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

Autor: Ivan Freire

EL PROBLEMA

- Robos a automotores blindados
- Intercepción en las comunicaciones y sistemas de geo posicionamiento de los mismos.

OBJETIVO GENERAL

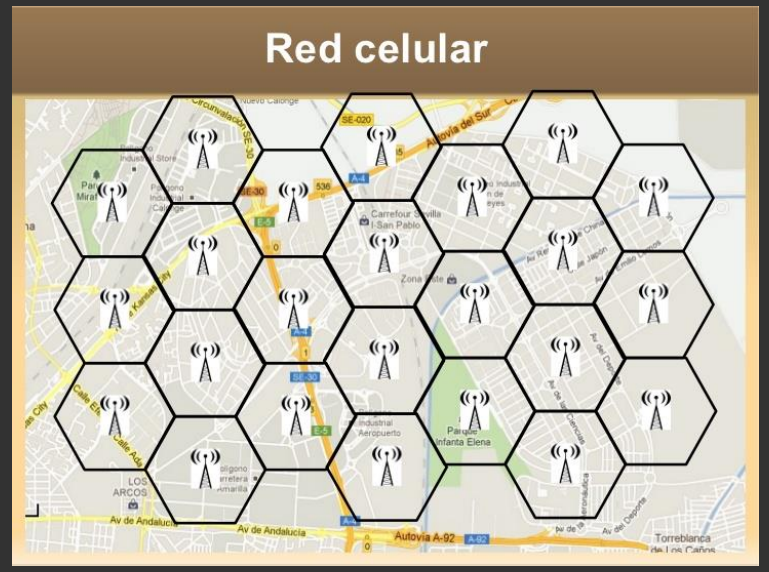
- Diseñar una arquitectura de comunicación segura, basada en los puntos asociados al dominio 10 Gestión de comunicaciones y operaciones, del estándar ISO/IEC 27002:2005.

OBJETIVO 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.

MARCO TEÓRICO

- Comunicaciones
  - Móviles
  - Redes celulares y de radiocomunicación
  - Sistema global para las comunicaciones móviles GSM
  - SMS



MARCO TEÓRICO

- Seguridad Móvil
  - Protección de las comunicaciones
  - Vulnerabilidades en sistemas telefónicos
  - Grados de seguridad

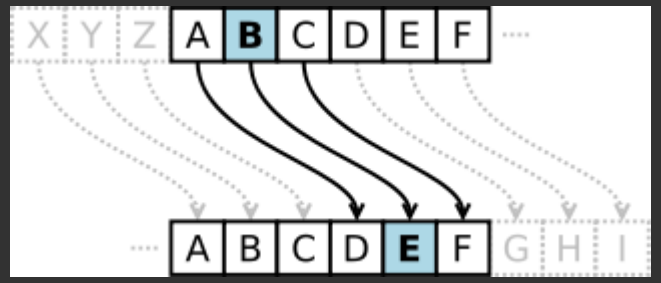
RIESGO		PROBABILIDAD			
		1 (Poco Frecuente)	2 (Frecuencia normal)	3 (Frecuente)	4 (Muy frecuente)
IMPACTO	5 (Extremo)	0	1	0	2
	4 (Mayor)	0	0	1	0
	3 (Moderado)	1	1	0	0
	2 (Menor)	1	0	0	0
	1 (Insignificante)	1	1	1	1

