Sistema de Seguridad Biométrico para Protección de la Información en Administración Pública Local

[1,2] FERNANDEZ, Miguel Antonio, [1] LOGGIO, Sebastián René, [1,2] BERÓN Gustavo, [1] ETCHART Graciela Raquel, [1]BENEDETTO Marcelo Gabriel, [1]ALVEZ Carlos Eduardo,

[1] Facultad de Ciencias de la Administración - Universidad Nacional de Entre Ríos

Monseñor Tavella 1424 – Concordia, Entre Ríos (3200)

[2] Municipalidad de Concordia – provincia de Entre Ríos

Mitre 76 - Concordia, Entre Ríos (3200)

{migfer, seblog, gusber, getchart, marben, caralv}@fcad.uner.edu.ar

Resumen: Los controles de accesos a los diferentes sectores, en los que se utilizan bienes susceptibles de ser atacados en su integridad, son considerados de vital importancia en la Administración Pública. Sin embargo, algunas áreas no cuentan con mecanismos de control adecuados, principalmente en lo que refiere a condiciones de accesibilidad. Este trabajo aborda el caso del sector destinado al funcionamiento de los servidores de la Dirección de Informática de la Municipalidad de Concordia, en donde actualmente, se presentan falencias de infraestructura, como así también, en el control de acceso a dicha sala. Esta situación, por los riesgos que implica, ha sido considerada como prioritaria por parte de la Gestión Política y ha motivado el desarrollo del presente proyecto. El mismo, contempla la adecuación del ambiente físico y del hardware (instalación de equipos y medidas de seguridad ambientales) y el análisis de diferentes tecnologías para implementar el control de acceso. Para esto último, se realizará un análisis comparativo de diferentes alternativas de tecnologías biométricas, debido a que en la actualidad representan los mecanismos más confiables para la autenticación. En dicho análisis, se tendrán en cuenta características tales como fiabilidad, resistencia a ataques, aceptabilidad y costo.

Palabras Clave: Seguridad, Sistemas biométricos, Restricciones de acceso.

1. Introducción

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.

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 07/G035 "*Identificación de personas mediante sistemas biométricos. Estudio de factibilidad y su implementación en organismos estatales*". Entre las tareas previstas en el convenio, se ha procedido a efectuar un relevamiento preliminar de las instalaciones y las

medidas de seguridad (en cuanto a accesibilidad se refiere), que se encuentran en estado operativo en todo el edificio donde se desarrolla la actividad municipal.

Como resultado del estudio realizado, se han manifestado en forma evidente algunas insuficiencias, de las cuales se ha tomado como una de las más significativas, a la relacionada con los niveles de protección de los equipamientos computacionales 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, como se amplía en el punto 2.

Por lo antes expuesto, y ante la decisión política de la gestión para resolver este problema, se han proyectado acciones que involucran tanto tareas de infraestructura como el análisis de mecanismos de control de acceso físico. Cabe destacar, que el Municipio ha destinado espacio físico con características adecuadas que permiten la protección de los equipos.

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 a implementar para el control de acceso.

Entre las acciones del personal municipal, se encuentran tareas como la instalación de equipos y medidas de seguridad ambientales entre las que se tienen: provisión de energía eléctrica de alta disponibilidad, condiciones medioambientales controladas para la optima operación de los equipos instalados (la instalación de equipos contra incendios se efectuará en función de los estipulado en el decreto 351/79 reglamentario de la Ley 19.587 de Higiene y Seguridad en el trabajo.

El personal de la UNER realizará un análisis comparativo entre dos tecnologías de control de acceso biométrico para la identificación de las personas que accedan 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 (sistema multi-biométrico): huella y rostro.

