Gestión de las Comunicaciones y Operaciones.

Para la cual se desarrolló dos Políticas de seguridad que norman las actividades de comunicación para la empresa confidencial desde ahora denominada EMPRESA DE TRANSPORTE DE VALORES. La primera política abarca los principios, objetivos, estándares utilizados y obligaciones. La segunda política detalla los controles específicos para las comunicaciones de radio y celular.

Política Preliminar de Seguridad de las Comunicaciones para la Empresa de Transporte de Valores

Articulo I. Términos y definiciones

Para la presente política se consideran las siguientes definiciones:

a) La seguridad de la información

Se define, en un ambiente empresarial, como la protección de la información contra la divulgación a personal no autorizado, modificación inadecuada y el no acceso cuando es requerida; de acuerdo al principio CIA[6] ampliamente aceptado.

La Seguridad de la Información es un catalizador para la continuidad del negocio, minimización del riesgo comercial, la maximización el retorno de las inversiones y la ampliación de las oportunidades comerciales.

b) Riesgo

Se define como una desviación positiva o negativa de un resultado esperado, debido a la falta total o parcial de información relacionada con la comprensión o conocimiento de un evento, su probabilidad de ocurrencia y consecuencias.

c) Gestión de Riesgos

Es un proceso sistemático que comprende la identificación, análisis y evaluación de riesgos; para determinar si estos deben ser modificados satisfaciendo los criterios de cada organización.

d) Alcance

La presente política constituye el conjunto de reglas y normas establecidas para brindar soporte a los objetivos de gobierno y los valores empresariales, mediante la implementación de controles a la EMPRESA DE TRASNPORTE DE VALORES.

[6] La Agencia Central de Inteligencia, cuyo nombre original en inglés es Central Intelligence Agency (CIA), es una de las mayores agencias de inteligencia del gobierno de Estados Unidos.

Artículo II. Objetivos

Los objetivos de la presente política son:

a) Establecer controles que permita a la empresa mitigar el riesgo operativo
b) Prevenir la intercepción de la información sensible
c) Promover comportamientos responsables con el uso de las comunicaciones.

Articulo III. Principios

La EMPRESA DE TRANSPORTE DE VALORES gestiona el envío y recepción de dinero de forma rentable y eficiente, aprovechando tecnología de punta, para automatizar sus procesos. Es por esto que la EMPRESA DE TRANSPORTE DE VALORES considera a la seguridad de la información como un elemento clave en el logro de sus objetivos, permitiéndole obtener el máximo beneficio de su plataforma tecnológica y de comunicaciones mientras mantiene controlados los riesgos asociados. Consecuente con la importancia reconocida, EMPRESA DE TRANSPORTE DE VALORES define los principios que regirán esta política a continuación:

a) Incluir, como un elemento clave, los principios y criterios técnicos de la Seguridad de la Información en las actividades empresariales.
b) Disponer de los recursos económicos y personal técnico especializado, que garanticen la implementación de programas de aseguramiento.
c) Controlar que las Tecnologías de la Información garanticen la Seguridad de la información y comunicaciones, en el cumplimiento del marco regulatorio de la normativa interna y procedimientos establecidos.
d) Promover la cultura de Seguridad de las Comunicaciones en todos los niveles de la empresa.

Artículo IV. Sobre el marco de referencia

Como marco de referencia principal se utiliza la norma ISO/IEC 27002:2005, dominio 10 Gestión de Comunicaciones y Operaciones, Objetivo de control 10.8 Intercambio de información, para el control y gestión de las comunicaciones de la Empresa de Transporte de valores, aplicándola según su orden jerárquico y especialidad. En caso de duda se observará la norma de rango superior.

El uso de otros estándares o marcos de referencia no están permitidos, a menos que exista la justificación necesaria para incluirlos y que su contenido no se contraponga con el marco principal de referencia o las buenas prácticas normalmente aceptadas.

Artículo V. Responsabilidades y obligaciones

Las autoridades de cualquier nivel jerárquico de la EMPRESA DE TRANSPORTE DE VALORES son responsables de la implementación de la presente política de acuerdo a su ámbito de acción y a las actividades asignadas en el plan de aseguramiento de la empresa.

Es obligación de todo el personal, contratistas y clientes de EMPRESA DE TRANSPORTE DE VALORES cumplir y hacer cumplir los lineamientos de la presente política.

a) El área de Talento Humano, será la responsable de comunicar al personal que ingresa a laborar a la EMPRESA DE TRANSPORTE DE VALORES, bajo cualquier modalidad contractual, sobre su obligación de cumplimiento con la Política de seguridad de las comunicaciones y los reglamentos o procedimientos adicionales derivados de esta.

b) Los propietarios de la información, entendiéndose como los responsables de su creación y explotación, tienen la obligación de clasificar, definir y documentar los niveles de protección y acceso a la misma.

c) Es responsabilidad del área de Seguridad de la Información de la EMPRESA DE TRANSPORTE DE VALORES, proponer y comunicar la Estrategia y el plan de aseguramiento. El área de Seguridad de la Información de EMPRESA DE TRANSPORTE DE VALORES será la responsable de revisar y proponer cambios al contenido de esta política, de forma periódica, considerando principalmente los ajustes que faciliten conseguir las metas empresariales, los requerimientos de las entidades de control y la regulación vigente.

d) La aprobación, de la presente política y sus modificaciones, será responsabilidad de las autoridades definidas en la normativa interna de la EMPRESA DE TRANSPORTE DE VALORES.

Artículo VI. Sanciones por incumplimiento

El incumplimiento de la política de Seguridad de la Información tiene como resultado la aplicación de diversas sanciones de acuerdo a las prescripciones de orden, obligaciones, prohibiciones y faltas disciplinarias establecidas en la normativa interna de la EMPRESA DE TRANSPORTE DE VALORES.

Política de comunicaciones seguras de radio y celular para la Empresa de Transporte de Valores

Estas políticas, cubren ámbitos específicos de la función de seguridad de las comunicaciones, y brindan guías más detalladas con respecto a las actividades de intercambio de información por medio de radio y telefonía celular.

Artículo I. Procedimientos de intercambio de información

Sección 1.01 Objetivo

Establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación de la EMPRESA DE TRANSPORTE DE VALORES.

Sección 1.02 Generalidades

a) El uso de dispositivos móviles para las comunicaciones de la EMPRESA DE TRANSPORTE DE VALORES, debe ser analizado de forma específica, considerando los riesgos y ventajas relacionadas con este tipo de dispositivos.
b) La asignación de privilegios de acceso en dispositivos móviles cumplirá con los mismos principios generales establecidos en la presente política.
c) Las medidas de seguridad específicas que se deberán incluir para el uso de dispositivos móviles son:
    - Encriptación de contenido
    - Borrado remoto
    - Respaldos periódicos
    - Restricción de instalación de aplicaciones de terceros

- Contratación de seguros especializados
- Capacitación a los usuarios de estas tecnologías

d) Las políticas referentes a dispositivos móviles, específicamente tabletas y teléfonos inteligentes, deben ser revisadas continuamente y validadas a medida que se implementen nuevas funcionalidades.

Sección 1.03 Métricas

Las métricas con las cuales se debe medir el éxito de la implementación de esta política son:

a) Número de violaciones de acceso por privilegios excesivos de los roles definidos.
b) Interrupción de las actividades debido a privilegios insuficientes.
c) Número de observaciones encontradas en auditorias por conflicto de intereses en los privilegios de acceso a la información empresarial.

Artículo II. Acuerdos de intercambio

Sección 2.01 Objetivo

Proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Sección 2.02 Generalidades

El área de comunicaciones es la responsable de verificar, monitorear y exigir los niveles de servicio con la empresa que brinde los enlaces de datos externos a la EMPRESA DE TRANSPORTE DE VALORES.

Los niveles de servicio deben estar documentados en acuerdos formales y deberán ser ajustados de acuerdo al monitoreo de la red y la carga efectiva de los enlaces.

