



ANÁLISIS DEL SECTOR DE LECTORES BIOMÉTRICOS DE HUELLA DIGITAL EN EL MERCADO MEXICANO

Para el periodo junio 2004 - 2005

benassini



www.benassini.com

CONTENIDO

Página

OBJETIVOS.....	3
PRINCIPALES HALLAZGOS.....	4
CONCLUSIONES.....	7
RECOMENDACIONES.....	9
ENTREVISTAS EN PROFUNDIDAD.....	12
FUENTES DE CONSULTA.....	32

OBJETIVOS

1. Dimensionar el tamaño, el valor y las características de los mercados actuales y potenciales de los equipos biométricos, específicamente orientados a generar confianza a través de la seguridad informática, de acuerdo con las siguientes categorías:
 - Productos que utilizan los usuarios corporativos para garantizar la seguridad y protegerse contra posibles fraudes en las transacciones que se llevan a cabo diariamente de manera interna. Para ello, es necesario instrumentar tecnologías altamente especializadas en la prevención de fraudes.
 - Productos dirigidos a cualquier tipo de organización que requiera autenticar la identidad de sus usuarios, de tal manera que éstos tengan la seguridad de realizar las transacciones que deseen, sin necesidad de llevar consigo un código especial. Este tipo de equipos puede tener aplicación en múltiples sectores de negocios, incluyendo Internet.
 - Productos dirigidos al control de acceso de empleados, clientes y proveedores de cualquier tipo de organización.
2. Identificar los detonantes más importantes del mercado:
 - Principales segmentos por sector de la economía
 - Tendencias de crecimiento, estimación de los tiempos de asimilación
 - Principales necesidades vs. capacidad instalada
 - Las grandes redes corporativas y su impacto en los sectores afines
 - Principales barreras de entrada, oportunidades y amenazas
 - Los servicios complementarios y los valores agregados
 - Sugerencias de estrategias de marketing y prioridades



PRINCIPALES HALLAZGOS

- De acuerdo con el Anexo 1, el valor aproximado estimado de las ganancias totales provenientes de la venta de lectores biométricos de huella digital en México será de \$70.0 millones de pesos para el 2004.
- La clasificación que utilizamos para identificar con mayor aproximación los sectores de la economía mexicana que presentan mayor demanda de este producto, es la realizada por la compañía estadounidense Allied Business Intelligence. La metodología agrupa los principales segmentos de clientes actuales a nivel mundial.

SECTOR	PARTICIPACIÓN
- Industria en general	25%
- Mercado de consumo	23%
- Sector financiero	14%
- Sector salud	13%
- Servicios de aeropuertos	2%
- Otros*	23%
- Total	100%

*** OTROS DIFÍCILMENTE CUANTIFICABLES:**

PIB del año 2002: Sector agropecuario, minería, construcción, electricidad, gas y agua.

ABI: Control de accesos, asistencia, productividad gobierno.

- Cada uno de estos sectores tiene problemas tanto de seguridad informática como de control de accesos. No es posible cuantificar por separado el mercado de cada una de estas aplicaciones para México. Sin embargo, las estadísticas sobre la tendencia mundial nos indican que solamente el control de accesos tiene una participación del 9%. Lo hemos considerado en el renglón de "Otros".

- Sabemos que el mercado de equipos biométricos para el control de accesos tiene dos grandes segmentos. El primero es el que ocupan las empresas de seguridad. En la sección de Entrevistas en Profundidad, podemos apreciar los precios de las catorce primeras agencias mexicanas dedicadas a esta actividad, así como las estrategias de las cinco más grandes. Es importante destacar que en México existen más de 2,000 compañías de este tipo, que hoy en día pueden representar un máximo del 10% de las ventas de equipos biométricos.
- La razón de la baja participación de los lectores biométricos, es que estas agencias muestran todavía una marcada preferencia por vender guardias en lugar de ofrecer soluciones de alta tecnología, más seguras y eficaces, ya que los guardias siguen siendo más rentables, aún cuando su operación diaria es sumamente conflictiva.



6. Sin embargo, si observamos la cartera de clientes de estas empresas, podremos apreciar que se trata de organizaciones grandes, muchas de ellas multinacionales y que, por lo tanto, están ligadas a una alta tecnología. Tarde o temprano, estos clientes estarán exigiendo a sus proveedores de seguridad, soluciones tecnológicas a sus problemas de control de accesos y, en algunos casos, también soluciones relativas a la seguridad informática.
7. De esta manera, las compañías de seguridad pueden tener un excelente potencial para convertirse en distribuidores de biométricos de huella digital en el mediano plazo. Sin embargo, es probable que la inversión en tiempo que hagamos con este segmento, no sea redituable en forma inmediata, por lo que sugerimos realizar una prospección de manera colegiada.
8. El segundo segmento es el de los distribuidores de software que venden los equipos biométricos directamente a los usuarios finales. Representa cerca del 90% del mercado. Sin embargo, a pesar de su proporción, está altamente pulverizado. Esto significa que no existe concentración geográfica, ni por tipos de negocios. Tampoco hay datos que nos permitan afirmar que los usuarios finales prefieren comprar el producto a los distribuidores locales, o a los extranjeros. La razón de esto es que el mercado se encuentra en su fase inicial del ciclo de venta del producto.

Dicha fase se caracteriza en México por lo siguiente;

- a. Existen todavía relativamente pocos compradores y ofertores, en comparación con el tamaño total del mercado.
 - b. Se conocen las características generales del producto, pero es considerado como inaccesible. Se piensa que todavía es caro y difícil de instrumentar.
 - c. La mayor parte de los distribuidores no son especialistas. Simplemente están añadiendo los lectores biométricos a sus líneas de productos.
 - d. Los productos sustitutos que ofrecen mayor competencia son los tradicionales, tales como los passwords en varios niveles de complejidad, y las tarjetas inteligentes. Éstos se usan individualmente o de manera combinada.
 - e. Ofrece una importante oportunidad de posicionamiento para aquellos distribuidores que ataquen el mercado asertivamente.
9. Cuando los productos se encuentran en su fase inicial del ciclo de vida, los clientes que los compran se llaman "innovadores". En el caso concreto de los biométricos digitales, encontramos que la adopción rápida estará en las empresas de tamaño mediano a grande, en los sectores de la economía que aparecen en los Cuadros 1 y 2

**ESTIMACIÓN DE LAS GANANCIAS TOTALES
DE LECTORES BIOMÉTRICOS DE HUELLA DIGITAL
EN MÉXICO PARA EL 2004**

**Cuadro 1
PIB POR SECTORES A PRECIOS DE MERCADO
México 1994-2002**

Participación porcentual Concepto	1994	1995	1996	1997	1998	1999	2000	2001	2002	2002 Ajustado
Producto interno bruto, a precios de mercado	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	-
Menos: impuestos a los productos, netos	8.0	8.6	9.1	9.5	8.5	8.4	9.3	9.3	8.4	-
Valor agregado bruto, a precios básicos	92.0	91.4	90.9	90.5	91.5	91.6	90.7	90.7	91.6	-
GD1. Agropecuaria, silvicultura y pesca	5.3	5.0	5.5	5.0	4.8	4.2	3.7	3.7	3.6	3.9
GD2. Minería	1.2	1.6	1.4	1.4	1.3	1.3	1.3	1.2	1.2	1.3
GD3. Industria manufacturera	17.3	19.1	19.6	19.4	19.5	19.3	18.5	17.8	17.0	18.3
GD4. Construcción	4.9	3.7	3.8	4.0	4.3	4.5	4.7	4.7	4.7	5.0
GD5. Electricidad, gas y agua	1.4	1.2	1.1	1.1	1.2	1.2	1.0	1.1	1.4	1.5
GD6. Comercio, restaurantes y hoteles	19.4	19.1	19.6	19.3	18.1	18.3	19.3	18.8	18.3	19.7
GD7. Transporte, almacenaje y comunicaciones	8.8	9.1	9.3	9.6	9.9	10.2	10.1	10.2	9.8	10.5
GD8. Sector financiero, seguros, inmobiliarias y alquiler	14.9	16.8	13.7	12.1	12.5	12.1	11.0	11.1	12.4	13.3
GD9. Servicios comunales, sociales y personales	21.9	20.7	19.3	19.9	20.8	21.7	22.2	23.7	24.6	26.5
Menos: Cargo por los servicios bancarios imputados	-3.0	-4.9	-2.2	-1.3	-0.9	-1.2	-1.1	-1.6	-1.4	-

FUENTE: INEGI. Sistema de Cuentas Nacionales de México. "Cuenta de Bienes y Servicios".

**Cuadro 2
ESTIMACIÓN DEL VALOR DE LOS SEGMENTOS DE LECTORES BIOMÉTRICOS
DE HUELLA DIGITAL EN EL MERCADO MEXICANO**

Segmentos del mercado mundial en el 2002*	Participación por segmentos	Distribución estimada del PIB en México en el 2003	Valor estimado de las ganancias totales en pesos en México en el 2004
Aeropuertos	7%	2%	\$ 1,400,000
Sector financiero	8%	14%	\$ 9,800,000
Mercado de consumo	9%	23%	\$16,100,000
Control de accesos	9%	ND	ND
Salud	10%	13%	\$ 9,100,000
Asistencia y productividad	10%	ND	ND
Gobierno	15%	ND	ND
Industria	11%	25%	\$17,500,000
Otros	14%	23%	\$16,100,000
TOTAL	100%	100%	\$70.0 MM

* Fuente: Allied Business Intelligence, 2002

SUPUESTOS METODOLÓGICOS

1. En el 2004, las utilidades del mercado total de equipos biométricos se estiman en \$310 millones de dólares.
2. Si México representara solamente el 4% del valor del mercado mundial, las ganancias en el 2004 deberán ser de \$12.4 millones de dólares aproximadamente.
3. Si los biométricos digitales representan el 50% del mercado mundial total, sus ganancias deberán estar cerca de los \$6.2 millones de dólares, aproximadamente \$70 MM de pesos.

CONCLUSIONES

1. EL MERCADO DE LOS EQUIPOS BIOMÉTRICOS EN EL ÁMBITO MUNDIAL Y EN AMÉRICA LATINA

- Muestra un comportamiento de tipo global. Aunque con diferencias entre algunas regiones, como América Latina, Asia y África, las necesidades tienden a ser las mismas.
- El mercado mundial creció cerca de un 39% en el 2003 y se espera un 100% en el 2004.
- Además obtuvo utilidades cercanas a los \$303.3 millones de dólares en el 2002, cifra que se estima ascenderá a \$3,548.2 para el 2009. Eso significa que aumentaría 11.7 veces en tan solo siete años, a una tasa promedio anual de 67%.
- El segmento de América Latina también está creciendo de manera acelerada. En el 2004 tendrá un valor de \$4.2 billones de dólares.
- La participación de la huella digital en el mercado mundial de biométricos es de cerca del 50%. Se estima que en el 2001, tan sólo en Estados Unidos, las compañías gastaron más de \$127 millones de dólares en biométricos, de los cuales el 44% correspondió a la huella digital. Y para el 2004, en ese país, el sector financiero invertirá \$1.800 millones anuales en el rubro.

- Un factor que favorece este hecho es el precio de los equipos, que ha disminuido notablemente. Un dispositivo de huella digital que costaba cerca de \$4.000 dólares, hoy se consigue por \$200. Así, estos instrumentos se han vuelto más accesibles a todas las organizaciones.

2. DETONANTES DEL CRECIMIENTO MUNDIAL Y NACIONAL

- Una mayor preocupación de todos los países del orbe por dar mejores soluciones al problema de la seguridad, en todas sus variantes. Este fenómeno provoca un uso cada vez mayor de los equipos biométricos por parte de los gobiernos y de las empresas.
- Algunos países y algunos sectores de la economía adoptarán el sistema de equipos biométricos en etapas más tempranas, exigiendo a toda la cadena adoptar estos estándares. Un caso de países es el de los Estados Unidos. Es probable que su gobierno acelere la implantación de este sistema de forma obligatoria para todos sus aeropuertos. Y que como etapa posterior, exija a otros países que adopten las mismas medidas de seguridad. Un caso de sectores es el financiero. Si este sector decide adoptar el sistema, la cadena de proveedores y clientes hará que el mercado crezca de manera acelerada en nuestro país.
- La elasticidad de la demanda, que obliga a los clientes a elegir equipos más baratos, aún cuando los niveles de seguridad que obtengan a cambio sean

menores. Sin embargo, en la medida en que los biométricos desciendan de precio, aumentarán sus ventas de forma acelerada. Por ejemplo, en Estados Unidos, una empresa con 50 empleados y dos puertas de entrada, que dispone de entre \$5,000 y \$10,000 dólares para el control de accesos, ya puede optar por un equipo biométrico, que le dará un nivel mucho mayor de seguridad.

- La capacitación eficaz a todos los niveles, ya que el exceso de información no necesariamente incrementa los niveles de conocimiento del producto y de seguridad. Sin embargo, sí genera costos innecesarios, derivados principalmente de la sub utilización del tiempo y el material.
- La fusión de las compañías fabricantes, que reducirá el tiempo de desarrollo de productos y propiciará la estandarización del mercado en el mediano plazo.
- El desarrollo de los mercados verticales en sustitución de los horizontales. Esto significa que si existe una integración entre todos los elementos de la cadena de un sector como el financiero, el hecho tendrá un impacto significativo sobre la demanda.
- El constante desarrollo tecnológico, y la introducción de nuevos productos, más seguros y económicos para las futuras necesidades de un mercado globalizado.