La importancia de la utilización de tecnologías biométricas radica en el hecho de que los mecanismos tradicionales, como las claves de acceso y tarjetas magnéticas, son altamente susceptibles a fallos. Por ejemplo, las tarjetas magnéticas se pueden extraviar o sustraer, las claves se pueden olvidar, ser observadas por alguien más, etc. Por esto, es importante emplear sistemas de reconocimiento biométricos o multibiométricos que permitan identificar a las personas y propender al refuerzo de la seguridad.

2. Situación-Problema u Oportunidad

La Municipalidad de Concordia desarrolla sus actividades en un edificio con más de 150 años desde su fecha de inauguración, y actualmente, tanto su capacidad en espacios físicos como la distribución funcional no cubren integralmente las necesidades para el adecuado funcionamiento de todas sus dependencias. Además, dichas instalaciones, no reúnen todos los requisitos necesarios tanto en lo relativo a capacidad, como a condiciones de accesibilidad.

En el caso puntual del sector destinado al funcionamiento de la Dirección de Informática, se ha generado una situación que, por los riesgos a los que está expuesto el sistema informático, ha sido considerado como prioritario por parte de la Gestión Política. Por este motivo, a la fecha se están realizando las tareas de infraestructura y servicios anexos, con el fin de dar solución a los problemas suscitados y que se detallan en párrafos posteriores.

Dentro de la consideración de mayor importancia de las diferentes necesidades de la Dirección, se ha priorizado la solución de la ubicación y condiciones de seguridad del equipamiento informático destinado a soportar las bases de datos de los sistemas de información del Municipio.

En la actualidad, los servidores en los cuales se almacenan estos datos y los sistemas aplicativos de los distintos sectores de la Municipalidad, se encuentran ubicados físicamente en la misma oficina de la Dirección del Departamento. Esto configura una situación sumamente delicada ya que los sistemas –especialmente los componentes de hardware– se encuentran expuestos a diferentes riesgos; tales como:

a) **Accesibilidad.** La oficina es el lugar de acceso a todo el sector, por lo que existe un flujo permanente de personas, tanto de aquellas que pertenecen al sector como las ajenas al mismo.

   Esto atenta contra uno de los principios elementales de seguridad, que establece la necesidad de no permitir el acceso de ninguna persona que no sea el responsable directo. El responsable deberá ser quien autorice el ingreso al sector restringido ante cualquier necesidad que se presente (reparaciones y mantenimiento por parte del personal técnico, personal de limpieza, etc.).

b) **Permanencia de personas**. En la misma oficina se encuentran trabajando habitualmente el Director del sector y una Secretaria. Por lo expuesto en el párrafo anterior, esto no es conveniente, ya que por regla general, los servidores deben ubicarse en un lugar en el que no se permita su acceso a excepción de tareas de mantenimiento correspondientes.

c) **Condiciones ambientales**. Al estar en un lugar abierto y con presencia permanente de personas, el equipamiento se encuentra expuesto a condiciones ambientales desfavorables, tales como polvo, temperatura, humedad, entre otras. Debe asegurarse que estas variables estén suficientemente controladas, puesto que son factores que pueden generar un funcionamiento incorrecto.

3. Solución propuesta

Dada la situación planteada en el punto anterior y, en miras de mejorar los servicios de la Dirección de Informática en todo el marco dentro del cual canaliza su actividad, la Secretaría de Hacienda del Municipio, con la aprobación de los organismos competentes, ha autorizado el desarrollo de las siguientes acciones:

a) Disponer de una oficina con las dimensiones necesarias para instalar los servidores y los distintos dispositivos de seguridad que posibiliten brindar un marco de resguardo y protección adecuada de la información.

b) Implementar un sistema confiable de control de acceso de personas a la oficina de servidores, que en lo posible permita la identificación y el registro de los accesos.

El espacio físico que se ha destinado se considera apropiado, reuniendo las características requeridas para su destino. Teniendo particularmente en cuenta el punto b), dicha oficina cuenta con una sola puerta de acceso, lo que facilita la instalación de un sistema de control de ingreso.

