Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO

Kenny Albanez Aceituno
Asesorado por el Ing. Jaime Alejandro García Soto

Guatemala, octubre de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA
DE LA FACULTAD DE INGENIERÍA
POR

KENNY ALBANEZ ACEITUNO

ASESORADO POR EL ING. JAIME ALEJANDRO GARCÍA SOTO

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL 1	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Luis Pedro Ortíz de León
VOCAL V	Agr. José Alfredo Ortíz Herincx
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing. Cesar Augusto Fernández Cáceres
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, en agosto de 2005.

Kenny Albanez Aceituno

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
ESCUELA DE CIENCIAS Y SISTEMAS

Guatemala 21 de octubre de 2009

Señores
Comisión de Revisión de Trabajos de Graduación
Carrera de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala
Guatemala, Ciudad

Respetables Señores:

El motivo de la presente es informarles que como asesor del estudiante Kenny Albanez Aceituno
He procedido a revisar el trabajo de graduación titulado Análisis Comparativo de las Técnicas de Surveillance con enfoque Bancario y que de acuerdo a mi criterio el mismo se encuentra concluido y cumple con los objetivos definidos al inicio.

He tenido reuniones periódicas con el estudiante y luego de haber revisado cuidadosamente el trabajo, considero que cumple con los requisitos de calidad y profesionalismo que deben caracterizar a un futuro profesional de la Informática.

Sin otro particular me suscribo de ustedes,

Atentamente,

Ing. Jaime Alejandro García Soto

[Firma]

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 28 de Abril de 2010

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **KENNY ALBANEZ ACEITUNO,** titulado: **"ANÁLISIS COMPARATIVO DE LAS TÈCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO",*** *presentado por el estudiante KENNY ALBANEZ ACEITUNO, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pèrez Turk
Director, Escuela de Ingenierìa Ciencias y Sistemas

Guatemala, 11 de octubre
2010

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 311.2010

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **ANÁLISIS COMPARATIVO DE LAS TÉCNICAS DE SURVEILLANCE CON ENFOQUE BANCARIO,** presentado por el estudiante universitario **Kenny Albanez Aceituno,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, 11 de octubre de 2010.

/gdech

DEDICATORIA

A Dios Por su ayuda, su apoyo y su amor en todo momento, a Él le debo todo lo que he logrado y lo que espero lograr.

A mis padres Adán Antonio Albanez Díaz y Marilúz de Albanez, por su amor sus sabios consejos y por su apoyo desde el inicio hasta la culminación de mis estudios.

A mis hermanos Marilena, Lesbia, Adán, Mirna, Rosa y Fernando, por su apoyo y sus consejos.

A mi asesor Ing. Jaime Alejandro García Soto, por compartir sus experiencias y profesionalismo, además de sus consejos y apoyo.

A mis amigos Por su amistad, compañerismo y tantos momentos compartidos. Porque cada uno de ellos alcance sus metas y que con el pasar del tiempo no olvidemos la amistad que forjamos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Algoritmo — Conjunto de sentencias o instrucciones en lenguaje nativo, los cuales expresan la lógica de un programa.

API (Aplication Program Interface) — Es el conjunto de rutinas del sistema que se pueden usar en un programa para la gestión de entrada y salida, gestión de ficheros etc.

Aplicación — Programa que realiza una serie de funciones y con el cual trabajamos en el ordenador.

App!et — Pequeño programa hecho en lenguaje Java.

Archivo — Unidad de información almacenada en el disco con un nombre específico. Tienen una extensión consistente en tres caracteres que lo identifican en su tipo o lo relacionan con un programa determinado.

Backup — Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

Base de datos — Es un almacenamiento colectivo de las bibliotecas de datos que son requeridas y organizadas para cubrir sus requisitos de procesos y recuperación de información.

Basilea Ciudad europea en donde se llevó a cabo la definición de estatutos para evaluar y prevenir el riesgo financiero.

Biometría Ciencia que estudia todo aquello relacionado con la identificación de una persona por medio de sus atributos físicos como la piel, ojos, huella digital, formación ósea, etc.

Cliente Computadora o programa que se conecta a servidores para obtener información. Un cliente sólo obtiene datos, no puede ofrecerlos a otros clientes sin depositarlos en un servidor. La mayoría de las computadoras que las personas utilizan para conectarse y navegar por Internet son clientes.

Cliente / Servidor Sistema de organización de interconexión de computadoras según el cual funciona Internet, así como otros tantos sistemas de redes. Se basa en la separación de las computadoras miembros en dos categorías: las que actúan como servidores (oferentes de información) y otras que actúan como clientes (receptores de información).

Dataveillance Se refiere a la vigilancia de datos o sea,

vigilancia aplicada a los datos que viajan en paquetes sobre la Internet o en documentos y más frecuentemente usada en el correo electrónico.

Dato

El término que se usa para describir las señales con las cuales trabaja la computadora es dato. Aunque las palabras dato e información muchas veces son usadas indistintamente, existe una diferencia importante entre ellas. En un sentido estricto, los datos son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

Encriptación

Método para convertir los caracteres de un texto de modo que no sea posible entenderlo si no se lo lee con la clave correspondiente. Es utilizado para proteger la integridad de información secreta en caso de que sea interceptada. Uno de los métodos más conocidos y seguros de encriptación es el PGP.

Entorno gráfico

Sistema operativo en el que la información que aparece en pantalla aparece representada en forma gráfica, como es el caso de Windows.

Escáner	Dispositivo periférico que copia información impresa mediante un sistema óptico de lectura. Permite convertir imágenes, por ejemplo de fotografías, en imágenes tratables y que pueden ser almacenadas por la computadora. El proceso de conversión se denomina digitalización. El término inglés scanner significa explorar o rastrear.
Hardware	Componente físico de la computadora. Por ejemplo el monitor, la impresora o el disco rígido. El hardware por sí mismo no hace que una máquina funcione. Es necesario, además, instalar un software adecuado.
Hacker	También conocido como pirata informático. Es una persona que tiene conocimientos sólidos de informática y que usa dichos conocimientos para robar información y violar la privacidad de personas y empresas.
Información	Es lo que se obtiene del procesamiento de datos, es el resultado final. Instrucción o sentencia, conjunto de caracteres que se utilizan para dirigir un sistema de procesamiento de datos en la ejecución de una operación.

Inteligencia artificial

Rama de la computación que analiza a la computadora y sus posibilidades de poseer inteligencia. La IA estudia las habilidades inteligentes de razonamiento, capacidad de extracción de conclusiones y reacciones ante nuevas situaciones de las computadoras y sus programas. El razonamiento es parecido al del cerebro humano (no es lineal, se aprende de cada situación).

Interfase

Cara visible de los programas. La interfase abarca las pantallas y su diseño, el lenguaje usado, los botones y los mensajes de error, entre otros aspectos de la comunicación computador - persona.

Internet

La red de computadoras más extendida del planeta, que conecta y comunica a más de 50 millones de personas. Nació a fines de los años sesenta como ARPANet y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar qué tipo de computadoras son, para intercomunicarse

utilizan el protocolo TCP/IP. Las computadoras que utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en general a través en un tipo de conexión llamado dial-in, utilizando un módem y una línea telefónica.

IP Protocolo de Internet definido en el RFC 791. Confirma la base del estándar de comunicaciones de Internet. El IP provee un método para fragmentar y rutear la información. Es inseguro, ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.

IP número o dirección IP Address. Dirección numérica asignada a un dispositivo de hardware conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números y cada uno de ellos puede ser de O a 255, las direcciones IP se agrupan en clases.

Red Dos o más computadoras conectadas para cumplir una función, como compartir periféricos (impresoras), información (datos, sistema de ventas) o para comunicarse (correo electrónico). Existen varios tipos de redes: según su estructura jerárquica se catalogan en

	redes cliente / servidor, con computadoras que ofrecen información y otras que sólo consultan información, y las peer-to-peer, donde todas las computadoras ofrecen y consultan información simultáneamente. A su vez, según el área geográfica que cubran, las redes se organizan en LANs , IVIANs ó WANs.
Software	Componentes intangibles (programas) de las computadoras. Complemento del hardware. El software más importante de una computadora es el sistema operativo.
Surveillance	Palabra inglesa que significa “vigilancia” y se refiere a toda aquella técnica, tecnología o acción de vigilancia que se emplea sobre algo o alguien.
Sniffer	Programa que captura cualquier información que viaje sobre una red y almacena dicha información para su posterior lectura.
W3C World Wide Web consortium	Organización que desarrolla estándares para guiar la expansión de la Web. Su Website es http://www.w3.org/.

WWW World Wide Web o W3	Conjunto de servidores que proveen información organizada en sitios, cada uno con cierta cantidad de páginas relacionadas. La Web es una forma novedosa de organizar toda la información existente en Internet a través de un mecanismo de acceso común de fácil uso, con la ayuda del hipertexto y la multimedia. El hipertexto permite una gran flexibilidad en la organización de la información, al vincular textos disponibles en todo el mundo. La multimedia aporta color, sonido y movimiento a esta experiencia. El contenido de la Web se escribe en lenguaje HTIVIL y puede utilizarse con intuitiva facilidad mediante un programa llamado navegador. Se convirtió en el servicio más popular de la red y se emplea cotidianamente para los usos más diversos: desde leer un diario de otro continente hasta participar de un juego grupal.

RESUMEN

Desde tiempos antiguos se han implementado técnicas de vigilancia y control dirigidas hacia personas, entidades jurídicas y tecnológicas, con el fin de brindar seguridad y tranquilidad en la realización de sus actividades regulares sin problemas y de la mejor manera.

Con el paso del tiempo y de la evolución en el aspecto informático, tanto en hardware como software, se ha observado el desarrollo de esta área en los diferentes ámbitos de la vida cotidiana, permitiendo así sacar el mejor provecho y ofrecer un resultado que permita brindar seguridad y tranquilidad a sus clientes en el caso de una empresa, a sus ciudadanos en el caso de un país y a la familia en caso de los hogares.

En los tiempos modernos vigilar y controlar ha llegado a convertirse en pilares importantes en las empresas, debido a que han aparecido personas inescrupulosas que cometen actos ilícitos y delincuenciales, aprovechándose de la antigüedad o vulnerabilidad de estas tecnologías, por lo mismo es que se tiene que ir evolucionando y fusionando técnicas para ofrecer un mejor nivel de desempeño y eficacia. Entidades como las financieras y de seguridad, son las que han logrado sacarle más provecho al uso y mezcla de estas técnicas y tecnologías para ofrecer a sus clientes tranquilidad y confianza, por lo mismo, dichas entidades han permitido que nuevos nichos de negocios se encuentren en desarrollo y algunos otros que se habían quedado atrás suban su nivel de nuevo.

Esta modernización y nuevas tecnologías conllevan a un dilema social como el respeto a la privacidad. Qué nivel de seguridad y vigilancia se debe implementar de forma que no se atente contra la privacidad y libre locomoción de las personas es la pregunta a contestar por cualquier entidad que quiera implementar esta tecnología. Por lo mismo la vigilancia a nivel de país es más restringida y delimitada de forma que no se atente contra dichos principios. A nivel empresarial se puede aumentar el nivel de vigilancia y control pero, al igual que a nivel del país, todo tiene un límite en cuestión, no invadir la privacidad de las personas.

El uso de Internet para realizar transacciones de compra, venta, inversión, etc. se ha vuelto muy común en nuestros tiempos, pero con esto se ha abierto una nueva brecha en donde la vigilancia y el control ha tenido que entrar con fuerza y con mayor urgencia porque se han visto ilícitos, como: la suplantación de identidad, robo de información de tarjetas de crédito, manejo ilícito de fondos a través de portales de bancos, por mencionar algunos.

En cuanto a entidades financieras, se ha llegado también a niveles altos de vigilancia, en transacciones internas, tomando en consideración los recientes eventos financieros que llevaron a una crisis a nivel mundial de la cual se ha iniciado una recuperación lenta. Tratando de evitar dichos problemas, se creó el comité de Basilea en el año de 1988 conformado por representantes de los mayores bancos a nivel mundial, cuyo objetivo primordial era evitar las crisis como la vista en nuestros tiempos. Se generaron acuerdos llamados BASILEA 1, 2 y 3 que enmarcan y delimitan el accionar de dichas entidades, así como, el uso de la tecnología para vigilar y prever cualquier situación adversa en el ámbito financiero. El problema que se vivió en este tiempo se derivó de que no todos los bancos llevaron a cabalidad la implementación de dichos acuerdos

por el mismo detalle de que les limitaba en su accionar en cuestiones de préstamos y movimiento de dinero.

Un aspecto interesante de la vigilancia en las entidades financieras es que permite controlar el flujo de dinero de forma que se pueda identificar transacciones anómalas o sospechosas provenientes de actos ilícitos, que por lo mismo, puedan afectar a dichas entidades en su buen nombre y estabilidad. Con la creciente necesidad de personas inescrupulosas de lavar dinero o de esconder el origen del mismo, se ha llevado a emplear mejores vigilancias en las transacciones físicas o por la web para evitar que entidades financieras sean usadas como escudos en hechos ilícitos contra terceras personas.

En estos tiempos en donde los escándalos financieros están a la vuelta de la esquina, la tecnología no podía quedarse por un lado, ya que es cuando más se necesita mantener una estrecha vigilancia a las entidades financieras para evitar dichos problemas. Con la tecnología se puede mantener un constante control en el capital de riesgo de las entidades para evitar a tiempo que estos problemas afecten a las personas y consumidores finales.

OBJETIVOS

General

Investigar, detallar y analizar las diferentes tecnologías de vigilancia, tanto de personas como de datos, para entender mejor el beneficio que estas le proveen a una entidad financiera.

Específicos

1. Investigar y detallar la tecnología que se utiliza para vigilar, delimitar sus alcances y definir sus pros y contras.

2. Analizar los riesgos que tienen las entidades financieras y definir como la tecnología puede ayudar a minimizar dichos riesgos.

3. Definir un marco comparativo en donde se pueda observar frente a frente las técnicas de vigilancia actuales con las modernas para encontrar un balance entre lo ya conocido y lo nuevo, que le brinde seguridad y confianza a los clientes de las entidades financieras.

INTRODUCCIÓN

El hombre ha practicado la vigilancia a lo largo de milenios. El texto de Sun Tsu, El arte de la guerra, escrito en el siglo V A.C. contiene detalles sobre la vigilancia y el uso de espías. Durante el último siglo se han producido crecientes avances tecnológicos en las prácticas de vigilancia, así como en las maneras de evitarla o de contrarrestarla.

Existen dos clases generales de vigilancia: directa e indirecta. La diferencia principal radica en que la vigilancia directa puede dar a quien la aplica una idea de las actividades de una persona u organización en el presente y, mediante un buen análisis, determinar sus planes futuros. La vigilancia indirecta únicamente proporciona acceso a las acciones pasadas a través de la información generada diariamente, por ello cualquier inferencia que se pueda hacer de las posibles actividades en el presente o en el futuro son susceptibles de error.[1]

La vigilancia ha sido un aspecto que ha tomado gran importancia en nuestros tiempos debido al aumento en la criminalidad a nivel mundial y también a los problemas financieros que se han venido suscitando a nivel mundial. [2]

En los tiempos antiguos era necesaria la vigilancia, pero era poco utilizada en la vida cotidiana y las personas comunes no tenían mayor conocimiento de técnicas y tecnología de vigilancia, esto se veía con frecuencia a nivel militar o a nivel país debido a las constantes amenazas de guerra que vinieron después de las guerras mundiales, pero tuvo su explosión en la llamada Guerra Fría donde era común saber de espionaje y vigilancia. Esto último dio paso al inicio de algo

[1] http://derechos.apc.org/handbook/ICT_23.shtml
[2] http://derechos.apc.org/handbook/ICT_23.shtml

que en nuestros tiempos ha abarcado aspectos de la vida cotidiana de toda persona. [3]

Ahora es común observar en bancos detectores de metales y cámaras de circuito cerrado o en los aeropuertos ver máquinas de rayos X, detectores de metales, detectores de componentes explosivos, televisión de circuito cerrado con identificador de rostros y por último no se podía quedar fuera el ámbito empresarial con lectores de huella, software de vigilancia de correos y llamadas, etc. [4]

A pesar de la evolución constante de la tecnología, de los sistemas de información y demás, se ha visto que no se logra ofrecer un canal de seguridad al 100%, porque lo que todas estas técnicas y tecnologías de vigilancia tienen en común es el factor humano que es lo que impide tener un 100% de efectividad. [5]

Con la puesta en marcha de portales por Internet que permiten realizar transacciones financieras, se generó un nuevo problema, la privacidad de la información que resguardan tan celosamente bancos, aseguradores, financieras y demás entidades. En este aspecto, las empresas han tenido que invertir bastante en mejorar la seguridad y así ofrecerles a sus clientes portales confiables. [6]

Pero con esto han necesitado de tener mejor información de los clientes para que, en cierta manera, se tenga una mayor confiabilidad de que la persona que está haciendo las transacciones, vía web o presencial, sea quien dice ser y no

[3] http://derechos.apc.org/handbook/ICT_23.shtml
[4] http://derechos.apc.org/handbook/ICT_23.shtml
[5] http://derechos.apc.org/handbook/ICT_23.shtml
[6] http://derechos.apc.org/handbook/ICT_23.shtml

esté haciendo transacciones ilícitas. Esto lleva a la pregunta ¿Qué nivel de seguridad puedo tener sin invadir la privacidad de las personas? Ya que entre mejor sea la vigilancia, mayor es la imposibilidad de las personas de tener privacidad y la privacidad es algo que, en la mayoría de países, es protegido por la constitución local. [7]

A lo largo de este trabajo se describirá, a mejor detalle, historia, antecedentes, proyectos, técnicas y tecnologías de vigilancia además de su uso, ventajas y desventajas de las mismas.