- El uso de combinaciones de productos, o de biométricos múltiples con tarjetas inteligentes, que también elevarán los niveles de seguridad.
- El incremento del número de distribuidores, con un efecto expansivo del mercado. Esto se ha podido comprobar recientemente en los mercados asiáticos.

3. LAS APLICACIONES MÁS FRECUENTES DE LOS PRODUCTOS BIOMÉTRICOS EN EL MUNDO

- Finanzas, e-commerce. Un caso es el de entidades como Citibank, que ya utiliza la huella digital para el control de acceso de sus empleados. El grupo ve la posibilidad de introducirla para la verificación de los clientes. Por otro lado, según PriceWaterhouse Coopers, el fraude en los servicios financieros vía Internet ha alcanzado los \$1.5 millones de dólares. Señala que la principal causa que frena el uso de los servicios bancarios online es la inseguridad de las operaciones. Los biométricos están considerados como los sistemas de seguridad más fiables para combatir este delito.
- Control de tiempos para efectos del pago de la nómina. A medida que las empresas requieren contratar mano de obra no sustituible por procesos automatizados, la medición se hace indispensable, porque los tiempos muertos pueden ser un

factor que les reste productividad y, por lo tanto, competitividad. Los sistemas tradicionales de control del tiempo real que trabaja un empleado no son 100% eficaces. Los biométricos pueden ser una excelente solución.

- Control de acceso de empleados, proveedores y visitantes.
- Seguridad informática en todo tipo de empresas.
- Emisión de visas y control de los aeropuertos.
- Transportación en general.
- Salud.
- Universidades.

4. LAS PRINCIPALES BARRERAS DE ENTRADA

- Los sistemas desarrollados por las diversas firmas de software no son compatibles entre sí, lo cual dificulta actualmente el cambio de proveedor.
- La percepción del público sobre el hecho de que los biométricos invaden la privacidad. Este problema irá subsanándose a través del tiempo con una mayor difusión de la cultura de la seguridad.
- La percepción de que estos equipos son caros y complejos de utilizarse.



RECOMENDACIONES

1. Dar preferencia a los siguientes segmentos, que son los que muestran tendencias de crecimiento superiores al 50% anual en promedio, para los lectores biométricos de huella digital, de acuerdo con los expertos.

Cuadro 3
RECOMENDACIONES SOBRE LOS SEGMENTOS MÁS RENTABLES
PARA EL DESARROLLO DE LECTORES BIOMÉTRICOS DE HUELA DIGITAL

Segmentos	Problemas	Probable tiempo de asimilación
INDUSTRIA EN GENERAL, PREFERENTEMENTE DE MEDIANA A GRANDE Participación estimada: 25%	a. Control de accesos a la planta y a las áreas restringidas b. Robo de patentes, modelos o marcas c. Robo hormiga por parte de los empleados d. Robo de piezas, refacciones y herramientas e. Robo de uniformes f. Complicidad con los vigilantes g. Falta de control en los accesos de ciertas áreas de las fábricas h. Baja productividad de los obreros, debida a la falta de control sobre los procesos asignados a las personas	Corto plazo
MERCADO DE CONSUMO Participación estimada: 23%	i. Robo por parte de clientes y empleados, con ciertos niveles de sofisticación j. Falta de control sobre el proceso completo, a veces no se detecta si el fraude es hecho desde los camiones repartidores k. Identificación de las áreas más sensibles de cada sector, como las comandas en el negocio de restaurantes y los departamentos de compras en general	Corto plazo, con gran capacidad de expansión, a través del efecto de marketing viral
SECTOR FINANCIERO Participación estimada: 14%	l. Control de accesos m. Fraudes informáticos n. Falta de homogeneidad en el sector o. Falta de seguridad en algunas operaciones	Corto plazo, con gran capacidad de expansión, a través del efecto de marketing viral
EMPRESAS DE SEGURIDAD Participación estimada: ND	p. Control de accesos q. Fragilidad del sistema de guardias y de sus servicios en general, ya que no pueden ser estandarizados porque dependen más de las personas que de la tecnología r. Poca lealtad en el sector, por no contar con un servicio diferenciador, casi todas ofrecen los mismos básicos y adicionales	Mediano plazo, es necesario fomentar la cultura de la tecnología

2. Para establecer prioridades entre los prospectos, se deberá tomar en cuenta las necesidades urgentes de seguridad, los recursos disponibles y la cultura de las organizaciones

Deseablemente, estos elementos deben existir en conjunto. La información recopilada en este estudio, revela que la sola necesidad de seguridad y la presencia de fraudes no son detonantes de la decisión. Debe combinarse con recursos que permitan desarrollar las soluciones y hacer demostraciones. Y la cultura tecnológica es también básica. Biometría Aplicada perdería mucho tiempo en capacitar a los clientes potenciales a niveles básicos. Desde este punto de vista, las empresas trasnacionales parecen ser un mejor prospecto.

3. Hay sectores como el financiero y el gobierno mismo, que pueden ejercer sobre sus clientes y proveedores el llamado marketing viral, que significa que al elegir un estándar de lector, el segmento crecerá de manera exponencial. Por esta razón, el acercamiento con la AMIB es una excelente oportunidad. Adicionalmente, están la ABM, la CNBV y la AMIS, que manifiestan gran preocupación en este sentido. Grupos como Wal-Mart pueden ser también prospectos interesantes, aunque debe tomarse en cuenta que su cultura es generalmente austera y conceden al proveedor una capacidad de negociación muy pobre.

4. Existe una gran necesidad por la capacitación sobre el tema de lectores de huella. La capacitación puede activar

algunos sectores, como el de las agencias de seguridad, además de que puede ser una excelente forma de prospección. La recomendación en este sentido son las pláticas a grupos colegiados, como el sector mencionado. Esto puede ahorrarnos el tiempo que tradicionalmente se llama "de siembra".

5. De acuerdo con las fuentes externas de consulta, los expertos opinan que la falta de compatibilidad en los sistemas biométricos a nivel mundial es una limitante para la expansión del mercado. Mezclada con la actitud de los clientes mismos, ésta se vuelve una barrera muy compleja. Banamex, por ejemplo, tiene la capacidad para hacer el cambio, pero manifiesta que ha invertido mucho en sus sistemas actuales y tiene que amortizarlos.

6. La competencia no parece ser una barrera importante para Biometría Aplicada. El mercado es muy vasto y presenta una importante oportunidad de posicionamiento. La experiencia que la empresa ha adquirido a la fecha, mezclada con una excelente política de servicio al cliente, pueden ser los elementos clave de su diferenciación. Sin embargo, el peligro que existe es el de un crecimiento demasiado acelerado, posiblemente anárquico, para alcanzar las necesidades del mercado. Esto le puede representar problemas en el futuro.

7. Finalmente, los valores agregados que más van a apreciar los clientes son los ya mencionados, la capacitación y el servicio al cliente sistematizado.

ENTREVISTAS EN PROFUNDIDAD



Existen dos funciones básicas que se relacionan estrechamente con la seguridad de Banamex. Son el control de accesos y la seguridad informática, ya que los instrumentos que se utilizan para cumplir con ambas funciones van de la mano. Por ejemplo, las claves de acceso para entrar en las instalaciones del Banco, pueden servir también para evitar las fugas y robos de equipo y de información. En Banamex, la seguridad en general involucra a dos o más personas, dependiendo de la importancia del resguardo. Si éste es de mayor valor, requiere de la aprobación de más personas, cada una con dos sistemas distintos. Además del PS, los accesos están restringidos por una tarjeta magnética.

Un ejemplo de la importancia de la seguridad informática es Inteligia, subsidiaria del Banco. Tiene 55 empleados registrados en su nómina. Pero para operar el site, solamente pueden entrar tres personas, con sus respectivas claves. El control de las transacciones informáticas se lleva a cabo en la garita, a través de la cual se registra a qué horas y qué tipo de transacción se está realizando.

Independientemente de la división en la que trabajen o de su ubicación geográfica, todos los ejecutivos involucrados con la seguridad del Banco reciben a diario información sobre seguridad informática. Esto es a través de un VTM, que es un instrumento que indica que hay disponibilidad tecnológica en el protocolo de Cisco. Si llegara a existir alguna alerta, inmediatamente quienes la

captan establecen comunicación con la central de seguridad informática, donde se examina el problema. Puede tratarse, por ejemplo, de los servidores. En poco tiempo deben recibir una respuesta sobre la posible existencia o ubicación del problema.

Utilizan una combinación de dispositivos físicos. Los más generalizados en el Banco son la tarjeta inteligente y unas claves que se cambian cada dos semanas. Los passwords más importantes de estas claves se guardan en cajas fuertes. Cada área tiene determinados privilegios, que no afectan la integridad de la operación. Esto quiere decir que en la Dirección de Tarjetas de Crédito pueden estar operando un protocolo que no debe afectar a la Dirección de Crédito Hipotecario, aunque se trate de los mismos clientes.

Además de los comunes a una buena parte del personal de seguridad, generalmente se utilizan otros passwords, que tienen privilegios para todo tipo de funciones, pero que muy pocas personas conocen y tienen acceso. La mayor parte del personal de Informática de cualquier división del Banco trabaja solamente sobre algún tipo de información. Es muy esporádico que existan privilegios para tener acceso a toda la información. Y en caso de que este patrón llegue a "dispararse" aparecen las alertas.

En cada División existen también candados particulares para los tipos de operaciones. Un caso se presenta cuando se manejan las cuentas individuales de los clientes, por ejemplo, la nómina de Inteligencia. Desde la entrada al sistema, los candados impiden que se pueda quitar dinero al personal al que se está depositando. Esto se controla mediante cargos y abonos, lo que significa que al realizar el depósito de la quincena, restándole los adeudos por concepto de ISR, IMSS e INFONAVIT, los saldos finales deben ser exactamente los mismos. No pueden variar ni siquiera por un centavo. De hecho, como las operaciones de depósito se realizan una por una, el sistema puede impedir que quien lo opere tenga el tiempo disponible para restar alguna cantidad.

El control de accesos a las instalaciones del Banco está un poco menos restringido, o en todo caso, menos estandarizado. En cada edificio y a veces en cada entrada de un mismo edificio existen diferentes sistemas de seguridad. Por este motivo, eventualmente se registran robos de equipos de menor tamaño, como teléfonos celulares, palms e incluso laptops. Esto se da principalmente entre los empleados.

Banamex destina muchos recursos a la seguridad. Existe toda un área de seguridad informática que regula la totalidad del Banco y da mayor énfasis a las operaciones y a los bienes de mayor importancia. Invierten en boletines que no necesariamente se leen. Mucha de la capacitación ESTÁ EN INGLÉS, lo cual dificulta su lectura y comprensión.

De acuerdo con el entrevistado, los biométricos podrían ser útiles para las dos funciones de seguridad del Banco, pero no son la panacea, porque no son 100% infalibles. Una de las soluciones informáticas que no han podido encontrar, son los mecanismos para llevar a cabo una medición correcta del pago quincenal que reciben los empleados. Esto se debe a que no existe en el mercado un software que ayude a llevar un control más estricto de las entradas y salidas de cada oficina o cubículo, que conlleve sus correspondientes tiempos perdidos.

Esto les preocupa más para sus clientes, porque ellos venden soluciones de nómina. En una División como Inteligencia, que tiene 55 empleados, el biométrico todavía no es funcional, porque a simple vista pueden darse cuenta de quiénes trabajan y quiénes no. Se les acercó una empresa llamada Kronos, pero no llegaron a ningún acuerdo, porque Banamex estaba buscando un sistema que controlara el acceso de los empleados y el tiempo que realmente están trabajando.

Opina que el mercado de los biométricos va a crecer mucho, aunque es necesario combinar la huella con las claves compartidas. Otros dispositivos, tales como el chip de la PGR injertado a los agentes, no garantiza que no sean corruptos. Las empresas que venden biométricos deben tener flexibilidad y adaptarse a las necesidades de cada negocio. El producto ideal para la seguridad depende básicamente del bien que se está resguardando en una institución. A mayor valor, mayor inversión.

Bansefi S.A.
Tecnología de la Información
Julio 26, 2004

Bansefi se encuentra todavía en una etapa de escasa tecnología. Actualmente trabajan de manera muy rudimentaria y sus operaciones son solamente locales. En otras palabras, las sucursales del Banco todavía no pueden tener comunicación entre sí porque el sistema no lo permite. Para compensar la falta de tecnología, la casa matriz recibe diariamente información sobre las operaciones realizadas y rápidamente hace una especie de concentración.

La CNBV ha hecho observaciones al respecto. Por esta razón, y por la gran necesidad de actualizarse, a partir de enero del 2005 la nueva plataforma de Bansefi tendrá mejores niveles de seguridad informática, utilizando productos como los biométricos.

