Hacia la Implementación de un Marco de Seguridad de la Información en la Municipalidad de General Pico

Autores:

Juan Manuel R. **Mosso**, *Bachuss*, Guemes 1982, Rosario {jmanuel@bacchuss.biz}; Guillermo **Covella**, Natalia **Stark**, Juan **Oliveto** , *Municipalidad de General Pico,* Av. San Martín Nº451 y *Facultad de Ingeniería de la UNLPam,* calle 9 esq. 110 General Pico {guillermo.covella, nataliastark, computación[@generalpico.gov.ar]}; Sandra **Ambrosino**, Diego **Morano**, Celia **Vargas**, *Municipalidad de General Pico*{webmaster, jefe_sistemas, celia.vargas[@generalpico.gov.ar]}

RESUMEN

La seguridad de la información es una cuestión clave en los nuevos paradigmas de la administración pública local. La gestión municipal moderna está basada esencialmente en una gran utilización de recursos tecnológicos que son explotados para llevar adelante un modelo de negocios que se apoya en el valor de los activos de información almacenados, procesados y transmitidos en consideración de crecientes requerimientos legales y normativos. El objetivo fundamental de este proyecto es el reconocimiento de las principales debilidades y vulnerabilidades asociadas a las operaciones de la Municipalidad de General Pico y la implementación de contramedidas destinadas a mitigarlas. Como valor agregado se comenzarán a establecer los basamentos políticos necesarios para dar soporte institucional a los instrumentos desarrollados en las distintas etapas del proyecto. La propuesta trasciende aspectos técnicos y pretende establecer un marco de colaboración y aprendizaje que enriquezca a todos los involucrados en base a la generación de transferencia de conocimientos en el área de seguridad. En este sentido es importante destacar que además de resolver su problemática tecnológica, la Municipalidad estará generando recursos humanos valiosos para servir a sus intereses de manera idónea y con elevados niveles de calidad. Este modelo de colaboración trae aparejado el desarrollo de recursos locales a la vez que favorece el desarrollo tecnológico de organizaciones similares en la región.

Introducción

El proyecto que aquí presentamos describe el problema y las posibles soluciones que debe afrontar y promover en la administración de los activos de información a su cargo, el área responsable de la gestión de las Tecnologías de la Información y Comunicaciones de la Municipalidad de General Pico, en adelante la MGP.

En general, el modelo de negocios de cualquier organización administrativa municipal moderna presupone el empleo masivo de recursos tecnológicos diversos para almacenar, transmitir y procesar información. Respetando, por un lado, requerimientos legales y normativos impuestos por la administración nacional, a saber: la Ley 25326 de Protección de Datos Personales, sus decretos y disposiciones anexas, el Decreto Nº1028/03 de la ONTI, la Decisión Administrativa 669/2004, y finalmente la Resolución SGP45/2005 sobre Políticas de Seguridad y, por otro lado, una creciente demanda de servicios cada vez más sofisticados por parte de sus usuarios, tanto internos (empleados, funcionarios) como externos (ciudadanos en general y contribuyentes en particular).

El caso que aquí se describirá no es la excepción, resaltándose además la necesidad de elaborar la propuesta en un contexto de importantes restricciones de todo orden, hecho que a su vez acrecienta el valor de la oportunidad que se intenta aprovechar, de carácter excepcional, en tanto se enfoca específicamente en el desarrollo tecnológico municipal.

En particular, consideramos que la solución al problema de administrar activos de información heterogéneos, de carácter público y almacenado en una gran variedad de soportes, requiere de un marco normativo, un modelo conceptual y un enfoque práctico sustentables, flexibles y a la vez sistemáticos, para ser implementada con éxito.

Situación-Problema u Oportunidad:

La situación-problema que da origen a este proyecto tiene su raíz en el diagnóstico realizado al principio de la gestión actual de la Dirección de Computación a mitad del año 2008. Allí se visualizaban claramente limitaciones en varios órdenes, con implicancias potencialmente negativas para la repartición y para toda la organización, especialmente en cuestiones vinculadas con la seguridad de los datos, tema que nos ocupa y motivación del presente trabajo.

Además, existía en el organización funcional de la DC una gran variedad de procesos, muchos de ellos relacionados entre sí, pero otros sin relación directa, más bien heredados de la estructura de los viejos “Centros de Cómputos” de los '80, cuando el área informática era más bien un apéndice de las direcciones de Rentas y los departamentos de Liquidación de Haberes.

En general, se observó que no existía una planificación estratégica ni operativa claramente especificada ni mucho menos comunicada, quedando en evidencia que los activos de información no estaban debidamente administrados ni protegidos ni a nivel de la repartición ni a nivel de la Organización.