Artículo III. Soportes físicos en tránsito

Sección 3.01 Objetivo

Proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Sección 3.02 Generalidades

a) Todos los sistemas que sean adquiridos de forma complementaria o que deban integrarse con las comunicaciones de la EMPRESA DE TRANSPORTE DE VALORES, deben mantener los estándares de seguridad definidos por la empresa.
b) Las validaciones de cumplimiento con las políticas y estándares deben ser verificados mediante procesos de prueba, antes y durante el periodo de adquisición formal.
c) Toda integración de un sistema de comunicaciones o nueva funcionalidad de los equipos que se agregue a esta política deben ser valorados en función del riesgo y de ser el caso se debe establecer los controles apropiados para tratar los mencionados.

Artículo IV. Mensajería electrónica

Sección 4.01 Objetivo

Proteger adecuadamente la información contenida en la mensajería electrónica.

Sección 4.02 Generalidades

a) Los archivos de claves criptográficas que forman parte de las comunicaciones deben estar protegidas contra modificación, pérdida y destrucción, mediante procedimientos de copias de respaldo, registros de auditoría y restricción de acceso.

b) Las claves comprometidas, por incidentes de seguridad o similares, deben ser destruidas o modificadas, considerando todos los aspectos de la continuidad del negocio.
c) En el caso de claves y certificados públicos se debe gestionar para que dichos elementos criptográficos sean verificados por una entidad certificadora reconocida, garantizando su autenticidad y el no repudio de la información generada por la EMPRESA DE TRANSPORTE DE VALORES.

Artículo V. Sistemas de información empresariales

Sección 5.01 Objetivo

Desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de geo localización.

Sección 5.02 Generalidades

a) Controlar el cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información por parte de la empresa contratada de servicios de geo localización.
b) Definir y comunicar la estrategia de seguridad de la información alineada con la estrategia de negocio.
c) Planificar, coordinar y mantener la arquitectura de comunicaciones seguras basado en la gestión de riesgos.
d) Formular y mantener el plan de contingencia de seguridad que garantice la disponibilidad, confidencialidad e integridad de la información.

2.2.2 Análisis de riesgo residual

Como se estableció en la sección 2.1.2.1 Factibilidad técnica del presente trabajo, se detalla un nuevo análisis posterior a la aplicación de los controles de la Política de comunicación segura, para obtener el riesgo residual que nos permite comparar el antes y después de aplicar las normativas. Y finalmente se diagrama el esquema de la solución técnica.

Tabla 18. Análisis de riesgo residual
Autor: Iván Freire

	Problema	Tipo	Control	Impacto	Probabilidad	Riesgo
1	Intercepción de comunicaciones	Mitigar	10.8.1 Políticas y procedimientos de intercambio de información	5	2	**10**
2	Inhibidor de señales celulares	Mitigar	10.8.5 Sistemas de Información Empresariales	5	2	**10**
3	Daño de equipos celulares o de radio	Mitigar	10.8.3 Soportes físicos en tránsito	4	2	**8**
4	Intercepción de GPS	Mitigar	10.8.2 Acuerdo de Intercambio	5	2	**10**

Comparación:

Antes de los Controles

Impacto	Probabilidad	Riesgo
5	4	**20**
5	4	**20**
4	3	**12**
5	4	**20**

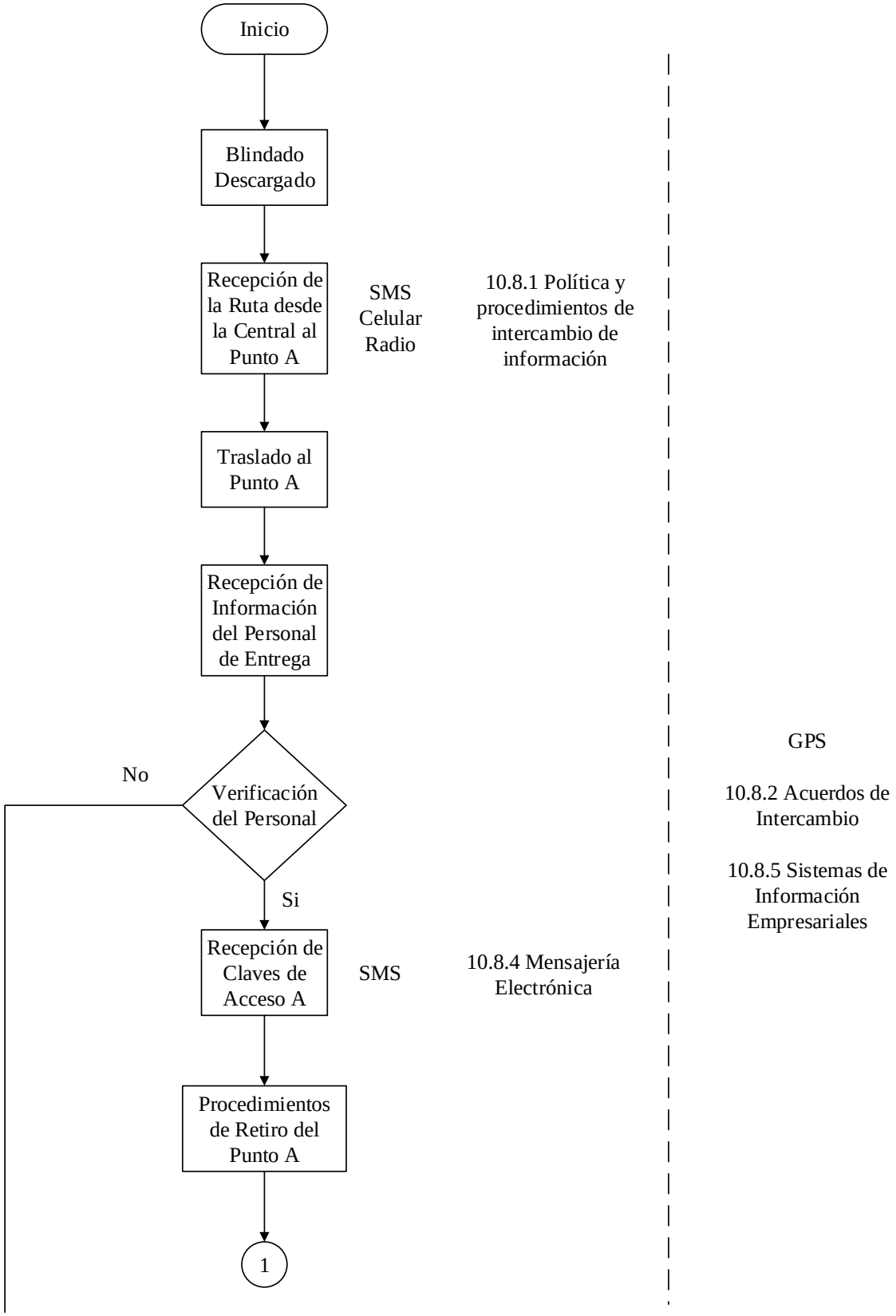
Después de los Controles

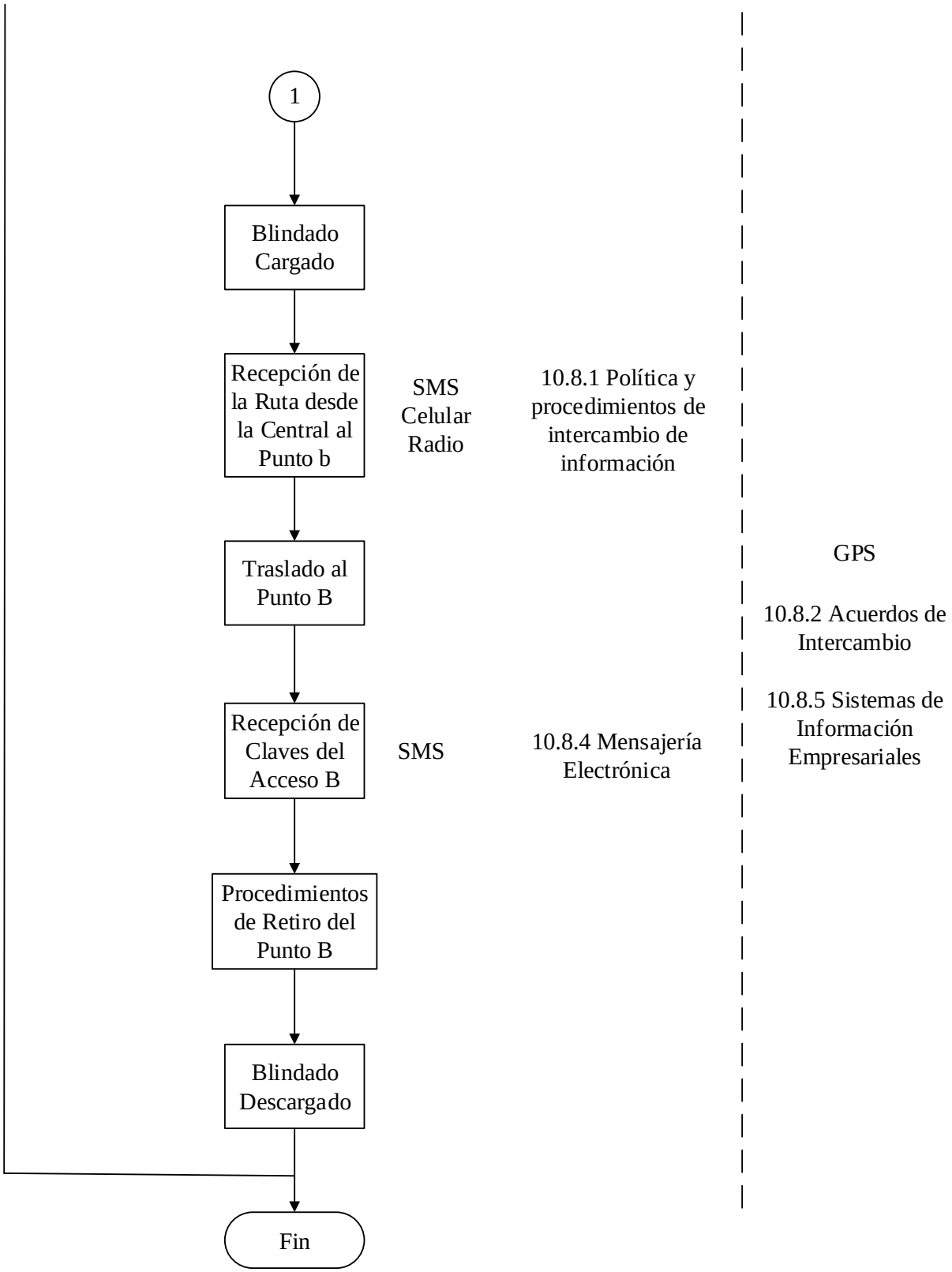
Impacto	Probabilidad	Riesgo
5	2	**10**
5	2	**10**
4	2	**8**
5	2	**10**

Ponderación:

Riesgo	Puntaje
Bajo	[0 - 4]
Medio	[5 - 8]
Alto	[9 - 14]
Muy alto	[15 - 20]

Figura 8. Recepción y Entrega de valores
Autor: Iván Freire




1
Blindado Cargado
Recepción de la Ruta desde la Central al Punto b
SMS
Celular
Radio
10.8.1 Política y procedimientos de intercambio de información
Traslado al Punto B
GPS
10.8.2 Acuerdos de Intercambio
Recepción de Claves del Acceso B
SMS
10.8.4 Mensajería Electrónica
10.8.5 Sistemas de Información Empresariales
Procedimientos de Retiro del Punto B
Blindado Descargado
Fin

CAPÍTULO III

RESULTADOS

3.1 CONSTRUCCIÓN

En este capítulo se enlista los procedimientos que se aplicaron en la implementación del presente proyecto, el cual inicia con el levantamiento de activos, además de otras herramientas de gran utilidad que identifican la importancia relativa de los diferentes procesos de los sistemas de comunicación, cuya información es considerada vulnerable.

Los pasos metodológicos, que se deben llevar a cabo para la implementación son los siguientes:

1. Levantamiento de activos.

2. Definición de procesos.

3. Análisis de riesgo inherente.

4. Estimación del impacto potencial.

5. Determinación de controles.

6. Riesgo residual.

3.1.1 Levantamiento de Activos

Se identificó los activos importantes asociados a cada sistema de comunicación, sus respectivos propietarios y su ubicación, posteriormente se elaboró un inventario con dicha información. El mismo debe ser actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

3.1.1.1 Clasificación de la Información

Se evaluó y se definió la información de acuerdo a las tres características en la cuales se define la seguridad, como son la confidencialidad, la integridad y la disponibilidad con diferentes niveles como se detalla a continuación:

a) Confidencialidad:

0- Información que es conocida y utilizada sin autorización por cualquier persona, sea empleado de la Empresa o no. PUBLICO.

1- Información que es conocida y utilizada por todos los empleados de la Empresa y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados causa riesgos o pérdidas leves para la Empresa, el Sector Público Nacional o terceros. RESERVADA – USO INTERNO

2- Información que sólo es conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Empresa, al Sector Público Nacional o a terceros. RESERVADA – CONFIDENCIAL

3- Información que sólo es conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Empresa, y cuya divulgación o uso no autorizados ocasiona pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

b) Integridad:

0- Información cuya modificación no autorizada se recupera fácilmente, o no afecta la operatoria de la Empresa.

1- Información cuya modificación no autorizada se repara aunque ocasiona pérdidas leves para la Empresa, el Sector Público Nacional o terceros.

2- Información cuya modificación no autorizada es de difícil reparación y ocasiona pérdidas significativas para la Empresa, el Sector Público Nacional o terceros.

3- Información cuya modificación no autorizada no es reparable, ocasionando pérdidas graves a la Empresa, al Sector Público Nacional o a terceros.

c) Disponibilidad

A continuación se detalla las posibles variables de confidencialidad, integridad y disponibilidad, para obtener una categorización de la información.

Tabla 19. Clasificación de la información
Autor: Iván Freire

Confidencialidad	Integridad	Disponibilidad	Total
3	3	3	9
3	3	2	8
3	2	3	8
2	3	3	8
3	3	1	7
3	1	3	7
1	3	3	7
3	2	0	6
3	0	3	6
0	3	3	6
3	2	0	5
2	3	0	5
1	3	1	5
3	1	0	4
2	2	0	4
1	3	0	4
3	0	0	3
2	1	0	3
1	1	1	3
2	0	0	2
1	1	0	2
1	0	1	2

Confidencialidad	Integridad	Disponibilidad	Total
1	0	0	1
0	1	0	1
0	0	1	1
0	0	0	0

Tabla 20. Categorización de la información
Autor: Iván Freire

De 9 a 7	Elevada
De 6 a 4	Normal
De 3 a 0	Reducida

3.1.1.2 Hardware

Se especificó todo el hardware del que dispone la Empresa para llevar a cabo sus procesos de comunicación.

Tabla 21. Activos de hardware de comunicación
Autor: Iván Freire

Cantidad	Tipo	Departamento
50	Radios	Área de Seguridad
20	Celulares	Área de Comunicaciones
2	GPS	Área de Control y geo posicionamiento

Tabla 22. Activos celulares
Autor: Iván Freire

Cantidad	Marca	Bandas	Conectividad	Tiempo batería
10	Samsung Galaxy	GSM 850 / 900 / 1800 / 1900 - HSDPA 850 / 900 / 1900 / 2100 - LTE Cat. 4	- GPS con soporte A-GPS - EDGE - 3G HSDPA - 4G LTE Cat. 4 - Wi-Fi 802.11 a/b/g/n/ac;	Hasta 10 horas

3.1.1.3 Software

En la descripción de software, se detallaron los programas que dispone la empresa de transporte de valores, esencialmente aquellos que están destinados a la comunicación. También, se especifica el nivel de protección del software con el que cuenta, para analizar posteriormente los riesgos a los que está expuesto.