Existen áreas del Banco que son más propensas a la inseguridad. Por ejemplo, una de las más sensibles es la Mesa de Dinero, porque no cuenta con un sistema de control interno que le permita conocer al instante las tasas que se están pactando. Actualmente Bansefi cubre esta deficiencia a través de los reportes que por ley debe entregar a la CNBV y al Banxico. Dichos reportes ayudan a identificar

cualquier anomalía. Claro que puede tomar tiempo detectar un fraude, porque los reportes son mensuales. A pesar de que esto no ha sucedido, un empleado sí podría realizar alguna operación y tratar de desaparecer al día siguiente.

Es posible que los bancos más pequeños, como Afirme y Banregio, también se encuentren operando con bajos niveles de seguridad. Pero el gran mercado potencial para Bansefi está en todas las Cajas de Ahorro, las Uniones de Crédito y las Sofoles, que a partir de julio de 2005 deberán adoptar las nuevas normas, tanto contables como informáticas.

Bansefi está ofreciendo su plataforma de sistemas para estas instituciones, a fin de que la información se procese desde el sistema central.

Hasta ahora, uno de los mejores servicios con los que Bansefi ha apoyado a las Cajas de Ahorro son la transferencia de remesas y los pagos de Oportunidades y Procampo. Por su parte, las Uniones de Crédito están más avanzadas y cuentan con equipos de cómputo más modernos. Hay 32 uniones en todo el país. Se estima que existen unas 700 instituciones, entre sociedades de

ahorro y préstamo o SAPS, y cooperativas. Las SAPS son las que han estado más reguladas hasta la fecha.

Un hecho que favorece la oferta tecnológica de Bansefi es que todas las instituciones financieras que dependen de la CNBV tienen que ser auditadas y supervisadas para poder verificar su buen funcionamiento tecnológico. Realizando esta auditoría pueden obtener la certificación. Sin embargo, las empresas financieras que estén operando bajo la plataforma de Bansefi, no necesitarán dicha auditoría.

Los beneficios que ofrece Bansefi a toda esta red de instituciones pueden ser de dos tipos: económicos, en concreto la operación, y particulares, es decir, soluciones para cada empresa en específico. Otro factor a favor de la plataforma es que la ley

que entrará en vigor en julio de 2005 contempla 120 reportes mensuales que deben enviarse a la CNBV. Todas aquellas instituciones que no entren a la plataforma, tendrán que elaborar a mano dichos reportes.

Actualmente, cada una de ellas realiza sus prácticas contables utilizando sus propios métodos. Sin embargo, cuando entre en vigor la ley, toda la contabilidad deberá ser estandarizada. Por ejemplo, las Cajas de Ahorro deben tener reservas contra el crédito otorgado, ya que actualmente no todas las tienen. Otro caso es el de la nueva obligación que tienen estas entidades de reflejar siempre una pérdida contable cuando ésta exista.

Todo esto puede representar una buena oportunidad para el negocio de equipos biométricos. La plataforma fue vendida por la empresa IBM, que será la encargada de seleccionar a sus proveedores.

Grupo Wal-Mart
Ex Director General de Auditoría
Actual Contralor de Radio Shack
Agosto 4, 2004

La auditoría de todas las empresas del Grupo tiene una gran complejidad, porque cada una se maneja con sus propias reglas y sus propios proveedores. En Grupo Wal-Mart se lleva a cabo de forma diaria y permanente. Incluso existen metas mensuales y anuales a alcanzarse y que se ven reflejadas directamente en las utilidades. La metodología para descubrir los fraudes es muy variada y está basada principalmente en la tecnología, aunque no siempre se usan los mismos mecanismos para cada función o para cada empresa.

Si lo vemos desde el punto de vista de departamentos o funciones del grupo, los focos rojos siempre están en primer lugar sobre el área de compras, que es la más conflictiva. Algunos casos por tipos de negocio son:

En Suburbia, los encargados de compras de ropa son los más auditados. El sistema de cómputo de auditoría manda señales cada vez que se rompe un patrón de conducta que venía siendo regular. Por ejemplo, una compradora de ropa para dama llegó a tener hasta veinte diferentes marcas, que eran más o menos las mismas desde hacía varios años. Las marcas y los proveedores se mantienen tradicionalmente por su calidad, aceptación de la marca y

precio. Y tienen que cumplir con muchos requisitos.

En el caso citado de ropa para dama, el número de marcas bajó de veinte a ocho en un lapso de un mes. Pero la cantidad de mercancía comprada no cambió, lo cual significaba que alguno o algunos de los proveedores estaban desplazando mucha más mercancía. Pedimos información sobre las razones, y el área correspondiente respondió que la encargada de compras de esos artículos tenía un permiso para asistir al maratón de Nueva York, ya que su novio iba a competir. Buscamos en Internet los nombres de los participantes mexicanos y encontramos que uno de los participantes era el propietario de la empresa a la que más le estábamos comprando.

Otro caso es el de las compras de farmacia. Ése es uno de los centros de negocio que compra en forma colegiada, por razones de precios. Hay farmacias en WalMart, Vip's y Superama. Los puestos en el área de compras de farmacia están muy cotizados, pero para llegar a ellos se requiere que los empleados cumplan con muchísimos requisitos. Para vigilar de manera permanente este tipo de actividades, auditamos también a los empleados de manera externa.

Por ejemplo, puede haber un encargado de compras que gana \$10 mil pesos mensuales. Este sueldo le permite tener un cierto estilo de vida. Cuando es corrupto, trata de aparentar el mismo estilo de vida por un cierto tiempo, pero tarde o temprano termina dando señales. Un día llega a trabajar con un auto costoso último modelo, o bien se cambia de casa. Tuvimos un caso en que el encargado de compras de farmacia pudo abrir su propia farmacia, surtida por nuestros proveedores a los mismos precios. Esto trabajando en el Grupo de forma simultánea.

El caso de Vip's, El Portón y Ragazzi también son especiales por ser restaurantes. Hay fraudes en el área de compras, pero también a través de las comandas, que son el punto álgido de todos los restaurantes. Para que exista fraude utilizándolas, los empleados tienen que estar coludidos. Por ejemplo, puede suceder que el total de la cuenta de una mesa no se contabilice y que se haga una nota separada por una parte de los alimentos. El cliente tiene que estar de acuerdo para ello, y paga en efectivo a la mesera el diferencial menos un descuento. Otro caso son las comandas que no se cobran y se calculan como si el platillo se hubiera caído de la charola.

Esto sucede mucho en otro tipo de restaurantes. El mesero llega con la cuenta y le dice al cliente que no le cobró x producto, y el cliente le da una propina mucho mayor que la esperada. En el caso de Vip's es más difícil hacer esto con frecuencia, porque hay estándares nacionales. Si los costos de

una unidad se disparan al alza, se enciende un foco rojo.

Los costos también pueden ir a la baja más allá del estándar. Una parte de la evaluación de los gerentes es la productividad de la unidad, por eso tratan de servir al cliente porciones menores. Tuvimos un gerente que dio órdenes para que cuando un niño pidiera una pechuga de pollo, se le sirviera la mitad. Esto se aplicaba también a otros platillos. Si el cliente no protestaba, el gerente le habría ahorrado al negocio un porcentaje que, acumulado, aparentaba mayor productividad. Para identificar estos fraudes, se utilizan los estándares de productividad y los mystery shoppers. Otro fraude lo cometen los meseros que rellenan las botellas.

Otro fraude es el robo hormiga, que se da en todos los niveles. En el caso de los restaurantes, se sabe que los empleados sustraen la comida y la meten entre su ropa. Para controlar esto, se usan los lockers con puertas transparentes. Además se pesa al empleado a la entrada y a la salida, o bien se busca entre su ropa. Obviamente que sí se encuentra mercancía, pero también es muy molesto para las personas que nunca han sustraído nada de la empresa.

En el caso de los autoservicios, los empleados no necesitan sacar la mercancía. Muchas veces se la comen dentro de las instalaciones. Esta pérdida se contabiliza en la merma, que está entre el 1% y el 2%, dependiendo de la ciudad y del tipo de negocio. Por ejemplo, un artículo muy difícil de

controlan son las medias para dama, ya que las empleadas las pueden llevar puestas. La ANTAD hace estudios constantemente para determinar la media nacional.

Repito que los sistemas siempre se pueden mejorar. Pero entonces los empleados descubren métodos más ingeniosos para robar. Hay dependientes muy hábiles. Por ejemplo, un empleado de farmacia puede sustraer un medicamento muy caro y colocarlo en la caja de uno muy barato.

Al llegar el supuesto cliente con el que está de acuerdo, solicita el producto y lo paga en esa misma caja. Aún cuando la copia del ticket especifique la hora, el monto y el nombre del despachador, esto no quiere decir que ese empleado fue quien hizo el fraude, porque dicho fraude puede provenir del camión de entrega del proveedor.

Lo más difícil de controlar son los clientes. Existen las famosas "farderas", que aparentan ser muy gordas y van colocando mercancía adentro de su ropa. Todos los días se puede detener a alguna, pero puede suceder que más de una salga de la tienda sin ningún problema. Para identificarlas, se colocan cámaras en sitios estratégicos, pero no siempre son efectivas. Es más, en ocasiones se comete el terrible error de confundir a una persona que no entró a robar a la tienda. Por eso, antes de hacer la acusación, tenemos que estar 100% seguros de que hubo robo.

Hay otro robo que también se considera dentro de la merma. Es el de los clientes

que llegan a la caja con un carrito lleno de mercancías con valor de \$1,500 pesos, pero dentro del autoservicio se comieron medio kilo de frutas y el menor que los acompaña abrió una bolsa de paletas y se comió una o dos. Hay personas que comen hasta camarones en el área de alimentos preparados.

Es importante señalar que los sistemas de control de Wal-Mart son únicos en el país. Conozco los procedimientos de las otras cadenas, y están muy distantes. A pesar de que algunas son de gran tamaño, aún no están interesadas en formar un departamento de auditoría, que realice un buen monitoreo. Supe del caso de un Gigante que abrió el año pasado en el estado de Oaxaca, poco antes de Navidad. Las ventas se dispararon, pero la merma fue de cerca del 10% porque los empleados eran de reciente contratación, no tuvieron capacitación, y se dedicaron a robar.

En otras empresas pasa lo mismo. Roban los clientes y los empleados. Hay alarmas con sensores que se colocan a la salida de las unidades, pero no existen en todas las tiendas, porque son muy caras. No se ha estandarizado un sistema nacional, ni se ha medido exactamente el impacto de la merma. Se sabe que está dentro de lo aceptable, que es el 1.5%, pero podría bajarse.

Es más peligroso y preocupante saber que el robo lo hizo un empleado. En algunas tiendas, un dependiente atiende a un cliente y le entrega la mercancía con un ticket. El mismo dependiente toma otro ticket por la misma cantidad y se lo da a otra persona.

En una distracción, esa persona toma otra vez el artículo, hace una devolución ficticia, recibiendo efectivo. El caso más peligroso es el de los empleados que están de acuerdo con las personas que entran armadas a alguna de las tiendas y se llevan buena parte de la mercancía. En ocasiones, las mismas videocámaras permiten apreciar que el vendedor participa del ilícito. Pero repito, como los sistemas no son los mismos a nivel nacional, no siempre encontramos a los cómplices, en caso de haberlos.



Una de las faltas de seguridad más graves es el sabotaje. Hace poco, alguien cortó los cables de los frenos de mi carro. El hecho coincide con algunos controles más estrictos que recientemente hice en el área financiera. Aún no sabemos si la acción fue contra mí o contra otro director, porque los dos autos son exactamente iguales. Estamos en la fase de averiguaciones, pero esto nos lleva a otro tipo de necesidad de seguridad, que deberá implantarse lo más pronto posible.

Sistema de Tiendas y Farmacias ISSSTE

Ex Director General del Sistema

Agosto 4, 2004

En el sistema comercial del ISSSTE hay dos problemas básicos de fraude. El primero es la merma, que está considerada como la más alta a nivel nacional. Y el segundo son los robos y fraudes, que pueden llevarse a cabo fácilmente en todos los niveles de esta organización. El sistema es tan noble, que a pesar de la gran cantidad de operaciones ilícitas, al final se termina el ejercicio anual con números negros y, en algunos años, con muy buenas utilidades.

La merma del Sistema ISSSTE es del 6%, mientras que el promedio de tiendas y farmacias a nivel nacional está entre el 1% y el 2%. La razón de las diferencias casi siempre está ligada con el fraude, que es una práctica muy común con algunas variantes. Por ejemplo, es probable que una tienda en la que el gerente es corrupto, el resto de los empleados también lo sean.

Hay diversas formas de robo. Por ejemplo, no hay control en el área de compras, ni mucho menos en la asignación de la mercancía a las tiendas que corresponden. En la tienda ubicada en la calzada Ignacio Zaragoza, podemos encontrar pasillos enteros llenos de implementos para uso de jardines, tales como mangueras, fertilizantes para flores y palas de uso doméstico. Pero en la zona geográfica de influencia no hay jardines, hace más de veinte años que está asignada a vivienda popular. Esto significa que

las compras se hicieron con dolo, y toda esa mercancía que no es útil, se queda en la tienda hasta que un día se remata o se regala.