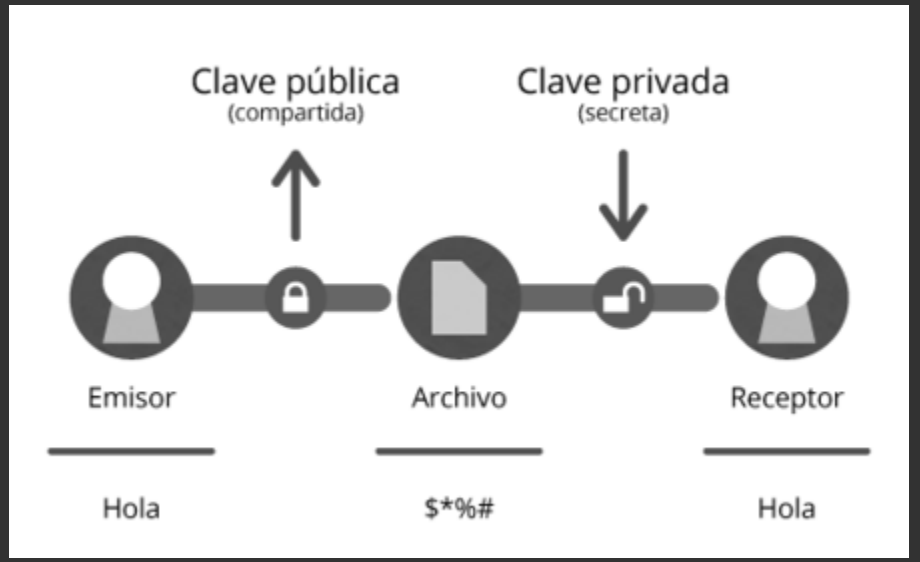
Riesgo = Probabilidad * Impacto

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

MARCO TEÓRICO

- Criptografía
  - Ocultación
  - Criptografía digital





ISO/IEC

- ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. (Merino Bada & Cañizares Sales, 2011)

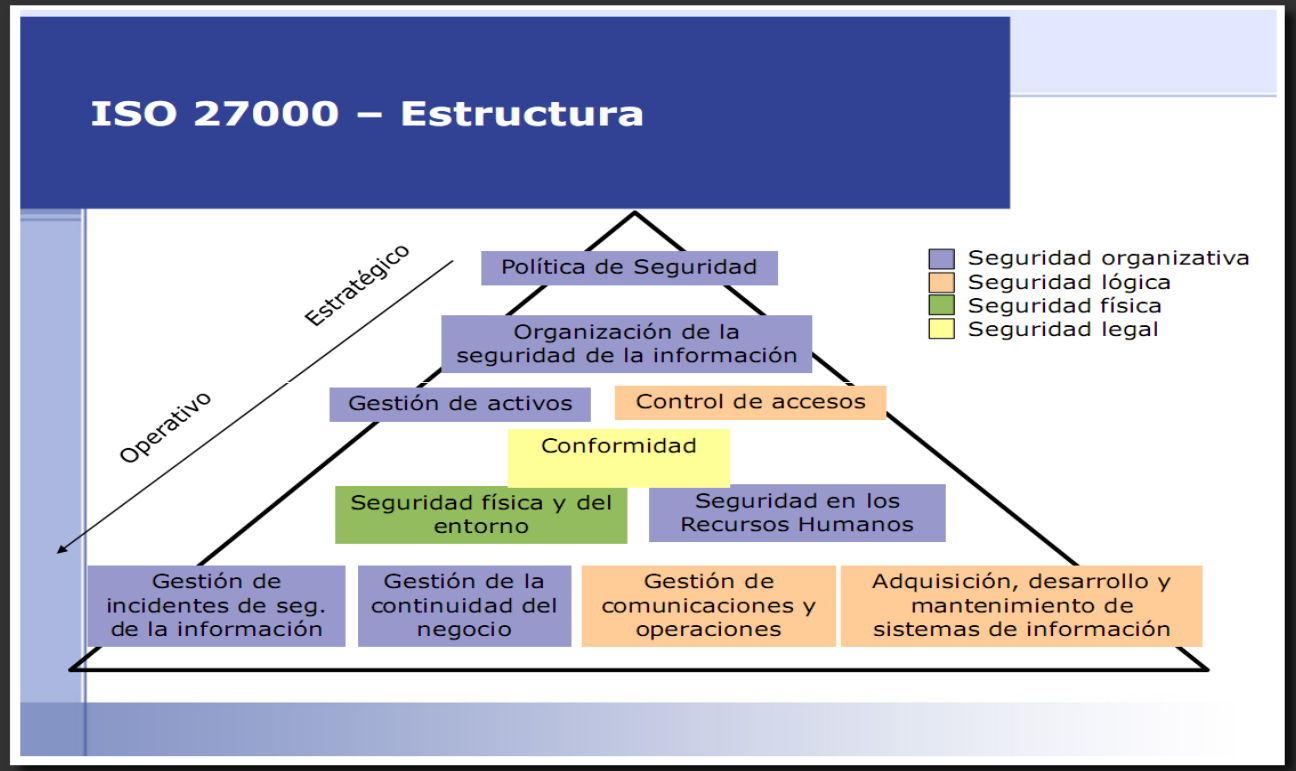
International Organization for Standardization

SERIE 27000

- 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.