Como ya se introdujo en el punto uno, aquí se propusieron dos soluciones biométricas. Para la elección de los rasgos a utilizar, se tuvieron en cuenta las siguientes características (*Till E., 2010*):

- **Universalidad**. Debe estar presente en todo individuo.
- **Distinción**. Debe ser único para cada individuo y distinto en la comparación con otra persona.
- **Permanencia**. Debe ser suficientemente invariable a lo largo del tiempo.
- **Registración**. La característica biométrica debe poder ser medida, cuantificada y registrada.

Otra cuestión importante que se tendrá en cuenta, además de las características antes citadas, es que los dispositivos utilizados cuenten con proveedores y soporte técnico dentro de la provincia de Entre Ríos.

Dentro de las distintas alternativas de solución mencionadas en el punto 1, existen en el mercado los siguientes dispositivos:

a) Equipo lector de geometría de la mano, con capacidad para el registro de 512 usuarios y más de 5000 transacciones en memoria. Este equipo cuenta con la posibilidad de ser parametrizado en forma remota admitiendo conexiones en red. El software permite efectuar comunicación entre equipos, enrolar usuarios y acceder a los datos de los mismos.

b) Equipo de reconocimiento de huellas y rostro, con capacidad de 700 rostros, 3000 huellas dactilares y hasta 100.000 fichajes de capacidad autónoma.

Entre los aspectos más importantes a analizar en estos equipos, se consideran:

a) **Fiabilidad**: Se la suele denominar también como rendimiento (performance) o nivel de exactitud. Referido al comportamiento de un sistema o dispositivo, se define como la "probabilidad de que el dispositivo desarrolle una determinada función, bajo ciertas condiciones y durante un período de tiempo determinado". Esta característica, hace referencia a la precisión del reconocimiento, los recursos requeridos y el entorno operativo. Los indicadores habitualmente utilizados para medir esta característica son: la tasa de falsas aceptaciones (FAR, de su sigla en inglés) que es la probabilidad de que un sistema biométrico identifique incorrectamente un individuo o falle a la hora de rechazar a un impostor, y la tasa de falsos rechazos (FRR, de su sigla en inglés) que es la probabilidad de que un sistema biométrico falle a la hora de identificar a un individuo autorizado.

b) **Resistencia a ataques.** Se la suele denominar también como resistencia del sistema biométrico a ser burlado. El término se refiere a la preparación y disposición que se hace anticipadamente para evitar un riesgo ante posibles intentos de violación al sistema. Por ejemplo, ante un intento de burla utilizando un dedo sintético caliente para engañar al lector de huellas, se puede evitar a través de un escáner de ultrasonido que, penetrando en cualquier material, permita obtener la huella original del usuario impostor.

c) **Aceptabilidad.** Las pruebas de aprobación o aceptación tienen como fin validar que el sistema cumple con los requisitos básicos de funcionamiento esperado y

permitir que el usuario determine la aceptación del sistema. Por este motivo, estas pruebas son realizadas por el usuario final que, durante este periodo de tiempo, debe plantear todas las deficiencias o errores que encuentre antes de dar por aprobado el sistema definitivamente. Significa el grado de aceptación de las personas en base a su cultura, al hecho de que no perjudique a las personas y que además sea higiénica.

d) **Costo aceptable.** Los componentes del costo en cualquier sistema biométrico incluyen hardware y software asociado para capturar la biometría, investigación y testeo del sistema biométrico, instalación, incluyendo los sueldos del equipo encargado de la implementación, montaje, conexión e integración del sistema de usuarios, capacitación de los mismos, alternativas para usuarios que no pueden registrarse, procesos de excepción a usuarios que no pasan la prueba biométrica, mantenimiento del sistema, administración de bases de datos centralizadas de imágenes/plantillas biométricas y poder de procesamiento del programa de respaldo.

e) **No intrusividad.** Un sistema biométrico es no intrusivo si el individuo no necesita contacto físico con un sensor o no tiene una connotación negativa, es decir, los datos pueden ser adquiridos, incluso, sin que el sujeto se percate de ello. Por el contario, un sistema biométrico es intrusivo si necesita que el individuo toque un sensor, se coloque un sensor cerca de su cuerpo o participe de una manera que no es confortable desde un sentido emocional o psicológico. Por ejemplo, una exploración con un haz láser de la retina es intrusiva, pero una captura de iris o rostro a distancia, no lo es.