En la misma ubicación Ignacio Zaragoza, hay pasillos llenos de implementos coreanos para sal, pimienta y especias que nunca se han desplazado, porque no es un tipo de artículo que compre la gente que vive cerca de ahí. También hay tiendas como la de Indios Verdes, en cuyas bodegas aparecieron doscientas cajas de cognac Courvoissier, que nadie conoce, ya que es excesivamente caro para el segmento, y que será muy difícil de vender. Es más, en el momento en el que fueron descubiertas, ya era necesario rematarlas.

En la tienda de Cancún se encontraron más de dos mil chamarras y guantes para invierno, todas de color negro, que obviamente no registraban movimiento. Igualmente muchos otros productos de invierno, como cobijas gruesas y chales. En Saltillo identificamos un lote de doscientos refrigeradores que no se habían promovido en mucho tiempo. Cuando intentamos sacarlos a remate, pudimos constatar que no tenían motor, teníamos que venderlos como chatarra.

Uno de los factores que marca una diferencia en la actitud hacia el fraude

benassini



www.benassini.com

es el hecho de que los empleados estén o no sindicalizados. El primer tipo muestra una mayor propensión al robo, respaldado por la seguridad que le da el grupo al que pertenece. También es importante la honestidad del gerente. Casi siempre hay más corrupción en aquellas tiendas en las que el gerente es corrupto y hasta cínico.

Incluso el personal de menores niveles en el departamento de compras da origen a otros fraudes que no se pueden comprobar de manera legal. Alguna vez, un proveedor de aceite comestible de marca muy conocida, recibió una orden de compra que solicitaba dos trailers de mercancía, que debían entregarse precisamente un viernes a las tres de la tarde, en una bodega previamente seleccionada. La compra era muy importante porque se acercaba la temporada de Navidad. El día de la entrega, el embarque estaba por llegar a su destino, pero dos calles antes fue interceptado por ladrones profesionales que portaban metralletas. Se llevaron los trailers completos y a la fecha no se ha encontrado al culpable.

Los robos dentro de las tiendas hechos por los mismos empleados son espectaculares. Un caso son las cajeras, que identifican a una persona conocida dentro de la fila para pagar. Y en lugar de registrar todos los productos por el lector óptico, solamente pasan la mitad. El problema es aún más grave en las zonas rurales, en las que el sistema computarizado y

el control de entradas y salidas aún no se implanta. Un cajero puede identificar a un familiar y solamente contabilizar una parte de los productos que quiere comprar. Los “cerillos” también tienen sus prácticas. Hay clientes que llegan a su casa y se dan cuenta de que su mercancía no está completa, aún cuando vieron cómo pasaba por la caja registradora.

También se da el caso de los empleados que se sirven “con la cuchara grande”. Por ejemplo, los domingos en la tarde es frecuente encontrar a los dependientes de una tienda tomando brandy con refresco y comiendo botanas, todo el material tomado del anaquel. Muchos de ellos son sindicalizados, así que no es fácil reportarlos o consignarlos.

Un caso excepcional. La gerente de una tienda foránea recibió la notificación de que al día siguiente comenzaría una auditoría en su unidad. Esa misma noche, la tienda que ella administraba sufrió un incendio, y la documentación que la inculpaba se perdió. Pero las averiguaciones lograron determinar que el incendio había comenzado precisamente en el área de farmacia, exactamente en el anaquel del alcohol. Una botella de alcohol de 96 grados se había derramado y se había esparcido linealmente, desde donde el envase se ubicaba, hasta el archivo de contabilidad que, curiosamente, se encontraba un piso arriba del derrame.

Promotora Internacional de Textiles S.A. de C.V.
Ex Director General
Agosto 4, 2004

Promotora fue una buena empresa durante más de quince años. Fabricábamos camisetas de todo tipo, maquilando para distribuidores y para la venta de artículos promocionales. La empresa cerró sus operaciones el año pasado principalmente porque la industria textil mexicana vive uno de sus peores momentos. Pero el problema de los robos internos también nos afectaba, tanto por sus repercusiones en los costos como porque representaba un malestar interno entre los obreros.

El principal tipo de robo que teníamos en la planta era el robo hormiga. Los obreros salían de la empresa con las camisetas puestas. Teníamos medidas de inspección de entrada y salida, siempre se revisaban las bolsas y las mochilas. Pero a pesar de ello persistía el robo. Pudimos detectar que los obreros estaban en contacto con los vigilantes, por lo que comenzamos a cambiar a los últimos más frecuentemente. Pero esto no dio resultado, cuando menos la mitad de las veces los robos persistieron.

De cada 70,000 prendas que producíamos a la semana, salían aproximadamente 300 sin que nos diéramos cuenta. Claro que solamente representaban menos del uno por ciento del total de la producción. Sin embargo, lo que nos preocupaba era saber que teníamos "el enemigo en casa". Además, algunas prendas eran más caras que otras, por lo que el monto del robo podía llegar a ser importante.

También teníamos el problema del robo de piezas y refacciones de los equipos. Para dar un ejemplo, el pie de una máquina de coser nos costaba alrededor de \$50 dólares. Pero no sólo era el precio. El principal problema derivado de este robo era que una parte de la producción se quedaba detenida. La segunda situación crítica era la obsolescencia de las partes robadas, porque llegaba a suceder que ya no estaban disponibles en el mercado cuando intentábamos reemplazarlas. Todo esto provocaba un retraso en el tiempo de sustitución de la pieza y, por lo tanto, en la fecha de entrega a nuestros clientes.

Como medida de prevención, optamos por cobrar las piezas a cada responsable del equipo. Pero esto generaba descontento entre todos los obreros, porque era factible que la persona que operaba la máquina de coser no necesariamente fuera quien había sustraído la refacción de la empresa. En menor escala, nos robaban los hilos y las agujas.

También llegó a suceder que nos robaran los logotipos y los diseños para hacer productos pirata, más corrientes y más baratos. Esto no lo podíamos evitar, porque los obreros estaban siempre en contacto con las prendas.



www.benassini.com

Llevábamos un control de las personas que tenían acceso a cada área de la planta. Pero no lo teníamos sobre las puertas abiertas. Podía suceder que la única persona autorizada entrara al área que le correspondía, pero otros empleados también entraban si la puerta permanecía abierta. Entendimos que el control tenía que ser completo, para garantizar que solamente esa persona entrara al almacén, y que al mismo tiempo la puerta permaneciera cerrada.

Otro problema eran las herramientas. Cuando la planta comenzó a operar, cada vez que entraba un nuevo empleado le entregaban sus herramientas de trabajo, tales como tijeras y un kit completo. Había ocasiones en las que al día siguiente de haberlo recibido ya no contaban con el material. La empresa optó por cobrar el material de trabajo desde el momento en que se le entregaba a cada obrero, lo cual también provocó descontento.

Tuvimos incluso que empezar a cobrar los uniformes. Había más de 300 batas en circulación, y en ocasiones los obreros se presentaban a trabajar sin ellas, por lo que teníamos que surtirlos constantemente. En ocasiones, el personal recibía su primera o su segunda bata, se iba con ella y ya no regresaba.

También identificamos que parte del personal se metía en los baños y se quedaba dormido hasta dos horas. Por eso decidieron implantar un sistema de control más

profesional, que consistió en lo siguiente: Las piezas de cada playera se entregaban todas juntas, acomodadas en un solo bulto. Cada pieza de cada bulto tenía un código de barras, que incluía el número de bulto, de pieza y de operación a realizar.

Cada paso del proceso de operación tenía un valor. Cuando un obrero terminaba ese paso, extraía la etiqueta a la pieza que había armado, y la pegaba en su propia hoja de control.

Al final del día, cada hoja de control de cada obrero se leía con láser y se determinaba cuánto debía pagarse a cada persona. Además, esto permitía al gerente de producción:

- Saber quién era la persona que llevaba a cabo cada proceso, en qué bulto.
- Identificar quién se ubicaba antes y después de cada operario.

El desarrollo del sistema tomó a la empresa cerca de dos años. Pero cuando lo instalaron al 100%, encontraron que los datos de los obreros más productivos eran contundentes, además de que podíamos saber con exactitud a quiénes despedir. El efecto en la nómina también fue impactante, porque la primera quincena lograron un ahorro de \$130,000.00 pesos. Al mismo tiempo, hubo personas que lograron triplicar sus ingresos. Y conservamos solamente a uno. Además del ahorro que esto implicó, pudimos suprimir

Facileasing: Una Empresa de Arrendamiento de Tamaño Pequeño a Mediano
Gerencia de Sistemas, Agosto 4, 2004

Somos una empresa pequeña que tiene alrededor de treinta empleados. Podemos ser una mediana en cuanto a los tipos y a los montos de las operaciones que realizamos. También somos de reciente creación, apenas tenemos cinco años en el mercado.

A pesar de que manejamos dinero, hasta la fecha no hemos tenido problemas de fraudes, ni internos ni externos. En el caso de la seguridad de la información interna, cada nivel de empleados involucrados tiene su propio código de acceso al sistema. Conforme se va ascendiendo en la importancia de los puestos, son menos las personas que tienen acceso, y también las claves son más complicadas, además de que se combinan. Por ejemplo, tenemos una tarjeta inteligente con un password. Otra razón por la cual no tenemos fraudes internos es nuestro tamaño. Si alguno de nosotros intentara hacer alguna operación fraudulenta, sería muy fácil detectarla.

Tampoco hemos recibido ataques externos contra nuestra información. Los sistemas han sido diseñados de tal manera que, a pesar de que alguien logre entrar en ellos, si no está habilitado dentro de la red, es imposible que vea la información que contiene.

Algo que sí se llevan los empleados y es muy difícil detectar, son todos los artículos de papelería, como los lápices, las plumas, el papel y objetos de ese tipo. Hay quienes incluso se llevan las tazas de café.

Utilizamos el sistema de lector de huella digital solamente para el control de acceso de los empleados. No aplica ni para proveedores ni para visitantes, aunque ambos tipos sean frecuentes. Al igual que en otras empresas, los proveedores y los visitantes tienen que anunciarse y pasar por los controles convencionales. Para asegurar los accesos internos a los que a veces llegan a entrar proveedores o visitantes, se utiliza una credencial. Y existen además áreas restringidas, que son oficinas a las que solamente pueden entrar algunos ejecutivos.

Compramos el biométrico de huella digital únicamente con su aplicación de llegadas y salidas de los empleados. No controlamos el tiempo que realmente trabajan. Esto es porque, por el número de empleados, es muy fácil darnos cuenta de quiénes pierden el tiempo.

Principales Empresas de Seguridad Industrial

Entrevistas con Directivos Diversos, Agosto 5 de 2004

Esta información es útil para conocer una parte de la competencia indirecta de los equipos biométricos, que son las empresas que ofrecen el servicio de seguridad, especialmente en el control de accesos. En el cuadro comparativo de precios, se aprecian las cantidades que una organización está dispuesta a pagar por el servicio de uno o varios guardias. Muchas de las empresas que contratan estos servicios utilizan herramientas tecnológicas complementarias.

Por motivos culturales, las compañías prefieren contratar guardias, adicionalmente o incluso en sustitución de otros mecanismos de seguridad. Sin embargo, los vigilantes son un dolor de cabeza para las agencias de seguridad. Algunas razones son:

- Muchos clientes piden guardias con ciertas características físicas. Quieren que sean rubios, que midan más de 1.75 metros y que sean al mismo tiempo muy corteses con el público, pero muy severos en cuestiones de seguridad. A veces se consigue este tipo de personal, pero en otras ocasiones no es posible. Y desde luego, son más caros.
- La rotación de los guardias es altísima. A veces su personalidad y su forma de trabajar son compatibles con la cultura que

prevalece en los lugares que les asignan, pero en otras ocasiones tienen conflictos y hay que cambiarlos, teniendo que sustituir al rubio de 1.75 metros por una persona común y corriente. Esto molesta a ciertos clientes.

- Cuando la demanda se incrementa, las agencias deben contratar a muchos vigilantes al mismo tiempo, y no hay tiempo para capacitarlos. Consecuentemente, la calidad del nuevo guardia no es la misma que se ofreció al cliente inicialmente. Sin embargo, sí se le cobra la cuota que había sido estipulada. También es un motivo de disgusto.
- Un factor que puede ser muy peligroso es que la necesidad de contratar a este tipo de personal de manera urgente, provoca que las agencias de seguridad no puedan ser muy rigurosas en el renglón de la experiencia y el currículum. Muchas veces no detectan que tienen entre su personal a individuos con antecedentes penales. O bien que, a pesar de tener un buen expediente, no son las personas más aptas para desempeñar esos cargos.