Tabla 23. Activos de software
Autor: Iván Freire

Cantidad	Nombre	Descripción	Nivel	Licencia
1	Kaspersky Antivirus Mobile	Protección de datos en dispositivos móviles	Alto	Si
1	Firmware v2.1	Software de radios digitales	Medio	Si

3.1.1.4 Identificación de riesgos

Como se describe en la apartado 2.1.2.2 Método de Mósler se aplicó ésta sistemática para análisis del riesgo en el recorrido que realiza el vehículo blindado que transporta valores:

Primer escenario: la Agencia Bancaria X se está ubicada en la Av. Colon y Reina Victoria, en una zona urbana de alta circulación vehicular. Las vías de acceso son normales pavimentadas, pero no cuenta con parqueaderos. De a seguridad del sector, se conoce de algunos hechos de inseguridad, hay apoyo policial a unos 500 metros de la agencia. La agencia cuenta con guardianía fija y la iluminación es clara. El vehículo blindado no puede ingresar a la localidad, razón por la cual espera en las inmediaciones de la entidad bancaria y el custodio tiene que recorrer unos 30 metros hasta alcanzar la localidad.

Segundo escenario: la Agencia Bancaria Y se encuentra ubicada en la Av. Mariscal Sucre y Av. Los Libertadores. Es una zona comercial de alta circulación vehicular con vías de acceso asfaltadas de varios carriles. Es un sector donde esporádicamente se presentan hechos menores de inseguridad. A unos 800 metros de la agencia se encuentra un UPC. La agencia está ubicada en un edificio compartido con buena iluminación y vigilancia permanente. El vehículo blindado no puede ingresar a la agencia razón por la cual el automotor espera en las inmediaciones del edificio y el custodio tiene que caminar unos 30 metros para la entrega-recepción de valores.

Tercer escenario: la Agencia Bancaria Z está ubicada dentro del Centro Comercial Recreo al sur de Quito en la Av. Maldonado, zona comercial de alta circulación peatonal y vehicular con vías de acceso asfaltadas y parqueaderos. Se han presentado casos de asaltos, existe apoyo policial a menos de un kilómetro, se dispone de vigilancia en el centro comercial y vigilancia armada en la agencia con buena iluminación. El vehículo blindado no ingresa a un parqueadero cerrado y queda en las inmediaciones del centro comercial y el custodio tiene que caminar más de 30 metros para ingresar a la agencia.

En base a lo expuesto y aplicando el método Mósler se obtiene los siguientes resultados:

Tabla 24. Matriz de análisis y evaluación de riesgos de la empresa de transporte de valores. **Fuente:** Iván Freire

MATRIZ DE ANALISIS Y EVALUACION DE RIESGOS METODO MOSLER																					RIESGO TOTAL
N°	Escenario / Riesgo	AGENCIA X							AGENCIA Y							AGENCIA Z							
		F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	
1	Asalto	5	5	5	5	4	4	800	5	5	5	5	3	3	450	5	5	5	5	4	5	1000	750
2	Robo	5	4	4	4	3	3	324	5	4	4	4	3	3	324	5	4	4	4	4	4	576	408
3	Hurto	4	3	3	2	2	2	72	4	3	3	2	2	2	72	4	3	3	2	2	2	72	72
4	Fraude / Estafa	4	3	4	2	2	2	80	4	3	4	2	2	2	80	4	3	4	2	2	2	80	80
5	Incendio	5	5	5	4	3	2	270	5	5	5	4	3	3	405	5	5	5	4	3	3	405	360
6	Daño Mecánico	4	4	3	1	2	2	76	4	4	3	1	2	2	76	4	4	3	1	2	2	76	76
7	Accidente Transito	5	5	5	4	4	4	720	5	5	5	4	4	5	900	5	5	5	4	4	5	900	840
Escenario más crítico								781							769							1036	

VALOR ENTRE	CLASE DE RIESGO
2 Y 250	Muy reducido
251 Y 500	Reducido
501 Y 750	Normal
751 Y 1000	Elevado
1001 Y 1250	Muy elevado

Conclusión: En base a la matriz del Método Mósler, se tiene un riesgo elevado en las Agencias X e Y, y un riesgo muy elevado en la Agencia Z. Como riesgos potenciales se identifican, el asalto y accidente de tránsito. El escenario más crítico se presenta en la Agencia Z.

3.1.2 Acciones Preventivas y de control

Las acciones preventivas y de control encaminadas a minimizar los riesgos de la Empresa de transporte de valores, son:

- Socializar la Política de Seguridad de las comunicaciones seguras.
- Entrenar al personal en uso y manejo de las Políticas.
- Capacitar al personal en temas específicos como: Criptografía aplicada en las comunicaciones y Uso de frecuencias seguras.
- Realizar inspecciones internas periódicas con el fin de detectar, eliminar y prevenir riesgos y posibles peligros en las comunicaciones.
- Llevar un registro de accidentes e incidentes con el fin de tomar acciones correctivas, y preventivas.
- Investigar y analizar las causas de accidentes.
- Efectuar simulacros programados con el propósito de entrenar al personal.
- Contar con un registro actualizado y permanente del personal.
- Realizar el mantenimiento preventivo de los activos de comunicación.
- Verificación del perfecto funcionamiento de los equipos.

3.2 IMPLEMENTACIÓN

3.2.1 Introducción

La Empresa X se dedica al transporte de valores en la ciudad de Quito, en los últimos trimestres ha sufrido robos de sus blindados con indicios de que sus comunicaciones vía

radiofrecuencia o celular fueron interceptados, motivo por el cual se requiere una nueva arquitectura segura para sus comunicaciones. A continuación se detalla la implementación:

3.2.2 Levantamiento de activos

3.2.2.1 Hardware

La Empresa X dispone de los siguientes equipos de comunicación:

Tabla 25. Activos de la empresa de transporte de valores
Autor: Iván Freire

Cantidad	Tipo	Departamento
30	Radios	Área de Comunicaciones
10	Celulares	Área de Comunicaciones
1	GPS	Empresa Contratada

Se detalló cada tipo de comunicación:

Tabla 26. Celulares de la empresa de transporte de valores
Autor: Iván Freire

Cantidad	Marca	Bandas	Conectividad	Tiempo batería	Modelo
5	Samsung Galaxy S5	GSM 850 / 900 / 1800 / 1900 - HSDPA 850 / 900 / 1900 / 2100 - LTE Cat. 4	- GPS - EDGE - 3G HSDPA - 4G LTE - Wi-Fi 802.11 a/b/g/n/ac; - Bluetooth v4.0	Hasta 10 horas	

Cantidad	Marca	Bandas	Conectividad	Tiempo batería	Modelo
3	Nokia Lumia 520	GSM 850 / 900 / 1800 / 1900 - HSDPA 900 / 2100 o HSDPA 850 / 1900 / 2100	- GPS - EDGE - 3G HSUPA 5.76Mbps - Wi-Fi 802.11 b/g/n - Bluetooth v3.0	Hasta 8 horas	
2	BlackBerry Curve 8520	GSM 850 / 900 / 1800 / 1900	- EDGE - Wi-Fi - Bluetooth	Hasta 5 horas	

Tabla 27. Características del equipo de radio de la empresa de transporte de valores
Autor: Iván Freire

Cantidad	Marca	Bandas	Canales	Modelo
10	Motorola EP 450	438-470 MHz	16	

3.2.3 Análisis de Riesgo Inherente

Una vez identificado los activos de comunicación de la Empresa X, se identificó los procesos de transporte de valores del punto A al punto B.