Por otro lado, se prestará especial atención a los actores que serán parte de la implementación. Para los empleados estatales, las soluciones tecnológicas basadas en biometría, pueden en algunos casos originar nuevos paradigmas respecto de la invasión a la privacidad de cada individuo/ciudadano. Por esto, la cultura organizacional y social se convierte en uno de los factores de éxito de los proyectos (Fuoco J., 2011).

4. Innovación e Inédito

En la mayoría de los Municipios, los dispositivos biométricos, sólo se utilizan con fines administrativos como ser el seguimiento de entradas y salidas del personal para calcular las horas efectivas de trabajo e informar al Sistema de Liquidaciones y Control Horario.

Aquí se propone utilizar dispositivos más fiables y para el acceso físico a dependencias. Además, estos dispositivos se personalizarán para adecuarse a los procedimientos de seguridad adoptados por el municipio y para poder colectar, no sólo información referente a horarios de acceso de las personas autorizadas, sino también, información estadística sobre el funcionamiento de los dispositivos (falsas aceptaciones o falsos rechazos) que permitan por un lado, calcular indicadores de fiabilidad de los dispositivos, y por otro, detectar intentos de accesos no autorizados (o ataques).

También, se implementará un sistema de alerta que enviará vía SMS y/o correo electrónico, mensajes al responsable directo del área, en caso de intentos fallidos de autenticación.

Por otro lado, aquí se realizará un análisis comparativo multimodal vs monomodal que involucrará los aspectos citados en la sección 3, como fiabilidad, aceptabilidad y resistencia a ataques. Además, teniendo en cuenta que es un ente estatal, en este estudio se tendrá en cuenta la idiosincrasia cultural de la organización, ya que la misma puede suponer un inconveniente para la implementación de determinados sistemas de reconocimiento.

5. Beneficiarios

Como beneficiario primario del presente proyecto, se tiene a la Municipalidad de Concordia. Sin embargo, es intención, aplicar los resultados en diferentes municipios y otras instituciones públicas.

Además, la investigación de los dispositivos biométricos y en particular el estudio comparativo presentado, permitirá ofrecer a diferentes empresas de la región, soluciones de identificación para aquellas áreas críticas de las organizaciones que así lo requieran.

6. Relevancia para el Interés Público

Los órganos de Gobierno de la Municipalidad, han planteado como objetivo prioritario, incrementar la vinculación con la comunidad con el fin de mantener un contacto más fluido, transparentar la gestión y poder así canalizar más eficientemente las inquietudes que surgen y dar pronta respuestas a sus necesidades. En este sentido, la utilización de las herramientas informáticas, deben jugar un rol importante como medio de comunicación.

No hay duda que la demanda social de información crece y que la mencionada transparencia representa cada vez más un compromiso de calidad en la gestión. Los espacios digitales están siendo una gran oportunidad para divulgar información mediante el acceso en línea a los documentos públicos y abriendo espacios de interacción antes impensados o inviables. El valor de la participación depende de la calidad de la información y no hay duda que este es un reto importante para los actores públicos. Además, en la medida que se produce más participación, esta genera más proximidad entre administración y ciudadanos y, a su vez, más confianza en las instituciones. La confianza con las instituciones se gana asegurando que los ciudadanos estén informados implicados e influyentes (Poggi E., 2008).