- La logística es también motivo de conflicto. Lo deseable es que quienes viven en una zona, sean asignados a empresas más o menos cercana. Pero debido a la alta rotación, terminan asignando una empresa en Tultitlán a un guardia que vive en Tláhuac. Esa persona viajará durante casi tres horas para llegar a su destino, después trabajará un turno de 24 horas, y deberá viajar otras casi tres horas para ir a descansar.
- Otro problema muy importante es el nivel socioeconómico y educativo de los guardias. Una buena parte de ellos terminaron solamente la primaria, aún cuando en teoría deberían tener un mayor nivel académico. Por eso se contratan en este tipo de empleos, que no requieren el desarrollo de muchas habilidades y conocimientos. Su sueldo generalmente es bajo, sin importar que la empresa contratante pague \$8,500 pesos mensuales a la agencia de seguridad. En promedio ganan \$2,500 pesos, recordando además que tienen jornadas de 24 horas seguidas, lo cual implica una gran responsabilidad. Este hecho los vuelve muy vulnerables a robar. Muchos de ellos no son maleantes, pero terminan robando mercancía o equipos, o bien proporcionando datos y acceso a terceros para que cometan un ilícito.
- La presencia de uno o varios vigilantes causa otro tipo de problemas en las empresas. Si están asignados a la recepción, muchos de ellos están platicando con la secretaria en lugar de hacer su trabajo. También es muy común que el departamento de personal piense que cuenta con un empleado más, y que es necesario "que desquite el sueldo". Entonces los podemos ver engrapando hojas, sacando copias, incluso envolviendo regalos y ayudando a adornar el árbol de Navidad.
- De las 2,000 empresas de seguridad que operan en nuestro país, muy pocas tienen permiso de la Secretaría de Gobernación, que es absolutamente indispensable, ya que tienen que cumplir con ciertos requisitos. Muchos de los dueños de las agencias carentes de permiso fueron agentes judiciales o policías despedidos, hecho que los vuelve poco confiables.
- La obligación de resguardar un lugar durante 24 horas seguidas es otro problema. Todos los vigilantes se duermen en algún momento de la noche, porque es parte de la naturaleza humana. En esos momentos los sitios vigilados se vuelven más vulnerables. Por ese motivo siempre habrá quejas. El problema se solucionaría con turnos de 12 horas, turnos que no son factibles por lo complejo de la logística.
- También es muy común que haya complicidad en las guardias

compartidas, como es el caso de los rondines. Puede ser que de las dos personas que deberían hacer un rondín nocturno, solamente una esté trabajando y la otra esté durmiendo. Y que la siguiente vez cambien el descanso. Una de las formas de controlar esto son los biométricos, porque cada vigilante deberá colocar su huella un número específico de veces durante su guardia.

Es importante señalar que en el mercado de las compañías de seguridad, éstas ofrecen en teoría una asesoría integral, para dar al cliente la mejor solución de seguridad. Sin embargo, en la práctica esto no es real. La consigna que dan a sus agentes de ventas es primero cumplir con una cuota de guardias, ya que son las más rentables.

Precios de los servicios de seguridad privada en México

Un análisis comparativo realizado entre las catorce empresas de servicios más grandes de México, se observa que el precio básico promedio de las guardias es de \$6,756.00. Una variante a considerar en el precio es el equipo de radiocomunicación. En el caso de Argos e Inter.-Con tiene un costo adicional de \$1,050.00. En el caso de Multisistemas ya está incluido, y Elim cobra \$506.00 adicionales.

Cuadro 4
PRECIOS DE LOS GUARDIAS DE LAS CATORCE EMPRESAS
MÁS GRANDES DE SEGURIDAD EN MÉXICO *

Lugar	Empresa	Precio mensual por guardia de 24 horas	Precio con equipo de radio comunicación	Precio sin equipo de radio comunicación	Con jefe de turno 24 horas	Con oficial de servicio por 24 horas
1	Eli	\$8,500	\$506	-	\$9,639	\$10,949
2	Multisistemas	\$8,500	Incluido	-	-	-
3	Spi Vam	\$7,800	-	-	\$8,250	\$8,700
4	Inter.-Con	\$7,500	\$1,050	-	\$8,500	-
5	G S I	\$7,231	\$900	-	-	-
6	Argos	\$7,183	\$1,050	\$350	\$8,300	\$10,000
7	CEIPSA	\$7,000	Incluido	-	-	-
8	Grupo Almaba	\$6,700	Opcional	-	-	-
9	Grupo Escarlata	\$6,520	-	\$350	-	-
10	Centinela	\$6,022	\$1,040	-	\$7,600	\$8,000
11	Security Man	\$5,900	\$900	-	-	-
12	Best Seguridad	\$5,804	Incluye celular	-	-	-
13	Coalición Profesional	\$5,434	-	-	-	-
14	Anáhuac	\$4,500	\$500	-	-	-

* Precios a enero de 2004

A continuación se detallan aspectos relevantes de algunas de estas agencias.

Securitas

1. Empresa trasnacional con tres años en el mercado mexicano.
2. Cuenta con 19 unidades de negocio, con sede en Monterrey. Tiene tres oficinas en Monterrey y tres en el D.F. Planea abrir cinco nuevas oficinas en el 2004.
3. Tiene una plantilla de 2,600 empleados.
4. Sus planes son consolidar sus operaciones, crecer de manera orgánica y liderar el mercado mexicano mediante adquisiciones de otras empresas.
5. Servicios: Oficiales de seguridad, sistemas de seguridad y consultoría e investigación.
6. Estiman su participación en México entre el 2% y el 3%
7. Tienen más de 200 clientes entre los que están: General Motors, Chrysler, AT&T, Whirlpool, Iusacel, Oracle, Cemex, Apasco, LG, Sony, Liverpool, Magna Formex, EDS y Tec de Monterrey.
8. Su misión es proteger hogares, lugares de trabajo y a la comunidad.
9. Su objetivo es aumentar utilidades antes de impuestos a un ritmo de crecimiento del 25% anual por un período de seis años a partir del año 2000.
10. Su participación en el mercado mundial es de casi el 7%. En Estados Unidos es del 20% y en México alcanza el 3%.
11. Sus ventas a nivel mundial fueron de \$7,800 millones de pesos en el 2003. En México fueron de \$28 millones de dólares, con incrementos anuales del 18%.

12. El 90% de su facturación proviene de los oficiales de seguridad para empresas. El 10% restante son productos de tecnología.
13. Core product: "Soluciones integrales de seguridad"

Inter-Con

1. Empresa trasnacional con quince años de operación en México.
2. Considerada como la "Principal Contratista del Año" por la NASA en Estados Unidos, al haber recibido la evaluación más alta por sus servicios. Su estrategia está basada en la explotación de su imagen, al presentarse como la primera compañía contratista en los Estados Unidos a cargo del suministro total de la seguridad para operaciones altamente clasificadas como confidenciales para ese gobierno.
3. Opera en 141 ciudades en 29 estados de la república mexicana.
4. Cuenta con más de 5,000 guardias a nivel nacional.
5. Su parque vehicular se compone de más de 200 patrullas.
6. Los servicios que ofrece son: Seguridad, alarmas y consultoría e investigación.
7. Tienen más de 450 clientes entre los que están: Coca-Cola Femsa, Elevadores Schindler, Lala, Gillette, Procter & Gamble, Shneider Electric, Kellogs, UPS, Wal Mart, Cinemex, Tiffany's, 7-Eleven, TMM, Teletón, Deutsche Bank, Microsoft y las embajadas de Estados Unidos, Reino Unido, Italia, Polonia, Holanda, Finlandia, Alemania y Canadá.

Elim

1. Empresa mexicana con dieciséis años de operación en México.
2. Su cobertura es D.F. y área Metropolitana
3. Cuenta con 250 unidades equipadas con radio de transmisiones.
4. Su estrategia se basa en la profesionalización de su actividad, por lo que crea el Centro
5. Formación Integral en Seguridad Privada Profesional, A..C.
6. Los servicios que ofrece son Guardias de seguridad
7. Cuenta con más de 1,000 clientes
8. Misión: Garantizar a los usuarios una solución de gran calidad a todo problema que se presente en el servicio que ofrecen como empresa e institución.
9. Core product: "Compañía totalmente profesional para su seguridad"

Multisistemas

1. Empresa mexicana con veinte años de operación en México.
2. Cuenta con 25 sucursales y 7,000 empleados a nivel nacional.
3. En los últimos años ha tenido un crecimiento del 39%.
4. Ofrece los servicios de Seguridad, alarmas y consultoría.
5. Principales clientes: Avon Cosmetics, Jafra, Chrysler, DHL, Elevadores Otis, Ferrioni, Hershey de México, Pepsico, Planta Texaco, Printaform, Prisma Envases, Ópticas Lux, Mc Donald's, Mancera Ernest Young, Iberia Líneas Aéreas de España, Instituto Cumbres.
6. Misión: Garantizar al mercado soluciones integrales en materia de seguridad patrimonial, basadas en el profundo conocimiento tanto de
9. crecimiento superior al 30% a partir del 2001.

las necesidades globales como de las específicas de cada cliente, para asegurar ventajas competitivas sostenibles y una alta calidad de servicio, hasta convertirse en el socio en seguridad de cada uno de sus clientes.

7. Core product: "Excelencia en seguridad".

Argos

1. Empresa mexicana con veinte años de operación en México.
2. Su objetivo es superar las 1,000 guardias en 2004.
3. Tiene presencia en el Distrito Federal, área metropolitana y estado de Guanajuato.
4. Plantilla de 584 guardias y 66 administrativos, parque vehicular de 14 unidades.
5. Central de monitoreo y sistema de alarmas. Para la supervisión electrónica utiliza la infraestructura de red del cliente que esté conectada a Internet y tenga una IP pública contratada y asignada por el proveedor del servicio; Servidor de comunicaciones Multimedia Alcatel 4400 con sistema de correo de voz CALLWARE, Red estructural para voz y datos.
6. Principales servicios: Vigilancia, alarmas y consultoría.
7. Principales clientes: Reebok de México, Colgate Palmolive, Dow Chemical, Universidad del Valle de México, Editorial. Santillana, Médica Móvil, Grupo Financiero Banamex-Citigroup
8. Misión: Brindar tranquilidad y confianza al cliente a través de servicios y productos de calidad que garanticen su seguridad. Su facturación de guardias ha tenido un crecimiento

Otros Testimoniales

Agosto 5 de 2004

“En los sites, que son los sitios donde están las computadoras, hay un sistema de seguridad con huella digital. Solamente pueden acceder los administradores, dependiendo de cada proyecto que manejen y de cada nivel. Todos los empleados tenemos una tarjeta con lector magnético para entrar a las instalaciones. En el caso de Internet, existe seguridad en las primeras cuatro capas.”

GEDAS MÉXICO, filial de Volkswagen

“Uno de los negocios que más se presta para hacer fraudes es el de la entrega de gas a domicilio. Una práctica muy común es que el chofer del camión vaya llevando el control de cuántos litros surten. Suponiendo que hacen una primera visita y surten \$500 pesos de gas, no necesariamente los facturan. Y en la siguiente visita, como tienen guardada una factura, surten la mitad del combustible pero cobran el doble.”



FUENTES DE CONSULTA



Biometrics Industry Report: An Interview with JohnChang, Allied Business Intelligence

Allied Business Intelligence Inc. is an Oyster Bay, NY-based technology research firm specializing in communications and emerging technology markets. ABI publishes research and technology intelligence on the broadband, security, wireless, electronics, networking and energy industries. Their most recent report is entitled, "Biometric Systems: Worldwide Deployments, Market Drivers, and Major Players". Details of the biometric study can be found at alliedworld.com.

FB

John can you fill us in on the background of ABI?

ABI

Yes, ABI...is a technology market research firm. We specialize in the communications industry; security, wireless, broadband, networking, energy and any other related emerging technologies.

FB

How did you execute your study? How many companies did you interview, and in which regions?

ABI

We interviewed all the key players including multiple biometric companies and middleware companies. We interviewed and performed a company analysis to determine what for example the revenue is for a particular biometric such as fingerprint. We broke the regions down into four sections North America, Europe Latin America and Asia.

FB

In 2003 you forecast a 39% increase in biometric revenues and a 100% increase for 2004. What did your research indicate to forecast the 100% increase for 2004?

ABI

What we are finding is that the US Government is exploring all the different biometric technologies. I'll give you one example to illustrate the anticipated growth: The Enhanced Border Security And Visa Reform Act will require visitors to the US, by 2004, to obtain a visa from the US Consulate with a biometric identifier. That is just one example. We are also finding that the securities in the airports are all going to expand. Right now we talking about less than 5% of the airports around the world have implemented biometrics. We definitely see large growth within the transportation, financial, and healthcare industries.

FB

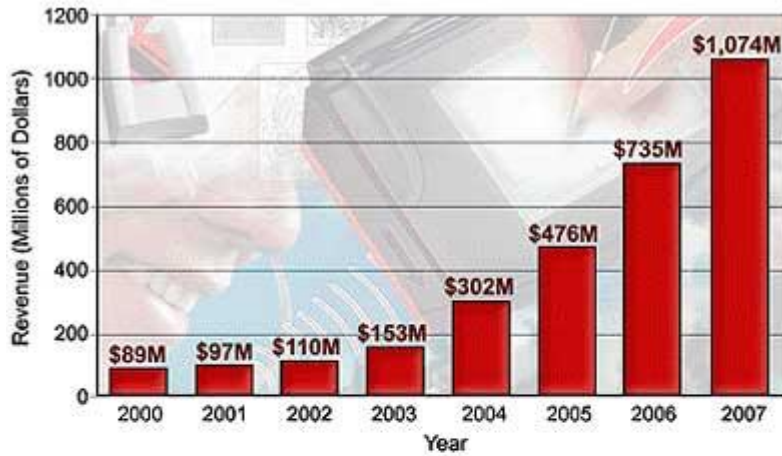
Biometrics is a global industry; were there certain areas that your research indicated would see the greatest growth?