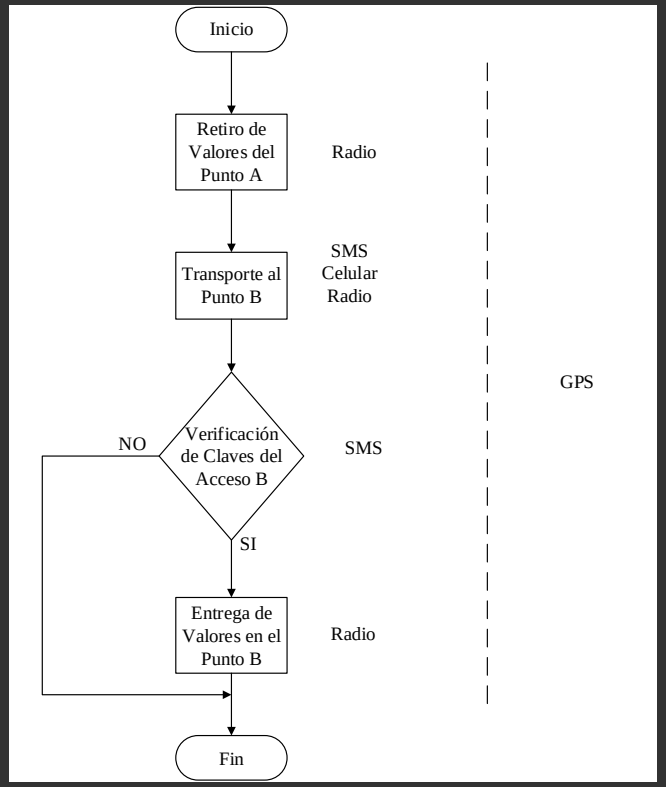
ISO/IEC 27002:2005

- Contiene 39 objetivos de control
- Divididos en 11 dominios de seguridad
- 133 controles.
- Para el presente trabajo se aplicó el dominio de Gestión de comunicaciones y operaciones.



METODOLOGÍA

- Esquema Inicial de Entrega y Recepción de valores



METODOLOGÍA

- Matriz de Observación Inicial

Proceso	Detalle
Proceso 1	Radio
Proceso 2	SMS GPS Radio
Proceso 3	SMS GPS
Proceso 4	Celular Radio

METODOLOGÍA

- Análisis FODA

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	Perdida 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

FACTIBILIDAD TÉCNICA

- Análisis de riesgo inherente

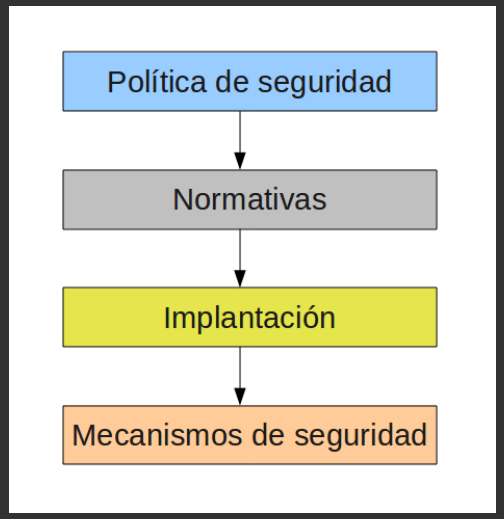
	Problema	Impacto	Probabilidad	Riesgo
1	Intercepción de comunicaciones	5	4	**20**
2	Inhibidor de señales celulares	5	4	**20**
3	Daño de equipos celulares o de radio	4	3	**12**
4	Intercepción de GPS	5	4	**20**

