APLICACIÓN DE SISTEMAS BIOMÉTRICOS EN LA ADMINISTRACIÓN PÚBLICA LOCAL PARA PROTECCIÓN DE LA INFORMACIÓN

Graciela Etchart[1], Carlos Alvez[1], Marcelo Benedetto[1], Miguel Fernández[2]
[1]Facultad de Ciencias de la Administración - Universidad Nacional de Entre Ríos
Av. Tavella 1424, Concordia, Entre Ríos - CP 3200
getchart@fcad.uner.edu.ar, caralv@fcad.uner.edu.ar, marben@fcad.uner.edu.ar
[2] Municipalidad de Concordia – provincia de Entre Ríos
Mitre 76 - Concordia, Entre Ríos (3200) - migfer@concordia.gov.ar

Resumen

Los entes estatales tienen la necesidad de proteger tanto bienes materiales como información de diverso tipo, ya sea en formato digital o de otra índole. Por esto es menester, contar con un alto nivel de seguridad a través de mecanismos eficientes y eficaces de control de acceso a las zonas restringidas donde se encuentran los bienes a proteger.

En el proyecto se trabajó el caso de la Municipalidad de Concordia, y en particular los sectores destinado al funcionamiento de la Dirección de Informática y al área de Tesorería ya que debido a los riesgos a los que está expuesto el sistema informático de estas áreas, ha sido considerado como prioritario por parte de la Gestión Política.

En lo que a acceso a ambos sectores se refiere, se realizará un análisis comparativo entre dos tecnologías de control de acceso biométrico para la identificación de las personas que accedan al sector de servidores y a Tesorería.

Palabras clave: Seguridad, Sistemas Biométricos, Administración Pública Local, Identificación de Personas.

Contexto

Este trabajo está encuadrado en el acta acuerdo entre la Municipalidad de Concordia y la Facultad de Ciencias de la Administración de la UNER, suscripto en el marco del proyecto de investigación PID UNER 7035 "Identificación de personas mediante sistemas biométricos. Estudio de factibilidad y su implementación en organismos estatales".

La Dirección de Informática, a través de su personal, se encargará de la adecuación del ambiente físico y del hardware y el personal de la UNER, del análisis de diferentes tecnologías de control de acceso a utilizar. Entre las acciones del personal municipal, se encarga de tareas como instalación de equipos y medidas de seguridad ambientales (control de incendios, control de temperatura, etc.).

El personal de la UNER realizará un análisis comparativo entre dos tecnologías de control de acceso biométrico para la identificación de las personas, un relevamiento y un diagnóstico de las dificultades de seguridad que se presentan en el personal que accede al sector de servidores. Uno de ellos es un sistema de reconocimiento biométrico basado en la geometría de la mano y, la otra alternativa es un sistema de autenticación basado en dos modalidades biométricas: huella y rostro.

Introducción

La importancia de utilizar tecnologías biométricas radica en el hecho de que los mecanismos tradicionales como las claves de acceso y tarjetas magnéticas son muy falibles. Por ejemplo, las tarjetas magnéticas se pueden extraviar o sustraer, las claves se pueden olvidar (o ser observadas por alguien más), etc. Por esto, es importante emplear sistemas de reconocimiento biométricos para identificar a las personas y de esta manera reforzar la seguridad de la institución.

Líneas de Investigación y Desarrollo

El proyecto desarrolló un estudio comparativo de los sistemas biométricos. El mismo, fue realizado tomando como base a un dispositivo mono-biométrico (geometría de la palma de la mano) contra un dispositivo multi-biométrico adquirido en el segundo año de ejecución del proyecto (de Rostro y Huella Dactilar).

Para la elección de los rasgos a utilizar, se tuvieron en cuenta principalmente las características de Fiabilidad, Resistencia a ataques, Aceptabilidad y Costo.

Objetivos y resultados

- Efectuar un estudio comparativo de los sistemas biométricos. El mismo, fue realizado tomando como base a un dispositivo mono-biométrico (geometría de la palma de la mano) contra un dispositivo multi-biométrico (de Rostro y Huella Dactilar).
- Adecuar las instalaciones con las dimensiones y características necesarias para instalar los servidores y los distintos dispositivos de seguridad que posibiliten brindar un marco de resguardo y protección de la información.
- Implementar un sistema confiable de control de acceso de personas a la oficina de servidores y al área de Tesorería, que permita la identificación y el registro de los accesos.

Del análisis realizado entre las distintas alternativas, desde el punto de vista técnico y financiero, se consideraron apropiados y se adquirieron los siguientes dispositivos:

- HANDPUNCH 1000: Lector de geometría de la mano, con capacidad para el registro de 512 usuarios y 5120 transacciones en memoria. Permite el reconocimiento 1 a 1 (verificación).
- ZKSOFTWARE IFACE 202: Equipo de reconocimiento de huella dactilar y facial, con capacidad de 700 rostros, 3000 huellas dactilares y hasta 100.000 fichajes de capacidad autónoma. Permite el reconocimiento 1 a 1 (verificación), como 1 a n (identificación). También permite el uso de tarjeta de proximidad.