En particular, cabe destacar la ausencia de un Plan Director de Seguridad de la Información que trate temas sensibles como contingencia, backup, ABM de usuarios, una política de seguridad y procedimientos documentados para la protección de la información.

Esta percepción, eminentemente cualitativa en principio, fue confirmada cuantitativamente con un trabajo inicial, de evaluación, realizado en 2009 con el objetivo de encuadrar adecuadamente la solución, tal como se presenta más adelante [ver Ilustración 3 y Tabla 1].

Considerando, complementariamente, que cualquiera fuera la solución diseñada se planteaban importantes restricciones tanto en la contratación de personal, como en la compra de tecnología y en el presupuesto para capacitación, todas áreas sensibles para un proceso de mejora importante, se realizó una jerarquización de los problemas más significativos.

Se tomó como referencia para la jerarquización el nivel de impacto que los riesgos involucrados podían causar y aquellas áreas que tuvieran, a su vez, un efecto positivo a corto plazo con el mayor alcance en la organización. De esa evaluación surgió claramente el área de Seguridad de la Información como uno de los más importantes. Incidió en ello, además de los factores objetivos la percepción existente en la Municipalidad de que cualquier problema con la información almacenada, transmitida o procesada electrónicamente era responsabilidad de la Dirección de Computación (DC) y que la información en papel u otro soporte alternativo no requería de mayor protección que el estar en manos de personal responsable.

Específicamente, situaciones como pérdida de información ante emergencias, falta de conocimiento del marco legal de protección de la información, denegación de acceso a los servicios por intrusión, uso compartido de llaves de acceso a las aplicaciones y los datos, etc. se mostraron como eventuales causas de hechos potencialmente dañinos para la organización.

Para la formulación del proyecto se consideró la oportunidad de tener que elaborar una solución empezando prácticamente desde cero, decidiéndose emplear un enfoque sistemático y sustentable, flexible y evolutivo; basado principalmente en estándares abiertos de la industria como ISO/IEC 17799:2005, y en base a los requerimientos formulados oportunamente por organismos de la administración pública.

Otra oportunidad estuvo dada en que la inversión necesaria para llevar adelante la solución se financiaría con aportes de la operatoria DETEM'08 del Consejo Federal de Ciencia y Tecnología, dependiente del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación. Para obtenerlos la DC concursó una Idea-Proyecto que fue aceptada , basada en tres pilares, uno de los cuales era un "Plan Director de Seguridad de la Información", que se detalla a continuación, en la Solución.

Solución

Historia, incumbencias y diferencias entre los estándares ISO/IEC de seguridad

El origen de la serie de estándares de seguridad de la información ISO/IEC 27000 (ISO/IEC 17799) se remonta al trabajo desarrollado inicialmente por el "Commercial Computer Security Centre" (CCSC) del Departamento de Comercio e Industria del Gobierno del Reino Unido (DTI/UKG).

Fundado en 1987, el CCSC tuvo dos funciones principales. La primera función consistió en soportar a los usuarios por medio de la definición de un código de prácticas recomendadas. Publicado inicialmente como un "Código de Prácticas para Usuarios" en el año 1989, su adopción y maduración siguieron hasta que en el año 1995 se instituyo como el "British Standard BS7799" (BS7799:1995). En 1999 se propone para que sea aceptado como un estándar ISO por medio del mecanismo de "Fast Track" hecho que se materializa en el año 2000 por lo que el BS fue aprobado y publicado como estándar ISO/IEC 17799:2000. Como resultado de procesos naturales de revisión dentro de ISO, el estándar fue revisado en 2005 y relanzado como ISO/IEC 17799:2005. Esta última revisión establece una división mas clara sobre cuestiones tales como requerimientos, implementación e información complementaria. Además agrega controles y explica de manera mas clara muchos de los preexistentes. El resultado final son 133 controles de seguridad en base a 11 capítulos, contra 127 controles y 10 capítulos de la versión del 2000. En 2007 la versión del estándar ISO/IEC 17799:2005 fue relanzada sin modificaciones como ISO/IEC 27002.