[7] http://derechos.apc.org/handbook/ICT_23.shtml

1. VIGILANCIA (SURVEILLANCE)

1.1 Historia

Hasta mediados del siglo XX, las posibilidades técnicas al alcance del Estado para vigilar a sus ciudadanos implicaban más que nada las tediosas rutinas del soplón. Se requería un creciente ejército de agentes para fisgonear las actividades de la gente y seguirla de cerca de un lado a otro, constatando con quién se reunían, escribiendo a máquina la información y poniéndola en archivos, con muy pocas posibilidades de correlación. Solamente los gobiernos dispuestos a llegar a extremos podían mantener un amplio control. [8]

La policía secreta de Alemania Oriental, por ejemplo, contaba con quinientos mil informantes (aproximadamente 1 por cada treinta y dos habitantes del país), incluyendo diez mil empleados a turno completo sólo para oír y transcribir conversaciones sospechosas por medio de intervenciones telefónicas o en lugares sembrados de micrófonos. [9]

Pero ahora, los rápidos avances tecnológicos, junto con el final de la guerra fría y la demanda de más eficiencia burocrática con menos personal, están promoviendo en todo el mundo el incremento de la capacidad para vigilarnos desde el nacimiento a la muerte, de lo que consumimos a lo que nos enferma, de la cuenta de banco a las opiniones políticas. Nuevas técnicas desarrolladas por el complejo militar-industrial se extienden a la policía, demás instancias oficiales y compañías privadas. Al mismo tiempo, leyes y regulaciones añejas se hacen de la vista gorda o no pueden contener la creciente carrera de

[8] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[9] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

violación de derechos humanos y control represivo a la sociedad que ello implica. [10]

El desarrollo de versátiles sistemas de computación capaces de procesar grandes cantidades de datos revolucionó la vigilancia. Además de los cuantiosos recursos destinados al desarrollo de métodos para hacer cumplir sus mandatos, los gobiernos aplicaron los nuevos medios informáticos para aumentar la eficiencia y el alcance de sus burocracias. Al mismo tiempo, el sector privado exploraba y explotaba inéditas posibilidades de ganancia. Compañías que ofrecían servicios tales como ventas por teléfono, seguridad privada, banca, empezaron a valerse del nuevo hardware y software informático no solamente para fortalecer sus capacidades administrativas, sino también aplicándolos al crédito, al mercadeo y otros usos. [11]

Hoy día, la reseña de casi cada persona en el mundo desarrollado (y de cada vez más gente en el Tercer Mundo) está archivada en un conjunto de bases de datos recogidas, analizadas y accesibles a gobiernos y grandes empresas. Más y más, estas computadoras están conectadas y comparten sus insidias cibernéticas. Usando redes de alta velocidad con inteligencia avanzada y números de identificación tales como el "Número del Seguro Social" en Estados Unidos, las computadoras pueden crear instantáneamente completos perfiles de millones de personas sin necesidad de un sistema centralizado. Nuevos adelantos en genética, en investigación biométrica, avanzados sistemas de registro telemático, de transporte inteligente de datos, y de cotejo de transferencias financieras han aumentado dramáticamente la cantidad de detalles disponibles. [12]

[10] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[11] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[12] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

Diversos convenios internacionales facilitan el intercambio de información a través de las fronteras, y al igual que las legislaciones nacionales, con el pretexto de garantizar la seguridad frecuentemente impiden que la sociedad civil pueda enfrentar, o incluso reconocer, tales invasiones a la vida de las personas. [13]

1.1.1 Termina una guerra, comienza otra

Siempre se ha vendido la imagen de una Norteamérica donde el Estado concede absoluta prioridad al respeto de los derechos ciudadanos, cuando lo cierto es que allí los organismos militares, policiales, de espionaje y las grandes corporaciones tienen una larga historia de burla e ignorancia a los límites promulgados para la protección de las libertades civiles, y esto puede constatarse claramente en múltiples ejemplos citados en las referencias que acompañan a este trabajo. De ahí que no es de extrañar que, con el final de la guerra fría, las agencias de inteligencia y defensa busquen nuevas misiones en el ámbito interno para justificar sus presupuestos y estén transfiriendo técnicas hacia aplicaciones civiles. [14]

La CIA y la Agencia de Seguridad Nacional (NSA por sus siglas en inglés), por ejemplo, hacen hincapié sobre el espionaje económico y recalcan la cooperación con instancias policiales en asuntos de terrorismo, tráfico de drogas y falsificación o lavado de dinero. En 1993, los Departamentos de Defensa y Justicia firmaron un acuerdo para Operaciones no Bélicas y Cumplimiento de la Ley, que facilita el desarrollo y utilización en conjunto de nuevas técnicas. [15]

[13] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[14] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[15] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

El sector oficial también se vale de su poder de financiamiento para influenciar en esa dirección la investigación y el desarrollo (R&D). Mientras que muchos subsidios federales se cancelan alegando recortes de presupuesto, generosos fondos aún fluyen para fomentar la cooperación entre los sectores público y privado para la innovación en tecnologías de espionaje. Los laboratorios nacionales, tales como Ames, Sandia y Los Álamos, mantienen asociaciones activas con el FBI; el Instituto Nacional de Justicia da becas y apoyo para transferir tecnología de punta a las policías estatales y locales. La Agencia de Proyectos Avanzados de Investigación (ARPA) del Departamento de Defensa, a través de su Proyecto de Reinversión Tecnológica, facilita decenas de millones de dólares a compañías particulares para ayudar el desarrollo de usos civiles de la tecnología militar de vigilancia. [16]

Para contrarrestar los recortes en los contratos militares comenzados en la década del ochenta, las compañías electrónicas y de computadoras se expanden por nuevos mercados domésticos y del extranjero con equipos originalmente desarrollados para el ejército. Empresas como E-Systems, Electronic Data Systems (propiedad de Ross Perot, el ex-candidato presidencial) y Texas Instruments están vendiendo equipos de computación y vigilancia avanzados a gobiernos estatales y locales que los usan para labores policiales, guardia de fronteras, y la administración de programas de control social como los relacionados con la "lucha contra la pobreza". Estas compañías también promueven sus productos en numerosos países del Tercer Mundo, en especial aquellos con tenebrosos historiales de irrespeto a los derechos humanos. [17]

[16] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[17] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

No sorprende que regímenes brutales como los de Tailandia, China y Guatemala usen equipos “made in USA” para aplastar la disensión político-social, ni tampoco nadie parece alarmarse porque los fabricantes del más aterrador instrumental de tortura carecen de mayor restricción burocrático-legal a sus operaciones, que son publicitadas por Internet sin ningún espanto por parte de quienes se quejan por la pornografía o las incitaciones al terrorismo que rondan en el ciberespacio. De hecho, los gobiernos de los países industrializados no dudan en apoyar y encubrir a estos "emprendedores empresarios", como se ha evidenciado repetidamente en Norteamérica y Europa, una prueba estremecedora de ello fue un reportaje televisado británico: “Back on the Torture Trail”, presentado en el programa Dispatches del 13 de marzo de 1996. [18]

1.1.2 Numerar para vigilar

En un mundo computarizado y conectado a la red, un número de registro único, personal y universal permite la fácil recuperación y consolidación de datos. Donde aún no lo hay, la presión para llegar a un identificador único, aparentemente para facilitar el intercambio de referencias con propósitos de administración, está en aumento y varios planes hoy día en vigor se deslizan hacia sistemas de identificación universal obligatorios. En los EEUU, el Número del Seguro Social (SSN) fue inventado en 1938 para determinar a los trabajadores elegibles para beneficios de jubilación gubernamentales. [19]

En 1961 el IRS (la agencia federal que recauda los impuestos) comenzó a usarlo como un número de identificación de contribuyente y poco a poco otras agencias le siguieron. Desde entonces los bancos y otras entidades no gubernamentales pueden legalmente rechazar a clientes que se nieguen a dar el SSN, su uso en el sector privado se da por descontado en todo, desde los

[18] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[19] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

seguros médicos a las solicitudes de crédito. Varias leyes pendientes en el Congreso crearían nuevas bases de datos nacionales afincadas en el SSN para todos los trabajadores y para uso de inmigración y asistencia social. [20]

Una vez que un sistema de identificación universal se ha establecido, no hay más que un paso para obligar a la gente a tener y llevar consigo carnet de identidad (por ejemplo la cédula venezolana, establecida como documentación obligatoria desde la década de los 40). [21]

La historia de los documentos de identidad es larga e infame. En el Imperio Romano tuvieron la forma de unas tablas de arcilla llamadas tesserae para identificar esclavos, soldados y ciudadanos hace más de dos mil años. El más notable ejemplo moderno, el passbook sudafricano, contenía relativamente poca información comparado con las tarjetas de hoy. Además del nombre, dirección y número de identificación, la reencarnación moderna de las tesserae incluye foto, huellas dactilares y cinta magnética o circuito micro electrónico para automatizar la inserción de datos en los sistemas digitales. [22]

En un proceso llamado "corrimiento de función" por sus críticos, las tarjetas originalmente concebidas para uso único están siendo rediseñadas para facilitar la conexión de bases de datos múltiples. Así, las tarjetas inteligentes, ampliamente utilizadas en Europa, tienen un circuito micro electrónico que puede guardar varias páginas de información. La aún más avanzada tecnología óptica, capaz de guardar cientos de páginas de datos en un microcircuito está en uso en los EEUU, con tal soporte, Columbia/HCA Healthcare Corporation anunció recientemente que iba a proveer a cincuenta mil residentes de la

[20] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[21] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[22] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

Florida con tarjetas conteniendo su historial médico, incluidos los rayos X. Los identificadores de función múltiple son el siguiente paso. [23]

Utah es uno de los varios estados que ha propuesto una tarjeta inteligente única para servicios tan diversos como el registro de vehículos y las bibliotecas. Otros proyectos en discusión, en la onda de lo que el actual Vicepresidente Al Gore denomina "re-inventar el gobierno", piden un registro único para beneficios de asistencia pública, sellos de comida, y otras tareas del gobierno federal. Florida y Maryland ya han experimentado con el concepto. Las tarjetas se vuelven cada vez más inteligentes. Placas activas, ya en uso en muchas compañías de alta tecnología, transmiten su ubicación y por lo tanto, la del portador. [24]

1.1.3 Vigilancia física

Si una compañía o un gobierno se gastan tanto en semejantes artilugios, necesita maneras de identificar definitivamente a los individuos y asegurarse de que no se confundan unos con otros. La verificación biométrica por medio de características físicas únicas empezó al final del siglo XIX con las huellas dactilares. Recientemente, sistemas automáticos que hacen un escaneo electrónico y digitalizan huellas han llevado la técnica más allá de la aplicación tradicional en investigaciones criminales, permitiendo por ejemplo que las autoridades de Jamaica avancen en un plan para identificar electores con el reconocimiento electrónico de su impresión dactilar. [25]

El FBI invirtió varios cientos de millones de dólares en los últimos años para crear un Sistema Automatizado de Identificación de Huellas (AFIS por sus siglas en inglés). Debido a las mejoras en el acceso, las huellas dactilares hoy día se usan en las solicitudes al nivel estatal. California y New York las exigen a

[23] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[24] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[25] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

todos los solicitantes de asistencia social. A pesar que un detenido estudio reveló que se detectaba muy poco fraude en ese ámbito, el gobierno estatal neoyorquino amplió el programa para imponer ese requisito a todos los miembros de la familia del subvencionado. [26]

Y, como en muchos otros casos, la tecnología va de los márgenes de la sociedad hacia el centro. California ahora requiere la huella del pulgar en las licencias de conductor. Varios bancos del sudoeste toman las huellas de sus no-clientes que quieren canjear cheques y un referéndum propuesto en California, en el marco de la reciente histeria anti-migratoria, exigiría que fueran tomadas impresiones dactilares a todos los recién nacidos y expedida de inmediato su tarjeta de identidad oficial. [27]

Un hito clave en la vía hacia la vigilancia universal se refiere al ADN (ácido desoxirribonucleico). La compleja estructura molecular que guarda el código genético de cada individuo está presente en la más diminuta parte del pelo, los tejidos, o los fluidos del cuerpo. Muchos estados de la unión americana disponen ya de la base legal para tomar muestras de ADN de los criminales convictos. El FBI ha gastado cientos de millones de dólares en la tecnología e infraestructura para crear una red de computadoras que enlace las bases de datos de todos los Estados para así crear de hecho un registro central. [28]

Pero el mayor banco de datos de ADN está siendo propuesto por el Departamento de Defensa, que tiene planes para crear un registro de todos los presentes y antiguos miembros de las fuerzas armadas y los soldados de reserva. Ostensiblemente diseñado para identificar a los caídos en operaciones militares, este inventario guardaría cuatro millones de muestras para el año

[26] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[27] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[28] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

2001 y sería ampliado eventualmente para contener 18 millones. Alegando lo impracticable de destruir las muestras cuando el individuo deja el servicio, el Departamento propone guardar el ADN por 75 años. Dos soldados han presentado demanda para impedir la obtención de su información genética, argumentando que es una violación de su privacidad y que no hay restricciones en cómo se puede usar el ADN. [29]

Menos agresivo físicamente es el sistema basado en la geometría de la mano, que mide la longitud y la distancia entre los dedos. Los EEUU, Holanda, Canadá, Alemania y Bermudas comenzaron en 1993 un programa piloto bautizado como INSPASS, en el cual los viajeros internacionales frecuentes recibirán una tarjeta inteligente que contiene sus medidas de mano individuales. Cada vez que esa persona pase por la aduana presentaba este documento y colocaba la mano en un lector electrónico que verificará su identidad, este aparato estaba conectado a numerosas bases de datos. Los Estados miembros han firmado un acuerdo internacional para compartir esa información y exigir en un futuro el uso de tales tarjetas a todo viajero entre países. Comercializadas por Canon de Japón y Control Data Systems, el programa tiene ya setenta mil registros personales. [30]

En todos estos métodos de verificación, el individuo generalmente sabe que está siendo chequeado y a menudo se requiere su cooperación. Para facilitar la identificación secreta, hoy día se hace mucha investigación en el campo del reconocimiento y la termografía facial. El reconocimiento facial se basa en medir las curvas del rostro desde varios ángulos, digitalizando la información y haciendo una comparación computarizada con imágenes ya existentes en la base de datos o en una tarjeta de identidad. NeuroMetric, un fabricante de

[29] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[30] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

Florida, dice que su sistema es capaz de reconocer veinte caras por segundo, y para 1997 podrá ver y comparar imágenes contra una base de datos de cincuenta millones de caras en pocos segundos. [31]

El Servicio de Inmigración y Naturalización (INS) está gastando millones en un programa experimental utilizando cámaras de vídeo y computadoras para identificar extranjeros ilegales reincidentes o conocidos criminales, terroristas, narcotraficantes y otras personas de interés especial para el gobierno de EEUU en aeropuertos y otros puntos de entrada. A.C. Nielsen, la gran compañía de mediciones de mercadeo y ratings, ha patentado recientemente un procedimiento que se sirve de la identificación facial para reconocer consumidores secretamente, siguiendo sus hábitos de adquisición de bienes y servicios a través de puntos de control en centros comerciales en un área geográfica determinada. En Manchester, Inglaterra, hay un sistema similar operando en el estadio de fútbol para detectar la presencia de hooligans con antecedentes violentos. [32]

La termografía facial mide las emisiones de calor características de cada rostro. La Mikos Corporation dice que su sistema FACES (Facial Access Control by Elemental Shapes) puede identificar individuos sin importar la temperatura ambiente, el vello facial o incluso la cirugía plástica, midiendo la temperatura de 65,000 puntos del rostro con un nivel de precisión superior a las huellas dactilares. Se estima que para 1999, a un precio de tan solo $1.000, estos aparatos podrían usarse en cajeros automáticos, terminales de venta, agencias de servicios sociales y redes de computadoras. Una falla seria, admitida por sus diseñadores con involuntario humor, es que el consumo de alcohol cambia el termo- grama radicalmente, de modo que este sistema tiene que

[31] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[32] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

complementarse con otros para garantizar eficiencia, por lo cual se está trabajando en áreas prometedoras como el reconocimiento individual de retinas.[33]

1.1.4 Aplicación internacional de la vigilancia

Los medios de difusión masiva occidentales presentaron la más aprobatoria imagen cuando los manifestantes por la democracia ocuparon la plaza de Tienanmen en Beijing. Después de todo China tiene un régimen que siempre han descrito como odioso. Lo que recibió menos prensa fue la cacería sistemática que siguió y el origen de los medios técnicos de los que se valió. Las autoridades chinas torturaron e interrogaron a miles de ciudadanos tratando de descubrir a los insurgentes. Pero aunque sus compañeros hubiesen aguantado los suplicios de la policía secreta, los perseguidos tuvieron poca oportunidad de permanecer anónimos. Montadas en diversos escondrijos a través de Tienanmen estaban cámaras de vigilancia, encargadas con ese propósito específico a compañías inglesas. Las imágenes que grabaron fueron transmitidas repetidamente por TV y usadas para identificar y localizar a casi todos los manifestantes. [34]

Lo de Beijing es sólo un ejemplo más de la tecnología de vigilancia occidental apoyando regímenes corruptos y totalitarios. Según un informe de Privacy International, empresas occidentales conectadas con la industria bélica internacional están invirtiendo grandes sumas en construir la base tecnológica para hacer realidad el Big Brother que George Orwell imaginara en su novela 1984. Más del 70% de los cientos de firmas fabricantes y comercializadoras de tecnología de vigilancia nombrados en el informe de Privacy International también exportan armamento convencional, armas químicas o hardware militar.