Así, se encuentran implementados, aplicativos que permiten a los ciudadanos, realizar trámites "*on line*" utilizando para ello, las conexiones web (consulta de expedientes, presentación de Declaraciones Juradas, Guía de Trámites, etc.). No caben dudas que, los servicios brindados a estos usuarios, deben encontrarse operativos en todo momento y responder eficientemente a los requerimientos por los cuales son utilizados.

La importancia del proyecto tiene relación con la mejora directa de la seguridad de la información sensible del Municipio, en lo que refiere al control de accesos de personas al área destinada para albergar los servidores donde se encuentra alojada esta información.

Además, los resultados obtenidos del análisis, así como también, la experiencia de la implementación, permitirán brindar asesoramiento y servicios en sistemas biométricos para la reproducción de esta solución en distintos entes gubernamentales.

7. Viabilidad Política, Técnica y Financiera

La Dirección Política reconoce la importancia de mantener los servicios en línea de manera confiable, como requisito indispensable para el sostenimiento de los aspectos económicos del Municipio. Como toda institución de naturaleza similar, necesita de sus ingresos que provienen de las recaudaciones por distintos conceptos, para el sostenimiento de los servicios prestados. Basta mencionar a modo ilustrativo, que en el año 2011, solamente por Tasa inmobiliaria y de Inspección e Higiene, se recaudaron más de 70 millones de pesos.

Del análisis realizado de las distintas alternativas, desde el punto de vista técnico y financiero, se consideró apropiado la instalación de alguna de las opciones de equipamiento que se detalla:

a) 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), y cuenta con proveedor y servicio técnico en la provincia de Entre Ríos.

b) 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. Cuenta con proveedor y servicio técnico en la provincia de Entre Ríos.

El costo presupuestado del equipamiento incluyendo el costo de instalación es de $ 23.000.- el que se encuentra dentro de los parámetros razonables, existiendo la posibilidad de disponer del crédito presupuestario para su instalación.

El crédito total asignado para cubrir la inversión inicial del proyecto contempla los montos necesarios para:

- el acondicionamiento de la oficina de servidores, y
- la cobertura del costo de adquisición e instalación de los equipos de seguridad.

Dentro del primer ítem se incluye:

a) Cableado eléctrico independiente.

b) Instalación de piso flotante.

c) Acondicionamiento para ambiente de temperatura y humedad.

d) Tableros de corte de energía para emergencia.

e) Protección ignífuga.

Es necesario señalar, que si bien el proyecto señala como uno de sus objetivos la comparación de dos dispositivos de control de acceso, el abordaje de la problemática por parte de la Municipalidad, está centrada en la efectiva instalación del equipamiento necesario para brindar un marco de seguridad en el resguardo de la información y sus procesos.

7.1 Indicadores financieros y retorno de la inversión

Las características intrínsecas del proyecto, cuyo objetivo es brindar condiciones de seguridad para el acceso a un espacio físico, se enmarca dentro del tipo considerado

preventivo. No implica consecuentemente, la generación de recursos monetarios tangibles. Sin perjuicio de ello, es posible enumerar los beneficios que reporta contrastándolo con los posibles inconvenientes que contribuye a evitar. Entre otros podrían mencionarse:

a) Menor frecuencia de caída de servicio del equipamiento que soporta las bases de datos, por encontrarse en un ambiente controlado.

b) Ahorros de costos relacionados con el acceso indebido ya sea a través de daños intencionales como involuntarios.

c) Ahorro de tiempo y costo de horas extras del personal técnico.

d) Optimización de uso de energía.

Considerando la experiencia de los últimos años en relación de los costos insumidos en horas extras destinadas al mantenimiento de los servidores, atención de reclamos de usuarios, e insumos destinados al mismo, es posible estimar algunos indicadores que permiten analizar la conveniencia del proyecto.

En Anexo I, se detalla el flujo de fondos con un horizonte temporal de cinco años, de donde se concluye:

a) Un valor actual neto de $ 2.551.91 positivo lo que da viabilidad financiera al proyecto.

b) Una Tasa Interna de Retorno del 17%.

c) Un período de recupero de la inversión levente superior a los 3 años.