La segunda función fue ayudar a la industria vinculada con la seguridad por medio del establecimiento de un criterio de evaluación de seguridad y de un esquema de evaluación y certificación asociado. En el año 1998 surge la segunda parte del estándar BS7799, el "BS7799-2:1998". El BS7799-2:1998 establece de manera clara y sencilla que las organizaciones y los asesores deben hacer para lograr alcanzar un proceso de certificación exitoso. Este estándar establece las bases sobre las cuales se debe evaluar el Sistema de Gestión de Seguridad de la Información (SGSI). El desarrollo de este concepto y su materialización llevaron a ver que esta idea fue mucho más poderosa que el código de prácticas desarrollado originalmente. En 2002, luego de mucho trabajo para madurar las ideas y conceptos surge el 7799-2:2002. Este nuevo estándar BS adoptó el modelo Planear-Hacer-Verificar-Actuar (PHVA) por lo que introdujo mecanismos para todas las fases del SGSI. Como consecuencia de la adopción del modelo PHVA, el estándar se armonizó con otros estándares de gestión como el ISO 9001:2000 y el ISO 14001:1996. En 2005, la versión del estándar BS 7799-2:2002 fue aprobada vía Fast Track en el ISO y publicada como ISO/IEC 27001:2005. Es importante destacar que el trabajo seminal realizado en torno a la evaluación y certificación de seguridad derivó posteriormente en nada menos que el "Common Criteria" (ISO15408).

Presentada la historia de los estándares ISO/IEC de seguridad de la información, sus concepciones fundamentales, sus alcances, diferencias y grado de maduración, es importante destacar que casi la totalidad del proyecto realizado en la MGP al momento se basa en el estándar ISO/IEC 17799:2005.

El Análisis de Seguridad en la Municipalidad de General Pico

Como es lógico imaginar en todo proyecto global de seguridad, aunque no una práctica común, este se inició en base a un proceso denominado "Análisis GAP" [6.] el cuál tiene como objetivo medir y determinar con precisión el grado de linealidad de la organización respecto a todos los controles de seguridad definidos en ISO/IEC 17799:2005.

El modelo de procesos destinado a determinar el estado de seguridad del organismo fue pensado en torno a las siguientes fases relevantes:

- Planeamiento

- Selección de los referentes
- Desarrollo de la metodología de Análisis GAP
- El Diagnóstico como activo
- El Plan de Mejora (y el Portafolio de Soluciones)

Es importante mencionar que el Análisis GAP conforma la primera parte del "Plan Director de Seguridad de la Información" (PDSI) y está destinado a la detección de debilidades y vulnerabilidades, a definir el Estado de Seguridad de la MGP.

Planeamiento y Referentes

El planeamiento del proyecto y la selección de las personas referentes se realizaron de acuerdo a una serie de requerimientos definidos inicialmente en un trabajo conjunto con la Secretaría de Hacienda y Producción y con la Dirección de Computación de la MGP en el marco del programa de Fortalecimiento del Proceso de Descentralización Administrativa de la Municipalidad, y Establecimiento de Nuevos Aplicativos y Servicios Tecnológicos. Además fue considerada la necesidad de la definición de un Marco de Seguridad para las Tecnologías de Información y Comunicaciones (TIC's) en la que hace a la homogeneización de criterios de requerimientos de seguridad sobre todos los servicios propios y externalizados.
En lo que hace a referentes, el proceso de selección se basó en dos motivaciones fundamentales: la primera de ellas consistió en identificar al grupo de personas con el mayor grado de conocimiento sobre cuestiones operativas y orgánicas en la MGP; mientras que la segunda consistió en lograr el compromiso y el aval de la dirección y áreas relevantes del organismo desde un principio, de tal modo de poder avanzar sin restricciones sobre las diferentes etapas del proyecto. El objetivo final de las reuniones iniciales consistió en transmitir a todos los involucrados en el proyecto, el objetivo, los alcances y el impacto final del trabajo. Como valor agregado se buscó y logró exitosamente la introducción de la temática de seguridad de la información como base para emprender el largo y difícil camino de despertar conciencia sobre la importancia que posee la temática para cualquier tipo de organización que haga uso intensivo de tecnologías, especialmente aquellas pertenecientes al sector público.
Para poder tratar cuestiones fundamentales del estudio entre las partes involucradas en el proyecto, se estableció y divulgó un glosario básico de términos entre los grupos de trabajo destinado a unificar los conceptos sobre los que se trabajará. Por ejemplo, se definieron conceptos como: *activos, valoración C.I.D (confidencialidad, integridad y disponibilidad), amenaza, debilidad, vulnerabilidad, salvaguarda, etc*.
El entendimiento de la problemática de seguridad por parte de las áreas jerárquicas de la MGP, la buena predisposición y transparencia de todos los recursos involucrados, y el compromiso de los directivos de las diferentes áreas, especialmente la Secretaría de Hacienda y Producción de General Pico y a la Dirección de Computación, fueron considerados factores clave para lograr establecer el punto de partida del trabajo.