ABI

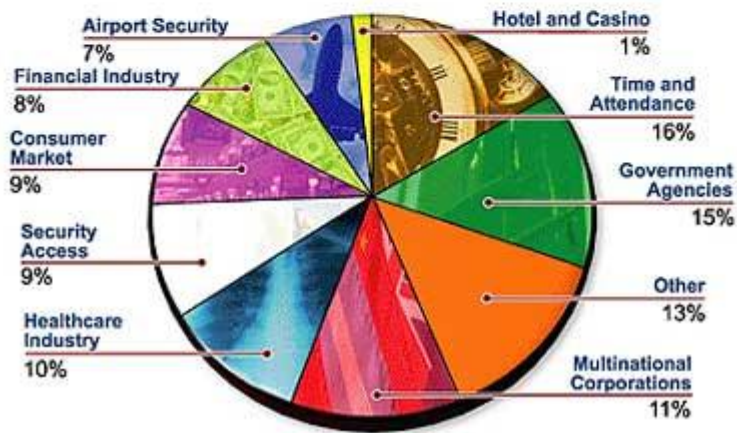
We're finding that certain technologies are being adopted in the certain regions. North America currently has a hold right now on the fingerprint and hand identification systems. Europe holds about 30 % of the voice authentication market right now. We

are finding that Europe and Asia are also quickly adapting to biometrics.

Total Biometrics Revenue World Market: 2000 to 2007
(Source: Allied Business Intelligence)



Total Biometrics Revenue Percentage by Industry: 2002
(Source: Allied Business Intelligence)



FB

What do you see as the ultimate benefit for the end user?

ABI

Let me give you a few examples: Some Universities have implemented biometrics identifiers for unlimited meal plans, thereby eliminating the swapping of cards between students and reducing the Universities food costs. Also, hand recognition has been implemented for access control providing significant cost savings is reducing the number of security personnel required to perform these functions.

FB

What do enterprises desire before they implement biometric solutions?

ABI

The enterprise presently does not have a way to get to the biometrics. Enterprises are looking for the larger security players to implement biometrics. For example, if I have a home security system and forget my pin code someone will call me to verify who I am and allow access. With biometrics as the same thing has to happen. Who will perform the same back office function for a biometric enterprise solution? Does this mean that the enterprise must hire a full time biometric technician?

The cost efficiencies of implementing may be offset by the fact that enterprise may have to provision the system. So it's not just the cost of the equipment, but the provisioning afterwards that's the

critical issue. The back office support issue must be addressed.

At this point in time, our research indicates the biometric companies have yet to fully satisfy the concern. This is where the larger security companies such as ADT come in.

FB

What did your report indicate were the market drivers for biometric Industry?

ABI

Some of the market drivers would include the cost reduction of equipment. For example if I have 50 employees and two door entries and I use the standard PIN number system to access, it would cost anywhere from \$5,000 and \$10,000 including installation for this exact service. You can get the same pricing point but a higher-level security by installing finger or iris recognition.

FB

So is the market driver the decrease in the cost of the biometric solutions combined with the fact there is an increased need for security?

ABI

Yes. That actually represents two market drivers. Another would be the improvement in the technology. Across all the different types of biometrics there has been significant improvements over the past several years. Improvements in technology include advancements of the chip sets. These chip sets require less power and cost less. Another driver would be the biometric technology standards. The governing

bodies, consortiums and committees include the BioAPI, NIST, M1. They are

working quickly to allow faster implementation of biometrics.

FB

What did your report indicate were the market barriers for the biometrics Industry?

ABI

We have talked already about the fact that there are no existing operational support systems. Another is the proprietary based technology that prohibits a company from switching from biometric vendor A to biometric vendor B. At this time they are not interoperable. Another potential market barrier is privacy. People feel that biometrics may be intrusive but education and familiarity will resolve this.

Our research indicated that the privacy issue is less of a market barrier than the back office and proprietary/interoperability issues.

FB

What did you personally find as the biggest surprise that surfaced from your study?

ABI

There will be further consolidation in the biometric industry, similar to Identix and Visionics merger. Our research indicated that the larger security players would be looking to acquire or merge rather than build the specific components that are needed. ABI expects these larger players to offer biometrics as part of their overall security solutions.

About John Chang

As a senior analyst with ABI, Mr. Chang's primary focus is emerging technology. He has authored numerous research spanning markets from broadband, telecommunications, cable television and security. Leveraging experience first garnered at IBM, Mr. Chang continues to expand his technical and research skill sets to fortify ABI's coverage of emerging technologies. John is frequently cited in major publications including Business Week, CNET News, EE Times, Reuters, Multichannel News, and America's Network. He received both his B.S. in Management Information Systems and M.B.A. from Binghamton University.

Siemens' Security Division Outlook April 9, 2002

An exclusive interview

Looking at 20 percent annual growth and to benefit from its international ties, Siemens Building Technology's North American Security Division has an optimistic outlook on the future. The division was created through the July 2001 acquisition of Security Technologies Group (STG), Plantation, Fla., the nation's largest provider of fully-integrated, electronic security systems to large commercial clients and institutions. "More than 75 percent of what we are right now is STG and the other 25 percent comes from the other two divisions (fire safety and building integration) that were involved in security projects before the acquisition," explains Mark Landis, president of Siemens' North American Security Division (and former president of STG).

Siemens is a Munich, Germany-based conglomerate with \$90 billion in yearly revenue per year. With offices in 90 countries, the company has about 450,000 employees all over the world. Siemens' building technology division generates \$5 billion dollars a year in revenues. The North American market (US and Canada) is responsible for a little less than \$2 billion out of the total.

Sandra Marina Johnson, editor of Seguridad Latina, our sister publication serving the Latin American market, interviewed Mr. Landis and Senior Vice President Steve E. Walin recently at their Florida offices. Here is a transcript:

LANDIS: "The expectation is that our business will grow dramatically over the next five years. We expect to quadruplicate our business in that period of time both by organic growth and by new acquisitions."

"Our division installs access control systems offering a variety of cards and technologies, including biometrics. We also install CCTV, intrusion and alarm systems. We have two central monitoring stations in the United States. All our clients are commercial entities to which we offer alarm monitoring. In some cases we also offer remote management of their access control systems. Since we install third parties products, we also invest in evaluating and reviewing products and technologies. We publish reports with the results of our analysis. "SBT's North America Security Division is growing the business at a rate ahead of the electronic security market growth, which is considered to be 12 per cent per year. We are growing at a 20 percent pace and we will grow more rapidly through acquisitions."

"SBT's North America Security Division works with companies such as General

Motors, print, Intel, Boeing, Dell Computers, which many times ask us to support them overseas.

Now that we are part of a company with offices all over the world we can do it. We can install a system in a U.S. based company and offer to control their overseas facilities over global networks. STG was already known as the best company installing large-scale geographically scattered projects operating over networks, but we couldn't take that overseas. Now we have the combination of having the technology and the expertise as well as the people who can implement it and support it in overseas locations. Right now we are working with several companies who are interested in having global security systems."

Q: What about the biometrics market?

LANDIS: "So far there is a lot of talking about biometrics but not a lot of sales. I think the interest in biometrics will continue to grow. There is a variety of biometric technologies, but so far the most popular is the fingerprint. We are not pushing any of these, but definitely we have already evaluated all the options available in the market."

WALIN: "My point of view is that the demand for biometric products has grown. He have seen an increase in requests of biometrics but our job as a system integrator is to solve our client's specific security problems by offering the best solution in each case. We can certainly integrate biometric products in our solutions, but as a percentage of our

business, biometrics is still a small but growing portion of our business."

Q: How has the security industry changed since Sept. 11:

LANDIS: "In a presentation I gave yesterday I quoted a special report on workplace security published on March 11 by the Wall Street Journal. The report said: 'In the wake of September 11, security seemed to be where the money was - and companies of all stripes wasted no time trying to get a piece of the action. Thus far, the biggest winners have been consultants and other advice givers. Seminars are also popular.'" "For the most part, the only organizations that have shelled out for new technologies to identify potential criminals have been public-sector operations and airports." "As they say, we haven't seen a big jump in spending but we have to take into consideration that all the corporations are suffering from the economy."

Q: What are the trends?

WALIN: "One of the trends we are seeing in this market is that the customer wants to deal with fewer suppliers and prefers to work with financially stable, strong companies. This is something that definitely differentiates us. We can take advantage of this trend because of the fact that we are stronger, larger and more stable than many other companies, which is a point of contrast."

LANDIS: "The way we are working in order to add new vertical markets is through a Vertical Markets Team. This team is in charge of opening new possibilities within the Chemical and

Government market segments. We are also trying to reach the transportation industry (with an emphasis on airports) as well as segments such as telecommunications, schools and universities. "SBT's North America Security Division buys the products we require for our client's installations, but yes, Siemens is interested in creating an area devoted to manufacturing some electronic security products or in acquiring a company that already manufactures this type of products. Right now we spend millions on buying products from third parties. This doesn't mean that we won't continue buying products from other companies, but that we will also offer a Siemens option. "Siemens is also interested in creating a global access control product that can be offered as an alternative to similar products available in the market. "The way we differentiate (ourselves) is by

the quality of our field implementation programs. Because our business is more high-end, more sophisticated, our field operation personnel and project managers are trained to be more effective in sales, installations and follow up services. "The other advantage is that Siemens in general is focused on customer satisfaction. For Siemens customer satisfaction is not only a word. Every three months, a large portion of Siemens security customers (between 150 and 200) are contacted surveyed by an outside company. They do a phone interview where the customer will be asked about its satisfaction with our service. All that information is saved in a database and according to the customers' answers each of the offices gets a rate. They will also receive an explanation of why the customer is not satisfied."

ASSA ABLOY Expands in Latin America

Hayward, Calif., April 30, 2001

ASSA ABLOY ITG (Identification Technology Group) recently announced the formation of a new operational business unit called ASSA ABLOY, Latin America.

The creation of the Latin American business unit is a result of ASSA ABLOY ITG's continued commitment to its international customers. ITG has expanded its international sales team with members who have diverse language skills and considerable market experience.

The new business unit will consist of CODAS Electronica SA, headquartered in Buenos Aires, Argentina, and a regional office in Mexico City. Future plans include establishing offices in Brazil and Uruguay.

Categories

<ul style="list-style-type: none">• Access control• Alarms & intruder detection• Asset management, eas• Business• Cables & connectors• Cctv• Communication• Containers, bags & seals• Enclosures, racks & consoles• Exhibitions• Fire & safety• Gate, door automation• Guarding products & services• Home automation• Id systems, biometrics• Integrated systems• Investigations• It security	<ul style="list-style-type: none">• Lighting• Locks & safes• Metal, bomb detection• News & events• Organizations• Outsourcing, facilities management• Perimeter security• Personal security• Power supplies & batteries• Regular column• Risk management• Securex• Showstoppers• Smart cards• System integrators, installers• Technology• Vehicle security
--	--

AXCESS Becomes a Supplier to PSA Security Network Find BIOMETRICS, October 10, 2003

Largest Security Industry Buying Cooperative to Add Network-Based Video Surveillance and RFID System Solutions for its Members AXCESS International Inc. (OTC Bulletin Board: AXSI) announced today it has become a supplier to PSA Security Network, the world's largest buying cooperative in the security industry, whose members are responsible for over \$1 billion in annual installations. AXCESS will provide video surveillance, access control, and asset protection systems to the member companies based upon its leading edge network-based, streaming video and radio frequency identification (RFID) technologies. AXCESS' technologies extend the typical security network while improving its productivity and effectiveness.

PSA member companies are an elite group of independently owned, engineered security systems specialists who design and install some of the most sophisticated electronic security systems utilizing video surveillance, access control and biometrics. There are over 100 companies in the network represented by over 1,100 staffed technicians who design, test, install, and maintain security systems in the US, Canada, Mexico and Latin America. "AXCESS offers solutions in the high demand applications of CCTV, access control, and asset protection. Our industry now sees network-based solutions in CCTV and the use of RFID as key automating technologies for improving a given security network by

making it more effective and easy to expand without increasing security personnel," said Bill Bozeman, President of PSA Security Network. "Providing timely, leading edge products to our members is an important role for PSA and we look forward to working with AXCESS."

"PSA has a heritage of providing select, quality, leading edge products to its members so they can deliver the best available security system to fit the need," said Allan Griebenow, President and CEO of AXCESS. "Their membership includes the type of security system integrator our company is designed to support and we are very pleased to have the opportunity to supply them best of breed solutions."

The AXCESS systems enable automated surveillance, monitoring, and control of personnel, vehicles, and assets. The RFID ActiveTag(TM) tagging solutions provide economic and reliable automatic identification of people, vehicles, and assets, improving the security and throughput for building access, at gated areas, as well as securing critical IT assets. For "hands-free," high speed personnel access control, current proximity-based I.D. cards can be retro-fitted with the AXCESS solution by attaching the card to a "docking" tag which adds transmit range and tracking capabilities and doesn't require a card to be presented by the holder to gain access. Vehicles are tagged to provide secure, automatic access to gated areas

such as parking facilities, again removing the requirement to present a credential or enter an access code. Assets are tagged for automatic location and identification, and are automatically protected from unauthorized removal from a secured area or from a facility. Personnel, vehicle, and asset tags can all be linked to provide an additional level of security.