Tabla 28. Matriz de procesos iniciales
Autor: Iván Freire

Proceso	Detalle
Retiro de Valores	- Se utiliza comunicación vía radio para las notificaciones de seguridad y ubicación. - Rastreo GPS del blindado
Transporte Punto a Punto	- Envío de rutas por medio de SMS, celulares o radio - Rastreo GPS del blindado - Cámaras internas de grabación y transmisión de video de vigilancia.
Verificación de Claves Acceso	- Se recibe claves de ingreso a bóvedas mediante SMS - Rastreo GPS del blindado
Entrega de Valores	- Confirmación de entrega de valores vía celular o radio - Rastreo GPS del blindado

Con los procesos identificados se realizó el análisis de riesgos inherentes, detallado en la siguiente tabla:

Tabla 29. Análisis de riesgo inherente de la empresa de transporte de valores
Autor: Iván Freire

	Problema	Impacto	Probabilidad	Riesgo
1	Intercepción de comunicaciones	5	4	**20**
2	Inhibidor de señales celulares	5	4	**20**
3	Daño de equipos celulares o de radio	4	3	**12**
4	Intercepción de GPS	5	4	**20**

Ponderación:

Riesgo	Puntaje
Bajo	[0 - 4]
Medio	[5 - 8]
Alto	[9 - 14]
Muy alto	[15 - 20]

Conclusión: Se tuvo un riesgo alto en todos los procesos de comunicación de la empresa de transporte de valores con problemas específicos, que se identificaron al observar la metodología de comunicación de un ambiente simulado.

3.2.4 Controles aplicados

3.2.4.1 Primer caso: Intercepción de comunicaciones

Aplicado a:

Comunicaciones por radio, celular y SMS.

Control:

Políticas de comunicaciones seguras de radio y celular para la Empresa de Transporte de Valores

Articulo I. Procedimientos de intercambio de información

Sección 1.02 Generalidades

c) Las medidas de seguridad específicas que se deben incluir para el uso de dispositivos móviles son:

Encriptación de contenido.

Soluciones designadas:

NIST: Análisis de vulnerabilidades para PBX (voz)

VIPER: incluye interfaz gráfica para el usuario, video en tiempo real VoIP, modificación de las funciones del teléfono IP, y soporte para varios códec de compresión.

WARVOX: es una suite de herramientas para explorar, clasificar, y auditar sistemas de telefonía.

3.2.4.2 Segundo caso: Inhibidor de señales celulares

Aplicado a:

SMS

Control:

Políticas de comunicaciones seguras de radio y celular para la Empresa de Transporte de Valores

Artículo II. Acuerdos de intercambio

Sección 2.02 Generalidades

a) El área de comunicaciones es la responsable de verificar, monitorear y exigir los niveles de servicio con la empresa que brinde los enlaces de datos externos a la EMPRESA DE TRANSPORTE DE VALORES.

Solución designada:

TRUECRYPT: software de cifrado de código abierto.

3.2.4.3 Tercer caso: Daño de equipos celulares o de radio

Aplicado a:

Comunicaciones por radio, celular y GPS

Control:

Políticas de comunicaciones seguras de radio y celular para la Empresa de Transporte de Valores

Artículo III. Soportes físicos en tránsito

Sección 3.02 Generalidades

a) Todos los sistemas que sean adquiridos de forma complementaria o que deban integrarse con las comunicaciones de la EMPRESA DE TRANSPORTE DE VALORES, deben mantener los estándares de seguridad definidos por la empresa.

Solución designada:

FOCA: Herramienta para por la extracción de metadatos en documentos públicos antes de proceder a su envío. La herramienta permite adicionalmente la realización de procesos en trabajos de auditoría web. La versión Free realiza búsqueda de servidores, dominios, URLs y documentos publicados, así como el descubrimiento de versiones de software en servidores y clientes.

3.2.4.4 Cuarto caso: Intercepción de GPS

Aplicado a:

GPS

Control:

Políticas de comunicaciones seguras de radio y celular para la Empresa de Transporte de Valores

Artículo V. Sistemas de información empresariales

Sección 5.02 Generalidades

a) Controlar el cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información por parte de la empresa contratada de servicios de geo localización.

Soluciones sugeridas:

Revisar los Acuerdos de Nivel de Servicio SLA periódicamente o previo a la renovación de los mismos, específicamente en los puntos de envío y recepción de posicionamiento.

3.2.5 Riesgo residual

Una vez que se aplicó los controles necesarios a la nueva arquitectura de comunicaciones para la empresa transporte de valores, se vuelve a realizar el análisis de riesgo, el resultado que se obtuvo se identifica como riesgo residual.

Tabla 30. Análisis de riesgo residual de la Empresa X
Autor: Iván Freire (ISO/IEC, 2005)

	Problema	Tipo	Control	Impacto	Probabilidad	Riesgo
1	Intercepción de comunicaciones	Mitigar	Artículo I. Procedimientos de intercambio de información	5	1	**5**
2	Inhibidor de señales celulares	Mitigar	Artículo II. Acuerdos de Intercambio	5	1	**5**
3	Daño de equipos celulares o de radio	Mitigar	Artículo III. Soportes físicos y en transito	4	2	**8**
4	Intercepción de GPS	Mitigar	Artículo V. Sistemas de información empresariales	5	1	**5**

Comparación:

Antes de los Controles

Impacto	Probabilidad	Riesgo
5	4	**20**
5	4	**20**
4	3	**12**
5	4	**20**

Después de los Controles

Impacto	Probabilidad	Riesgo
5	1	**5**
5	1	**5**
4	2	**8**
5	1	**5**

Ponderación:

Riesgo	Puntaje
Bajo	[0 - 4]
Medio	[5 - 8]
Alto	[9 - 14]
Muy alto	[15 - 20]

Conclusión: Se ha disminuido el riesgo inicial de las comunicaciones de la empresa de transporte de valores.

CAPÍTULO IV

DISCUSIÓN

4.1 CONCLUSIONES

- Luego del estudio, análisis e implementación de las políticas de comunicación segura de radiofrecuencia y celular basada en la norma ISO/IEC 2700:2005, en la empresa de transporte de valores, permitió identificar deficiencias, como la falta de encriptación de la información enviada por medio de radiofrecuencia y el mínimo uso de estándares de control en los procesos actuales de comunicación.

- Con la práctica de intercepción de comunicación vía radiofrecuencia, se evidenció la vulnerabilidad de este tipo de comunicación y fue la base para desarrollar los controles que permitieron mitigar el riesgo identificado.

- Posterior al análisis de riesgo inherente, se desarrolló dos políticas de seguridad de la información que sugirieron varios cambios a los procesos de comunicación para radio y celular, que proporciona una guía a seguir en los procesos de operaciones seguras.

- Lograr una norma específica y adaptada al modelo de negocio de transporte de valores en su sección de comunicaciones permitió reducir el riesgo residual y aporta a las futuras actualizaciones.

- La selección del Dominio 10: Gestión de las Comunicaciones y Operaciones, de la norma ISO/IEC 27002 en su versión 2005, facilitó la elaboración de la política de seguridad, puesto que sus controles son específicos para los procedimientos de intercambios de información en el transporte de valores.

4.2 RECOMENDACIONES

Se recomienda:

- Realizar un seguimiento a la correcta aplicación del modelo y evaluar trimestralmente los resultados obtenidos utilizando la metodología de Análisis de riesgo.

- Elaborar diagramas de flujo y de procesos con rutas específicas obligatorias a seguir por parte de los vehículos blindados, lo que permitirá disminuir el riesgo de intercepción de comunicaciones. Y planificar ambientes simulados para mejorar las políticas de seguridad y los procesos de transporte de valores.

- Continuar con el desarrollo de los objetivos de control, 10.9 Servicios de comercio electrónico y 10.10 Supervisión de la norma ISO/IEC 27002:2005 para obtener registro previos para auditorias futuras.

BIBLIOGRAFIA

Tanenbaum, A. (2003). *Redes de computadoras.* Nueva York: Pearson Educación.

Areitio Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Editorial Paraninfo.

Carmen de Pablos Heredero. (2004). *Informática y comunicaciones en la empresa.* Madrid: ESIC Editorial.