Desarrollo de la metodología de Análisis GAP

La metodología de Análisis Gap llevada adelante en la MGP se abordó atendiendo a la problemática, no solo desde el punto de vista técnico de seguridad, sino que además se estudiaron cuestiones organizativas y legales. Durante el proceso se evaluó el nivel de linealidad o cumplimiento de la MGP contra el estándar ISO/IEC 17799:2005 en base a la determinación de métricas específicas. La metodología empleada se centró en información de la realidad a analizar, utilizando el know-how y experiencia de especialistas y las herramientas de cálculo adecuadas.
El estudio se desarrolló a partir de:

- Entrevistas: con la Intendencia, los directivos y las principales áreas relacionadas con la gestión de los sistemas de información de MGP (Ej.: Secretario de Hacienda y Producción, Dirección General de Asuntos Legales, Dirección General de RRHH y RRII, Contaduría General, Dirección de Computación).
- Cuestionarios: de recolección, basados en ISO 17799:2005 y aspectos organizativos y regulatorios de la seguridad.

Toda la información obtenida sirvió de base para realizar:

- Un detalle de las métricas existentes y sus debilidades y vulnerabilidades asociadas.
- La relación de cada debilidad/vulnerabilidad, a una determinada recomendación.
- Las recomendaciones agrupadas, basándose en proyectos.
- Los proyectos en secuencia de ejecución o dependencia.

En base a los procesos mencionados se elaboró una serie de informes en la cuál se estableció el grado de cumplimiento del organismo con cuestiones de seguridad. La metodología de trabajo generó la siguiente estructura de documentos como resultado:

- Diagnóstico de seguridad. Analiza el grado de cumplimiento de seguridad según el estándar ISO/IEC 17799:2005, así como los aspectos legales y regulatorios de la seguridad.
- Conclusiones. Se trata de un sumario muy breve del documento con objeto de poner de manifiesto los aspectos más importantes

La metodología de Análisis GAP establece un marco de revisión y evaluación de los controles destinados a mejorar la seguridad de la información. Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuanta para cada objetivo y un conjunto de “sugerencias” para cada uno de esos controles. El estudio realizado alcanzó a la evaluación y el análisis del "estado de seguridad" de la MGP en base a los siguientes dominios:

- Política de Seguridad de la Información.
- Organización de la Seguridad.
- Gestión de Activos.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes de Seguridad.
- Gestión de la Continuidad del Negocio.
- Cumplimiento.

Con el estudio de cada uno de los dominios definidos ha sido posible determinar las debilidades y vulnerabilidades que podrían causar, en caso de ocurrir, efectos negativos o impactos no deseados en los diferentes activos de información que conforman la estructura de Sistemas y Redes de la MGP. A partir de la identificación de las debilidades halladas se da cuerpo al Diagnóstico para posteriormente establecer y proponer medidas correctoras y preventivas. Estas acciones, establecidas claramente en un documento específico conforman la segunda parte del “Plan Director de Seguridad de la Información” de la MGP.

El Diagnóstico como activo

Como resultado del proceso de Análisis GAP se logró alcanzar una visión global, no condicionada e integradora sobre el estado de situación actual de la MGP en cuanto a seguridad de la información. Los resultados del proceso completo de análisis se presentan en un documento denominado "Diagnostico GAP ISO17799_MGP". El contenido del trabajo expone información sobre las diferentes debilidades y vulnerabilidades de seguridad presentes en la MGP, no solo a nivel de tecnología y comunicaciones, sino a nivel orgánico, de procesos, legales y de gestión. Los resultados expuestos han surgido de la aplicación de la metodología, de entrevistas, de la documentación aportada, de una serie de cuestionarios, y de los conocimientos y la experiencia de los consultores externos que han realizado el estudio.

El análisis arrojó un total de **doscientos ocho (208)** debilidades y vulnerabilidades detectadas. Dichas debilidades y vulnerabilidades se encuentran asociadas a diferentes tipos de activos que han sido identificados, y su distribución puede observarse en la Ilustración 1.

Ilustración 1. El Diagnóstico y el Nivel de Cumplimiento

Una de las cuestiones fundamentales que aporta el Diagnóstico consiste en una métrica base denominada Nivel de Cumplimiento. Esta métrica establece un valor que representa el índice de linealidad o cumplimiento de la organización contra las recomendaciones del estándar ISO/IEC 17799:2005. Mientras mas controles sean verificados y cumplidos, mayor será el valor de Nivel de Cumplimiento.