FACTIBILIDAD TECNOLÓGICA

- **Equipo Uniden BC125AT**
- 500 Canales con Etiquetas: Le permite nombrar todos los canales para facilitar la identificación de quién habla.
- Bandas aéreas civiles y militares:
- Servicio de búsqueda
- Modo de banda corta y Pasos
- Pantalla LCD retroiluminada
- Tamaño compacto

DISEÑO

- La presente propuesta 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 comunicaciones vía radio y celular para EMPRESA DE TRANSPORTE DE VALORES



POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES DE LA EMPRESA DE TRANSPORTE DE VALORES

- Articulo I Términos y Definiciones
- Artículo II. Objetivos
- Articulo III. Principios
- Artículo IV. Sobre el marco de referencia
- Artículo V. Responsabilidades y obligaciones
- Artículo VI. Sanciones por incumplimiento

POLÍTICAS ESPECÍFICAS DE COMUNICACIONES SEGURAS DE RADIO Y CELULAR PARA LA EMPRESA DE TRANSPORTE DE VALORES

- Articulo I. Política y procedimientos de intercambio de información
- Artículo II. Acuerdos de intercambio
- Artículo III. Soportes físicos en tránsito
- Artículo IV. Mensajería electrónica
- Artículo V. Sistemas de información empresariales