ENISA. (2010). *Information security risks, opportunities and.* Obtenido de http://enisa.europa.eu

ISO/IEC. (2005). *Norma ISO 27002:2005*. Obtenido de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

Mera, A. S. (2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP Petroecuador deacuerdo a la norma ISO/IEC 27002 y Cobit 5.* Sangolquí: Escuela Politécnica del Ejército.

Merino Bada, C., & Cañizares Sales, R. (2011). *Implantación de un sistema de gestion de seguridad de la información según ISO 21001.* Madrid: Fundación confemetal.

Mora, H. (2008). *Manual del vigilante de seguridad.* Madrid: Enfoque Ediciones.

Murillo, M. &. (2003). *Logistica de seguridad.* Quito: Enfoque Ediciones.

Nacional, U. T. (2014). *Políticas de seguridad de la información.* Buenos Aires: Comite de seguridad de la información.

Nichols, R., & Lekkas, P. (2003). *Seguridad para comunicaciones inalámbricas.* New York: Mc Graw Hill.

Rodriguez Paez, A. G. (2013). *Guía general de la aplicación de las medidas mínimas de seguridad exigidas a las entidades financieras y de transporte de valores en el ecuador.* Escuela Politécnica del Ejército.

Romo, D., & Joffre, V. (2012). *Análisis em implementación de la norma ISO 27002 para el departamento de sistemas de la universidad politécnica salesiana sede guayaquil.* Guayaquil: Universidad Politécnica de Guayaquil.

Sosa, R. (2005). *Manual de medios técnicos de seguridad.* Bogotá: Coleccion de seguridad.

Técnicos, E. T. Estudios. (1998). *Seguridad en entidades bancarias.* Madrid: Mapfre.

ANEXOS

Reportajes de prensa

EL UNIVERSO

Miércoles, 22 de octubre, 2014 | 12h12

Un muerto y tres heridos deja asalto a blindado en Sucumbíos

VÍCTOR GÓMEZ | Sucumbíos

(Actualizado a las 23:40)

Una persona falleció y otras tres resultaron heridas este miércoles durante el asalto a un carro blindado de la compañía Vaserum, que había contratado el Banco Pichincha para el traslado de 3'700.000 dólares, informó la entidad financiera en un comunicado.

El hecho ocurrió al mediodía en el kilómetro 100 de la vía Lago Agrio-Quito, en el sector del volcán Reventador, en Limoncocha. El vehículo transportaba dinero con destino a Lago Agrio, provincia de Sucumbíos.

"Los vehículos fueron embestidos en la carretera por dos volquetas que lograron detener su avance. De estas se bajaron un numeroso grupo de delincuentes quienes, con bombas Molotov y armas sofisticadas, entre las que luego se identificaron un fusil FAL, una ametralladora y un fusil AK47, abrieron fuego y buscaron incendiar los vehículos. Los guardias se defendieron hasta agotar sus municiones, momento en el que debieron abandonar los blindados", detalló el banco.

El fallecido es **Marco Salazar**, añadió el comunicado del Banco Pichincha.

Los heridos, guardias de la compañía según informaron las Fuerzas Armadas en un **comunicado**, fueron trasladados al hospital Dr. Marco Vinicio Iza, de Nueva Loja.

El dinero fue recuperado luego de un enfrentamiento armado entre los presuntos asaltantes y la Policía, que acudió a apoyar a los guardias de la compañía.

Según las Fuerzas Armadas, en manos de los presuntos delincuentes se encontraron 2 fusiles FAL (peruano), 1 fusil AK (ruso), 1 alimentadora, 300 cartuchos calibre 7.62 mm, 12 alimentadoras, 1 alimentadora de fusil AK y 3 cargas explosivas.

Además, confirmaron que prestaron su contingente en apoyo a la persecución y captura de los delincuentes que asaltaron vehículo blindado en el sector del volcán Reventador.

Una fuente indicó que existen detenidos para investigaciones.

Fuente: http://www.eluniverso.com/noticias/2014/10/22/nota/4134716/muerto-tres-heridos-deja-asalto-blindado-lago-agrio

ecuavisa

DINERO DEL BLINDADO ASALTADO ERA DE BANCO PICHINCHA

MIÉRCOLES 22 DE OCTUBRE DE 2014 09:36 PM

El Banco Pichincha informó hace minutos que los dos blindados de la compañía Vaserum transportaban 3 millones 700 mil dólares que iban destinados a las agencias de la entidad financiera en la provincia de Napo.

Además, recalcaron que producto de la explosión uno de los blindados se incendió y provocó que se quemen un elevado número de fundas que contenían el efectivo. Otros paquetes con dinero fueron sustraídos por los asaltantes que luego huyeron del lugar.

RECOMENDACIONES

NOTICIAS

Un muerto y 2 heridos tras el asalto a blindado en Lago Agrio

Los vehículos blindados número 100 y 101 de la compañía Vaserum fueron interceptados en el kilómetro 100 de la vía que une Quito con Lago agrio. Fruto del asalto, uno de los guardias del blindado perdió la vida, y dos más quedaron heridos.

Para el asalto, los delincuentes habrían usado cargas explosivas. el comandante de la policía, Fausto Tamayo, confirmó lo sucedido.

"Producto de esto incendian los dos blindados. hay algún dinero que se ha sustraído y otro tanto que está bajo evidencia. también hay algunos detenidos y un fallecido", indicó Tamayo.

Los dos heridos fueron trasladados a Lago Agrio, en donde fueron ingresados en el Hospital Marco Vinicio Iza.

Según la información de los testigos, una volqueta se colocó al frente y otra en la parte posterior de los blindados para bloquear su paso, luego los hicieron explotar para llevarse el dinero.

Reportado el hecho, se inició una persecución en la que participó la Policía y las Fuerzas Armadas, que terminó con la captura de dos de los presuntos asaltantes y se decomisaron tres fusiles, 13 alimentadoras y tres cargas explosivas.

Fuente: http://www.ecuavisa.com/articulo/lo-mas-visto-del-2014/lo-mas-visto-octubre/85733-dinero-del-blindado-asaltado-era-banco

El Diario
Manabita de libre pensamiento

Delincuentes que asaltaron blindado ya están identificados, según jefe de Policía

Lunes 04 Agosto 2014 | 12:27

Romel Tapia, jefe de la Policía Judicial, aseguró que la entidad ya tiene identificados a los delincuentes que intervinieron en el asalto a un blindado esta mañana, en los exteriores de Servipagos, en Portoviejo.

En declaraciones a Manavisión, Tapia agregó que en el hecho intervinieron 8 delincuentes, quienes se movilizaban en una camioneta.

De acuerdo a esa misma fuente, se conoció que uno de los presuntos ladrones resultó herido durante el asalto, el cual fue trasladado por sus cómplices al interior del vehículo, para luego darse a la fuga.