AXCESS Prism Video(TM) products offer a complete, networked digital video system for the enterprise providing remote and local CCTV to the desktop for video surveillance and recording. The product line includes network cameras, network transmitters, software-based recording, and multiple viewing options providing customers with the lowest cost overall enterprise-wide solution. High speed, real-time video and audio provides true visibility into operations to reduce theft and terrorism, increase criminal apprehensions, improve life safety, improve enterprise operations, observe sales programs, and to monitor compliance with both legal and corporate guidelines.

AXCESS Inc. (OTC Bulletin Board: AXSI), headquartered in greater Dallas, Texas, provides intelligent electronic security surveillance systems that locate, identify, track, monitor, count, and protect people, assets, and vehicles. The network-based systems reduce loss, liability, and security system costs, while boosting effectiveness and extending system coverage. AXCESS

utilizes two patented and integrated technologies: battery-powered wireless tagging (commonly referred to as Active-Radio Frequency Identification or RFID) and network-based, streaming digital video (or CCTV). A particular focus is on automatic incident detection, recording, and notification. The main applications are network-based security video recording and surveillance, automatic personnel and vehicle access control, and automatic electronic asset surveillance, management and protection. AXCESS is a VennWorks LLC partner company. More information is available at <http://www.axsi.com/>.

Established in 1974, PSA Security Network is the world's largest electronic security cooperative whose members are responsible for over \$1 billion dollars of electronic security and life safety installations. PSA member companies specialize in the design, installation and integration of CCTV, access control, and life safety systems for security, management control and communications. More information is available at <http://www.psasecurity.com/>. This release contains forward-looking statements as defined in Section 21E of the Securities Exchange Act of 1934, including statements about future business operations, financial performance and market conditions. Such forward-looking statements involve risks and uncertainties inherent in business forecasts. SOURCE AXCESS International Inc.

Showcases

<ul style="list-style-type: none"> • Fingerprint • Iris Recognition • Hand & Finger • Facial Recognition • Voice/Speaker • Consultants 	<ul style="list-style-type: none"> • Smart Cards/Multimodal • Signature/Keystroke • 2D Barcodes • Sensors • Middleware/Software • Integrators/Resellers
--	---

Biometrics Adoption Depends on PriceValue Balance

Tekrati Research News, Frost & Sullivan, June 9, 2004

A Frost infosec study concludes that despite higher biometric security, the trade-off between price and value received needs to be favorable to the customers. Thus, Frost expects the price-value balance to be critical in determining the scale of deployment of individual biometric technologies.

Biometrics technologies are likely to be the vital component in tomorrow's security systems, as governments and private enterprises worldwide emphasize on establishing the positive identity of people in high-security areas to prevent unauthorized access. Such measures are likely to accelerate the global adoption of various biometric technologies.

While acquiring a high degree of security is a priority among many customers post-9/11, the cost of the project is still a key-deciding factor for implementing biometric security solutions.

New analysis from Frost & Sullivan, World Biometrics Market, reveals that this market generated revenues worth \$303.3 million in 2003 and is likely to reach \$3548.2 million by 2009. "Although the prices of biometric systems have been declining over the years, they are still more expensive than alternative security solutions," says Frost & Sullivan

Biometrics Program Manager Prianka Chopra.

When end-users prioritize on price, they tend to adopt less expensive though less secure solutions. Industry participants, however, will be compelled to continue investing substantially in research and development to remain competitive in a market characterized by frequent performance improvements, rapidly changing technologies, and the resulting price declines.

Market success will depend on a participant's ability to keep pace with technological developments and introduce new products with sophisticated features that cater to end-users' current as well as future requirements.

Additionally, biometric companies will be required to meet the emerging industry standards to prevail in this dynamic market such as the BioAPI, CBEFF, and X9.84 standards to prevent customers from being locked into proprietary solutions.

Apart from battling issues related to price, technology, and standards compliance, privacy concerns regarding misuse of biometric data and illegal tracking of consumer activities also need to be addressed. Failing to

do so could hamper deployment of biometric solutions.

“It is critical to establish clear-cut principles and guidelines to safeguard the interests of the public and ensure that the same are followed to the book right from the beginning of the project,” concludes Chopra.

The World Biometrics Market, part of the Global Biometrics Subscription, examines the demand for following biometric technologies: non-AFIS fingerprint, face recognition, iris recognition, hand geometry, voice verification, and signature verification. It also analyzes the market based on application segments (physical access control/time and attendance; government and law enforcement, PC/network security, transactional authentication, and others), vertical markets (government, financial, healthcare, travel and transportation, and others), and geographic regions (North America, Europe Middle East Africa (EMEA), Asia Pacific, and Latin America).

Frost & Sullivan Growth Partnership Service

Based on extensive and in-depth research, real-world consulting work, and new theories tested in hundreds of companies across many industries, Frost & Sullivan has evolved its Growth Partnership Services (GPS) program that provides established and emerging

firms with powerful growth visions. Moving beyond token mission statements, GPS provides an actionable vision to growth consulting partners by illustrating how key intelligence and strategic research based on defined goals can guide day-to-day behavior and overall company direction. The foundation of Frost & Sullivan's GPS includes:

- Assisting companies to reach their full potential in the core business
- Providing growth strategies to help companies expand into related businesses
- Preemptively redefining the core business during market turbulence
- Applying the Frost & Sullivan framework to identify and address common mistakes resulting from misaligned corporate strategies
- Recommending growth management strategies through continuous partnership

To maximize the potential for growth within a firm's internal and external environment, Frost & Sullivan consultants facilitate the creation of strategic programs that deliver improved market success. Frost & Sullivan's strengths lie in combining strategic understanding with market expertise and applying these with absolute commitment to its clients' growth.

Certicom Moves Into Latin America, and Announces Partnerships and Licensees in Argentina, Brazil and Chile Hayward Calif., April 30, 2001

Certicom (Nasdaq: CERT; TSE: CIC) a leading provider of mobile e-business security, today announced that it has expanded its international efforts to include Latin America. The Company is announcing key partnerships and licensees in the countries of Argentina, Brazil and Chile including Cirilo Ayling S.A., Montreal Informatica, TakeNet and Biotech Technologies Chile S.A. Certicom is working with these companies to provide complete e-business security solutions based on Certicom's industry leading toolkits and public key infrastructure (PKI) products that will be used to deliver advanced levels of security to the Latin American e-commerce and m-commerce markets.

"We are excited to be expanding our International efforts to include Latin America, an area that is quickly growing and realizing the need for end to end e-security solutions," said Richard Depew, Certicom's executive vice president. "Certicom's partnerships with local companies will play an important role in promoting the adoption of security infrastructure solutions for e-business in Latin America and around the globe."

The Hayward, California based company has expanded its Latin American presence in response to a growing market. A recent study by IDC predicts that a booming cellular market in Latin America is expected to fuel the

development of mobile data, driving the market value of this segment to US\$4.2 billion by 2004.

In Argentina, Certicom has formed an alliance with Cirilo Ayling S.A. to enable businesses to meet the significant growth in demand for secure online payments in the financial and communications market. Cirilo Ayling is leading provider of information technology and cryptography services and products to the Argentinean banking, financial and retail industries.

In Brazil, Certicom is working with Montreal Informatica and TakeNet Ltda. to provide security solutions for top government agencies and financial clients. Montreal Informatica, a leading information technology firm with 6 regional offices throughout Brazil, will be a strategic Certicom partner in the Brazilian marketplace. TakeNet, a wireless technology company, has licensed Certicom's wireless security technology to launch the country's first mobile browser for the Palm Series as well as Pocket PC running on Windows CE.

In Chile, Certicom has partnered with Biotech Technologies Chile S.A., a security cryptography and biometrics company, to provide a trusted and secure solution for mission critical communications for its banking and governmental clients.

"Certicom's leading products and solutions are certainly a critical element in providing the highest levels of security required by corporations and financial institutions in the Brazilian market place," said Marcel Lapido Barbosa, project manager of Montreal Informatica. "By working with them, we are providing our customers the most advanced levels of both wired and wireless security available today."

"Certicom's leadership in end to end security solutions enables TakeNet to provide our customers with strong security from a name that is trusted internationally," Daniel Rodrigues Costa, president and CEO of TakeNet. "Certicom's experience in providing advanced wireless security allows us to build strong and efficient encryption into our products."

Certicom is a leading provider of information security software and services that address the need for end to end security solutions. Certicom's robust suite of products and services include WTLS Plus™ for WAP

implementations, Security Builder® cryptographic toolkit, Trustpoint™ PKI products, MobileTrust™ managed certificate service and the movianVPN handheld client.

Certicom is a leading provider of information security software and services, specializing in solutions for mobile e-business. The company's products and services are specifically designed to address the challenges imposed by a wireless data environment. Certicom's solutions incorporate its efficient encryption technology and are based on industry standards for information security that utilize public key cryptography. Certicom's products are currently licensed to more than 150 customers including ePocrates, Inc., Motorola, Inc., NeoPoint, Inc., Nortel Networks, Openwave Systems, Palm, Inc., Pixo, Inc., QUALCOMM, Inc., Research In Motion Ltd. and Sony International (Europe) GmbH. Certicom's headquarters and worldwide sales and marketing operations are based in the Silicon Valley in Hayward. For more information, visit Certicom's Web site at <http://www.certicom.com/>.

Multi-Modal Biometrics: The Future of Biometrics

By Paul Mehra, Post, September 11, 2001

Biometric technologies came into focus as never before. Since then, various government agencies and private enterprises across the world have depicted keen interest in implementing the highly secure biometric solutions. The choice of a particular biometric technology for implementation largely depends on the type of application and the level of security required. Though biometrics is a useful tool to address these newfound concerns of the customers, no single biometric technology has the capability of fully satisfying the customer demands.

Multi-Modal biometrics - the use of multiple biometric indicators for implementation - has thus emerged as a possible alternative. The use of more than one physiological or behavioral characteristic for enrollment and verification or identification is expected to enhance the security features of complete solution. Multi-modal biometrics usage is being actively considered in applications involving Border Control, Physical Access Control, and PC/Network security.

Advantages of Multi-modal Biometrics

The integration of two or more types of biometric verification systems helps to meet stringent performance requirements set by security-conscious

customers. Here is a brief look at a few advantages of implementing multi-modal biometric solutions: Using multiple biometrics helps in improving the accuracy of the overall system. Such solutions also provide a secondary means of enrollment and verification or identification in case sufficient data is not extracted from a given biometric sample. They also have the ability to detect attempts to spoof biometric systems through non-live data sources such as fake fingers.

Key Industry Trends

Different combinations of biometric technologies can be used such as those involving finger-scan along with face recognition, face recognition with iris recognition, and face recognition with iris recognition and finger-scan for commercial deployments. Another interesting combination involves the use of face recognition, voice verification and lip movement recognition.

Solutions based on face recognition and iris recognition are expected to occupy the majority market share in the multi-modal biometrics market in future. The use of a common imaging device for capturing the face and iris template is expected to cut down the overall cost of implementation. This development is expected to be the major driver for the growth in implementations based on iris recognition and face recognition. This combination would also boast of high accuracy as the underlying iris recognition solutions are deemed to be most accurate among biometric solutions.

The increased usage of smart cards across the globe has also boosted the potential in biometrics market. Growing demand for high memory smart cards of 32k and 64k memory enable storage of more than one biometric template in one card.

Another positive development is the steady growth in the number of vendors offering multi-modal biometrics solution across the world especially; in Asia-Pacific. Vendors such as Alpha Engineering, BlueNics, DreamMIRH, Evermedia Co. Ltd., HumanScan, ID Tech Co. Ltd. and Keyware are expected to play a significant role in contributing to the growth in multi-modal biometrics market.

Despite these positive trends, actual implementations will act as reference sites for future customers and will determine the rate of adoption of multi-modal solutions. The success of these reference projects would prompt new customers to implement these solutions.

Another important issue that has to be tackled is of adoption of common standards. Over the last few years, efforts have been made by organizations such as BioAPI to develop common standards for each of the biometric technologies. However, vendors have been a little slow in adopting these standards and this factor could also hinder the growth in multi-modal biometrics implementations.

The total cost of implementing multi-modal solutions would also be an important criterion affecting the final choice of the customer. The higher security provides would have to be justified by a higher price paid for by the customer.

Thus, keeping all these factors into consideration, one can predict a steady growth in demand for multi-modal biometrics solutions in future. The adoption rates though, would depend on the effectiveness of these solutions to address the concerns of customers.

Enormous Emphasis on Security after 9/11 Boosts Biometrics Adoption

The devastating impact of the 9/11 terrorist attacks is still resonating across the world and security concerns have escalated during the past two years. This has led to the emergence of a new security paradigm, requiring a dynamic and adaptive approach to confront the evolving security threats. Biometrics is likely to be the vital component in tomorrow's security systems, as governments and private enterprises worldwide emphasize on establishing the positive identity of persons in high-security applications/areas to prevent unauthorized access. Such measures are likely to accelerate the global adoption of various biometric technologies.