El Nivel de Cumplimiento surge como un valor promedio compuesto por los aportes individuales de la valoración definida para cada uno de los dominios de seguridad analizados. Este hecho permite que el mismo pueda ser utilizado como herramienta de evaluación global destinada a establecer el grado de madurez de la organización respecto a temas de seguridad. A continuación, en la [Tabla 1] se muestra el valor del Nivel de Cumplimiento y los valores individuales de cada dominio:

Dominio de Seguridad	DIAGNOSTICO
Política de Seguridad de la Información	0,00 %
Organización de la seguridad	10,00 %
Clasificación y control de activos	0,00 %
Seguridad de los Recursos Humanos	0,00 %
Seguridad Física y Ambiental	39,02 %
Comunicaciones y operaciones	24,73 %
Control de accesos	36,43 %
Adquisición, desarrollo y mantenimiento de software	7,10 %
Gestión de Incidentes de Seguridad	0,00 %
Continuidad de la actividad	0,00 %
Conformidad/Cumplimiento	0,00 %
Nivel de Cumplimiento	**10,66 %**

Tabla 1. Nivel de Cumplimiento

Como consecuencia del valor arrojado por el estudio para el Nivel de Cumplimiento, es menester generar un plan de acción para mejorarlo, hecho que derivó en la confección del "Plan de Mejora (Portafolio de Soluciones)" en el contexto del PDSI.

El Plan de Mejora (PM)

El objetivo final del PM consiste en realizar una propuesta planificada del conjunto de acciones y proyectos encaminados a corregir las debilidades y vulnerabilidades detectadas en la MGP, y elevar su nivel de seguridad de la Información con un horizonte de cumplimiento de 100% respecto al estándar ISO/IEC 17799:2005.

Considerando el hecho de que la seguridad no es algo que se deba o pueda alcanzar, sino algo que se debe gestionar de forma continua, teniendo en cuenta al conjunto de activos de información de carácter crítico pertenecientes a la MGP, y en base a los resultados del Diagnóstico, el PM establece una estimación del esfuerzo necesario para acometer un plan de acción que permita llevar adelante progresivamente una serie de proyectos concretos orientados a elevar el nivel de seguridad y de este modo poder gestionar su seguridad. Este plan se basa en un Portafolio de Soluciones (PS) el cuál queda definido en base a un documento único denominado "Plan de Mejora y Portafolio de Soluciones" (PMPS). El PMPS ofrece un recurso invaluable al momento de establecer mecanismos válidos destinados a gestionar las debilidades y vulnerabilidades que podrían causar efectos negativos o impactos no deseados en los distintos activos que conforman la estructura de Sistemas de Información y Redes de la MGP.

En términos prácticos, el PM propone una serie de medidas correctivas y preventivas (contramedidas) encaminadas a minimizar o evitar los expuestos identificados por medio de la mejora de las prácticas relacionadas al manejo de la información y así elevar el nivel de seguridad de la MGP, abarcando el detalle de proyectos, divididos por plazos, y caracterizados y catalogados por urgencia, interrelación o dependencia, y el esfuerzo necesario para su implantación (tanto en recursos como en tiempo). El PM se establece en torno a tres cronogramas distintos de implementación, *corto, mediano y largo plazo*; en función del riesgo presentado por cada una a los objetivos de negocio de la organización. Las contramedidas propuestas, si bien en su mayoría son aplicables individualmente, por razones de efectividad y eficacia deben ser abordadas de forma conjunta y agrupadas en subproyectos.
Esta división de tiempo se ha realizado teniendo en cuenta la posibilidad de ejecutar proyectos en paralelo así como la de facilitar a la MGP la reserva de presupuestos para abordar los mismos. En la Ilustración 2 puede verse el aporte de cada clase de proyectos al Niveles de Cumplimiento:

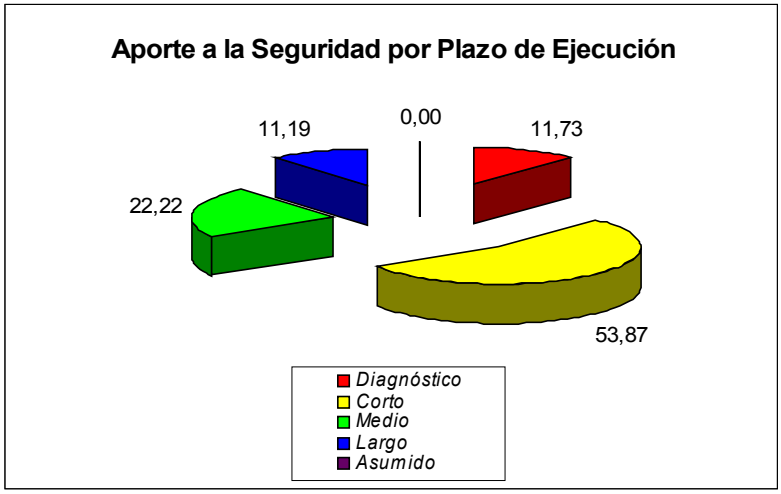

Ilustración 2. Aporte a la seguridad por plazos

En la Ilustración 3 puede verse el aporte de cada fase propuesta en el PM a la seguridad de la información en la MGP, considerando los diferentes dominios de seguridad:

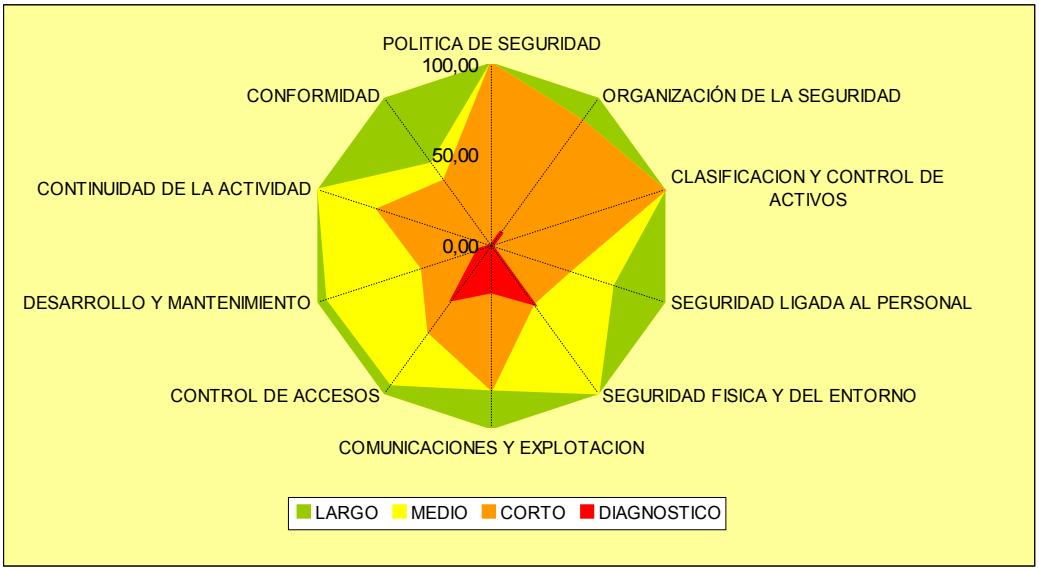

Ilustración 3. Plan de Acción a Corto, Medio y Largo Plazo, Vista Radial

Finalmente, en la Tabla 2 puede verse el esquema propuesto a MGP como PM, y los aportes de cada dominio:

PLAZO	DESCRIPCIÓN DEL PROYECTO	APORTE
CORTO	Adecuación Ley Protección Datos Personales (Ley 25.326)	**0,80**
	Adecuación a Requisitos Legales	**2,79**
	Antivirus	**0,22**
	Arquitectura de Seguridad	**2,94**
	Clasificación de la Información	**6,60**
	Consultoría de Seguridad	**1,38**
	Gestión de Usuarios	**2,94**
	Hacking Continuo	**0,32**
	Inventario de Activos	**3,40**
	Normalización	**20,31**
	Organización de Seguridad	**4,00**
	Plan de Continuidad de Negocio	**6,65**
	Procedimientos Operativos de Seguridad en Sistemas	**0,60**
MEDIO	Cifrado en Datos	**2,20**
	Formación y Concientización en Seguridad	**3,73**
	IDS (Intrusion Detection System)	**0,12**
	Mejora de la Seguridad Física	**6,10**
	Monitoreo de la Seguridad	**0,88**
	PKI (Public Key Infrastructure)	**0,70**
	Plan de Contingencias	**3,13**
	Segmentación de Red	**1,78**
	Seguridad en Desarrollo	**3,39**
LARGO	Auditoria global	**4,43**
	Cifrado en Comunicaciones	**0,06**
	Generación de Datos de Prueba	**0,90**
	Gestión de Backups	**0,60**
	Política de Backups	**1,55**
	Seguridad en Accesos Remotos	**0,08**
	Seguridad Microinformática	**0,77**
	Sistema de Respuesta ante Incidentes de Seguridad	**3,00**

Tabla 2. Aportes de Cada Dominio a la Seguridad General

Es importante desatacar que la valoración cuantitativa de los proyectos ha sido realizada de manera aproximada, con el objeto de que la MGP pueda establecer una serie de reservas presupuestarias que le permitan acometer estos proyectos.

La puesta en marcha y ejecución de los planes identificados como necesarios en el corto plazo generaran una elevación del nivel de seguridad en un **53,86%, logrando un Nivel de Cumplimiento del 64,52%**. Este valor de Mejora en el estado de situación de la MGP deberá ser reevaluado en el futuro, al menos ante la finalización de la etapa de corto plazo propuesta en el PM para validar los resultados.