Este equipamiento fue instalado en las dependencias de Tesorería y la Dirección de Informática, áreas estas que por su función ya fueron previamente definidas como estratégicas en el proyecto en lo que a Identificación de personas se refiere.

Ambos dispositivos fueron sometidos a pruebas de acceso durante un mes por el personal involucrado en dichas oficinas y, en base a las características analizadas, se pudieron establecer los siguientes resultados comparativos:

Sistema Biométrico Característica	Geometría de la mano (mono-biométrico)	Huellas y (multi-biométrico)
Fiabilidad	Alta	Muy alta
Resistencia a ataques	Alta	Muy alta
Aceptabilidad	Alta	Muy alta
Costo	Alto	Medio

Por lo expuesto, en el caso estudiado, con los dispositivos involucrados y con las pruebas realizadas, se concluye que el sistema multi-biométrico presenta actualmente mayores beneficios para su implementación.

La razón de ello, radica en que al incorporar dos sistemas de identificación en un mismo dispositivo, los parámetros de medición mejoran notablemente el rendimiento y la exactitud de la comparación.

Cabe destacar además y de acuerdo a los relevamientos efectuados durante el desarrollo del proyecto, que los dispositivos de geometría de la mano en un futuro podrían perder en la industria, el mercado que actualmente poseen. Las razones, radican fundamentalmente en que los mismos tienen un costo alto, una permanencia media del rasgo de lectura y que los factores ambientales lo afectan en forma negativa respecto a otros dispositivos.

Entrevistas realizadas

A los efectos de relevar datos significativos sobre la visión del personal vinculados con los temas de seguridad, y los riesgos a los que se encuentran expuestos a situaciones que pudieran comprometer el normal funcionamiento de sus tareas; se conceptuó importante abarcar dos sectores considerados claves para los objetivos del proyecto: el área de informática y el sector de tesorería.

Para dicho relevamiento se confeccionó un formulario de entrevista, con 10 ítems que incluyeron temáticas tales como gestión de la información, protección de los datos, normas de seguridad, y cuestiones relacionadas con los sistemas y dispositivos existentes para la identificación de las personas con acceso a dichos sectores.

Fueron entrevistadas doce (12) personas del área informática (90% de la planta total) y seis (6) personas del sector tesorería (75% del total).

Se detalla a continuación los resultados de las entrevistas, producto de la compilación efectuada, resaltando en cada caso los aspectos más importantes de las opiniones vertidas por los encuestados.

Resultados de las entrevistas.

¿En qué soporte se encuentra la información que maneja su área (digital, papel, etc.)?.

En la oficina de Informática se manifestó que el 80% de los datos se encuentran soportados en dispositivos digitales y el resto consiste en documentación impresa, particularmente aquella que respalda tareas sensibles y que requiere de autorizaciones de niveles superiores.

En la oficina de Tesorería los encuestados manifestaron que en promedio el 50% de la información es provista mediante acceso a terminales de computación (medio digital), pero que el 50% restante conforman un archivo donde se almacenan los comprobantes de respaldo necesarios para el funcionamiento de dicha oficina.

¿ Conoce los procedimientos o normas de seguridad que posee el organismo?

En el sector informático solamente una persona manifestó desconocer normas de seguridad, por lo que el 92% manifestaron estar informados sobre algunas normativas y/o procedimiento en este sentido. Seis encuestados, de los once en total, expresaron que las normas no son suficientemente completas y que no se encuentras debidamente sistematizadas, ya que han sido emitidas por diferentes niveles jerárquicos y aparecen un tanto desarticuladas.

En el sector Tesorería el 100% de los encuestados expresaron conocer procedimientos y/o normas de seguridad, aunque con distintos grados de opinión sobre si las mismas eran suficientes. Es interesante destacar como dato complementario, que la mitad de los encuestados (50%) opinan que las normativas no contemplan en forma integral los aspectos de seguridad.

¿Existe un manual de procedimiento para la seguridad de la organización?. ¿Se encuentra disponible y es de fácil acceso?.

La totalidad de los encuestados del área informática manifiesta que no existe un manual específico que sistematice las diferentes normas de seguridad del sector. Remiten su opinión a la pregunta anterior.

En el sector Tesorería todas las personas coincidieron en expresar que no existe un manual. Las normativas se encuentran en carpetas de "Resoluciones" firmadas por Directores y Secretarios. Solamente una persona manifestó no conocer el lugar de archivo mientras que las cinco restante expresaron su conocimiento y facilidad de acceso.