7.2 Indicadores de seguimiento

Entre los indicadores que permitirán monitorear la marcha del proyecto se pueden mencionar:

- Cantidad de horas de caída del servicio.
- Cantidad de horas de trabajo para normalizar los servicios caídos.
- Importe erogado para la compra de componentes destinados a las reparaciones por rotura y/o desperfectos.
- Cantidad de personas ingresadas al sector de servidores.

8. Facilidad de Reproducción

Los resultados y experiencias de este proyecto se volcarán en un documento que permitirá su uso posterior en otras dependencias u otros organismos de la administración pública. Esto facilitará la reproducción de implementaciones similares para la protección de la información u otro bien sensible tanto en otras dependencias de este municipio (por ejemplo el área de Tesorería), así como también en otras entidades.

Este documento, contendrá la información del grado de facilidad tecnológica y financiera relacionada con la implementación de este proyecto.

9. Ambiente de Hardware y Software

Para la implementación de la nueva sala de servidores, se prevé un cambio integral de infraestructura (Ver Anexo II).

La sala contará con acceso a internet mediante dos conexiones ADSL con distintos proveedores de 3 y 5 MB en un mismo servidor para implementación de QoS y balance de carga.

La conectividad, será provista por una red Ethernet con cableado estructurado según normas categorías ISO/IEC 5e (5 mejorada) e ISO/IEC 6. Con algunas dependencias la conectividad será con fibra óptica. Para aquellas oficinas más remotas se utilizará enlace inalámbrico. También se prevé la creación de VPNs (Redes Privadas Virtuales) para lograr eficiencia en la LAN.

Los dispositivos a instalar (HANDPUNCH 1000 o ZKSOFTWARE IFACE 202, según resultado del análisis comparativo) serán conectados a la red por cable según la norma ISO/IEC 6 y almacenarán la información recopilada a una Base de Datos SQL Server. Esta información corresponde a datos de enrolamiento de usuarios, archivos de respaldo y estadísticas de uso (intentos de accesos autorizados y no-autorizados). El software de gestión de los mismos correrá en el sistema operativo Windows 2000 Server. Los dispositivos utilizarán un sistema de alimentación ininterrumpida con tecnología avanzada de PWM con detector de falla y control de sobrecargas y cortocircuitos.

Referencias

[1] Eduardo Till. Biometría y Políticas de Seguridad: de la Ciencia Ficción a la Agenda Pública. En Gabriel Casal, Mercedes Rovolta. Biometrías. Herramientas para la Identidad y la Seguridad Pública. Jefatura de Gabinete de Ministros. Presidencia de la Nación. pp 15-40. Noviembre de 2010.

[2] Julio Fuoco. Tendencias Biométricas, desafíos y oportunidades. En Biometrías 2. Jefatura de Gabinete de Ministros. Presidencia de la Nación. pp. 99-112. Octubre de 2011.

[3] Eduardo Poggi. Experiencias de Innovación. En Interoperabilidad en la Administración Pública. Mariano Greco. Jefatura de Gabinete de de Ministros. Presidencia de la Nación. pp. 219-272. Octubre de 2008.

Anexo I

Implementación de seguridad para gabinete de servidores basado en identificación biométrica.