Innovación e Inédito:

El carácter novedoso del trabajo, al menos a nivel municipal en la Provincia de La Pampa, se debe a un abordaje integral del problema de Seguridad de la Información para la Municipalidad de General Pico, en el cuál se consideró a la misma como un conjunto de personas, activos de información y procesos que permiten desarrollar el modelo de administración/negocio de la organización. El empleo de normas y estándares de seguridad para el desarrollo del trabajo constituye otro pilar novedoso, pues da fortaleza, actualidad y seguridad a la propuesta, en oposición a las propuestas ad-hoc, que suelen generar dependencia de quién la ofrece y no constituyen referencias para el sostenimiento y el avance a lo largo del tiempo. También permite una articulación madura con otros organismos fuertemente regulados y controlados, como los del sector financiero-bancario y de fiscalización. Finalmente, la utilización de

estándares permite reutilizar todos los esfuerzos realizados y los productos del proyecto con el objetivo de validar las prácticas y los procesos contra órganos de certificación nacionales e internacionales.

Beneficiarios:

Los beneficiarios del Proyecto son, en primer lugar aunque indirectamente, los usuarios de los servicios de la Municipalidad de General Pico, pues los datos personales y organizacionales que están bajo la custodia de la Municipalidad serán objeto de un tratamiento riguroso en cuanto a su almacenamiento, utilización y divulgación. Se trata nada menos que de los contribuyentes, proveedores, licenciatarios de servicios públicos, empresas de recaudación y otros organismos públicos de la seguridad social y de fiscalización y control.

Por otro lado y en forma directa, se beneficiarán los empleados y funcionarios de la MGP, pues la propuesta del Proyecto tiende a minimizar los riesgos de seguridad vinculados con la confidencialidad, integridad y disponibilidad de todos los activos de información del organismo. Se propone, también, poner en conocimiento la responsabilidad de cada uno frente a la utilización de activos de información sensibles de custodia y protección y llevar adelante un importante proceso de sensibilización y capacitación en todos los niveles de la organización. En particular, la primera etapa del proyecto involucrará a los funcionarios, solidariamente al personal jerárquico correspondiente, en la responsabilidad de promover la Seguridad de la Información a todos los niveles de la Organización, tal como se sugiere en distintas normas y documentos de organismos de referencia a nivel nacional

Relevancia para el Interés Público

La relevancia para el interés público está dada por el carácter significativo que tiene la información bajo la tutela y administración de los organismos públicos en general, En particular, en la Municipalidad actualmente se gestiona información de sus contribuyentes y beneficiarios, de Servicios Públicos concesionados, de organismos de recaudación y fiscalización. En forma continua se celebran convenios y contratos que involucran intercambio de datos en diversos formatos y se publican información de deudas y acreencias, como también se informa al Poder Judicial en casos de requerimientos pertinentes.

Indicadores objetivos de la relevancia que tiene la propuesta puede rastrearse en la Auditoria Ciudadana[2.] realizada en General Pico por la Subsecretaría para la reforma Institucional de la Jefatura de Gabinete de Ministros entre los años 2004-2005, particularmente en el punto 4.1, "*Existencia de Legislación o regulaciones específicas sobre disponibilidad y acceso a la información pública en poder de las instituciones Municipales (…) y acciones desarrolladas para su efectivo cumplimiento*", y en 4.3 "*Percepción Ciudadana sobre la disponibilidad, cantidad, calidad, utilidad y veracidad de la información de las instituciones públicas municipales*" donde los ciudadanos expresan claramente su intención de contar con más y mejor información pública por parte de la Municipalidad, tanto en calidad como en cantidad. Concretamente respecto al punto 4.1 no existía directamente la legislación reclamada.

En todo caso es evidente que resulta beneficioso disponer de un marco de Seguridad de la Información pues se trata de una garantía respecto a como son tratados los datos y la información derivada que se eventualmente se divulgue o se transmita para su posterior procesamiento o utilización.

Viabilidad Técnica, Financiera y Política Organizacional

Desde el punto de vista técnico el proyecto es viable en tanto se cuenta con un diagnóstico apropiado y, al menos hasta la etapa de implementación de las soluciones de corto plazo, se cuenta con el financiamiento de la operatoria DETEM.

En relación a la cuestión organizacional, se cuenta con el apoyo de las más altas autoridades de la MGP, tanto en la jerarquía superior de la DC, como el Contador General y el Sec. de Hacienda y Producción, y también del Intendente Municipal. Se prevé formalizar ese apoyo en la redacción y promulgación de una resolución que facilite la implantación de una Política de Seguridad de la Información en el ámbito del Departamento Ejecutivo Municipal en base a lo establecido por medio de la Decisión Administrativa 669/2004 y la Resolución SGP45/2005.