¿Qué perjuicio ocasionaría una eventual pérdida de equipamiento o información?.

En el sector de Informática todos los encuestados manifestaron diversos tipos de acontecimientos que podría originar la pérdida de los equipos instalados y particularmente de la información contenida en ellos. Existe suficiente conciencia sobre la magnitud de los riesgos considerando que, por ejemplo, en los servidores se encuentra soportada toda la información del municipio. El 83% expresó que si bien existen sistemas de respaldo de todos los datos, la caída de los sistemas puede originar en algunos casos la paralización de las actividades de todo el municipio por un tiempo variable en función de las características del hecho.

En el sector Tesorería, las seis personas encuestadas expresaron que la pérdida de equipamiento informático retrasaría las tareas por el tiempo que demanda su reemplazo. En idéntica magnitud respondieron que la pérdida de la documentación soportada en papel, podría originar inconvenientes al momento de ser necesario respaldar fehacientemente algún acto administrativo.

¿Existe algún control para las personas que acceden al lugar físico de trabajo?.

En el caso del Sector de informático hubo coincidencia en las respuestas a esta pregunta separando dos sectores:

Sala de servidores. Posee una sola puerta de acceso con una cerradura común como única medida de de protección, que permanece cerrada y solo se la habilita para las tareas de mantenimiento. La llave de la puerta está en poder de los responsables del sector quienes controlan el ingreso de las personas.

Sala de Desarrollo y Operaciones. Posee dos puertas con cerraduras comunes que permanecen abiertas solamente durante el horario de trabajo (de 07:00 a 13:00 hs.). Todos los encuestados manifestaron que no existe ningún tipo de control dentro de dicho horario.

En el sector tesorería existe una puerta única de acceso de madera con vidrio esmerilado. Los

seis encuestados manifestaron conocer el sistema de control con sistema de apertura eléctrica que es accionado desde el interior de la oficina, ante la solicitud de ingreso de una persona. No existe normativa alguna para autorizar los ingresos, ya que el mismo personal de tesorería acciona la cerradura y permite el ingreso de personas que son de su conocimiento personal.

¿Existe alguna medida de seguridad para acceder a la información?.

En la oficina de informática, el 100% de las personas responden afirmativamente para el caso de la información digitalizada. Existen medidas que exigen la identificación del usuario para acceder a cualquier dato informatizado, como así también las claves de identificación. Respecto de la información soportada en papel, ocho casos de los encuestados expresan que la documentación archivada en carpetas y biblioratos comunes se ubican físicamente en armarios comunes, sin cerraduras, a los que cualquier persona.

En el sector tesorería todos los encuestados señalaron que para acceder a la información "grabada en la computadora" debían previamente acceder con una clave que solamente era conocida para cada una de las personas. Tres personas (el 50%) manifestó que resultaba "tedioso" la exigencia de cambiar las claves en forma periódica, tal como se les exige. Para el caso de la documentación guardada en archivos, alguna información se encuentra bajo llave, pero mucha otra no tiene medidas de control de acceso (dentro del personal afectado al sector).

Conoce que son los métodos biométricos para identificación de personas?.

En el sector informático todos los encuestados expresaron conocer algún tipo de metodología biométrica para la identificación de personas.

Por su parte, en el sector tesorería, el 100% expresó que conocía el sistema que tiene instalado el municipio para el control de ingreso y egreso del personal (huella dactilar).

¿ Cuáles conoce ?:

En esta pregunta se detallaban algunos sistemas y los encuestados debían marcar los que conocían. Se resume las respuestas de cada sector:

Sector informático: todos los encuestados manifestaron conocer los sistemas consignados. En el ítem "Otros" un 50% detalló sistemas multi-biométricos.

En el sector tesorería manifestaron conocer: Huella dactilar: 6 personas (100%); Voz: 1 persona (17%); Palma: 2 personas (33%); Iris: 1 persona (17%).

¿Cree que un sistema de identificación de las personas basado en biometría contribuiría a dar seguridad a su área?.

A esta pregunta, en ambas oficinas respondieron afirmativamente la totalidad de los encuestados.

A su criterio, qué cualidades o características debería tener un sistema de identificación de personas?

En esta pregunta se detallaban algunas características y los encuestados debían marcar las que les parecían pertinentes. Se resume las respuestas de cada sector:

Sector informático: Universalidad: 10 personas (83%); Fiabilidad: 12 personas (100%); Facilidad de administración: 8 personas (67%); permanencia de rasgos: 8 personas (67%).

En el sector tesorería: Facilidad de operación: 6 personas (100%), Comodidad: 4 personas (67%).