[33] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[34] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

Las mayores fuentes son EEUU y el Reino Unido, seguidos por Francia, Israel, Holanda y Alemania. [35]

Algunas compañías de electrónica e informática se conectaron con el negocio de la represión muy temprano. La IBM de los EE.UU. y la firma de computadoras británica ICL (International Computers Limited) proveyeron la infraestructura tecnológica para el sistema de passbook de Sudáfrica, que desde los años 60 fue uno de los detestables recursos para instrumentar el apartheid y la más sangrienta represión contra la población negra. A finales de los años 70, la corporación inglesa Security Systems International suplió tecnología de seguridad al brutal régimen de Idi Amín en Uganda. En los años de 1980, la firma israelí Tadiram (recientemente adquirida por Electronic Data Systems, de los EE.UU.) desarrolló y exportó la tecnología para la lista de la muerte computarizada usada por los militares y la policía de Guatemala. PK Electronics proveyó a las autoridades chinas con equipos de intervención telefónica. Gran parte de la tecnología exportada por estas compañías es crucial para el mantenimiento de la infraestructura de represión, en un abanico de países del Tercer Mundo que comprende desde las criminales dictaduras militares de Nigeria e Indonesia hasta las cuestionables "democracias" de México y Venezuela; en todos ellos sirve para escudriñar las actividades de los militantes por los derechos humanos, periodistas, activistas estudiantiles, minorías, sindicalistas y la oposición política. [36]

La técnica también se usa para el control barato y eficiente de grandes sectores de la población, captando, analizando y transmitiendo transacciones financieras, comunicaciones y los movimientos geográficos de millones de personas. La tecnología basada en las computadoras aumenta el poder de las

[35] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[36] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

autoridades y pone novedosos mecanismos de vigilancia político-social a su alcance. [37]

Un ejemplo representativo es el caso de Tailandia. El banco de datos central de la población del país y su sistema de documentos de identidad desarrollados por Control Data Systems de EE.UU., son los elementos claves de un procedimiento de información múltiple que ha sido usado por el ejército tailandés para fines de represión política (parecidos sistemas de tarjetas inteligentes de identidad han sido comercializados en más de una docena de países del Tercer Mundo, y en Venezuela ya se han oído propuestas al respecto). Dichas tarjetas de identidad tienen huellas dactilares electrónicas e imágenes del rostro, y hay la posibilidad de confrontarlas por enlace telemático con una base de datos que cubre la totalidad de la población. La base abarca casi todas las agencias del gobierno y está controlada por el poderoso Ministerio del Interior, dominado por la policía y el ejército. [38]

Después de un largo proceso para determinar lo que requerían las autoridades tailandesas, Control Data Systems diseño un sistema que permite acceso a una gran variedad de bases de datos incluyendo: Base Central de la Población, Sistema Electoral Nacional, Base de los Miembros de Partidos Políticos, Listas de Votantes, Sistema de Registro Electrónico de Minorías, Sistema de Identificación de Huellas Electrónico, Sistema de Identificación Facial Electrónico, Sistema de Información de Población y Vivienda, Sistema de Recaudación de Impuestos, Sistema de Información de Pueblos, Sistema de Información Secreto, Sistema de Opinión Publica, Sistema de Investigación Criminal, Sistema de Seguridad Nacional, Sistema de Control de Pasaportes, Sistema de Control de Conductores, Sistema de Registro de Armas, Sistema de

[37] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[38] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

Registro Familiar, Sistema de Control de Extranjeros y Sistema de Control de Inmigración. [39]

La Smithsonian Institution de EEUU estuvo tan impresionada ante el proyecto y sus resultados que otorgó al gobierno tailandés el premio anual de 1995 "por el uso innovador de la tecnología", patrocinado por ellos y por la revista Computer World, lo cual no dejó de ser aprovechado por el Ministerio del Interior tailandés para rebatir las críticas internas y externas originadas por su multiplicada capacidad de represalia contra toda expresión de descontento. [40]

[39] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml
[40] http://www.monografias.com/trabajos20/estado-de-informacion/estado-de-informacion.shtml

2. TÉCNICAS ACTUALES DE VIGILANCIA

2.1 Audio-sensores avanzado

Las instalaciones para el desarrollo de prototipos del FBI y ARPA en el Laboratorio de Investigación de Quántico, Virginia, está produciendo sistemas electrónicos micro miniaturizados, equipos de vigilancia únicos hechos a la medida de cada investigación. Esperan poder fabricar en 24 horas sistemas de escucha específicamente diseñados, con un micrófono que pueda reducirse al tamaño de un circuito integrado. El FBI ya ha desarrollado un prototipo de micrófono guiado electrónicamente del tamaño de un maletín que puede oír conversaciones discretamente en espacios abiertos. A nivel estatal y local, jurisdicciones como Washington D.C. y Redwood City, California, están considerando sistemas audio-sensores diseñados originalmente para detectar submarinos. Colocados en una ciudad, podrían escuchar disparos y dar la localización a la policía. [41]

2.2 Cámaras de televisión de circuito cerrado (CCTV) y video digital

Los avances técnicos han aumentado las capacidades y rebajado el costo de los equipos de video, convirtiéndolos en un guardián frecuente en tiendas y áreas comunes. Efectivas incluso con muy poca iluminación, las cámaras pueden leer un paquete de cigarrillos a más de 90 metros. En el Reino Unido, según cifras de la Asociación Británica de la Industria de la Seguridad, hay ahora 150,000 aparatos enfocando lugares públicos, empresas y hogares. Docenas de ciudades de ese país tienen sistemas de CCTV centralmente controlados capaces de seguir a individuos donde quiera que vayan, incluso dentro de edificios cuyas cámaras internas es factible integrar a la red urbana. Así, en Liverpool es sencillo para la policía local seguir en video directo a un

[41] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

peatón o vehículo hasta por 2 millas (3.2 kilómetros) sin interrupción. Por cierto que los crímenes mayores en la zona controlada se han reducido, pero en la misma proporción en que han aumentado para otras áreas no monitoreadas de la ciudad. [42]

Figura 1. Cámara de vigilancia de 360º

El modelo de lo que esto significa lo anticipa la pequeña ciudad de Kings Lynn, en East Anglia, que se enorgullece de vigilancia completa por CCTV en todas sus calles y avenidas principales. De la suma de arrestos atribuibles a la presencia de este sistema, 70% corresponden a menores fumando o bebiendo en la vía pública, evasión del pago de parquímetros, arrojar basura a la calle y orinarse en la acera. Un éxito notorio fue cuando las cámaras, gracias a su mirada telescópica y visibilidad al infrarrojo, permitieron capturar cierta oscura noche en un parque boscoso del poblado a un sujeto que se dedicaba a

[42] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

complacerse en solitario.9 Tal vez bajo la impresión de estos logros en la lucha anti-delictiva, la Alcaldía de Baltimore anunció recientemente planes para colocar 200 cámaras en el centro de esa ciudad. [43]

Figura 2. Vistas de una cámara de vigilancia

El FBI ha miniaturizado unidades CCTV que pueden colocarse en una lámpara, radio, maletín, bolso, marco de fotografías, postes de electricidad, teléfonos públicos, libros, etc. y después controlarlas remotamente. [44]

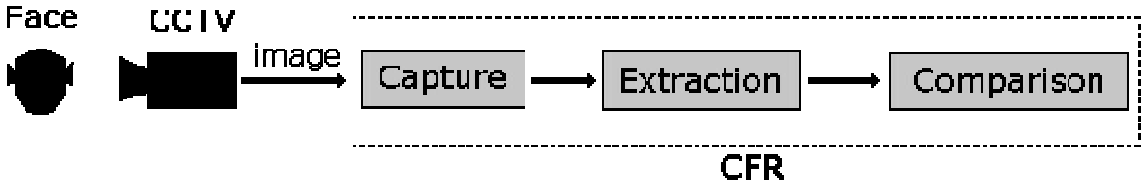
2.3 CFR – Reconocimiento de patrones aplicado a CCTV

Incorporando CFR dentro de sistemas de CCTV, es posible utilizando cámaras escondidas para obtener identidades de personas específicas de interés. La principal ventaja de usar CFR como oposición a otras tecnologías de identificación, es que es pasivo y no intrusivo. Es mucho más fácil de obtener una imagen de un sospechoso que utilizar otras técnicas biométricas como las huellas dactilares, escaneo de retina o sistemas de geometría de la mano.

[43] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[44] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

Anteriores intentos de incorporar CFR en tiempo real requirieron de computadoras poderosas y caras, las cuales normalmente eran lentas y producían resultados inadecuados. Un nuevo estilo de peinado de persona podía confundir y derrotar muchos sistemas.

Figura 3. Proceso de reconocimiento facial.



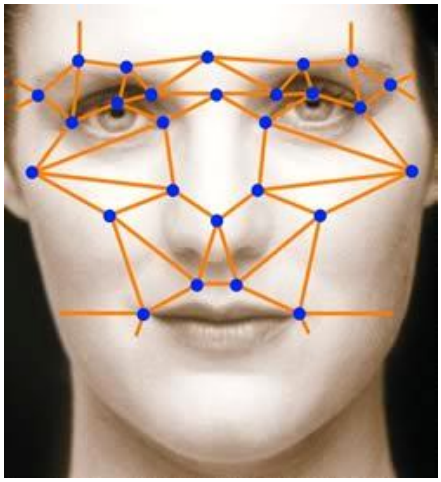
Identificando un individuo por medio del análisis de su rostro es un proceso complejo el cual usualmente requería inteligencia artificial sofisticada y técnicas de aprendizaje de máquina. La inteligencia artificial es necesitada para simular interpretaciones humanas de los rostros.

Las personas si cambian conforme pasa el tiempo. El vello facial, anteojos y la posición de la cabeza pueden afectar la forma en que el CFR puede hacer coincidir el rostro de uno con otro. El aprendizaje de máquina (Machine Learning) es importante adaptarla a estos cambios y así compara de forma más refinada las nuevas muestras con plantillas previamente grabadas.

2.3.1 Proceso de reconocimiento facial

En CFR, las computadoras realizan tres distintas tareas pero a la vez relacionadas entre sí:

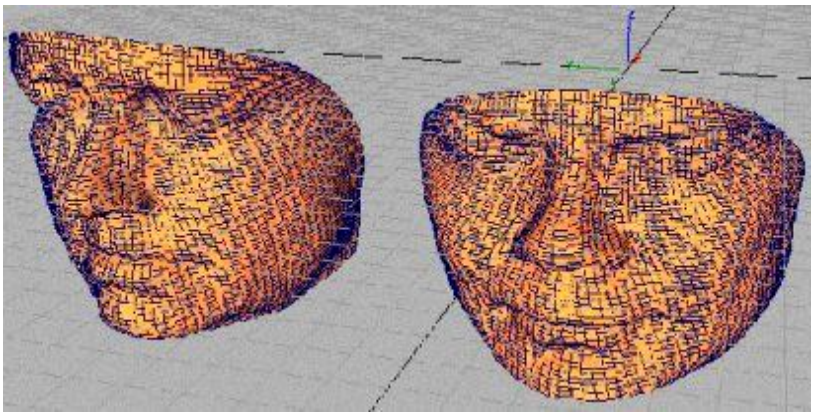
Figura 4. Mapeo facial por programa



2.3.1.1 Capturar

El rostro debe estar localizado dentro de una imagen. Esto puede ser simple (localizando dos círculos y asumiendo que son los ojos), o puede consistir de unos algoritmos de mini reconocimiento complejos que dividen la imagen completa dentro de pequeñas sub imágenes y tratan de reconocer un rostro en cada sub imagen. Una vez ha sido encontrado un número de puntos en el rostro, es mapeado.

Figura 5. Mapeo en varias dimensiones.



2.3.1.2 Extraer

La imagen del rostro es convertida en un patrón y después en un código matemático único. Este es almacenado como una plantilla en una base de datos.

2.3.1.3 Comparar

Para reconocer la plantilla de un objetivo, ésta es comparada con todas las plantillas en la base de datos hasta que una le cace. La verificación es considerada una tarea mucho más simple que la de reconocimiento, porque solo se necesita una simple comparación.

Figura 6. Programa de comparación facial

2.3.2 Limitaciones del CFR

La naturaleza compleja del reconocimiento facial aún posee muchas dificultades, aún hoy con el advenimiento de redes neuronales y DSP's. La precisa posición de los rostros de los usuarios y de la luz y condiciones del medio ambiente pueden afectar el desempeño de los sistemas.

Los seres humanos son inconsistentes y sus características físicas pueden cambiar bastante con el pasar del tiempo. Esto es por qué los sistemas de CCTV modernos que utilizan CFR deben permitir el cambio de esto para que pueda colocarse un límite. Esto puede tomar una forma inadecuada de puntaje.

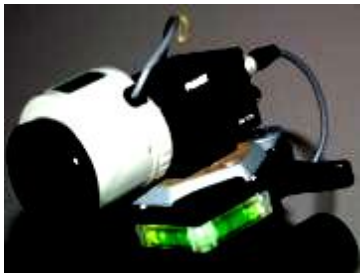
Aquí, la comparación entre la plantilla y un nuevo objetivo debe exceder el límite del sistema antes de encontrar alguna que está grabada. El hecho de que el CFR pueda ser usado en una gran variedad de aplicaciones y no solamente en el contexto de vigilancia puede significar que hay un gran incentivo para los científicos e ingenieros de lograr solucionar estas dificultades. Será solo cuestión de tiempo antes de que veamos el CFR ser usado en muchos aspectos de nuestras vidas.

2.4 Forward Looking InfraRed (FLIR, visor infrarrojo de anticipación)

Inventado originalmente para aplicación en aviones caza y helicópteros localizando aeronaves enemigas, el FLIR puede detectar un diferencial de temperatura de 0,18 grados C, precisión mucho mayor que los detectores de calor antes usados. Texas Instruments y otros están comercializando modelos de mano o para acoplar en automóviles y helicópteros, que pueden ver a través de las paredes para vigilar actividades dentro de inmuebles. Se ha empleado en ciudades norteamericanas para medir variaciones de temperatura en casas donde se usa luz artificial para cultivar marihuana. También se recurre al FLIR para perseguir automotores en la frontera de México - EE.UU. y para buscar personas desaparecidas y fugitivos en áreas despobladas. [45]

[45] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/

Figura 7. Rayo infrarrojo.



2.5 Detectores de masa por ondas de milímetro

Desarrollados por la Militech Corporation, estos artefactos usan una especie de radar para ver bajo la ropa. Mirando la porción de ondas de milímetros del espectro electromagnético emitido por el cuerpo humano, el sistema es capaz de detectar objetos como armas y drogas a una distancia de 3.5 metros o más. También puede captar actividad al otro lado de una pared normal. Militech obtuvo un subsidio de $2 millones del ARPA para financiar su desarrollo para las policías locales. [46]

2.6 Monitor Van Eck

Cualquier computadora emite bajos niveles de radiación electromagnética del procesador central, la pantalla y otros aparatos periféricos. Aunque los expertos no están de acuerdo si el alcance es unos cuantos metros o más de un kilómetro, estas señales pueden ser remotamente recreadas en otra computadora. Asistido por un transmisor para aumentar la señal, en 1994 el FBI uso el efecto Van Eck para extraer información de la computadora del espía Aldrich Ames y transmitirla para ser analizada. [47]

2.7 Sistemas de transporte inteligentes

Se refiere a un número de tecnologías para el control del tráfico aéreo, terrestre y acuático, incluyendo sistemas de evitar choques, colectores de peaje

[46] http://www.psicologiasocial.vivalau.com/2009/09/estado-economia-y-control-social/
[47] http://historiaingenieriavenezolana.blogspot.com/2009/01/las-tecnologas-del-leviatn-estado.html

automáticos, rastreadores de posición por satélite, y reguladores del costo de peaje según tráfico. Para facilitar estos servicios, el sistema sigue los movimientos de la gente que usa transporte público o privado. Según ha propuesto TRW, empresa líder en el desarrollo de estas técnicas, los datos recogidos durante un viaje estarán disponibles para el uso de la policía y entidades privadas como las empresas de mercadeo directo. La colecta de peaje automática ya está operando en varios estados, incluyendo New York, Florida y California. Sistemas de seguimiento para investigaciones de "contrainteligencia" también han sido instalados en New York, donde el FBI dispone de un sistema de seguimiento físico en tiempo real. [48]

A nivel comercial, las compañías de seguros están persuadiendo a los propietarios de automóviles a que instalen el Lojack, que se supone ayuda a recuperar carros robados emitiendo señales de localización una vez que el sistema es activado remotamente. Puesto que los teléfonos celulares transmiten información sobre la ubicación a la oficina central para determinar la ruta de la llamada, también pueden ser usados para automatizar el seguimiento del que llama. En 1993 el capo de la droga colombiano Pablo Escobar fue localizado a través de su teléfono celular. Actualmente se trata de desarrollar un sistema 911 para teléfonos portátiles que daría información sobre la ubicación de cada unidad celular. [49]

2.8 Dinero digital

En potencia, esta innovación creará uno de los sistemas más completos para recabar información individualizada. Utilizando programas de computadora y tarjetas inteligentes para reemplazar el efectivo, el consumidor puede gastar dinero virtual en transacciones pequeñas como leer el periódico electrónico on-line, hacer llamadas desde teléfonos públicos, pagar peaje electrónicamente,

[48] http://historiaingenieriavenezolana.blogspot.com/2009/01/las-tecnologas-del-leviatn-estado.html
[49] http://historiaingenieriavenezolana.blogspot.com/2009/01/las-tecnologas-del-leviatn-estado.html

comprar al detalle, así como cualquier operación que hoy día se hace con tarjetas de crédito. Puesto que la mayoría de los procedimientos en desarrollo (como el de Mondex en Canadá y el Reino Unido) retienen información sobre cada venta de bienes o servicios, crean un índice de datos sin precedentes acerca de las preferencias individuales y los hábitos del consumidor. Otro sistema, Digicash, que da acceso a transacciones anónimas on-line, está siendo ofrecido por el Mark Twain Bank de St. Louis, Missouri. Cabe agregar que la DEA y el Departamento del Tesoro de EE.UU. se han manifestado contra el dinero digital anónimo basados en que puede ser un camino para el "lavado" de narco-dólares. [50]

2.9 Métodos de vigilancia técnica

Tradicionalmente, los Estados han utilizado la interceptación de las comunicaciones como un medio de descubrir los planes de individuos o de grupos. Aunque cada Estado puede tener su manera particular de manejar este proceso, generalmente debe existir alguna forma de vigilancia judicial o garantía para autorizar la interceptación de las comunicaciones privadas. Sin embargo, la vigilancia que no incurre en la intromisión de la privacidad de las comunicaciones no siempre requiere de un control judicial. Los controles sobre la intromisión en las comunicaciones privadas se han debilitado en el contexto de la "guerra contra el terrorismo", permitiendo que el Estado intervenga en las comunicaciones so pretexto de vigilar la actividad criminal y de terroristas. Los controles más significativos consisten en el uso de datos sobre las comunicaciones que están en posesión de las compañías de telecomunicación y de los servidores de Internet. [51]

[50] http://historiaingenieriavenezolana.blogspot.com/2009/01/las-tecnologas-del-leviatn-estado.html
[51] http://derechos.apc.org/handbook/ICT_23.shtml

2.10 Intercepción de las comunicaciones telefónicas

La interceptación del correo postal es probablemente la cuestión menos problemática para quienes trabajan con las tecnologías de la información y la comunicación. Casi todos los países que otorgan licencias para los servicios postales o de mensajería incluyen cláusulas relativas a la interceptación de correo en sus procesos de licitación. Pero la interceptación de las comunicaciones telefónicas es más problemática. La interceptación de correo postal requiere de la confiscación y apertura de la correspondencia física, mientras que la interceptación de teléfonos solo necesita que la línea sea intervenida en la central telefónica, y la información intervenida sea encaminada a otra línea telefónica para que la información llegue al teléfono que realiza el operativo de vigilancia. [52]

La interceptación de tráfico telefónico se ha hecho más sofisticada en los últimos años. Hace cuarenta años cada teléfono intervenido requería de un operador para controlar cada una de las interconexiones por las que se encaminaba la llamada. Ya que actualmente las principales centrales utilizan la tecnología digital, el tráfico telefónico puede ser controlado por una computadora. En lugar de conexiones manuales es posible establecer intervenciones telefónicas mediante el cambio de ruta de la llamada. De este modo la llamada puede copiarse y ser encaminada a la agencia que realiza el control de las llamadas para el Estado. También se cuenta con otros dispositivos que permiten la identificación instantánea del origen de las llamadas, como el "ID (identificador) de usuario)" que transmite por la línea y muestra el número de teléfono del autor de la llamada. [53]