PRÁCTICA DE INTERCEPCIÓN

ANÁLISIS DE RIESGO RESIDUAL

	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

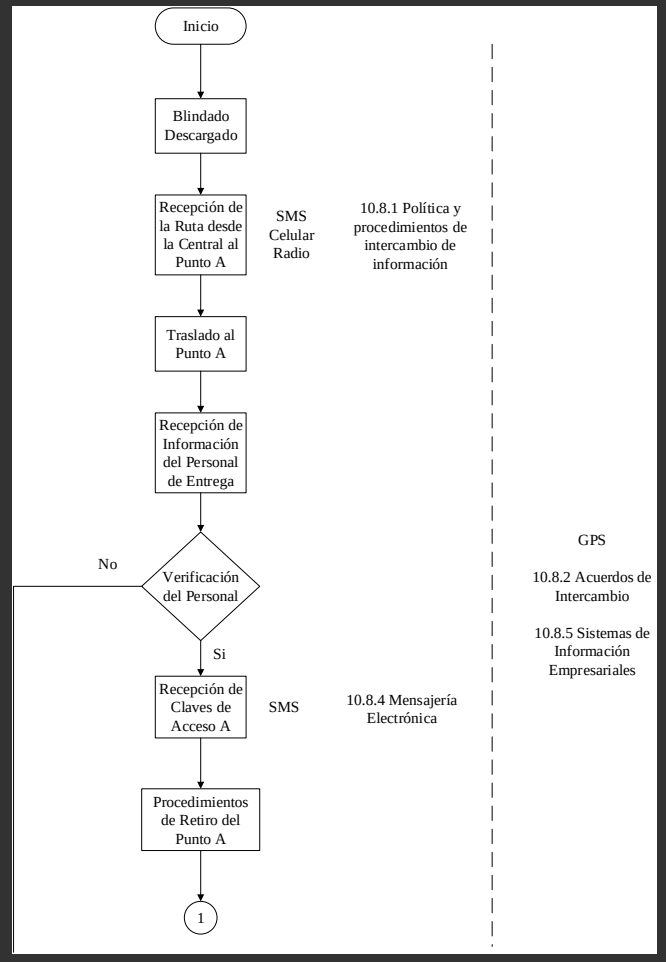
Antes de los Controles

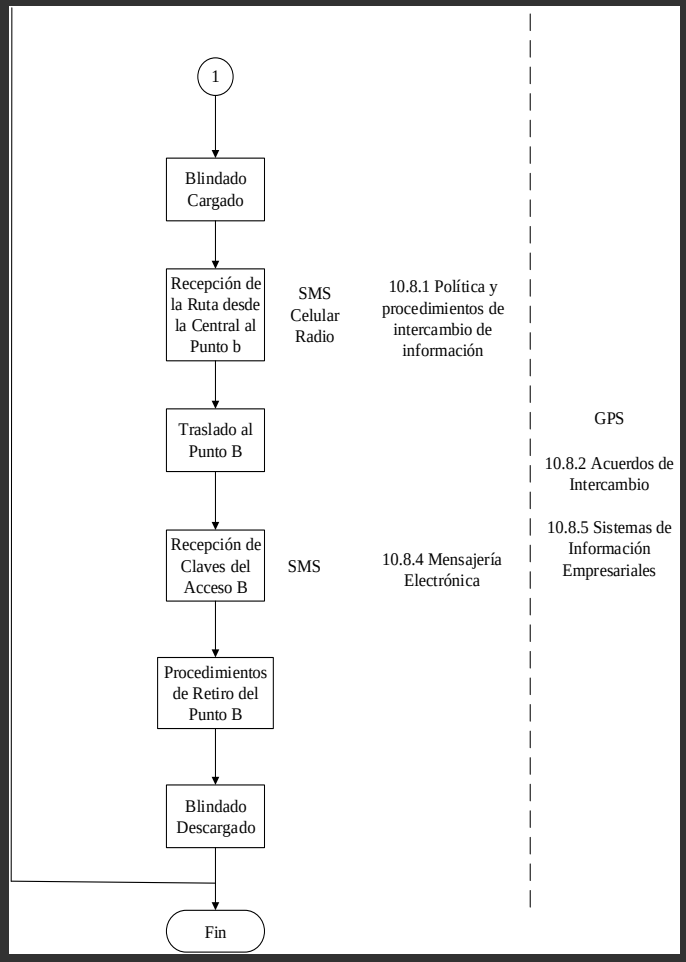
Impacto	Probabilidad	Riesgo
5	4	20
5	4	20
4	3	12
5	4	20

Después de los Controles

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

ESQUEMA GENERAL DE LA SOLUCIÓN





CONSTRUCCIÓN

- 1. Levantamiento de activos
- 2. Procesos
- 3. Análisis de riesgo inherente
- 4. Estimación del impacto potencial
- 5. Determinación de controles
- 6. Riesgo residual

IMPLEMENTACIÓN

- La Empresa confidencial 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 radios o celulares fueron interceptados, motivo por el cual se requiere una nueva arquitectura para sus comunicaciones. A continuación se detalla la implementación:

LEVANTAMIENTO DE ACTIVOS

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	
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	

LEVANTAMIENTO DE ACTIVOS

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

MATRIZ DE PROCESOS INICIALES

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

ANÁLISIS DE RIESGO INHERENTE DE LA EMPRESA X

	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

DETERMINACIÓN DE CONTROLES 1ER PROBLEMA INTERCEPCIÓN DE COMUNICACIONES

- **Política 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**

DETERMINACIÓN DE CONTROLES
1ER PROBLEMA: INTERCEPCIÓN DE COMUNICACIONES

- **Aplicado a:**
  - Comunicaciones por radio, celular y SMS

DETERMINACIÓN DE CONTROLES
2ER PROBLEMA: INHIBIDOR DE SEÑALES CELULARES

- **Política 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 será 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.

DETERMINACIÓN DE CONTROLES
2ER PROBLEMA: INHIBIDOR DE SEÑALES CELULARES

- **Aplicado a:**
  - Comunicaciones por celular
  - Sistemas GPS

DETERMINACIÓN DE CONTROLES
3ER PROBLEMA: DAÑO DE EQUIPOS CELULARES O DE RADIO

- **Política 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, deberán mantener los estándares de seguridad definidos por la empresa.

DETERMINACIÓN DE CONTROLES
3ER PROBLEMA: DAÑO DE EQUIPOS CELULARES O DE RADIO

- **Aplicado a:**
  - Comunicaciones por radio, celular
  - Sistemas GPS

DETERMINACIÓN DE CONTROLES
4TO PROBLEMA: INTERCEPCIÓN DE GPS

- **Política 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.

DETERMINACIÓN DE CONTROLES
4TO PROBLEMA: INTERCEPCIÓN DE GPS

- **Aplicado a:**
  - Sistemas GPS

RIESGO RESIDUAL

	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

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

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.

CONCLUSIONES

- 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.

- 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.

RECOMENDACIONES

- 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.

RECOMENDACIONES

- 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.

FIN DE LA PRESENTACIÓN

Gracias