This Frost & Sullivan research examines the world biometrics market based on the following: technologies – non-AFIS, face recognition, hand geometry, voice verification, and signature verification; application segments – physical access control/time and attendance, government and law enforcement, PC/network security, transactional authentication, and others; vertical markets – government, financial, healthcare, travel and transportation, and others; and geographic regions – North America, Europe, the Middle East and Africa (EMEA), Asia Pacific, and Latin America.

Growing Public Awareness Drives Market Uptake

The level of public awareness about biometric technologies has increased substantially following enormous media attention and exposure post 9/11. Several government agencies and private enterprises evaluated different biometric

technologies to choose the best among them for meeting their security requirements and have already begun pilot and full-scale projects.

"Despite such enormous interest shown, revenue flow for biometrics solution providers was well short of expectations during both 2002 and 2003," says the analyst. This was mainly due to the delay in spending from the government sector, the main target vertical of biometric technologies. However, this trend is likely to reverse in 2004 with the gradual revival of government spending. On the enterprise front, financial, and healthcare sectors are expected to show keen interest in adopting biometric technologies.

Trade-off between Price and Value Received Decides Customers' Preference

The biometrics market is likely to enter the high-growth stage within the next two to three years. Several government legislations mandating deployment of biometric security solutions and the concerted efforts of industry associations in fostering international biometric standards have set the platform for such sustained growth. Additionally, falling prices coupled with enhanced performance and accuracy levels of various biometric technologies are likely to catapult market uptake.

However, biometrics solutions are still more expensive than alternative security solutions. When end users prioritize on price, they tend to adopt inexpensive though less secure solutions. "In the final decision-making process, the cost of the project is still critical for most customers," says the analyst. Ultimately, the trade-off between price and value received needs to be favorable.

World Hand Geometry Biometrics Markets Frost & Sullivan Research Report, March 5, 2004

Large Size of Hand Geometry Readers Limits Application Expansion

The large size of hand geometry readers restricts their use in certain applications and poses challenges in implementing the technology in applications that require small user interfaces. For instance, the PC/network security market that presents significant growth opportunities for biometric technologies might be difficult to penetrate for hand geometry solutions. This market is expected to be dominated by the relatively smaller and inexpensive finger-scan technology devices. In fact, finger-scan biometrics is a major competitor to the use of hand geometry technology in physical access and time and attendance applications, two of its key markets. Despite such obstacles, participants are expected to achieve strong growth by showcasing the efficiency of hand geometry technology in reducing 'time fraud'. Heightened security concerns after 9/11 and the nonintrusive nature of hand geometry readers are also likely to assist them in their quest for higher market share.

This Frost & Sullivan research examines the world hand geometry market by geographic regions {North America; Europe, Middle East, and Africa (EMEA); Asia Pacific; and Latin America} and application segments (physical access control; time and attendance; and others). The study provides rigorous analysis of each geographic region and application segment, seven-year revenue forecasts, and an overview of emerging market trends that will enable participants to assess the current and future growth prospects.

High Durability and Throughput – Strong Points of Hand Geometry Devices

"Hand geometry solutions are exceptionally robust, handle a large volume of transactions, and function accurately in harsh environments where other biometric technologies may not work," says the Program Manager of this research service. These devices have the ability to work under extreme temperatures ranging from negative 30 to 150 degree Fahrenheit and still provide reliable results for long periods. "This is exactly why hand geometry readers are installed outside physical premises and are extensively used for physical access control and time and attendance applications across the world despite their relatively higher implementation costs," explains the Program Manager.

Physical Access Control and Time and Attendance to Continue as Dominant Applications Hand geometry solutions enable significant cost savings for customers by reducing 'time fraud' and 'buddy punching' while keeping track of employees' work hours and maintenance of payroll systems. Such ways of reducing costs have assumed greater importance with government and corporate enterprises battling the ongoing economic downturn to remain competitive.

The distinct advantage of hand geometry technology is that its performance remains unaffected by soiled or dirty hands. This attribute is especially useful in foundries and construction sites where workers perform a fair degree of manual labor. These wide-ranging benefits are likely to encourage several verticals such as travel and transport, healthcare, financial services, universities, and utilities to step up the installation and upgradation of hand geometry identification solutions in the future.

Despite the Hype, Microchip Implants Won't Deliver Security, Martin Reynolds, July 1, 2004

On 16 July 2004, media reports stated that more than 100 employees of the Mexican attorney general's office have received surgical implants containing tracking microchips that control access to secure physical locations. The reports follow an interview in which the attorney general stated that he has had a microchip implanted in his arm to allow access to a crime database and to make it possible for law enforcement authorities to locate him if he is kidnapped.

Analysis

A microchip surgically implanted in the human body could be used to maintain access control for secure locations. The microchip transmits radio frequency identification (RFID) signals to a reader, and the user opens doors and accesses computer systems simply by placing the body part containing the implant close to the reader. The implants cannot be lost or forgotten, and the devices are difficult to remove and almost impossible to counterfeit.

However, the media reports that the Mexican implants could help locate kidnap victims are almost certainly overblown. The devices' deliberately short range makes them nearly useless for this purpose. The media reports may stem from a clever "disinformation" campaign to discourage kidnapping, which is widespread in Mexico. Gartner believes it is

unwise to rely on these devices as a kidnap victim locator — and particularly unwise to announce which body part contains the implant.

Implanted devices are highly unsuitable for virtually all security purposes. Only the body part containing the implant — not the entire employee — is required for access permission, so this approach will not work against people willing to commit bodily harm.

Gartner believes contactless smart cards represent a better means of physical access control than microchip implants. These devices have already been deployed in Japan and Hong Kong as a substitute for cash, allowing users to purchase goods and services such as public transit subway fares. Unlike many other technologies, contactless smart cards cannot be counterfeited, and they are appropriate as a replacement for existing access control systems. They could substitute for the implant devices, and the Mexican government may well shift to nonimplanted technology.

Recommendations: Do not implement surgically implanted microchips as a security mechanism. When preparing for new access control systems, consider contactless smart cards instead.

Analytical Source: Martin Reynolds, Gartner Research

Parece una historia sacada de las películas de ficción. El protagonista escapa de sus enemigos y tiene que entrar en un lugar con extremas medidas de seguridad. Con solo poner su mano sobre un lector especial, todas las puertas se abren a su paso. El lector ha reconocido que el personaje tiene autorización para entrar. Por inverosímil que parezca, esta realidad está más cerca de lo que se cree. Y en el país, más pronto de lo que se piensa, estos sistemas revolucionarán la manera en que operan los sectores financiero, de salud, de seguros y telecomunicaciones, entre otros.

Con la vulnerabilidad a la que se han expuesto los sistemas de seguridad del mundo entero luego del 11 de septiembre, la manera de garantizar la seguridad en todas las organizaciones se ha redefinido. Lo anterior ha obligado a las empresas a buscar nuevos instrumentos que permitan mitigar las posibilidades de ataques, fraudes y acceso a información privada. "El mercado de tecnología para la seguridad estaba prácticamente dormido hasta el 11 de septiembre. Los países se sintieron vulnerables y la seguridad pasó a ser la prioridad número uno. Con esto en mente y con la caída de sus costos de implementación, se empezó a hablar de la biometría", afirma Guillermo Gómez, presidente de eCorporation Global, empresa de consultoría en tecnología que presta el servicio de tecnología biométrica de huella digital.

De la tinta al scanner

La biometría permite el análisis estadístico de las características biológicas de los individuos. Ya hay

varias tecnologías con aplicaciones biométricas que permiten la identificación de los individuos por medio del reconocimiento facial o de la huella digital, el iris, la voz y la geometría de la mano, entre otros. De todas ellas, la tecnología de huella digital es la que más acogida ha tenido en el mercado pues el reconocimiento por este método ha sido utilizado de tiempo atrás. El público está acostumbrado a considerar la huella digital como su marca única e intransferible, por lo cual el único cambio que representa la utilización de estos sistemas es el hecho de que en vez de tener que poner los dedos sobre una almohadilla entintada, debe posarlos sobre un scanner.

En el mundo, la participación de la tecnología de huella digital en el mercado de instrumentos biométricos es de cerca del 50%, según eCorporation Global. Solo en Estados Unidos, por ejemplo, de acuerdo con Meridien Research Inc., durante el 2001, las compañías gastaron más de US\$127 millones en instrumentos biométricos, de los cuales más del 44% correspondieron a herramientas de tecnología de huella digital. Y para el futuro se espera que el mercado siga creciendo de manera vertiginosa. Según la firma IDC, para el 2004, el sector financiero invertirá cerca de US\$1.800 millones anuales en tecnología biométrica.

Los costos de estos sistemas también han experimentado un cambio significativo que ha beneficiado su demanda. Mientras hace 2 años un dispositivo de huella digital podía costar cerca de US\$4.000, hoy se consigue por US\$200. Así, estos instrumentos se han vuelto más accesibles a todas las organizaciones. Las aplicaciones de estos sistemas, además, son numerosas. Para las empresas de cualquier sector, la tecnología de huella digital les permite mantener un control de acceso de la más alta calidad. MasterCard, por ejemplo, está usando estos sistemas desde 1995 y ya tiene un récord de más de 38.000 empleados. En Estados Unidos, entre tanto, en más de 42 aeropuertos se usa esta tecnología, para chequear la entrada de sus empleados a zonas restringidas. Para las entidades financieras, por ejemplo, esta tecnología tiene un enorme potencial pues les permite verificar la identidad del usuario en segundos, sin necesidad de códigos y contraseñas. Así, la agilidad en las transacciones mejora considerablemente y evita tantos papeles y verificaciones. En el mundo, entidades como Citibank, que ya viene utilizando la tecnología de huella digital para el control de acceso de sus empleados, están evaluando la posibilidad de introducirla para la

verificación de los clientes. En Colombia, Bancafé está próximo a introducir esta tecnología para sus clientes.

"Actualmente, la solución está siendo implementada en varias entidades bancarias de América Latina, y Colombia no se ha quedado atrás... Dentro de poco, los clientes de varias entidades financieras del país, al retirar su dinero en las cajas, en cajeros automáticos o al acceder al sistema de banca por internet, solo necesitarán poner un dedo en un dispositivo biométrico", afirma Guillermo Gómez. Para él, al finalizar el año ya se habrán concretado negocios con cinco organizaciones de gran tamaño en el país que quieren utilizar tecnología de huella digital.

Para los sistemas de votación, además, esta tecnología puede resultar bastante exitosa pues se evitaría la manipulación, el fraude y la suplantación que se cometen en los procesos electorales.

La tecnología de huella digital aún tiene mucho potencial, pues sus aplicaciones son numerosas. El mundo ya está reconociendo que un sistema que garantice una mayor seguridad le puede evitar bastantes dolores de cabeza. Pronto llegará el día en que recordar una clave sea cosa del pasado

La Seguridad Digital en la Huella Dactilar

Madrid, julio 24 , 2001

Madrid, 24 de abril de 2001 – ipsCA, <http://www.ipsca.com/>, ha anunciado la firma inmediata de un acuerdo de colaboración con Midia Lab, empresa dedicada al desarrollo, soporte y consultoría de software, así como al outsourcing de personal técnico especializado. En virtud de este acuerdo, ipsCA distribuirá la tecnología de verificación de identidades de Midia Lab, que autoriza el acceso a los equipos tras contrastar e identificar la huella dactilar del usuario como complemento a su propia tecnología de seguridad para el comercio electrónico y para estimular dicho mercado en nuestro país.

Según PriceWaterhouse Coopers, el fraude en los servicios financieros vía Internet ha alcanzado en lo que va de año la cifra de 1.500 millones de dólares. La consultora señala que la principal causa que frena la popularización de los servicios bancarios online es la inseguridad con que clientes y empresas perciben la ejecución de las operaciones electrónicas. Por esta razón, los dispositivos biométricos están considerados como los sistemas de seguridad más fiables que hay en la actualidad.

A partir de ahora, **ipsCA** ofrecerá el dispositivo **Finger Logon** de **Midia Lab** junto con sus certificados digitales para aplicarse principalmente en el ámbito del comercio electrónico B2B y B2C. Por su parte, **Midia Lab** se beneficiará de la

actual cartera de clientes de **ipsCA**, así como de su prestigio como empresa pionera en seguridad tanto fuera como dentro de nuestro país, ampliando así el mercado de su tecnología biométrica.

Basado en tecnología alemana de reciente creación, **Finger Logon** incorpora conexión para puerto paralelo, de serie y USB, lo cual permite una fácil, cómoda y rápida instalación. Al ser compatible con Windows 95/98/2000/NT 4.0, puede utilizarse en cualquier ordenador portátil o desktop y red de trabajo, permitiendo a su vez un elevado retorno de las inversiones tecnológicas. Este dispositivo no sólo reduce el tiempo y los pasos necesarios para que empresas o particulares se conecten a cualquier servicio online, sino que aumenta la seguridad de las transacciones, simplifica los protocolos de identificación e incrementa el valor añadido de los propios servicios Internet.

En palabras de Rodolfo Lomascolo, director general de ipsCA, “la incorporación de la tecnología biométrica de Midia Lab a nuestra oferta de soluciones integrales de seguridad informática refleja nuestro interés por dotar al mercado español del e-commerce con los mecanismos de verificación de identidades más innovadores y avanzados. Este acuerdo permitirá a ambas compañías convertirnos en parte instrumental del desarrollo de los servicios online en España.”