La capacidad de las interconexiones digitales de emitir facturas detalladas para

[52] http://derechos.apc.org/handbook/ICT_23.shtml
[53] http://derechos.apc.org/handbook/ICT_23.shtml

sus clientes también refleja el nivel de información que puede generarse para realizar operaciones de vigilancia. En muchos países esta "información sobre las comunicaciones" no está sujeta a los mismos procedimientos de control estrictos que debe observarse sobre el contenido de las llamadas propiamente dicho. [54]

Esto significa que las agencias de vigilancia pueden utilizar los datos de facturación de las compañías de teléfonos y de cualquier otra organización que tenga información personal detallada de su vida, sin estar sujetas a los controles que se establecen en el caso de la intervención directa de las llamadas. Aunque el contenido de esta información no contenga detalles particulares de las comunicaciones o acciones realizadas, es posible cotejar los datos de facturación de ciertos individuos, lo cual permitiría establecer relaciones y costumbres entre éstos que ayudaría a revelar información igualmente valiosa. [55]

La imagen que se tiene en los medios de comunicación de la interceptación telefónica es la de un operador de vigilancia con un equipo de grabadoras magnetofónicas. Pero éstas han sido también reemplazadas por los sistemas digitales, al igual que en los sistemas telefónicos. Los sistemas actuales de vigilancia telefónica discriminan entre llamadas de fax y llamadas telefónicas almacenadas en los datos de la computadora (y almacenan los faxes/datos de computadora para ser investigados posteriormente). También se concentran en la ocurrencia de palabras clave en el transcurso de las conversaciones o en la presencia de una determinada voz en la línea, lo que hace que la llamada quede marcada para su posterior análisis por parte de un agente operador. Ello

[54] http://derechos.apc.org/handbook/ICT_23.shtml
[55] http://derechos.apc.org/handbook/ICT_23.shtml

contribuye a incrementar el número de llamadas y líneas intervenidas que cada agente operador puede gestionar más fácilmente. [56]

2.11 Intercepción del tráfico de la Internet

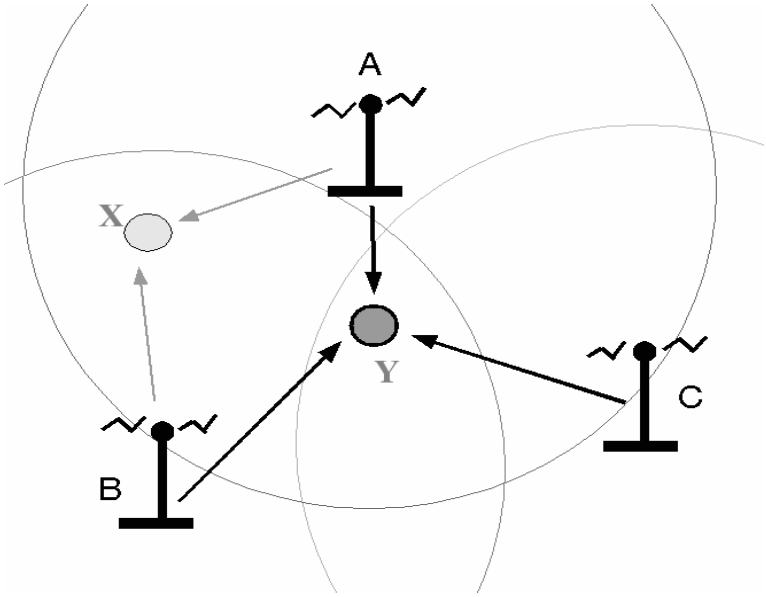
La interceptación del tráfico por Internet es más problemática desde el punto de vista técnico. El único medio de recoger información enviada o recibida por un individuo consiste en interceptarlo en el punto en donde la persona accede a Internet (es decir, su línea telefónica o su conexión a la red). Ello es debido a que la información se reparte en pequeños "paquetes" de datos que pueden ser encaminados a través distintos canales de comunicación. Por esta razón, algunos Estados se han mostrado preocupados por controlar Internet en la última década. Su respuesta es, en breve, controlar todo y compilar los "datos de comunicación" recogidos durante este proceso para su posterior uso. El rastreo de los usuarios de la Red incluye el nivel más bajo de la identificación de la direcciones IP utilizadas por Internet. La mayoría de los sistemas de Internet, como los servidores de correo electrónico, registran datos adicionales. La mayor parte de servidores de correo registran el "encabezado" de los correos electrónicos que transmiten. Como mínimo éstos incluyen la dirección de correo del remitente, la dirección del destinatario y la fecha y hora. Esto proporciona una manera más rápida de encontrar el origen, puesto que una dirección de correo electrónico puede ser directamente asociada a una cuenta de usuario que aparece vinculada a una identidad real en los registros del servidor. Esta identidad puede ser revelada de manera sencilla mediante una búsqueda on-line del nombre real del usuario. Aunque la dirección de origen del correo electrónico sea falsa o 'inventada', el servidor de correo mantiene un registro de la dirección IP de la computadora desde la que fue realizado el envío y, por lo tanto, puede ser rastreado. [57]

[56] http://derechos.apc.org/handbook/ICT_23.shtml
[57] http://derechos.apc.org/handbook/ICT_23.shtml

2.12 Rastreo de teléfonos celulares

También es posible rastrear la ubicación física de la persona utilizando dispositivos tales como los teléfonos celulares o las redes de computadoras inalámbricas. Los teléfonos celulares permanecen en comunicación constante con la estación base más cercana a su red (si se mantienen encendidos). Conociendo la ubicación de dicha estación base es posible determinar la posición geográfica aproximada. Pero también es posible que el operador del sistema telefónico recoja datos de otras estaciones base a fin de rastrear la ubicación del teléfono en cuestión. [58]

Figura 8. Triangulación para rastreo.



Además de registrar cuál es la estación base más cercana, la mayoría de sistemas de teléfonos también registran un "radio de señal-ruido" (signal to noise ratio - SNR) que mide la fuerza de la señal en el teléfono- y envía el dato a las estaciones base adyacentes. Mediante la obtención del SNR de las estaciones base cercanas al teléfono (lo que puede realizarse en tiempo casi

[58] http://derechos.apc.org/handbook/ICT_23.shtml

real con la ayuda de la operadora telefónica) se puede calcular la posición del teléfono entre dos estaciones con bastante precisión. [59]

Cuanto más estaciones base existan, y más cercanas estén unas de otras, tanto mayor será la exactitud con que se determine la posición del teléfono. En las zonas rurales las estaciones pueden estar a una distancia de entre cinco y diez kilómetros. En las zonas urbanas esta distancia será de pocos kilómetros, y menos aún en ciudades densamente urbanizadas. Ello quiere decir que la posición de una persona puede determinarse fácilmente con aproximación cercana a las decenas de metros en zonas urbanas o un tanto más para las zonas rurales. [60]

Los nuevos teléfonos celulares de tercera generación (3G) tienen una distancia menor de separación entre estaciones base. También se ha propuesto que los teléfonos 3G utilicen el dispositivo de rastreo rutinariamente como parte de sus operaciones. Y esto no solo con el fin de localizar a la persona sino también para facilitar la identificación de números de teléfono (servicios públicos, información publicitaria, etc.) para los usuarios. [61]

Ello quiere decir que se generará más información sobre la localización de la persona en una fecha y hora específica y que ésta será transmitida de manera habitual a los interesados. Las políticas de privacidad y seguridad de los estados relativas a este tipo de información ayudarán a determinar si el uso de los teléfonos 3G constituirá una amenaza a la privacidad en años venideros. Si los entes reguladores de la comunicación y la privacidad buscan proteger de este tipo de información al igual que se hace con otro tipo de datos personales, solo el uso previsto por la ley será posible. Pero si los datos no están sujetos a

[59] http://derechos.apc.org/handbook/ICT_23.shtml
[60] http://derechos.apc.org/handbook/ICT_23.shtml
[61] http://derechos.apc.org/handbook/ICT_23.shtml

un buen control, el recojo o difusión de esta información podría producir una situación de intromisión en la vida privada o la intimidad de las personas. Ello podría contribuir a la desprotección de las personas frente al fraude u otros delitos, puesto que sus perpetradores podrían fácilmente localizarlos. [62]

En el futuro, y a medida que su uso se generalice, las cuentas de teléfonos y televisores digitales, o de celulares 3G, deberán ser autentificadas por cada propietario individual del dispositivo. Esta tendencia actual de autentificación del usuario está en la vanguardia de las últimas novedades en tecnología de la información y permitirá un uso expandido de los servicios de pago o suscripción on-line. Esto es posible a través de sistemas estándar como el ".Net" de Microsoft que busca incorporar la autentificación en sus sistemas en red. Éste utiliza un "pasaporte" on-line individual que queda registrado en un servidor de verificación de la identidad para todas las operaciones efectuadas on-line. Pero al mismo tiempo se incrementa la capacidad de rastrear y reducir el anonimato de manera parecida a la forma en que las operaciones de tarjetas de crédito quedan fácilmente asociadas a cada titular. [63]

2.13 Vigilancia por programas computacionales

Las computadoras, y en general los sistemas de información, pueden ser vigilados de formas muy diversas. Ello se debe a que los sistemas técnicos operan sin que el usuario tenga una comprensión cabal de su funcionamiento. El software de aplicaciones espía (spyware) constituye un nuevo sector que tiene por objeto recoger información sobre las costumbres de los usuarios de estos sistemas. Además existen compañías especializadas en "seguridad informática" que producen aplicaciones de software capaces de pedir

[62] http://derechos.apc.org/handbook/ICT_23.shtml
[63] http://derechos.apc.org/handbook/ICT_23.shtml

información a una computadora, así como las claves de acceso e incluso los archivos eliminados. [64]

Muchos sistemas de computación mantienen rutinariamente un registro de uso. También hay programas como los navegadores de la Web o los procesadores de texto que registran información relativa al uso del programa, a los archivos consultados y la identidad de las personas que acceden o modifican dichos archivos. Estos registros pueden ser extraídos por alguien que tenga acceso a la computadora, y constituyen una fuente de información fundamental en el campo de la llamada "informática forense". El desarrollo de software espía que ante todo busca acceder a la información del usuario constituye un serio riesgo para la privacidad. Aun cuando no existan facilidades de registro en la computadora, es posible instalar este tipo de programas a fin de controlar determinados usos de la computadora. Estos programas pueden recoger información de las teclas tapeadas por el usuario, o del correo electrónico o las direcciones de Internet que han sido contactadas. El programa luego almacena esta información para ser recuperada posteriormente, o bien puede ser enviada de manera encubierta por correo electrónico mientras el usuario revisa su buzón de correo. Como ejemplo, podemos citar el programa Magic Lantern del FBI. [65]

Éste fue diseñado para introducirse en algunos sistemas de computadoras y enviar detalles acerca del contenido de las mismas, las contraseñas de cuentas y claves de encriptación. La polémica se produjo cuando el FBI intentó llegar a un acuerdo con los autores de software antivirus para que sus productos no alertaran sobre la presencia o instalación de Magic Lantern en una computadora. [66]

[64] http://derechos.apc.org/handbook/ICT_23.shtml
[65] http://derechos.apc.org/handbook/ICT_23.shtml
[66] http://derechos.apc.org/handbook/ICT_23.shtml

Un medio rutinario de obtener información para la vigilancia consiste en recoger lo que las personas desechan. Es muy común que muchas personas boten información importante. Para los usuarios de sistemas de información, el contenido de los materiales eliminados proporciona información sobre procedimientos de seguridad e incluso grandes cantidades de datos confidenciales. Por ejemplo la eliminación de disquetes y CD defectuosos puede revelar información importante, para quienes puedan acceder a estos soportes dañados. [67]

2.14 Vigilancia de datos

Aun cuando las personas manifiestan temores por la vigilancia electrónica, lo cierto es que el origen más frecuente de las filtraciones de información lo da la propia naturaleza humana; se trata de errores, olvidos o filtraciones involuntarias. Existen técnicas de vigilancia indirecta especializadas en el análisis de la información generada por las actividades diarias de las personas.[68]

El proceso más significativo de la vigilancia indirecta constituye la búsqueda de rastros de auditorias y documentos. Antes del uso extendido del procesamiento de datos esta labor era muy engorrosa puesto que requería del análisis de gran número de papeles. Actualmente este proceso es mucho más sencillo, pues la información es digitalizada e incluso vendida en grandes cantidades por los gobiernos y las corporaciones. Por esta razón, se ha convenido en llamar vigilancia de datos a toda acción de vigilancia indirecta sobre el uso que se da a la información digital. [69]

[67] http://derechos.apc.org/handbook/ICT_23.shtml
[68] http://derechos.apc.org/handbook/ICT_23.shtml
[69] http://derechos.apc.org/handbook/ICT_23.shtml

La información debe ser organizada mediante un índice o clave. La clave que suele tener cada individuo es la de su nombre. Pero esta clave no es única. Muchas personas que viven en una gran ciudad y, desde luego, dentro del territorio de un país, comparten el mismo nombre. Por esta razón se hace indispensable acompañar la clave del "nombre" con otros identificadores como, por ejemplo, la dirección, el número de identificación nacional, del seguro social o de la tarjeta de crédito. Cuanto mayor sea el número de valores clave adicionales que agrupemos, tanto mejor podremos asegurar la posibilidad de identificación de un único sujeto vigilado. [70]

El Estado, a través de sus agencias de seguridad y la policía, puede acceder a grandes cantidades de información digital. Esto puede realizarse a través de los organismos del Estado como la agencia tributaria o la de seguridad social, o bien haciendo uso de atribuciones legales que les permiten pedir información personal a entidades privadas como bancos y compañías telefónicas. Tanto la policía como otras autoridades están en capacidad legal, dependiendo de la naturaleza de la "infracción" que se investiga, de interceptar las comunicaciones directas e incluso registrar un inmueble a fin de obtener la información necesaria para completar su análisis. [71]

Mediante este proceso se crea un "archivo de datos" que contiene toda la información relativa a la persona, con detalles sobre su estilo de vida, su trabajo, amistades, gustos y costumbres. El cruce de informaciones o fusión de datos provenientes de varias áreas es de gran utilidad para establecer un "mapa" de las relaciones entre varias personas. Ello puede proporcionar información adicional de utilidad para determinar los modos de relación que existen entre una organización y las personas que la apoyan. El cruce de

[70] http://derechos.apc.org/handbook/ICT_23.shtml
[71] http://derechos.apc.org/handbook/ICT_23.shtml

informaciones que contienen datos geográficos como la ubicación de las compras realizadas o los datos del rastreo de llamadas desde celulares permiten también mostrar pautas de actividad colectiva como las reuniones o los viajes a un lugar determinado. [72]

2.15 Tarjeta de aproximación inteligente

Originalmente, las tarjetas electrónicas fueron sustitutas de las llaves comunes, las cuales eran muy fáciles de reproducir. La primera en su tipo utilizó barium ferrite como puntos magnéticos adheridos a la capa magnética. Este fue un avance significativo sobre las tarjetas perforadas, ya que eran fácilmente de reproducir.

En el principio de los años 70, las tarjetas con bandas magnéticas eran producidas por IBM, las cuales aún son utilizadas en las tarjetas de crédito y son de cierta forma más seguras. Pero aun así, son muy fáciles de hacer y deben de pasar por una lectora de banda magnética.

En el principio de los años 80, el advenimiento de tecnología ASIC (Application Specific Integrated Circuit), resultó en lo que rápidamente se conoce como "tarjetas inteligentes", las cuales podían almacenar una variedad de códigos e información para hacer su mal uso o duplicación casi imposible. Esta fue la primera tarjeta de proximidad, la cual no requería contacto directo con una grabadora de tarjetas.

Figura 9. Chip inteligente.

[72] http://derechos.apc.org/handbook/ICT_23.shtml

La tarjeta de proximidad básicamente es un transportador, un dispositivo electrónico que replica a una señal de radio que la interroga. El modelo de rango extendido no requiere tan siquiera colocarlo cerca de una lectora de tarjetas, transmite a un receptor desde varios pies de distancia.

El uso de las tarjetas de aproximación inteligentes puede ser usado para el control de acceso y como tarjeta de identificación.

- Las tarjetas contienen datos usados para identificar a sus portadores, así como también sus diferentes derechos de acceso. La parte sin contacto de las tarjetas es usado para acceder a edificios y a otras áreas protegidas.
- La parte de contacto puede ser utilizada para acceso a redes, al igual que para Internet.

Las lectoras de aproximación instaladas en los muros de un edificio permiten la localización de tarjetas (y por consiguiente a sus portadores) dentro de las instalaciones. Incluso se puede medir el tiempo que a un empleado le toma el ir a la cafetería y dejar su estación de trabajo sin atención. Toda esta información puede ser almacenada para posterior uso por los empleadores.

3. PROYECTOS DE VIGILANCIA EXISTENTES

3.1 ECHELON

Es un proyecto con mayor cobertura en monitoreo de datos. Virtualmente cada persona en el mundo que hace uso de teléfonos, fax o correo electrónico interactúa con ECHELON en una diaria base, pero difícilmente alguien sabe sobre su existencia e incluso su funcionamiento. En resumen, ECHELON es un componente computacional de un sistema global espía primariamente controlado y diseñado por la Agencia de Seguridad Nacional (NSA por sus siglas en inglés), en los EEUU con socios globales en Canadá, Australia, Nueva Zelanda y Gran Bretaña. Hasta este día, muchos detalles de ECHELON permanecen en secreto.

ECHELON trabaja interceptando mensajes desde instalaciones de intercepción secreta donde las computadoras filtran los mensajes de forma que se eliminen aquellos que no tienen relevancia. Algunas instalaciones monitorean comunicaciones satelitales, otras redes de comunicaciones terrestres y otras comunicaciones por radio. ECHELON une todas estas instalaciones. Los mensajes son leídos simultáneamente en 'tiempo real' donde los diccionarios de ECHELON son utilizados para buscar palabras clave, donde las palabras clave son agrupadas dentro de categorías identificadas por un número de cuatro dígitos. Diferentes estaciones de intercepción, capturan diferentes tipos de comunicaciones. Algunas interceptan comunicaciones satelitales y otras terrestres. Las estaciones de intercepción están estratégicamente localizadas alrededor del mundo en los países miembros de ECHELON para que virtualmente todas las comunicaciones alrededor del mundo puedan ser interceptadas.

ECHELON también ha traído muchos problemas ya que es ilegal para los EEUU el espiar a sus propios ciudadanos y lo mismo es para Gran Bretaña, pero Gran Bretaña puede espiar a ciudadanos americanos y viceversa lo cual es técnicamente pensar como legal aunque levanta problemas éticos.