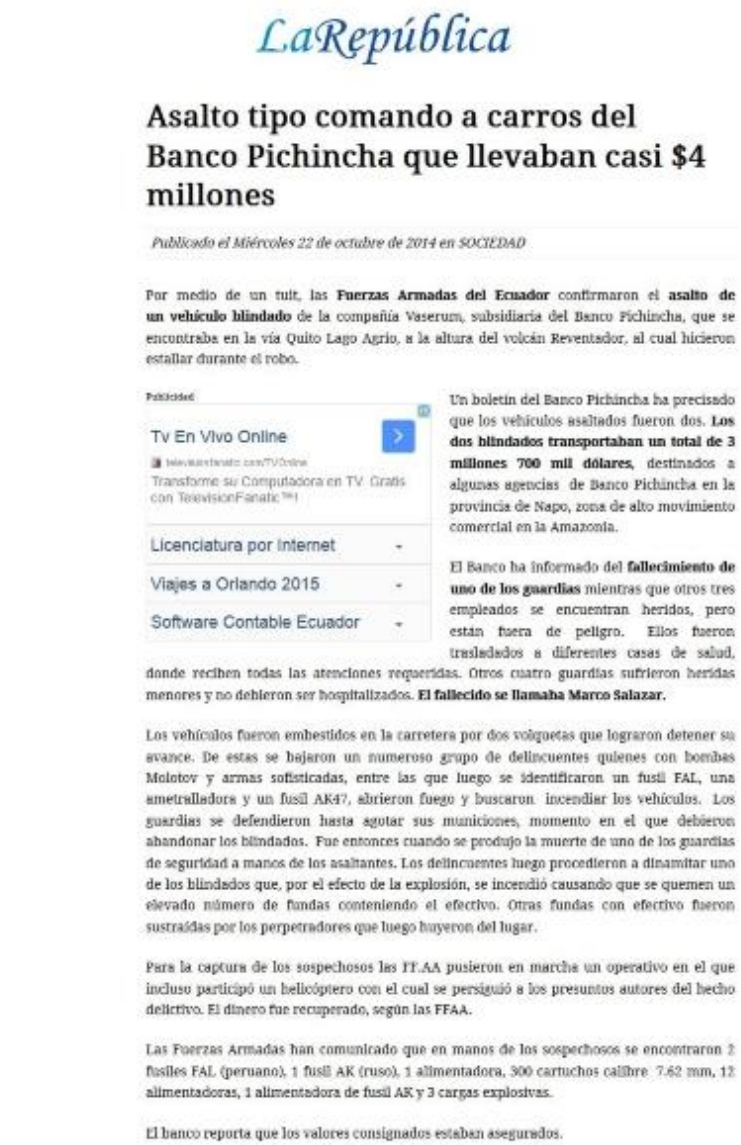
Luego de ello, el herido fue trasladado a otro auto, mientras que la camioneta fue abandonada en el callejón León, cerca de la calle Gabriela Mistral.

HERIDOS. Durante el asalto también resultó herido un guardia de la compañía G4S, quien fue trasladado a una casa de salud. Mientras que uno de sus compañeros también recibió atención médica, al sufrir un ataque de pánico.

HECHOS. La mañana de este lunes, varios **delincuentes abordaron a los guardias de un blindado**, cuando se disponían a entregar una bolsa con dinero a la agencia de Servipagos ubicada en la avenida Manabí.

Durante el asalto se registró un cruce de balas, que dejó dos heridos.

En el lugar de los hechos se vivieron momentos de temor, ya que los comerciantes del lugar se sintieron en peligro.



LaRepública

Asalto tipo comando a carros del Banco Pichincha que llevaban casi $4 millones

Publicado el Miércoles 22 de octubre de 2014 en SOCIEDAD

Por medio de un tuit, las **Fuerzas Armadas del Ecuador** confirmaron el **asalto de un vehículo blindado** de la compañía Vaserum, subsidiaria del Banco Pichincha, que se encontraba en la vía Quito Lago Agrio, a la altura del volcán Reventador, al cual hicieron estallar durante el robo.

Un boletín del Banco Pichincha ha precisado que los vehículos asaltados fueron dos. **Los dos blindados transportaban un total de 3 millones 700 mil dólares**, destinados a algunas agencias de Banco Pichincha en la provincia de Napo, zona de alto movimiento comercial en la Amazonia.

El Banco ha informado del **fallecimiento de uno de los guardias** mientras que otros tres empleados se encuentran heridos, pero están fuera de peligro. Ellos fueron trasladados a diferentes casas de salud, donde reciben todas las atenciones requeridas. Otros cuatro guardias sufrieron heridas menores y no debieron ser hospitalizados. **El fallecido se llamaba Marco Salazar.**

Los vehículos fueron embestidos en la carretera por dos volquetas que lograron detener su avance. De estas se bajaron un numeroso grupo de delincuentes quienes con bombas Molotov y armas sofisticadas, entre las que luego se identificaron un fusil FAL, una ametralladora y un fusil AK47, abrieron fuego y buscaron incendiar los vehículos. Los guardias se defendieron hasta agotar sus municiones, momento en el que debieron abandonar los blindados. Fue entonces cuando se produjo la muerte de uno de los guardias de seguridad a manos de los asaltantes. Los delincuentes luego procedieron a dinamitar uno de los blindados que, por el efecto de la explosión, se incendió causando que se quemen un elevado número de fundas conteniendo el efectivo. Otras fundas con efectivo fueron sustraídas por los perpetradores que luego huyeron del lugar.

Para la captura de los sospechosos las FF.AA pusieron en marcha un operativo en el que incluso participó un helicóptero con el cual se persiguió a los presuntos autores del hecho delictivo. El dinero fue recuperado, según las FFAA.

Las Fuerzas Armadas han comunicado que en manos de los sospechosos se encontraron 2 fusiles FAL (peruano), 1 fusil AK (ruso), 1 alimentadora, 300 cartuchos calibre 7.62 mm, 12 alimentadoras, 1 alimentadora de fusil AK y 3 cargas explosivas.

El banco reporta que los valores consignados estaban asegurados.

Fuente: http://www.larepublica.ec/blog/sociedad/2014/10/22/hacen-estallar-auto-blindado-durante-robo/

Práctica de intercepción

Introducción

En esta Práctica desarrolló el objetivo específico del proyecto de Tesis titulado:

"Diseño e implementación de una arquitectura de comunicaciones seguras de radio y celular para una empresa confidencial basada en el estándar ISO 27000"

Objetivo Específico

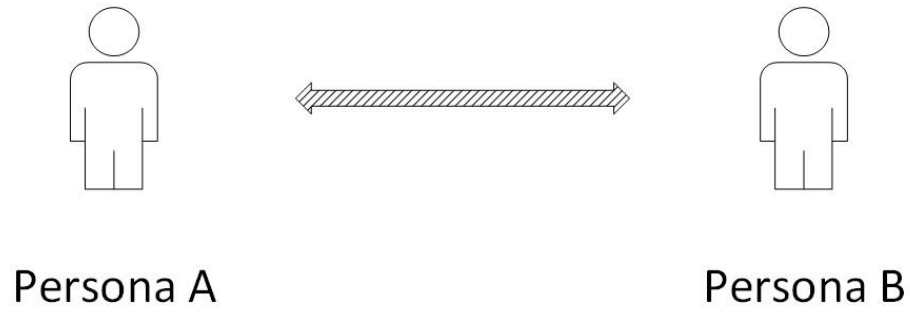
- Analizar la seguridad de la información en las transmisiones de radio utilizando un equipo interceptor.

Equipos

- 2 Radios de comunicación
- Escáner de Frecuencias (interceptor)

Desarrollo

1er Escenario de comunicación: Inicial

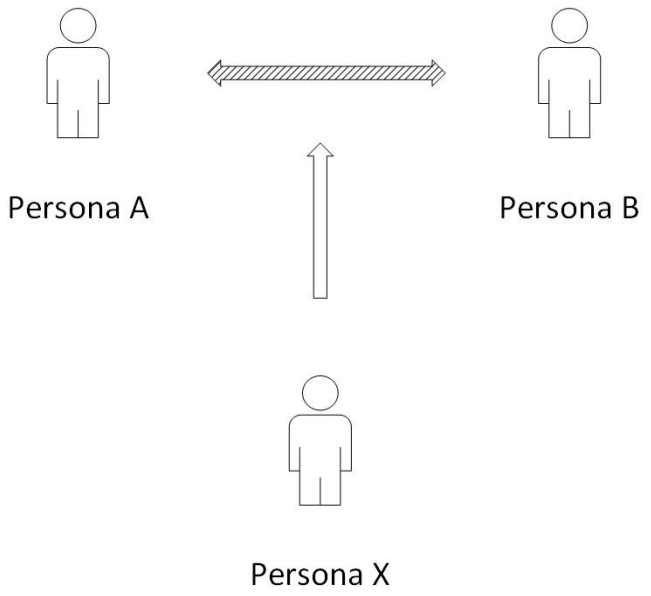


- La Persona A inicia la comunicación desde un lugar apartado.
- La Persona B recibe el mensaje

Mensaje:

"Latitud Norte 0 grados 18 minutos, 0 segundos; Longitud Oeste 79 grados, 1 minuto, 0 segundos"

2do Escenario de comunicación: Interceptada

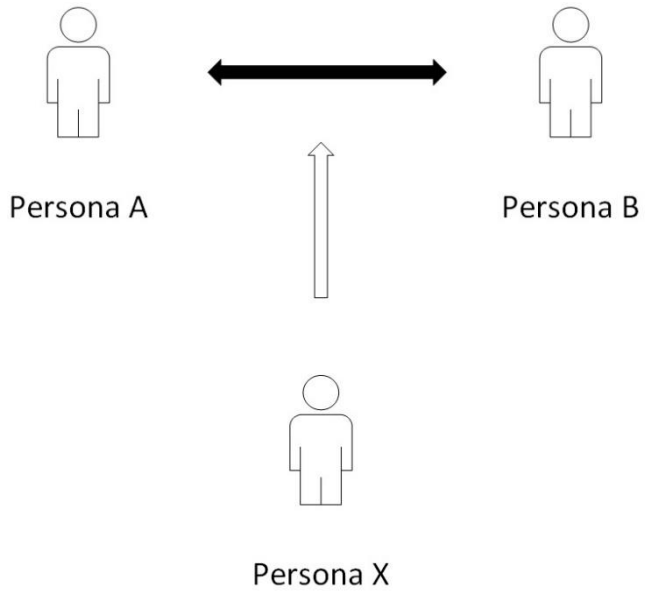


- La Persona A inicia la comunicación desde un lugar apartado.
- La Persona B recibe el mensaje
- La Persona X intercepta la comunicación y recibe el mensaje.

Mensaje:

"Inicia la ruta por las calles Colon y 9 de Octubre"

3er Escenario de comunicación: Implementando Controles



Control a utilizar:

10.8.1 Políticas y procedimientos de intercambio de información

Metodología:

Encriptación de la información

- La Persona A inicia la comunicación desde un lugar apartado y cifra su mensaje.
- La Persona B recibe el mensaje, y lo descifra
    - Argentina -> Contraseña
    - Juega -> Ingreso
    - Copa América -> Bóveda
- La Persona X intercepta la comunicación y pero no sabe el mensaje.

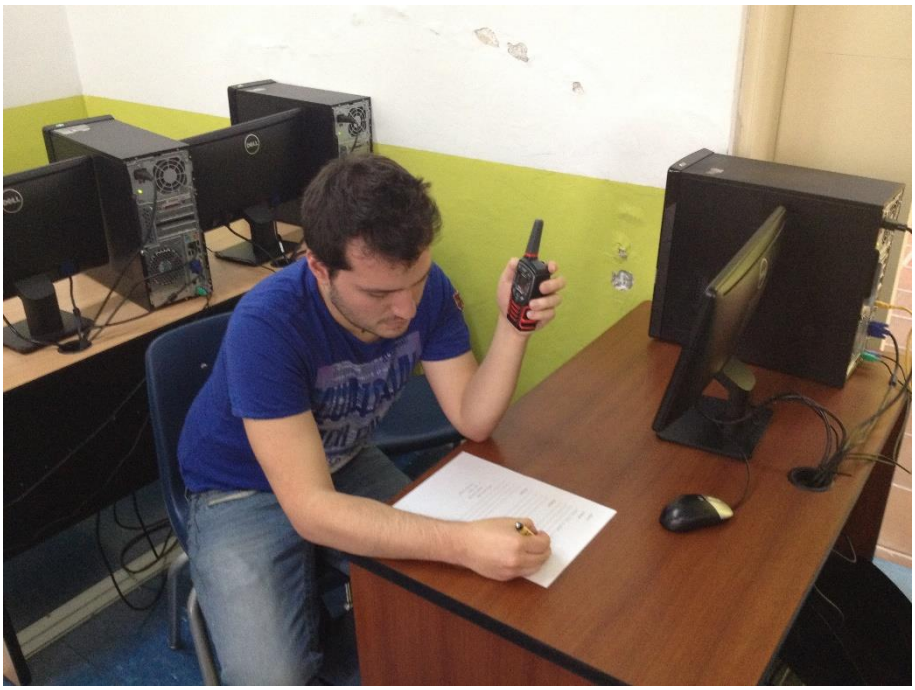
Mensaje:

"Argentina juega Copa América"

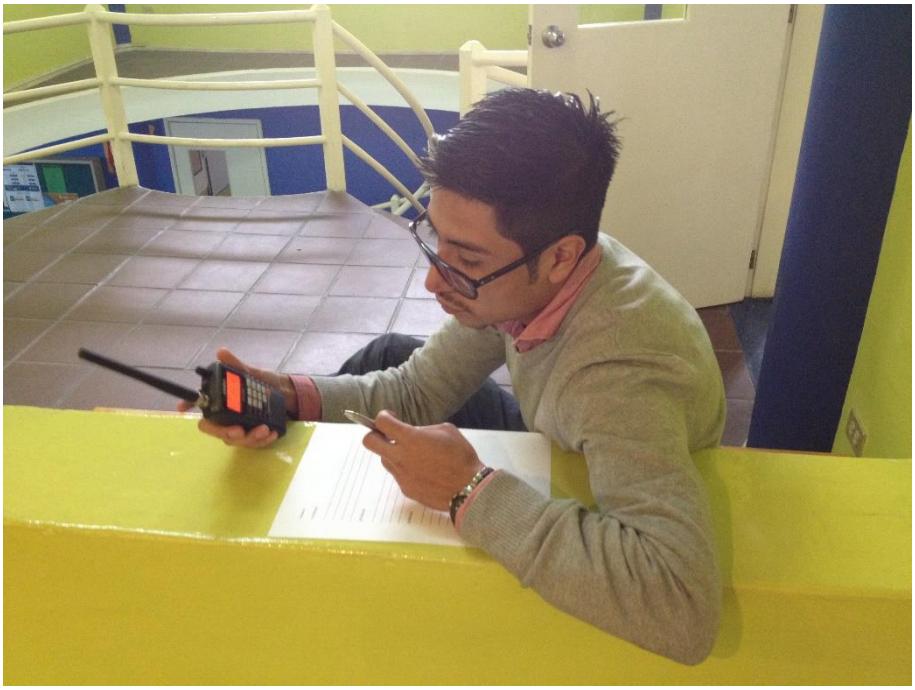
Representaciones

Persona A – Emisor

Persona B – Receptor



Persona X - Interceptor



Resultados:

Persona A

1er Mensaje:

"Latitud Norte 0 grados 18 minutos, 0 segundos; Latitud Oeste 79 grados, 1 minuto, 0 segundos"

2do Mensaje:

"Inicia la ruta por las calles Colon y 9 de Octubre"

3er Mensaje:

"Argentina juega Copa América"

Persona B

1er Mensaje:

Latitud Norte 0 grados Bpnts Latitud Oeste 79 grados 1 min 05

2do Mensaje:

Inicia la ruta por las calles Colón y 9 de Octubre

3er Mensaje:

Argentina Juega Copa América

Contraseña Ingreso Bóveda

- Utiliza el siguiente código
  - Argentina -> Contraseña
  - Juega -> Ingreso
  - Copa América -> Bóveda

5

Persona X

1er Mensaje:

2do Mensaje:

Colon y 9 de octubre
Recta Colon y 9 de octubre
Inicio la ruta por las calles colon y 9 de Octubre

3er Mensaje:

Argentina juega copa america

6

Conclusiones:

- Se evidenció el estado actual de las comunicaciones vía radiofrecuencia, al interceptar las varios escenarios de comunicación vía radio con un escáner de frecuencias o equipo interceptor.
- Al aplicar el control de la norma ISO/IEC 27002:2005 en su dominio, Gestión de las comunicaciones, objetivo, Políticas y procedimientos de intercambio de información, se mitigó el riesgo de intercepción.

Video Práctica

Adjunto en el CD.

Norma ISO 27002:2005