En base observaciones realizadas en las instalaciones, relevamiento efectuado a través de entrevistas a informantes claves y al personal de Tesorería y Dirección de Informática del Municipio de Concordia respecto a la identificación de personas que acceden a su oficinas, se detectó la siguiente problemática:

- Carencia e los niveles de protección de los equipamientos informáticos afectados a la Dirección de Informática del Municipio. El equipamiento actualmente no cuenta con un ambiente físico adecuado como tampoco con mecanismos de acceso seguros. Adecuación del ambiente físico y del hardware como ser la instalación de equipos y medidas de seguridad ambientales (control de incendios, control de temperatura, etc.) y el análisis de diferentes tecnologías de control de acceso a utilizar.
- Desconocimiento y falta de normas referidas al acceso e identificación de personas a dependencias claves en la administración pública local por parte de sus agentes.

- Falta de inversión en tecnología de control de acceso biométrico para la identificación de las personas que accedan a los sectores antes mencionados. La importancia de utilizar tecnologías biométricas radica en el hecho de que los mecanismos tradicionales como las claves de acceso y tarjetas magnéticas son muy falibles. Por ejemplo, las tarjetas magnéticas se pueden extraviar o sustraer, las claves se pueden olvidar (o ser observadas por alguien más), etc. Por esto, es importante emplear sistemas de reconocimiento biométricos para identificar a las personas para reforzar la seguridad.

Formación de Recursos Humanos

Se brindó a los integrantes del proyecto, formación en lo que se refiere a sistemas de identificación de personas basados en la biometría.

Los integrantes del proyecto, se desempeñan en cátedras relacionadas directamente o indirectamente con el tema central de la investigación, por lo que este trabajo tendrá impacto directo e inmediato en la docencia.

Se procederá a dirigir becarios de investigación, así como también tesinas finales de grado, dirigidos por el director del proyecto de investigación y/o por los docentes-investigadores del mismo. Para estos casos, también se prevé la presentación a convocatorias de becas ante organismos provinciales y nacionales.

Los integrantes participarán de reuniones científicas y técnicas que permitan actualizar los conocimientos en el tema de interés. También se trabajará en la presentación de trabajos en congresos nacionales e internacionales relacionados con el área del proyecto. Estos trabajos servirán para divulgar los conocimientos obtenidos durante el trabajo de investigación.

Uno de los principales objetivos del proyecto es que el personal docente de la UNER dedicado al mismo avance y/o concluya con sus estudios de posgrado, así como también se incorporen becarios realizando investigaciones en temas afines a la temática del proyecto.

Referencias

1. Wing B. ANSI/NIST-ITL 1-2011. Information Technology: American National Standard for Information Systems Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. November, 2011.
2. Carlos E. Alvez, Marcelo G. Benedetto. “Los Sistemas Biométricos y su Factibilidad de Aplicación en los Organismos Estatales”. XII Workshop de Investigadores en Ciencias de la Computación (WICC 2010), El Calafate, Santa Cruz Argentina, 5 y 6 de Mayo de 2010, Universidad Nacional de la Patagonia San Juan Bosco. Páginas 247-251.
3. Graciela Etchart, Lucas Luna, Carlos Leal, Marcelo Benedetto, Carlos Alvez. Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales. CGIV - XIII Workshop de Investigadores en Ciencias de la Computación (WICC 2011), 5 y 6 de Mayo de 2011. Universidad Nacional de Rosario. Rosario – Argentina. Páginas 339-343.
4. Graciela Etchart, Lucas Luna, Rafael Leal, Marcelo Benedetto, Carlos Alvez. “Sistema adecuado a estándares de reconocimiento de personas mediante el iris”. CGIV - XIV Workshop de Investigadores en Ciencias de la Computación (WICC 2012), 25 y 26 de Abril de 2012. Universidad Nacional de Misiones. Posadas – Argentina. Páginas 321-325.
5. Alvez Carlos E. Modelos para la recuperación de imágenes por similitud en Bases de Datos Objeto-Relacionales. Tesis Doctoral. Santa Fe, Argentina, Abril de 2012. ISBN 978-987-33-2249-5.
6. Casal Gabriel, Rovolta Mercedes. Biometrías. Herramientas para la Identidad y la Seguridad Pública. Jefatura de Gabinete de Ministros. Presidencia de la Nación. Noviembre de 2010.
7. Julio Fuoco, Tendencias Biométricas, desafíos y oportunidades. En Biometrías 2. Jefatura de Gabinete de Ministros. Presidencia de la Nación. Octubre de 2011.
8. Alvez C., Benedetto M., Berón G., Etchart G., Luna L. y Leal C. Desarrollo de un sistema multi-biométrico mediante reconocimiento de iris y voz, adecuado a estándares, para su aplicación en organismos públicos. SIE 2011 – Simposio de Informática en el Estado. Córdoba, 31 de Agosto, 01 y 02 de Septiembre de 2011. 40° JAIIO. Páginas: 206 - 220.