3.2 CIPHERWAR: contraatacar a ECHELON

La razón fundamental del día de Jam Echelon es utilizar la lista de palabras clave ECHELON disponible públicamente para confundir el sistema desbordando Internet con correo electrónico que contengan la lista de palabras clave que detecta el sistema, así como aumentar el conocimiento público de la existencia de ECHELON y del hecho que las comunicaciones personales pueden estar siendo controladas. [73]

3.2.1 Metamute encuentra echelon - una competición literaria[74]

Una crítica del proyecto Jam Echelon es que ECHELON es demasiado sofisticado para atender simples listas de palabras. Según se dice, Echelon analiza la estructura gramatical de las frases y el contexto en el que las palabras clave aparecen. Coincidiendo con el Jam Echelon 2001, Metamute propuso un concurso: Metamute Encuentra Echelon, creado para motivar la producción de obras (ficción, novela...) que utilicen la lista de palabras ECHELON con un grado de contextualización sofisticada que pueda actualmente motivar al sistema y, en consecuencia responder. O al menos quedar seriamente confundido. Los participantes pueden utilizar palabras procedentes del diccionario ECHELON para crear una original obra de cualquier género literario: cuentos, drama, poesía, discursos, cartas, etc. El trabajo no debe tratar sobre ECHELON bajo ningún aspecto, y el término "ECHELON" no debe aparecer a lo largo del trabajo en ninguna ocasión. Los artículos se juzgan bajo dos criterios:

[73] http://www.nettime.org/Lists-Archives/nettime-lat-0109/msg00051.html
[74] http://www.nettime.org/Lists-Archives/nettime-lat-0109/msg00051.html

1) El mérito literario del trabajo y
2) El número de palabras de la lista ECHELON presentes en el trabajo.

3.3 CARNIVORE

Es un programa de interceptación, que captura los contenidos de un mensaje electrónico (en las dos direcciones) y también captura datos de tráfico, en dos direcciones. A diferencia de un sniffer, que captura indiscriminadamente todo el tráfico que circula por un servidor, CARNIVORE se limita a interceptar mensajes de correo electrónico dirigidos a una dirección específica y enviados desde una dirección específica. En palabras del FBI: "CARNIVORE es un sistema computacional diseñado para permitir al FBI que, en colaboración con un proveedor de Internet (ISP), se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación". Aquí encontraréis porqué aparece, quién lo ha programado, qué aspecto tiene, el porqué de su nombre y qué tipo de amenaza supone. Todo lo que usted siempre quiso saber sobre CARNIVORE... y nunca supo dónde encontrar. Español. [75]

3.3.1 Detener a Carnivore

Stop Carnivore es una organización dedicada a la única tarea de paralizar el despliegue de la herramienta de espionaje CARNIVORE por parte del FBI. En su página se pueden encontrar los artículos y noticias más recientes sobre él, así como varias propuestas y acciones para darlo a conocer y detenerlo. [76]

[75] http://www.interzona.org/transmisor/PP/privacidad.html
[76] http://www.interzona.org/transmisor/PP/privacidad.html

4. LA BIOMÉTRICA

Una nueva área de seguridad física que ha estado ganando popularidad, y cuya importancia se incrementará exponencialmente a medida que resulte más sencillo implementarla y su necesidad sea más evidente, es la Biométrica o Bio-Acceso. La Biométrica no es utilizada solamente en el acceso a edificios o computadoras, sino que a la brevedad será utilizada para acceder a sus cuentas bancaria, sus tarjetas de crédito y hasta para realizar una llamada telefónica. [77]

La Biométrica garantiza el acceso basado en la identificación personal, a través de un patrón de reconocimiento pre programado, de manera tal que provee no sólo identificación, sino también validación. Para que esto pueda funcionar, debemos tener en mente la teoría de que los rasgos fisiológicos son únicos en cada persona. Les daré una breve reseña de lo que ocurre cuando un sistema de Biométrica es utilizado. El proceso de identificación se inicia con un pedido de reconocimiento por parte de la persona que envía cierta información biológica.

Esta es luego comparada con la existente en la base de datos. La velocidad del proceso depende del tamaño de la base de datos, tamaño del archivo (generalmente grande), y velocidad de procesamiento de las computadoras. Las nuevas tecnologías de compresión están reduciendo el tamaño de estos archivos, permitiendo para una mayor capacidad de proceso una mayor cantidad de datos a comparar. En la mayoría de los casos, la Biométrica requiere de contacto físico con partes del cuerpo. Debido a las posibilidades de

[77] http://cuerdasyenergia.files.wordpress.com/2008/06/breve-introduccion-a-la-biometrica.pdf

transmisión de enfermedades, tecnologías de escaneo en video y láser están siendo implementadas en muchas aplicaciones de manera tal de eliminar la necesidad de contacto físico. Con el uso constante de las computadoras hoy en día, asegurar el acceso y la información ya no es un tema de negocios solamente, sino que la gente tiene que darse cuenta de que también se trata de proteger su privacidad. Hay siete categorías biométricas que se aplican hoy en día: huellas dactilares, geometría de la mano, escaneo de retina, escaneo de iris, geometría facial, verificación de voz y verificación de firma. Todas ellas son consideradas parte de la seguridad biométrica.

El análisis de huellas dactilares es de las más antiguas y comunes de todas estas categorías. Pero ha evolucionado del viejo sistema de tinta y papel. El sistema actual toma imágenes en video de la huella dactilar y la separa en varios componentes. Los cantos de la huella son transformados en llaves matemáticas, de manera tal de que cada huella es realmente una serie de ecuaciones matemáticas. Asimismo, mientras más huellas se utilicen, más acertado será el proceso de verificación.

Figura 10. Huella digital escaneada.

Pero, obviamente, esto también implica, duplicar, triplicar y hasta cuadruplicar el tamaño de almacenamiento necesario para llevar a cabo dicho proceso. La gran resolución de los sistemas permite llevar a cabo más de estas ecuaciones, lo que redunda en una mayor exactitud en los resultados. La lectura inicial y almacenaje pueden tomar de 5 a 10 segundos, y la verificación sólo 1 o 2 segundos.

La geometría de la mano es muy similar al sistema de huellas dactilares. En realidad es una extensión del mismo sistema. Crea ecuaciones matemáticas basadas usualmente en la altura, el ancho y largo de la mano. Esto puede llevar a un posible problema con algunos gemelos casi idénticos que tienen el mismo tamaño de mano.

El escaneo de retina requiere examinar el ojo a una distancia cercana (unos 5 centímetros). Esto es muy intrusivo y es un proceso largo, por lo cual sólo ha sido aplicado en lugares que tienen grandes requerimientos de seguridad.

El escaneo de iris realiza un mapeo matemático del área del iris (circundante a la pupila). Con aproximadamente 200 puntos de referencia dentro del iris, es bastante sencillo de hacer y puede discriminar bastante dependiendo de la cantidad de puntos que tome como referencia y procesados. Dado que el color del ojo no es un tema a tener en cuenta, las cámaras en blanco y negro pueden utilizarse en ese sistema, lo que redunda en un abaratamiento de costos de implementación. Las imágenes tomadas son almacenadas y comparadas durante el proceso de verificación. Este sistema es mucho más preciso que el sistema de geometría de mano, ya que miembros de la misma familia, incluso hermanos idénticos, tendrán diferente iris.

La geometría de la cara es el resultado del reconocimiento mediante geometría de mano y de huellas dactilares. Se toman imágenes en video y se seleccionan puntos faciales como referencia, de manera tal de garantizar el acceso. El uso más común de este sistema toma como referencia la distancia entre dos puntos de la cara. Otro uso implica medir los puntos de calor con cámaras infrarrojas (lo que se traduce en un encarecimiento del sistema). Esto soluciona los problemas ocasionados por objetos cubriendo la cara de la persona.

La verificación mediante voz se ha estado convirtiendo en algo popular. Analiza la voz, su velocidad y patrón, y la transforma en una firma digital personal. Muchos sistemas han sido mejorados al agregar un patrón de palabras para ser utilizadas en la identificación y confirmación. Este sistema, asimismo, garantiza la ausencia de contagio de enfermedades, ya que no requiere de ninguna clase de contacto físico. El reconocimiento de firma divida la firma de una persona en dos partes: una parte abarca los rasgos que se mantienen, la otra parte los rasgos cambiantes. Este sistema usualmente requiere de la utilización de plaquetas de costosas plaquetas de escritura.

Han aparecido muy diversas implementaciones para esta clase de bio-accesos. Muchas requieren alguna clase de acceso mediante tarjeta, utilizándose alguno de los métodos arriba detallados a modo de verificación.

Este proceso es más rápido, ya que la computadora sólo debe comparar los datos biométricos de la persona con los que se encuentran almacenados en la tarjeta para garantizar (o no) el acceso. Futura tecnología utilizará tarjetas inteligentes en reemplazo de las bases de datos. Dichas tarjetas contendrán los datos a comparar ellas mismas. Pero se podría imaginar qué pasaría si alguien (y se sabe que lo harán) lograra piratear una de esas tarjetas inteligentes.

La gente podría ser capaz de crear sus propias identidades fácilmente y de esa manera ganar acceso a lugares restringidos sin demasiado esfuerzo de su parte, dado que la computadora los dejaría. Y las computadoras nunca mienten.

Muchos fabricantes de estos sistemas utilizan diferentes protocolos y debido a ello no se puede disponer de un archivo “universal” para ser utilizado en todos los sistemas de seguridad en todas partes todavía. Pero obviamente esto es

algo que el gobierno apoyará no sólo de palabra sino que también con fondos. Con la posibilidad de mantener las características únicas de cada persona en archivo (y no mencionemos qué más sería posible) y quizás hasta ni siquiera necesitar almacenar archivos en sus computadoras, teniendo las nuevas tarjetas inteligentes. Un comité conocido como Bio-API ha sido formado para tratar de encontrarle estándares a la industria. Otros estándares desarrollados por varios desarrolladores industriales, el gobierno y hasta el MIT es el llamado SVAPI (Speaker Verificación-API). Existe un software de desarrollo gratuito para Win9x o NT que puede ser bajado de Internet.

La biométrica es de por sí un método tan intrusivo e invasivo que muchos sostienen que necesita un sistema propio de seguridad. Sin embargo, hasta el momento no hay regulación ni ley que controle la venta o transferencia de información biométrica adquirida en marco de legalidad. Esto significa que si alguien se postula para un trabajo y le es requerido un escaneo biométrico, la agencia de control no brinda ninguna protección para su información privada. Hay en California una petición pendiente, la AB50, que pretende detener la copia de información biométrica. Otro asunto de cuidado es la eficiencia de los mencionados sistemas.

¿Son realmente necesarios? ¿Va a dejar la gente de usar los cajeros automáticos porque se van a hartar de tener que esperar el escaneo de retina para obtener su dinero, debido a algún problema del sistema? Bueno, el Centro Nacional de Testeo de Biometría (National Biometrics Test Center), ha desarrollado estándares de pruebas para evaluar el desempeño de los equipos de acceso biométrico, antes sólo realizado por los fabricantes. La mejor oportunidad de estandarización la tiene la Asociación Nacional de Seguridad de Computadoras (Nacional Computer Security Association), que ha creado un

programa de certificación para sistemas y componentes, que se encargará de establecer tasas de error basadas en métodos de prueba estandarizados.

Ahora, se puede mirar a esta nueva tecnología de la manera en que se plazca. Si es dejada en manos de los sectores privados y de negocios, e implementado de manera tal de que no discrimine ni elimine las opciones de la gente para hacer cosas, puede ser algo bueno y un valor agregado para la seguridad de las personas en sus casas, y para las empresas temerosas del espionaje industrial o cualquier otra paranoia que tengan.

Sin embargo, si se pone esta tecnología en manos del gobierno, se estaría dando aún más poder, que los habilitaría para controlar y monitorear las vidas humanas. Dependiendo en dónde sean hechos estos sistemas, el gobierno podría observar a las personas cuando van y vienen de sus hogares, se conectan a las computadoras, extraen dinero del cajero automático y hasta incluso saber qué clase de películas se contratan con el sistema pago por evento. Eso, mis amigos, asusta bastante, y espero no tener que pensar en ello alguna vez como una realidad.

5. UNA PERSPECTIVA AL FUTURO, LA VIGILANCIA DE LA BANCA ELECTRÓNICA

Los medios de pago electrónico tendrán un lugar preponderante en el desarrollo del comercio electrónico y los servicios y productos bancarios electrónicos para consumidores, incluyendo el dinero electrónico, podrían crear nuevas oportunidades para los bancos. La banca electrónica podría permitir a los bancos ampliar sus mercados para sus actividades tradicionales de recepción de depósitos y otorgamiento de créditos, y ofrecer nuevos productos y servicios o fortalecer su posición competitiva en la oferta de servicios de pago ya existentes. Además, la banca electrónica podría reducir los costos de operación de los bancos. En general, el desarrollo continuado de la banca electrónica y del dinero electrónica podría contribuir a mejorar la eficiencia del sistema bancario y de pagos y a reducir el costo de las transacciones con los consumidores a nivel nacional e internacional. Esto podría dar como resultado un aumento de la productividad y del bienestar económico. Los consumidores y los comerciantes podrían incrementar la eficiencia con la que hacen y reciben pagos y disfrutar de una mayor comodidad al respecto. La banca electrónica podría además permitir el acceso al sistema financiero, de aquellos consumidores que anteriormente tenían un acceso limitado. [78]

Las deliberaciones sobre este tema son generales ya que la tecnología de la banca electrónica y dinero electrónico cambia rápidamente, y los productos y servicios del futuro podrán ser muy diferentes de los disponibles en el presente. En esta fase inicial de desarrollo de algunas actividades de la banca electrónica y dinero electrónico, no se pueden medir algunos aspectos de los riesgos. Un

[78] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

sistema de reglamentación prematuro podría paralizar la innovación y la creatividad en estas áreas. Por lo tanto, los supervisores deberían incitar a los bancos a que desarrollen un proceso de gestión de riesgos que sea lo suficientemente riguroso y amplio como para tratar los riesgos importantes, que se conocen, y los suficientemente flexibles como para acomodar cambios en el tipo e intensidad de los tres riesgos asociados con sus actividades de banca electrónica y dinero electrónico. Este proceso de gestión de riesgos será eficiente en la medida en que evolucione en forma constante. [79]

Dos de los aspectos fundamentales de la banca electrónica son: las características de los canales de entrega y los medios disponibles a los consumidores para acceder a estos canales. Los canales de entrega más comunes incluyen redes "cerradas" y "abiertas". Las "redes cerradas" limitan el acceso a los participantes (instituciones financieras, consumidores, comerciantes y suministradores de servicios para terceros) que son miembros en virtud de un acuerdo específico. Las "redes abiertas" no tienen estos requisitos de membrecía. Actualmente, los productos y servicios de la banca electrónica son suministrados a los consumidores por medio de una variedad de dispositivos de acceso, como ser, terminales en los puntos de venta, cajeros automáticos, teléfonos, computadoras personales, smart cards y otros. [80]

Los bancos pueden participar en los esquemas de dinero electrónico como emisores, pero pueden, también, realizar otras funciones. Estas incluyen la distribución de dinero electrónico emitido por otras entidades; el rescate de las ganancias de las transacciones en dinero electrónico para los comerciantes, el

[79] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[80] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

manejo del procesamiento, compensación y liquidación de las transacciones de dinero electrónico y el manejo de registros de transacciones. [81]

5.1 Riesgo operativo

El riesgo operativo se genera del potencial de pérdida debido a deficiencias importantes en la confiabilidad e integridad del sistema. Los aspectos de seguridad son de la mayor importancia, ya que los bancos pueden sufrir ataques externos o internos a sus sistemas o productos. El riesgo operativo puede generarse también por el mal uso de los clientes, y por sistemas de banca electrónica y dinero electrónico mal diseñados o ejecutados. Muchas de las manifestaciones específicas posibles de estos riesgos, se aplican tanto a la banca electrónica, como al dinero electrónico. [82]

5.1.1. Riesgos de seguridad

El riesgo operativo se genera en relación a los controles del acceso a los sistemas contables y de gestión de riesgos del banco, a la información que transmite a terceros y, en el caso de dinero electrónico, las medidas que utiliza el banco para detectar y controlar dinero falso. Controlar el acceso a los sistemas de los bancos se ha vuelto cada vez más complejo, en vista del crecimiento de las capacidades de los sistemas de computación, la dispersión geográfica de los puntos de acceso, y el uso de varias vías de comunicación, incluyendo redes públicas, como el Internet. Es importante hacer notar que en el caso de dinero electrónico, una violación de seguridad puede dar como resultado la creación fraudulenta de obligaciones del banco. En el caso de otras formas de banca electrónica, el acceso no autorizado puede conducir a

[81] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[82] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

pérdidas directas, un incremento de las obligaciones de los clientes y otros problemas. [83]

Pueden ocurrir una variedad de problemas específicos de acceso y autenticación. Por ejemplo, los controles insuficientes pueden resultar en un ataque exitoso de usuarios inescrupulosos del Internet, quienes podrían acceder, recuperar y utilizar información sobre clientes del banco y en la introducción de un virus por terceras personas que entran en el sistema del banco. Además de los ataques externos a los sistemas de dinero electrónico y banca electrónica, los bancos se exponen a riesgos operativos relacionados con fraudes de empleados: los empleados podrían recuperar datos de autenticación a fin de acceder a las cuentas de clientes, o robar tarjetas de valor almacenado. Los errores involuntarios de los empleados pueden también comprometer los sistemas del banco. [84]

Una de las preocupaciones más importantes de las autoridades de supervisión es la fabricación de dinero electrónico falso, y esta preocupación se intensifica cuando los bancos no incorporan medidas suficientes para detectar y controlar este tipo de actividad delictuosa. El banco se enfrenta a un riesgo operativo generado por la falsificación de dinero, ya que puede ser responsable por el saldo del dinero electrónico falsificado. Además, pueden existir costos asociados con la reparación de un sistema alterado. [85]

[83] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[84] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[85] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

5.1.2 Diseño, ejecución y mantenimiento de sistemas

Un banco se enfrenta al riesgo de que los sistemas que selecciona no estén bien diseñados o ejecutados. Por ejemplo, un banco se expone al riesgo de una interrupción o retraso de sus sistemas cuando el sistema de banca electrónica o dinero electrónico que escoge es incompatible con las exigencias de los usuarios. [86]

Muchos bancos confiarán, probablemente, en suministradores externos de servicios y expertos externos para ejecutar, operar y apoyar partes de sus actividades de dinero electrónico y banca electrónica. Esta dependencia puede ser conveniente porque permite a los bancos contratar, fuera de la compañía, ciertos aspectos de la provisión de banca electrónica y actividades de dinero electrónico que no pueden proveer ellos mismos en forma económicamente rentable. [87]