Flujo de fondos

Horizonte temporal evaluación: 5 años

Ingresos	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Sueldos y horas extras personal mantenimiento		13.500,00	13.500,00	13.500,00	13.500,00	13.500,00
Sueldos y horas extras personal atención reclamos		2.700,00	2.700,00	2.700,00	2.700,00	2.700,00
Disminución roturas y reparaciones		4.200,00	4.200,00	4.200,00	4.200,00	4.200,00
Optimización insumos		2.400,00	2.400,00	2.400,00	2.400,00	2.400,00
Subtotal Ingresos	0,00	22.800,00	22.800,00	22.800,00	22.800,00	22.800,00
Egresos						
Costo de acondicionamiento del espacio físico	30.000,00					
Costo del equipamiento e instalación del sistema de accesibilidad	23.000,00					
Acondicionamiento y mantenimiento sala		1.200,00	1.200,00	1.200,00	1.200,00	1.200,00
Consumo eléctrico adicional (Aire Acondicionado)		528,00	528,00	528,00	528,00	528,00
Subtotal egresos	53.000,00	1.728,00	1.728,00	1.728,00	1.728,00	1.728,00
FF Neto	-53.000,00	21.072,00	21.072,00	21.072,00	21.072,00	21.072,00

Sueldos y horas extras personal mantenimiento	15 horas mensuales a $75 la hora por 12 meses
Sueldos y horas extras personal atención reclamos	3 horas mensuales a $75 la hora por 12 meses
Disminución roturas y reparaciones	350 pesos mensuales
Optimización insumos	200 pesos mensuales

Costo oportunidad	0,15
VAN	$ 15.336,18

Acondicionamiento y mantenimiento sala	1200 pesos anuales
Consumo eléctrico adicional (Aire Acondicionado)	200 kw mes por $0,22 el kw

Anexo II

	Situación Actual	Situación Prevista
Servidores	Base Datos Producción: IBM con 6 años de servicio con SO W2000 Servidor de Dominio: : IBM con 6 años de servicio con SO W2000 Servidor Pruebas Desarrollo: VMware 4.0 y SO W200 y Linux Debian - Genérico con arquitectura servidor. Servidor de Backup: Genérico con arquitectura servidor con SO W2008. Servidor Enlace Internet Punto a Punto: Genérico con arquitectura servidor con SO W2000 Servidor Enlace ADSL: Genérico con SO Linux Debian. Servidor Web de la Municipalidad. Firewall antes y después enlaces: Genéricos con SO W2000.	2 servidores IBM rackeables con Vmware 5 y máquinas virtuales con SO W2008 para: Base Datos Producción Servidor Primario de Dominio Servidor Secundario de Dominio Firewall lógicos en ambos servidores Servidor Pruebas Desarrollo: VMware 4.0 y SO W200 y Linux Debian - Genérico con arquitectura servidor. Servidor de Backup: Genérico con arquitectura servidor con SO W2008. Servidor Enlace Internet Punto a Punto: Genérico con arquitectura servidor con SO W2000 Servidor Enlace ADSL: Genérico con SO Linux Debian. Servidor Web de la Municipalidad. Firewall antes y después enlaces: Genéricos con SO W2000.
Acceso a Internet	Punto a punto 2 MB 2 ADSL con distintos proveedores: 3 y 5 MB	Punto a punto 2 MB 2 ADSL con distintos proveedores: 3 y 5 MB en un mismo servidor para implementación de QoS y balance de carga.
Alimentación eléctrica	Línea separada dentro de la Municipalidad. UPS 3000VA	Línea trifásica y pura desde la calle independiente de las líneas municipales. 3 UPS 3000VA Instalación independiente por cada fase a cada UPS y a cada fuente redundante de los servidores.
Refrigeración	Aire Acondicionado	Aire Acondicionado
Conectividad	Ethernet con cableado estructurado según normas categorías 5e y 6. Fibra óptica con algunas dependencias. Enlaces inalámbricos para oficinas remotas más importantes. Switch administrables capas 2 y 3.	Ethernet con cableado estructurado según normas categorías 5e y 6. Fibra óptica con algunas dependencias. Enlaces Inalámbricos para oficinas remotas más importantes. Switch administrables capas 2 y 3. Creación de VPN para lograr eficiencia en la LAN.
Situación edilicia	Oficina del Director y servidores con libre acceso de personas. Matafuego tipo ABC.	Oficina de servidores con acceso restringido de personas. Matafuego tipo B. Rejas en puerta y ventana.