Sin embargo, la dependencia de fuentes externas expone al banco a riesgos operativos. Los suministradores de servicios pueden no tener la experiencia necesaria para ofrecer los servicios esperados por el banco, o pueden no actualizar su tecnología en forma oportuna. [88]

Las operaciones de un suministrador de servicios pueden ser interrumpidas por problemas con sistemas, o dificultades financieras, impidiendo la entrega de productos o servicios por parte del banco. El ritmo acelerado que caracteriza los cambios de tecnología de la información representa otro riesgo para los bancos, es decir, el de los sistemas obsoletos. Por ejemplo, los programas de

[86] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[87] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[88] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

computadora que facilitan el uso por los consumidores de los productos de banca electrónica y dinero electrónico necesitarán ser actualizados, pero los canales de distribución de los programas actualizados presentan un riesgo para los bancos, ya que criminales o individuos maliciosos pueden interceptarlos y modificarlos. Además, los cambios rápidos de tecnología pueden no dar el tiempo necesario al personal para que comprenda bien los sistemas utilizados por el banco. Esto podría resultar en problemas operativos para los sistemas nuevos o actualizados. [89]

5.1.3 Mal uso por los clientes de los productos y servicios

Como es el caso con los servicios bancarios tradicionales, el mal uso por los clientes, ya sea intencional o involuntario, es otra fuente de riesgo operativo. Este riesgo puede verse intensificado cuando un banco no educa adecuadamente a sus clientes en cuanto a precauciones de seguridad. [90]

Además, ante la ausencia de medidas adecuadas para verificar las transacciones los clientes pueden repudiar transacciones que previamente han autorizado, creando pérdidas financieras para el banco. Los clientes que utilizan información personal (por ejemplo, información sobre la autenticación, números de tarjetas de crédito, o números de cuentas bancarias) en una transmisión electrónica insegura podría permitir a los criminales acceder a las cuentas de clientes. Como consecuencia el banco podrá incurrir en pérdidas financieras debidas a transacciones no autorizadas por los clientes. [91]

---

[89] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[90] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[91] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

Otra preocupación es el lavado de dinero como se señala en el informe de abril del Grupo de los Diez: “Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross-Border Issues”. [92]

5.2 Riesgo legal

El riesgo legal surge de las violaciones o incumplimientos de las leyes, reglas, reglamentos o prácticas establecidas, o cuando los derechos y obligaciones legales de las partes de una transacción no están bien definidos. Dada la relativa novedad de las actividades de banca electrónica y dinero electrónico, los derechos y obligaciones de las partes de dichas transacciones son, en algunos casos, poco precisas. Por ejemplo, la aplicación de algunos reglamentos de protección del consumidor a la banca electrónica y las actividades de dinero electrónico pueden no ser claras en algunos países. Además, el riesgo legal puede resultar de la incertidumbre en cuanto a la validez de los acuerdos suscritos por medios electrónicos. [93]

Los sistemas de dinero electrónico pueden ser atractivos para el lavado de dinero cuando ofrecen límites flexibles de saldos y transacciones, y disponen una posibilidad limitada de auditoría de las transacciones. La aplicación de reglas de lavado de dinero puede no ser apropiada para algunas formas de pagos electrónicos. Puesto que la banca electrónica puede ser conducida a distancia, los bancos pueden enfrentarse a mayores dificultades para aplicar métodos tradicionales de prevención y detección de la actividad criminal. [94]

---

[92] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[93] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[94] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

Los bancos que se dedican a la banca electrónica y a las actividades de dinero electrónico pueden enfrentarse a riesgos legales relacionados con divulgaciones a los clientes y protección de la confidencialidad. Los clientes que no reciben una información adecuada sobre sus derechos y obligaciones pueden iniciar acciones legales en contra del banco. La falta de una protección de la confidencialidad adecuada puede también someter al banco a sanciones de reglamentación en algunos países. Los bancos que eligen mejorar su servicio al cliente conectando sus lugares en el Internet a otros lugares, pueden también enfrentar riesgos legales. Un experto en computadoras puede utilizar el lugar para estafar a un cliente del banco, y el banco se enfrentaría a un litigio con dicho cliente. [95]

A medida que se expande el comercio electrónico, los bancos probablemente buscarán participar en sistemas de autenticación electrónica, como ser los que utilizan certificados digitales. El rol de autoridad de certificación puede exponer al banco a un riesgo legal. Por ejemplo, un banco que actúa como autoridad de certificación puede ser responsable de pérdidas financieras incurridas por las partes que confiaron en la certificación. Además, el riesgo legal puede presentarse si los bancos participan en sistemas nuevos de autentificación y no se especifican con claridad los derechos y obligaciones pertinentes. [96]

5.3. Gestión de riesgos

Para un número cada vez mayor de bancos, existe una razón estratégica para involucrarse en actividades de banca electrónica y dinero electrónico. Además, un mayor uso de la banca electrónica y dinero electrónico puede incrementar la eficiencia del sistema bancario y de pagos, beneficiando a clientes y

[95] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[96] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

comerciantes. Al mismo tiempo, y como se mencionó anteriormente, existen riesgos para los bancos que se dedican a actividades de banca electrónica y dinero electrónico. [97]

Estos riesgos deben compararse con los beneficios y los bancos deben ser capaces de manejar y controlar los riesgos y absorber toda pérdida asociada, si fuese necesario. Los riesgos que presentan la banca electrónica y el dinero electrónico deben ser evaluados en el contexto de los otros riesgos que enfrenta el banco. Si bien las actividades de banca electrónica y dinero electrónico pueden representar una parte relativamente pequeña de las actividades totales de los bancos, los supervisores pueden aun así exigir a la administración superior la seguridad que los sistemas esenciales no se ven amenazados por los riesgos que toma el banco. El ritmo acelerado de las innovaciones tecnológicas probablemente cambiará las características y el alcance de los riesgos que enfrentan los bancos con relación a la banca electrónica y al dinero electrónico. Los supervisores esperan que los bancos pongan en práctica procesos que permitan a la administración del banco responder a los riesgos actuales y adaptarse a los riesgos nuevos. [98]

Un proceso de gestión de riesgo que incluye los tres elementos básicos de evaluación de riesgos, control de riesgos y seguimiento de riesgos ayudará a los bancos y a los supervisores en el logro de estos objetivos. Los bancos pueden emplear un proceso de este tipo al comprometerse con nuevas actividades de banca electrónica y dinero electrónico y al evaluar los compromisos ya existentes. [99]

---

[97] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[98] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[99] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

Es de suma importancia que los bancos pongan en práctica un proceso general de gestión de riesgos, vigilado por el directorio y la administración superior. A medida que se identifican y evalúan nuevos riesgos en la banca electrónica y dinero electrónico, se debe mantener informado al directorio y a la administración superior de estos cambios. Antes de comenzar toda actividad nueva, se debe realizar un análisis amplio para que la administración superior pueda asegurarse que el proceso de gestión de riesgos es adecuado para evaluar, controlar y seguir todo riesgo generado por la nueva actividad propuesta. [100]

5.3.1 Evaluación de los riesgos

La evaluación de los riesgos es un proceso continuo, que comprende, normalmente, tres pasos. Primero, el banco puede realizar un análisis riguroso para identificar los riesgos y, donde sea posible, cuantificarlos. Si los riesgos no pueden ser cuantificados, la administración puede aún así identificar cómo pueden presentarse los riesgos potenciales y los pasos que ha dado para responder y limitar dichos riesgos. La administración del banco debe formarse un criterio razonable de la magnitud de todo riesgo con respecto, tanto al efecto que podría tener sobre el banco (incluyendo el efecto potencial máximo), como a la probabilidad que dicho evento ocurra. [101]

El segundo paso en la evaluación de riesgos es la determinación por parte del directorio y de la administración superior de la tolerancia al riesgo del banco, basado en la evaluación de las pérdidas que el banco podría sostener en el evento de la materialización de un problema dado. Finalmente, la

[100] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[101] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

administración puede comparar su tolerancia al riesgo con su evaluación de la magnitud del riesgo para confirmar si la exposición al riesgo se adapta a los límites de tolerancia. [102]

5.3.2 Manejo y control de los riesgos

Habiendo realizado una evaluación de los riesgos y de su tolerancia al riesgo, la administración del banco debe dar pasos para manejar y controlar los riesgos. Esta fase del proceso de gestión de riesgos incluye actividades tales como la ejecución de políticas y medidas de seguridad, la coordinación interna de las comunicaciones, la evaluación y actualización de productos y servicios, la ejecución de medidas para garantizar el control y manejo de los riesgos de contrataciones fuera de la compañía, la provisión de divulgaciones y educación del cliente y la preparación de planes para contingencias. La administración superior debe asegurar que el personal responsable de la aplicación de los límites de riesgo tiene autoridad independiente de las unidades de negocios encargadas de las actividades de banca electrónica y dinero electrónico. Los bancos aumentan su capacidad de controlar y manejar los diferentes riesgos inherentes a toda actividad, cuando las políticas y los procedimientos se incluyen en documentos escritos, puestos a la disposición del personal pertinente. [103]

5.3.2.1 Medidas y políticas de seguridad

La seguridad es la combinación de sistemas, aplicaciones y controles internos utilizados para salvaguardar la integridad, autenticidad y confidencialidad del procesamiento de datos y de los procesos de operación. Una seguridad

[102] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[103] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

adecuada depende de la formulación y ejecución de políticas acertadas y medidas de seguridad para los procesos del banco y para la comunicación entre el banco y las partes externas. Las políticas y medidas de seguridad pueden limitar el riesgo de ataques externos e internos a los sistemas de banca electrónica y dinero electrónico, así como el riesgo a la reputación generado por las violaciones de seguridad. [104]

La política de seguridad refleja la voluntad de la administración para apoyar la información sobre seguridad, y proporciona una explicación de la organización de seguridad del banco. Además, esta política establece principios directivos que definen la tolerancia al riesgo de seguridad del banco. Puede también definir las responsabilidades del diseño, ejecución y aplicación de medidas de información sobre seguridad, así como establecer procedimientos para evaluar el cumplimiento con las políticas, aplicar medidas de disciplina e informar sobre violaciones de seguridad. Las medidas de seguridad son una combinación de herramientas de hardware y software, y administración de personal, que contribuyen a la elaboración de sistemas y operaciones seguras. [105]

La administración superior debe analizar la seguridad como un proceso amplio que es tan fuerte como la parte más débil del proceso. Los bancos pueden escoger de una variedad de medidas de seguridad para prevenir o mitigar los ataques internos o externos para el mal uso de la banca electrónica. Estas medidas, incluyen, criptogramas, claves, firewalls, controles de virus, y pre-selección de empleados. [106]

---

[104] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[105] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[106] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

Para los criptogramas se utilizan algoritmos criptográficos para codificar datos claros de textos en textos cifrados para evitar observaciones no autorizadas. Las palabras claves, frases claves, números de identificación personal, fichas basadas en el hardware, y la biometría son técnicas que se usan para controlar el acceso e identificar a los usuarios. [107]

Los firewalls son combinaciones de hardware y software que seleccionan y limitan el acceso externo a los sistemas internos conectados a redes abiertas como el Internet. Los firewalls pueden también separar segmentos de las redes internas utilizando tecnología de Internet (Intranets). [108]

La tecnología de los firewalls, cuando es diseñada y ejecutada en forma correcta, puede ser un medio efectivo para controlar el acceso y salvaguardar la confidencialidad e integridad de la información. Dado que esta tecnología es de diseño complejo y costoso, sus puntos fuertes y capacidades deben ser proporcionales a la sensibilidad de la información a ser protegida. Un diseño bien planificado debería incluir requisitos de seguridad para toda la empresa, procedimientos de operación claros, separación de funciones, y selección de personal confiable responsable de la configuración y operación del firewall. [109]

Si bien los firewalls seleccionan los mensajes que son recibidos, no necesariamente protegen contra los programas con virus que son recuperados del Internet. Consecuentemente, la administración debe elaborar controles de prevención y detección para reducir las probabilidades de un ataque de virus y la destrucción de datos, particularmente en el caso de la banca a distancia. Los

[107] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[108] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[109] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

programas normalmente utilizados para mitigar el riesgo de una infección por virus pueden incluir controles de red, políticas para el usuario final, entrenamiento de los usuarios y programas para la detección de virus. [110]

No todas las amenazas a la seguridad provienen del exterior. Los sistemas de banca electrónica y dinero electrónico deben también ser protegidos, hasta donde sea posible, contra las autoridades no autorizadas de los empleados actuales y anteriores. Como es el caso con las actividades tradicionales de la banca, la verificación de los antecedentes de nuevos empleados, empleados temporales y consultores, así como los controles internos y la separación de funciones son precauciones importantes para la protección del sistema. [111]

En el caso del dinero electrónico, existen medidas de seguridad adicionales que pueden ayudar a evitar los ataques y el mal uso, incluyendo la falsificación y el lavado de dinero. Estas medidas podrían incluir una comunicación interactiva con el usuario o con un operador central; el seguimiento de las transacciones individuales; el mantenimiento de registros acumulables en una central de datos; el uso de dispositivos a prueba de alteraciones incorporados en las tarjetas de valor almacenado y en el hardware comercial; y el uso de límites de valor y fechas de vencimiento en las tarjetas de valor almacenado. [112]

5.3.2.2 Evaluación y perfeccionamiento

La evaluación de productos y servicios antes de su comercialización generalizada puede también ayudar a limitar los riesgos operativos y a la

[110] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[111] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[112] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

reputación. La realización de pruebas comprueba que los equipos y sistemas funcionan adecuadamente y producen los resultados deseados. Los programas piloto o los prototipos pueden ser útiles para el desarrollo de nuevas aplicaciones. El riesgo de la interrupción de los sistemas puede también ser disminuido con políticas de revisión regular de las capacidades del hardware y software existentes. [113]

5.3.3 Riesgos de seguimiento

Un seguimiento constante es un aspecto importante en todo proceso de gestión de riesgos. En el caso de la banca electrónica y del dinero electrónico el seguimiento es particularmente importante, ya que la naturaleza de estas actividades puede cambiar rápidamente a medida que se producen innovaciones y debido a la dependencia de ciertos productos del uso de redes abiertas, como el Internet. Dos elementos importantes del seguimiento son la verificación y la auditoria de los sistemas. [114]

5.3.3.1 Verificación y vigilancia de los sistemas

La verificación de la operación de los sistemas puede ayudar a detectar actividades inusuales y advertir problemas, interrupciones y ataques importantes al sistema. Las pruebas de penetración se dirigen a la identificación, aislamiento y confirmación de fallas en el diseño y ejecución de los mecanismos de seguridad mediante intentos controlados de penetrar el sistema fuera de los procedimientos normales. La vigilancia es una forma de seguimiento para la cual se utilizan aplicaciones de software y auditoria para controlar la actividad. Contrariamente a las pruebas de penetración la vigilancia

[113] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[114] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

se concentra en el seguimiento de operaciones de rutina, la investigación de anomalías y la formulación de criterios relacionados con la eficiencia de la seguridad, verificando el cumplimiento con las políticas de seguridad. [115]

5.3.3.2 Auditorias

Las auditorias (internas y externas) brindan un mecanismo de control independiente para detectar deficiencias y reducir, a un mínimo, los riesgos que comporta el suministro de servicios de banca electrónica y dinero electrónico. El rol de un auditor es velar por la elaboración de normas, políticas y procedimientos apropiados, y confirmar el compromiso del banco con los mismos. El personal de auditoria debe tener la experiencia necesaria para llevar a cabo un análisis preciso. El auditor interno debe ser independiente de los empleados que intervienen en la toma de decisiones relacionadas con la gestión de riesgos. Para completar la auditoria interna, la administración puede hacer uso de auditores externos calificados, como ser, consultores en seguridad u otros profesionales, para obtener una evaluación independiente de las actividades de banca electrónica o dinero electrónico. [116]

Como conclusión, la banca electrónica o e-banking es una buena oportunidad para los bancos de ampliar sus servicios, productos e incluso su alcance, pero a su vez debe de mantener una buena vigilancia y métodos de protección para impedir que estos servicios sean usados de forma errónea e ilegalmente de forma que la cause más problemas al banco que beneficios. Actualmente los bancos con este tipo de servicios agruparon los servicios de forma que para hacer uso de cierto grupo (transferencias entre cuentas, etc.) se debe solicitar por teléfono y en ocasiones de forma personal llenando un formulario para el

[115] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf
[116] http://asbaweb.org/Documentos/publicaciones/98-PUB-ESP-Gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf

caso y otro grupo (pagos, consultas, etc.) de forma normal haciendo uso de su PIN o contraseña para accederlos.

6. BASILEA Y EL RIESGO FINANCIERO

6.1 Riesgo financiero

El riesgo es la probabilidad de un evento y sus consecuencias. El riesgo financiero se refiere a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras para una organización. [117]

El concepto debe entenderse en sentido amplio, incluyendo la posibilidad de que los resultados financieros sean mayores o menores de los esperados. De hecho, habida la posibilidad de que los inversores realicen apuestas financieras en contra del mercado, movimientos de éstos en una u otra dirección pueden generar tanto ganancias o pérdidas en función de la estrategia de inversión. [118]

6.2 Tipos de riesgos financieros [119]

Riesgo de mercado, asociado a las fluctuaciones de los mercados financieros, y en el que se distinguen:

- Riesgo de cambio, consecuencia de la volatilidad del mercado de divisas.
- Riesgo de tipo de interés, consecuencia de la volatilidad de los tipos de interés.
- Riesgo de mercado (en acepción restringida), que se refiere específicamente a la volatilidad de los mercados de instrumentos financieros tales como: acciones, deuda, derivados, etc.
- Riesgo de crédito, consecuencia de la posibilidad de que una de las partes de un contrato financiero no asuma sus obligaciones.
- Riesgo de liquidez o de financiación, y que se refiere al hecho de que una de las partes de un contrato financiero no pueda obtener la liquidez

[117] http://es.wikipedia.org/wiki/Riesgo_financiero
[118] http://es.wikipedia.org/wiki/Riesgo_financiero
[119] http://es.wikipedia.org/wiki/Riesgo_financiero

necesaria para asumir sus obligaciones a pesar de disponer de los activos —que no puede vender con la suficiente rapidez y al precio adecuado— y la voluntad de hacerlo.

6.3 Antecedentes de BASILEA

6.3.1 BASILEA 1

En 1988, el Comité de Basilea, compuesto por los gobernadores de los bancos centrales de Alemania, Bélgica, Canadá, España, EE. UU., Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza publicó el primero de los Acuerdos de Basilea, un conjunto de recomendaciones alrededor de una idea principal. Se trataba de un conjunto de recomendaciones para establecer un capital mínimo que debía tener una entidad bancaria en función de los riesgos que afrontaba. [120]

El acuerdo establecía una definición de capital regulatorio compuesto por elementos que se agrupan en dos categorías si cumplen ciertos requisitos de permanencia, de capacidad de absorción de pérdidas y de protección ante quiebra. Este capital debe ser suficiente para hacer frente a los riesgos de crédito, mercado y tipo de cambio. Cada uno de estos riesgos se medía con unos criterios aproximados y sencillos. [121]

6.3.2 BASILEA 2

6.3.2.1 Introducción

La principal limitación del acuerdo de Basilea I es que es insensible a las variaciones de riesgo y que ignora una dimensión esencial: la de la calidad crediticia y, por lo tanto, la diversa probabilidad de incumplimiento de los

[120] http://es.wikipedia.org/wiki/Basilea_II
[121] http://es.wikipedia.org/wiki/Basilea_II

distintos prestatarios. Es decir, consideraba que todos los créditos tenían la misma probabilidad de incumplir. [122]

Para superarla, el Comité de Basilea propuso en 2004 un nuevo conjunto de recomendaciones. Éstas se apoyan en los siguientes pilares que a continuación se describen. [123]

6.3.2.1.1 Pilar I: el cálculo de los requisitos mínimos de capital

Constituye el núcleo del acuerdo e incluye una serie de novedades con respecto al anterior: tiene en cuenta la calidad crediticia de los prestatarios (utilizando ratings externos o internos) y añade requisitos de capital por el riesgo operacional. [124]

La norma de Basilea I, que exige fondos propios > 8% de activos de riesgo, considerando: (riesgo de crédito + riesgo de negociación+ riesgo de tipo de cambio) mientras que ahora considera: [125]

(Riesgo de crédito + Riesgo de negociación+ Riesgo de tipo de cambio + Riesgo operacional)

El riesgo de crédito se calcula a través de tres componentes fundamentales: [126]

- PD, o probabilidad de incumplimiento
- LGD, o pérdida en el momento de incumplimiento (también se conoce como "severidad")
- EAD, o exposición en el momento del incumplimiento

[122] http://es.wikipedia.org/wiki/Basilea_II
[123] http://es.wikipedia.org/wiki/Basilea_II
[124] http://es.wikipedia.org/wiki/Basilea_II
[125] http://es.wikipedia.org/wiki/Basilea_II
[126] http://es.wikipedia.org/wiki/Basilea_II

Habida cuenta de la existencia de bancos con distintos niveles de sofisticación, el acuerdo propone distintos métodos para el cálculo del riesgo crediticio. En el método estándar, la PD y la LGD se calculan implícitamente a través de las calificaciones de riesgo crediticio publicadas por empresas especializadas (agencias de rating) utilizando una serie de baremos. [127]

En cambio, los bancos más sofisticados pueden, bajo cierto número de condiciones, optar por el método de ratings internos avanzado (AIRB), que les permite utilizar sus propios mecanismos de evaluación del riesgo y realizar sus propias estimaciones. [128]

Existe un método alternativo e intermedio (fundación IRB) en el que los bancos pueden estimar la PD, el parámetro de riesgo más básico, y utilizar en cambio valores pre calculado por el regulador para la LGD. [129]

Hasta la fecha, muchas entidades bancarias gestionaban su riesgo crediticio en función de la pérdida esperada, EL = PDxLGDxEAD, que determinaba su nivel de provisiones frente a incumplimientos. La nueva normativa establece una nueva medida, el RWA, que se fija no en la media sino en un cuantil elevado de la distribución de pérdida estimada a través de una aproximación basada en la distribución normal. [130]

[127] http://es.wikipedia.org/wiki/Basilea_II
[128] http://es.wikipedia.org/wiki/Basilea_II
[129] http://es.wikipedia.org/wiki/Basilea_II
[130] http://es.wikipedia.org/wiki/Basilea_II

El riesgo de crédito se cuantifica entonces como la suma de los RWA correspondientes a cada una de las exposiciones que conforman el activo de la entidad. [131]

Dentro del riesgo de crédito se otorga un tratamiento especial a las titulizaciones, para las cuales se debe analizar si existe una transferencia efectiva y significativa del riesgo, y si son operaciones originadas por la entidad o generados por otras. [132]

El riesgo de negociación y el riesgo de tipo de cambio se siguen calculando conforme a Basilea I. [133]

El riesgo operacional se calcula multiplicando los ingresos por un porcentaje que puede ir desde el 12% hasta el 18%. Existen tres métodos alternativos para calcularlo dependiendo del grado de sofisticación de la entidad bancaria. [134]

Por último, la definición de capital regulatorio disponible permanece casi igual a la de Basilea I. [135]

Hay que advertir una objeción en este cálculo del riesgo, que se ignora los efectos agravantes/mitigantes de la concentración/diversificación de riesgos (estructura de correlación probabilística entre las diversas exposiciones). Esta es una de las principales diferencias entre capital regulatorio y capital económico. [136]

[131] http://es.wikipedia.org/wiki/Basilea_II
[132] http://es.wikipedia.org/wiki/Basilea_II
[133] http://es.wikipedia.org/wiki/Basilea_II
[134] http://es.wikipedia.org/wiki/Basilea_II
[135] http://es.wikipedia.org/wiki/Basilea_II
[136] http://es.wikipedia.org/wiki/Basilea_II

6.3.2.1.2 Pilar II: el proceso de supervisión de la gestión de los fondos propios

Los organismos supervisores nacionales están capacitados para incrementar el nivel de prudencia exigido a los bancos bajo su jurisdicción. Además, deben validar tanto los métodos estadísticos empleados para calcular los parámetros exigidos en el primer pilar como la suficiencia de los niveles de fondos propios para hacer frente a una crisis económica, pudiendo obligar a las entidades a incrementarlos en función de los resultados. [137]

Para poder validar los métodos estadísticos, los bancos estarán obligados a almacenar datos de información crediticia durante periodos largos, de cinco a siete años, a garantizar su adecuada auditoria y a superar pruebas de stress.[138]

Además se exige que la alta dirección del banco se involucre activamente en el control de riesgos y en la planificación futura de las necesidades de capital. Esta auto evaluación de las necesidades de capital debe ser discutida entre la alta dirección y el supervisor bancario. Como el banco es libre para elegir la metodología para su auto evaluación, se pueden considerar otros riesgos que no se contemplan en el cálculo regulatorio, tales como el riesgo de concentración y/o diversificación, el riesgo de liquidez, el riesgo de la reputación, el riesgo de pensiones, etc. [139]

Para grupos financieros multinacionales se establecen colegios supervisores que, bajo la coordinación del supervisor de la entidad matriz, se encargan de la coordinación internacional de la supervisión del grupo financiero.

[137] http://es.wikipedia.org/wiki/Basilea_II
[138] http://es.wikipedia.org/wiki/Basilea_II
[139] http://es.wikipedia.org/wiki/Basilea_II

6.3.2.1.3 Pilar III: La disciplina de mercado

El acuerdo establece normas de transparencia y define la publicación periódica de información acerca de su exposición a los diferentes riesgos y la suficiencia de sus fondos propios. El objetivo es: [140]

1) La generalización de las buenas prácticas bancarias y su homogeneización internacional.

2) La reconciliación de los puntos de vista financiero, contable y de la gestión del riesgo sobre la base de la información acumulada por las entidades.

3) La transparencia financiera a través de la homogeneización de los informes de riesgo publicados por los bancos. [141]

Inicialmente la información incluirá: descripción de la gestión de riesgos (objetivos, políticas, estructura, organización, alcance, políticas de cobertura y mitigación de riesgos), aspectos técnicos del cálculo del capital (diferencias en la consolidación financiera y regulatoria), descripción de la gestión de capital, composición detallada de los elementos del capital regulatorio disponible y requerimientos de capital por cada tipo de riesgo (indicando el método de cálculo utilizado). [142]

El requisito inicial es que se publique al menos anualmente, aunque es previsible que la frecuencia será mayor (al menos resumida) y a sus contenidos mínimos se irá añadiendo la información que el mercado exija en cada momento. [143]

[140] http://es.wikipedia.org/wiki/Basilea_II
[141] http://es.wikipedia.org/wiki/Basilea_II
[142] http://es.wikipedia.org/wiki/Basilea_II
[143] http://es.wikipedia.org/wiki/Basilea_II

6.3.2.2 Implantación

El Comité de Basilea ha creado un subgrupo de trabajo para colaborar en la implantación internacional del acuerdo con el Accord Implementation Group (AIG). [144]

A través de una encuesta realizada por el Financial Stability Institute (FSI), al menos 95 países (adicionales a los 13 miembros del Comité de Basilea) indicaron que implantarían BIS II. [145]
Muchos países han anunciado ya calendarios de implantación. Basilea II ya se ha implantado en la toda la Unión Europea, Japón y Australia (13 países en toda Asia) [146]

La implantación en Asia está sentando tendencias que se imitarán en el resto del mundo, especialmente en lo referente al Pilar III (información pública). La Implantación en Europa se ha realizado a través de directivas (leyes de obligado cumplimiento en todos los países de la UE), y cuenta con la colaboración especial del CEBS (Comité de Supervisores Bancarios Europeos). En ciertos aspectos está liderando el desarrollo futuro de la regulación, como por ejemplo en las reglas de funcionamiento de los colegios de supervisores. [147]

En América, la implantación va más atrasada. Estados Unidos está siendo un caso especial, ya que no será generalizada para todos sus bancos y tendrá normas especiales. Canadá la implantación va más avanzada que en los Estados Unidos, y algunos países latinoamericanos están siendo muy activos en la adaptación de sus normas nacionales para que sea posible la transición

[144] http://es.wikipedia.org/wiki/Basilea_II
[145] http://es.wikipedia.org/wiki/Basilea_II
[146] http://es.wikipedia.org/wiki/Basilea_II
[147] http://es.wikipedia.org/wiki/Basilea_II

(no puede ser más rápida por la necesidad de cambiar leyes y porque también están adoptando las normas internacionales de contabilidad -NICs-).[148]

6.3.2.3 Críticas y modificaciones previstas

Las principales críticas se han centrado en que se considera que es demasiado "pro cíclico" (podría acentuar la debilidad económica en caso de recesión y fomentarla en época de bonanza). [149]

Algunas imperfecciones del modelo se han puesto de manifiesto con la crisis económica actual y ya se están proponiendo algunas modificaciones. Los puntos más discutidos son: [150]

- Titulizaciones
- Divulgaciones del Pilar III
- Riesgo de mercado
- Sistemas de control de riesgos
- Hipotecas
- Los sistemas de Información y BASILEA

Los sistemas de reporte de créditos y préstamos, que proporcionan un rápido acceso a la información estandarizada sobre el pasado desempeño de los deudores (incluyendo el historial de empresas y consumidores), son un importante elemento institucional para los mercados financieros. Hasta hace poco, estos sistemas habían recibido limitada atención pero esta situación está cambiando en diversas formas. [151]

[148] http://es.wikipedia.org/wiki/Basilea_II
[149] http://es.wikipedia.org/wiki/Basilea_II
[150] http://es.wikipedia.org/wiki/Basilea_II
[151] http://es.wikipedia.org/wiki/Basilea_II

Los avances en las tecnologías de computación y telecomunicaciones en los países en desarrollo han facilitado y abaratado el desarrollo de bases de datos efectivas. Muchas agencias de supervisión bancarias han establecido o expandido los registros de crédito, con el objeto de mejorar la información de exposiciones agregadas de riesgo de los deudores. En la mayoría de los países los supervisores están diseñando normas que adapten las características de sus sistemas financieros a las nuevas recomendaciones emitidas por el Comité de Supervisión de Basilea, conocidas como Basilea II, en las que es condición fundamental para el cálculo del riesgo crediticio es mantener un registro adecuado de los créditos. Los instrumentos de decisión, tales como la calificación de crédito, han incrementado también el valor de los historiales de crédito y reforzado los incentivos para que los bancos compartan sus datos sobre crédito. [152]

Muchos de los países de América Latina y el Caribe encaran dificultades similares con respecto a los sistemas de información de crédito, incluidos problemas con el marco legal, la falta de capacidad institucional para hacer cumplir las leyes y regulaciones sobre información de crédito, limitada disponibilidad de datos positivos sobre crédito y varias debilidades en los registros de crédito operados con propósitos de supervisión. Estos asuntos han sido también identificados como objeto de preocupación en los FSAP en los países de la región. [153]

En los países de América Latina y el Caribe la industria del registro de crédito está típicamente dominada por una sola firma o por organizaciones no lucrativas, tales como las cámaras de comercio o asociaciones bancarias, que colectan datos sobre crédito en beneficio de sus miembros. Las limitaciones de

[152] http://es.wikipedia.org/wiki/Basilea_II
[153] http://es.wikipedia.org/wiki/Basilea_II

los registros de crédito privados, junto con, en algunos casos, un marco legal y regulador que desalienta el compartir información en el sector privado, han inducido a los funcionarios gubernamentales en muchas naciones, a establecer registros de información crediticia públicamente operados, típicamente a través del banco central o la agencia de supervisión bancaria. [154]

6.4 Seguridad de la información - mejores prácticas - BCRA 4609 (Basilea II)

El 27 de diciembre de 2006, el Banco Central de la República Argentina publicó la Comunicación A 4609, dirigida a entidades financieras y a las cámaras electrónicas de compensación, sobre los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con la tecnología informática y sistemas de información. El 1 de julio de 2007 vencía el plazo para implementar la norma y se habló de prórrogas. Así mismo, se mencionó que en septiembre del 2009, comenzaron las primeras auditorias.[155]

El objetivo es encaminar la actividad financiera a un marco estándar de las mejores prácticas, dicho marco es Basilea II, documento que publicado en junio de 2004 por el Comité de Supervisión Bancaria de Basilea. Comenzando a regir en diciembre del 2006 para los países del G-10 (Bélgica, Canadá, Francia, Alemania, Italia, Japón, Holanda, Suecia, Suiza, UK y USA), convirtiéndose así en un estándar a nivel internacional para la medición y gestión de riesgos, siendo reconocido por más de 130 países, el Fondo Monetario Internacional y el Banco Mundial como una buena práctica internacional. [156]

[154] http://es.wikipedia.org/wiki/Basilea_II
[155] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf
[156] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf

Así mismo el BCRA, publico la Hoja de ruta para la implementación de Basilea II, cuya introducción es como sigue. [157]

En junio de 2004 el Comité de Supervisión Bancaria de Basilea publicó el documento "Convergencia internacional de medidas y normas de capital. Marco revisado" (Basilea II o Nuevo Marco), el que establece nuevos criterios para la determinación del capital regulatorio de las entidades financieras. [158]
A diferencia de su antecesor -el Acuerdo de Basilea de 1988- el Nuevo Marco tiene una visión integral del tratamiento de los riesgos asumidos por las entidades, al mismo tiempo que brinda mayor flexibilidad que el Acuerdo de 1988 al ofrecer una gama de enfoques (en lugar de una única alternativa) para la medición del capital regulatorio. Basilea II está estructurada en tres "pilares", el primero referido a los requisitos mínimos de capital; el segundo respecto del proceso de revisión del supervisor y el tercero, sobre disciplina de mercado. [159]

Respecto de los requisitos mínimos de capital correspondientes al Pilar I, el Banco Central de la República Argentina (BCRA) ha resuelto la adopción del enfoque estandarizado simplificado para riesgo crediticio, cuya implementación efectiva regirá a partir de enero del año 2010, y dado el enfoque determinado, no implicará mayores modificaciones ni variaciones en el cálculo ni en la exigencia global de capital para las entidades financieras. En lo que hace a la exigencia de capital por riesgo operacional, el BCRA considera conveniente seguir analizando entre las alternativas disponibles para su medición en orden a identificar la que mejor se aplica al sistema financiero local, no obstante lo cual propiciará la adopción de buenas prácticas en materia de administración de este riesgo. Adicionalmente, el BCRA mantendrá el esquema de cómputo de la exigencia de capital por riesgo de mercado, el que se encuentra en línea con

[157] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf
[158] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf
[159] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf

las disposiciones dadas por el Comité de Basilea en el año 1996 y respecto del cual Basilea II no introdujo modificaciones, así como la exigencia de capital por riesgo de tasa de interés, la que es incorporada por Basilea II dentro de los riesgos a ser cuantificados en el Pilar II. [160]

También, se prevé la adopción de las medidas necesarias para la plena implementación de los Pilares II y III del Nuevo Marco, con anterioridad a la plena vigencia de los requisitos de capital contenidos en el Pilar I, tal como lo establecen las buenas prácticas sugeridas por el Comité de Basilea para una sana implementación del Nuevo Marco. [161]

El proceso de adopción de Basilea II se prevé que se realice de manera gradual hasta su implementación completa a partir del año 2010. El esquema a continuación contiene los lineamientos generales de los pasos a realizar en pos de la adopción del Nuevo Marco de Capitales. El BCRA irá dando a conocer cronogramas con las tareas específicas a desarrollar, a medida que se avance en el proceso de implementación. [162]

[160] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf
[161] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf
[162] http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf

7. ACTUALIDAD DE LA VIGILANCIA EN EL ÁREA BANCARIA

Es habitual ver cualquier tipo de vigilancia en los bancos que se visitan, ya que lo que tratan de hacer es que el cliente se sienta seguro cuando está dentro de la institución, además de darle la seguridad a los cuenta habientes de que su dinero no corre peligro y mantenerles fija la idea de que el banco es el mejor lugar para guardar su dinero.

Con los constantes robos a bancos y a cuenta habientes, las mismas instituciones se han visto en la necesidad de mejorar sus sistemas de vigilancia. Como se sabe, la vigilancia en los grandes bancos de los países desarrollados está a un nivel tecnológico que muy pocos pueden imaginar, pero es normal ya que la información y los valores que guardan tienen un alto valor. Pero que pasa con los bancos pequeños o los bancos de países no tan desarrollados como en Guatemala, pues ellos han tenido que ingeniárselas para sobrevivir con sistemas de seguridad baratos, aunque en ocasiones no tan eficientes como se desearía.

Los bancos pequeños que encontraban muy caro el pagar por un sistema de vigilancia análogo, pueden verse beneficiados de los últimos adelantos tecnológicos en el ramo, como por ejemplo, la vigilancia por video digital (grabación digital). En el caso del video digital, representaría un costo menor, imágenes más claras y una flexibilidad en el almacenamiento.

Aunque la tecnología ha avanzado mucho en nuestros tiempos y además de los últimos avances en el ramo de la inteligencia artificial, siempre es necesaria la presencia de seres humanos para que se encarguen de manejar los aparatos, de instalarlos y de darles mantenimiento. Pero a largo plazo la institución

bancaria vería sus frutos de la inversión al proporcionar un sentimiento de seguridad a sus cuenta-habientes y empresas que ellos manejen.

A pesar de las varias tecnologías de vigilancia existentes, se observa una tendencia en el área de sistemas de vigilancia por video digital. En la página de la NYBA (New York Bankers Association) se puede encontrar un artículo que habla sobre el sistema IRIS (Image Retentioin Information System) donde ellos comenta “Con el sistema de video digital IRIS, los bancos miembros pueden implementar un sistema de vigilancia efectivo en el costo, flexible, modular y escalable...”, como se observa, la vigilancia por medio de video cámaras no ha pasado de moda sino que ha ido evolucionando a través de los tiempos.

La vigilancia, como concepto global, ha ido incrementado su interés en distintos campos de aplicación siendo uno de ellos el área bancaria. Desde lo eventos ocurridos el 11 de septiembre, el desarrollo de tecnología de vigilancia dio un salto enorme, debido a la necesidad de vigilar cualquier individuo, actividad o grupo que fuera una amenaza latente para los intereses de un país, sociedad o institución. Pero no todo es malo, aunque la privacidad se ha visto mermada por dicho avance tecnológico, depende de cómo y a qué se aplique la tecnología puede ser catalogada como buena o mala.

En el área de bancaria que es el área de estudio a la que se enfoca esta investigación, puede verse el lado bueno de la tecnología de vigilancia, no solo para mantener un ambiente seguro dentro de la institución sino que también para ser un banco que pueda remarcar la palabra seguridad en cualquier documento, conversación, etc.

8. TÉCNICAS VIABLES DE VIGILANCIA PARA EL ÁREA BANCARIA

De todas las técnicas mencionadas en los primeros capítulos de esta investigación, solo algunas son viables para los bancos de Guatemala. Tomando en cuenta que algunas de ellas no consiguen mejorar la seguridad y además pueden ser difíciles de implementar en un espacio cerrado como las instalaciones de un banco.

A continuación se muestra una tabla comparativa entre las técnicas que se consideraron viables para un banco. Se tomaron varios aspectos para poder evaluar a cada una de las técnicas seleccionadas.

Tabla I Comparación de técnicas de surveillance.

Nombre	Nivel de Seguridad	Costo	Ubicación recomendada
Equipo biométrico	Medio	Medio	Bóvedas y puertas
Video digital y CCTV	Medio	Medio	En cualquier lugar dentro del edificio que se quiera vigilar.
Reconocimiento de patrones corporales	Alto	Medio	Igual que con el CCTV, ya que esta se adhiere al software utilizado en video digital.
Sensores de audio y micrófonos.	Bajo	Medio	Bóvedas y oficinas donde se guarde

			información valiosa
FLIR, visor infrarrojo	Alto	Alto	Igual que con los sensores de sonido
Detectores de masa por ondas de milímetro	Alto	Medio	Entradas y salidas de la estructura física del banco
Intercepción del tráfico de Internet y de la red interna.	Medio	Bajo	Desde el servidor o desde una máquina acondicionada para dicha tarea y se aplica para cualquier PC conectada a la Red.
Rastreo de celulares	Bajo	Bajo	Oficina de seguridad
Reconocimiento de patrones de voz y palabras clave	Alto	Medio	Bóveda
Tarjetas de proximidad inteligentes	Alto	Alto	En cualquier puerta ya que su uso común es en lugar de las llaves normales.

De las anteriores, la más popular es la del circuito cerrado de televisión o CCTV. Dicha tecnología, por su costo de implementación y adquisición, es la más utilizada por cualquier banco, ya sea grande o pequeño. Por tal razón se han creado mejoras a dicha técnica, como el uso de video digital para almacenar imágenes en una base de datos y el video por IP que es solamente el acceso al CCTV de una institución por medio de la Internet o de cualquier red.

Aunque las otras técnicas no son tan utilizadas o reconocidas, ayudan a subir el nivel de seguridad que un banco puede tener, así como el control sobre sus empleados y actividades que se desarrollan dentro de él. Tomando en cuenta que el CCTV puede verse limitado por objetos que obstruyan su visibilidad (con intención o sin intención) o la posición en la que se encuentran instalados.

En resumen, todas las técnicas se complementan de forma que una técnica apoya a otra en aspectos que esta no toma en cuenta o que no puede acceder por su ubicación física. Con el uso de cada técnica en conjunto y las otras se obtiene un mejor desempeño de las herramientas de vigilancia y un mejor nivel de seguridad tanto para las instalaciones como para la información de los cuenta habientes y de la misma entidad bancaria.

9. BENEFICIOS OBTENIDOS DE LAS TÉCNICAS Y TECNOLOGÍA DE VIGILANCIA PARA EL ÁREA BANCARIA

9.1 CCTV y video digital

EL circuito cerrado de televisión (CCTV) aunado a las cámaras de video digital provee una mejor detección y prevención de amenazas, a un bajo costo y una disminución en la responsabilidad.

También permite la revisión remota de videos, tomando en cuenta que los mismos son almacenados en una computadora, desde cualquier parte de la red. Además de iniciar eventos de grabación automáticos, tales como de intrusos, alarma de incendios o detección de movimiento. El sistema entonces puede activar una secuencia de actividades automatizadas, tal como contactar a la empresa que le brinda seguridad o a otras autoridades.

En pocas palabras, reduce la interacción manual que se mantenía con los sistemas análogos, ya que el software hace prácticamente todo.

9.2 Equipo biométrico

Permite el restringir el acceso al personal a áreas del banco, además de poder dejar un registro almacenado en una PC sobre la identidad de la persona que ingreso a dicha área. De esa forma se sabrá con exactitud a qué hora y fecha ingreso y egreso un empleado de alguna área protegida.

9.3 Reconocimiento de patrones corporales

Esta técnica puede decirse que es aunada a la técnica mencionada con anterioridad de CCTV y video digital. Lo que promueve es que los rostros y

formas humanas obtenidas digitalmente, sean almacenadas por aparte para cada empleado, así el sistema puede aprender patrones de conducta de los empleados al detectarlos por el sistema de video y mantener una bitácora de sus actividades dentro de las instalaciones.

Esto a su vez permitiría lo que se conoce como detección en tiempo real de anatomía humana, lo cual permitiría reconocer actividades anómalas del personal tal como si esta persona ingresara en alguna área del banco a la que nunca había entrado, etc.

9.4 Sensores de audio y micrófonos

Permitirían el grabar conversaciones, ruidos o voces en una habitación, de forma que pueda detectarse amenazas para la institución, para los clientes del banco e incluso para el personal.

9.5 FLIR (Visores infrarrojos)

Estos detectan las ondas de calor que emite el cuerpo humano, incluso aunque se tenga de por medio muros. Estos visores ayudan a las CCTV y al video digital a mantener la vigilancia tomando el caso de que las cámaras fueran obstruidas, tapadas, removidas e incluso averiadas, los visores mantendrían siempre las imágenes de las actividades que se realicen. Además, suelen ser usados en lugares con poco acceso interno o con poca luz.

Estos visores permiten diferenciar un ser vivo de un objeto inanimado en lugares con escasa luminosidad.

9.6 Detectores de masa por ondas de milímetro

Estos son los que vienen a reemplazar a los detectores de metales comunes que aprecia en cualquier entrada de los bancos del sistema. Estos no detectan el metal, sino que captan la porción de ondas de milímetros del espectro

electromagnético emitido por el cuerpo humano, con esto se logra detectar objetos (su forma) que no pertenezcan al cuerpo y esta imagen es proyectada en los monitores, esto es catalogado por sus creadores como ver bajo la ropa.

9.7 Intercepción del tráfico de Internet y de la red interna

Permite vigilar los sitios e información que los empleados bancarios accedan tanto de Internet como de la red interna. Esto permite detectar el uso indebido de las herramientas de trabajo para obtener información de los clientes de forma ilícita, realizar transacciones sin autorización o simplemente acceder a información relevante del banco. Con Internet sería para mantener una vigilancia al contenido de los sitios que visita, los correos electrónicos que envía y recibe, etc.

9.8 Rastreo de celulares

Esto se logra mediante varios métodos, el más común es el de la triangulación y lo que permite conocer la ubicación del aparato que emite la señal, con esto se podrá observar actividades anormales como el uso del celular para comunicarse con personas que estén cerca del banco (eso no es lógico) y este tipo de anomalías es lo que permite que personal interno se comunique con personas ajenas al banco para hacerles de su conocimiento si algún cuenta habiente ha retirado una cantidad de dinero considerable.

Esto ha pasado recientemente en Guatemala y con esta técnica se podría detectar dicho patrón y avisar a las entidades correspondientes antes de que suceda.

9.9 Reconocimiento de patrones de voz y palabras clave

Ya que el intervenir o grabar las conversaciones telefónicas sería una tarea agotadora y muy laboriosa, se puede simplemente el monitorear las conversaciones en las cuales aparezca cierta palabra clave (definida por los

empleadores) de forma que se puede enfocar el sistema en grabar solo aquellas conversaciones que contengan alguna de las palabras claves definidas. Además de reconocer las voces de las personas que conversan.

Esto puede utilizarse también como medio para restringir el acceso a áreas del banco y para mantener una bitácora de los lugares en donde un empleado a estado.

9.10 Tarjetas de proximidad

Estas permitirían reemplazar las llaves usuales de cada puerta por dispositivos más fiables y que contengan más información relevante de su portador (como permisos de acceso), además por su dificultad de duplicar mantienen un nivel alto de seguridad.

Permitirían también que los empleados no perdieran el tiempo buscando la llave correcta para una puerta sino que esta se abriría (si el empleado tuviera permiso para ello) al detectar la señal de la tarjeta.

9.11 Correo electrónico e Internet entre los empleados del banco

El correo electrónico y el Internet son dos herramientas muy utilizadas dentro las empresas hoy en día y que lo seguirán siendo debido al auge de la Internet. Pero para una institución bancaria se debe de tomar en cuenta que el hecho de permitirles a los empleados el uso de estas herramientas conlleva a la creación de políticas por parte de la institución para que su uso no afecte en ninguna forma el equipo bancario.

Se ha puesto de moda el envío de basura (SPAM) a los correos electrónicos, aunque algunos de estos correos no son dañinos, existen otros que llevan adjuntos archivos que a simple vista son inofensivos pero que en realidad son

virus, los cuales infectan la máquina del usuario que los abre, y si se toman en cuenta que esa máquina se encuentra conectada a otras por medio de la red del banco podría infectarlas también, con lo cual el funcionamiento del banco se vería afectado además de comprometer la integridad de la información que él se posee o se maneja.

Por este motivo se han creado políticas para el uso de Internet y del correo electrónico para evitar dichos problemas, la mayoría prefiere tener su propio servidor de correo para tener un mejor control de los correo que se reciben y así también vigilar su contenido, algunos hasta han llegado a bloquear correo de cualquier otro dominio de correo que no sea el de la empresa para evitar el que personas se hagan pasar por usuarios acreditados.

Viendo otro punto de vista, el permitirle al empleado tener libre acceso a estos servicios conlleva en mejorar la vigilancia de su uso para contar con información que diga en qué invierte su tiempo el empleado y que uso le da a estos servicios de forma que pueda ser detectada cualquier acto que pueda afectar los intereses de la institución. Ya que no se puede vigilar al empleado físicamente en todo momento ni auditar su trabajo, se puede vigilar el acceso a dichos servicios y las actividades que realiza para llevar un mejor control de su desempeño. Algún software como firewalls y antivirus permiten activar una opción que guarda en bitácora las actividades que se realizan en dicha máquina, más las actividades que conlleven una conexión a Internet.

CONCLUSIONES

1. Todas las técnicas de vigilancia tienen como objetivo primordial brindar mayor seguridad tanto en bienes como servicios, pero dicho objetivo puede ser llevado a tal grado que puede llegar a violar la privacidad de las personas a su alrededor.

2. En el caso de los bancos puede obviarse dicho límite, ya que los empleados están sujetos a un reglamento interno de la institución; además al inicio de su contratación como empleado de la institución se les informa de todas aquellas políticas, lineamientos y atribuciones que el banco tiene sobre su privacidad.

3. Las técnicas de vigilancia han evolucionado con el pasar de los tiempos, convirtiéndose en herramientas vitales para toda institución y aún más para los bancos, tomando en cuenta que son los objetivos más codiciados por los delincuentes.

4. La técnica preferida por los bancos alrededor del mundo es la que se conoce como CCTV o televisión de circuito cerrado. Esta técnica ha sufrido grandes cambios y adelantos de modo que con el uso de tecnología digital puede verificarse en el momento los rostros de personas y compararlas contra una base de datos previamente establecida que contiene, prácticamente, todos los rostros de las personas que visitaron el banco. De dicha forma puede impedirse el que personas que sean una amenaza para el banco ingresen a la institución sin ningún problema.

5. Otras técnicas utilizadas junto con la de CCTV son las de láseres infrarrojos y sensores de movimiento, que en algunos casos no son muy utilizados pero todavía se encuentran instituciones, más las de tamaño grande, que las emplean para mejorar su seguridad.

6. La biométrica ha alcanzado un nivel de aceptación como técnica de vigilancia y de seguridad a tal grado que puede encontrarse, incluso, en lugares como parqueos, puertas, documentos de viaje, licencias, etc. La biométrica permite conocer a ciencia cierta quién y en qué momento estuvo en cierto lugar, además de conocer la identidad de dicha persona y así impedir el ingreso a personas no válidas en lugares restringidos.

7. Como se ha observado, cada una de las técnicas por separado no tiene un buen desempeño, pero en conjunto puede alcanzarse un nivel de vigilancia y seguridad mejor, aunque siempre hay que cuidar el no llegar a un nivel de pánico en donde se controle hasta los tiempos de ocio y hábitos (higiénicos y conductuales) de los empleados y personas que estén en el banco. Cada técnica mejora la seguridad en cierto aspecto y proporciona una mejor información para que el personal de seguridad atienda amenazas a tiempo o tome decisiones sobre una situación dada.

8. En un mundo globalizado, la vigilancia y el control en la información y en los sistemas informáticos conllevan el uso de tecnología cada vez más moderna y poderosa para tener las herramientas de identificar y prever problemas en las entidades financieras, esto debido al efecto dominó que se ha visto en la actual crisis financiera, en donde los problemas que aparecieron en las entidades financieras de los EEUU han ido afectando poco a poco al resto del mundo, desde los países más industrializados hasta los pequeños del llamado “tercer mundo”.

Y pensar en aplicar convenios como el de BASILEA II en estos momentos es de analizarlos seriamente porque podrían incrementar los problemas en lugar de ser una solución para esta crisis.

RECOMENDACIONES

1. Una opción con una gran aceptación es la de CCTV, aunque debe tenerse en cuenta que para que dicha técnica funcione de la mejor manera posible, debe ser CCTV digital y que las imágenes escaneadas de las personas sean almacenadas en una computadora específica para dicha tarea.

2. Entre más tecnología para vigilar se utilice, la seguridad y su percepción mejora, aunque debe tenerse en cuenta no llegar a un nivel de pánico y querer vigilar prácticamente todo.

3. La biometría es la mejor opción para mejorar la seguridad de documentos y también para mejorar el acceso del personal a las diferentes áreas de la institución.

4. Las tarjetas de proximidad son la mejor opción para almacenar los datos de los empleados y así restringir el acceso a los diferentes lugares que componen a la institución bancaria.

5. Todas las técnicas deben almacenar todos sus registros de acciones en una computadora para posterior análisis o toma de decisiones.

6. Toda información que maneje el banco de forma digital debe ser adecuada tratando de usar términos que no sean mal interpretados por terceros, esto es en el caso de los proyectos como ECHELON y

CARNIVORE que capturan información que viaja en la red y que le podrían traer problemas al banco o al usuario.

7. Se le debe hacer conciencia al usuario (ya sea cliente del banco o empleado del mismo) que la información que envíe y las palabras que utilice sean correctas y estrictamente válidas para el uso del banco.

8. En el ámbito de los problemas financieros, se ha visto que la implementación de BASILEA II en Europa no tuvo el esperado resultado que se preveía debido a la estrecha relación de sus entidades financieras con los EEUU. Sin embargo, esto no dice que tenga algo de malo dicha relación, ya que con la implementación de BASILEA se corrigieron problemas locales pero no globales, que son los que a largo plazo tienen mayor impacto. Se debe llevar un mejor control en la información de las entidades financieras y la forma en que están trabajando, no solo con entidades y clientes locales sino también con entidades internacionales, siempre cuidando su autonomía y privacidad, para evitar problemas en el futuro.

BIBLIOGRAFÍA

1. Clarke, Roger. ***Dataveillance: Delivering '1984'.*** Australian National University, Xamax Consultancy Pty Ltd, 1992-3

2. Comité de Basilea sobre supervisión bancaria. ***Administración y Supervisión de Banca Electrónica Transfronteriza.*** Suiza, octubre del 2002.

3. **IESE Bussines School – Universidad de Navarra** http://www.iese.edu/es/files/Art_Soley_Basilea_Jul04_ESP_tcm5-7365.pdf. Consultado en: mayo de 2010.

4. **International Monetary Fund** http://www.imf.org/external/pubs/ft/fandd/spa/2008/06/pdf/saurina.pdf. Consultado en: mayo de 2010.

5. **ISTP Bussines School** http://www.iberfinanzas.com/index.php/Articulos-de-opinion/Puntazos-de-la-crisis-financiera-global.-A-Basilea-III-desde-Basilea-II.html, Consultado en: mayo de 2010.

6. Lyon, David. ***Computers, Surveillance and Privacy*** coeditado con Elia Zureik. Minnesota, 1996.

7. Lyon, David. ***Textos***. Universidad de Queens, Ontario, Canada

8. Lyon, David. ***Surveillance as Social Sorting.*** Routledge, 2002.

9. **Revista Bussines Week**
http://www.gerente.com/revistas/businessweek/0808/colombia/bw1c_0808.html. Consultado en: mayo de 2010.

10. Singh, Sajai & otros. ***Technology Surveillance***. Bangalore, India.

11. ***Surveillance Techniques and Technologies***
http://www.iis.ee.ic.ac.uk/~frank/surp99/report/fb97/main.html.
Consultado en: mayo de 2010.

12. Vittone Dávila, Alberto **Revista Alfa-Redi de Derecho informático**
Riesgos de la contratación bancaria electrónica en el derecho comparado con la legislación colombiana. No. 082, mayo de 2005. (http://www.alfa-redi.org)

13. **Wikipedia** http://es.wikipedia.org/wiki/Basilea_II

14. Wood, David. *The hidden geography of transnational surveillance* Tesis Doctoral. Universidad de NewCastle, United Kingdom. 2000 – 2008

15. Word, David. Revista On-line: ***Surveillance & Society*****,** Universidad de NewCastle, United Kingdom