Además de la Política de Seguridad, la MGP se encuentra en vías de formalización del Comité de Seguridad, de la definición de su modelo de gestión y de la definición de sus funciones según requerimientos legales y normativos

Este apoyo es significativo, no sólo para que el proyecto se transforme en una iniciativa exitosas sino también porque implica un cambio organizacional importante, pues se espera cambiar gradualmente la estructura de la Dirección y de la Municipalidad incorporando el área de Seguridad de la Información, tal como se puede ver inicialmente en la Ilustración 4.

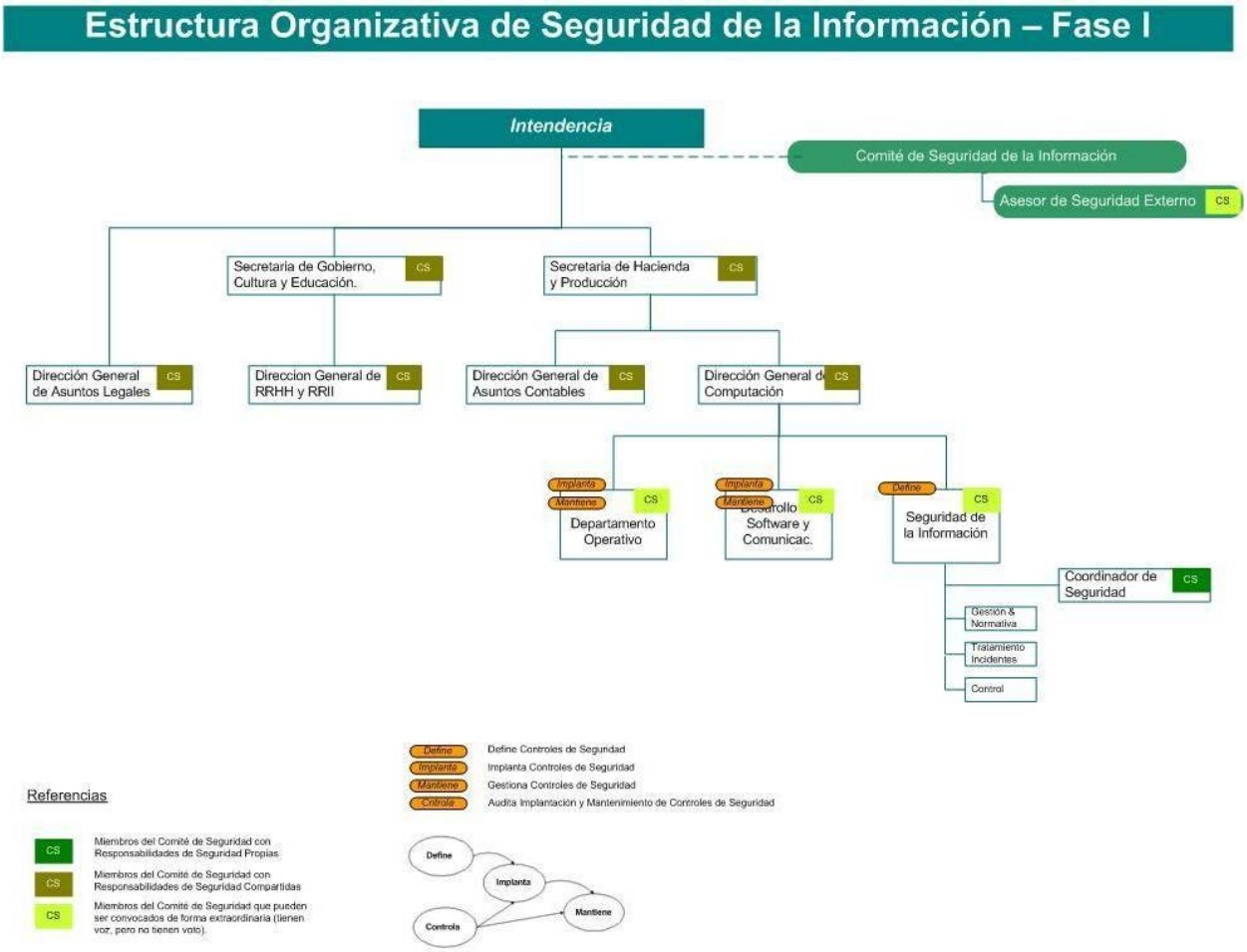

Ilustración 4. Primera Fase de la Evolución del Organigrama de Seguridad en el Marco General.

Para considerar el grado de avance del proyecto y el nivel de éxito se ha elaborado un diagnóstico, ya visto en [Tabla 1], y también un plan de acción basado en un conjunto de subproyectos con el objetivo de alcanzar metas de corto, mediano y largo alcance [ver Ilustración 5] que posicionen a la Municipalidad en una situación de control total de sus activos de Información.

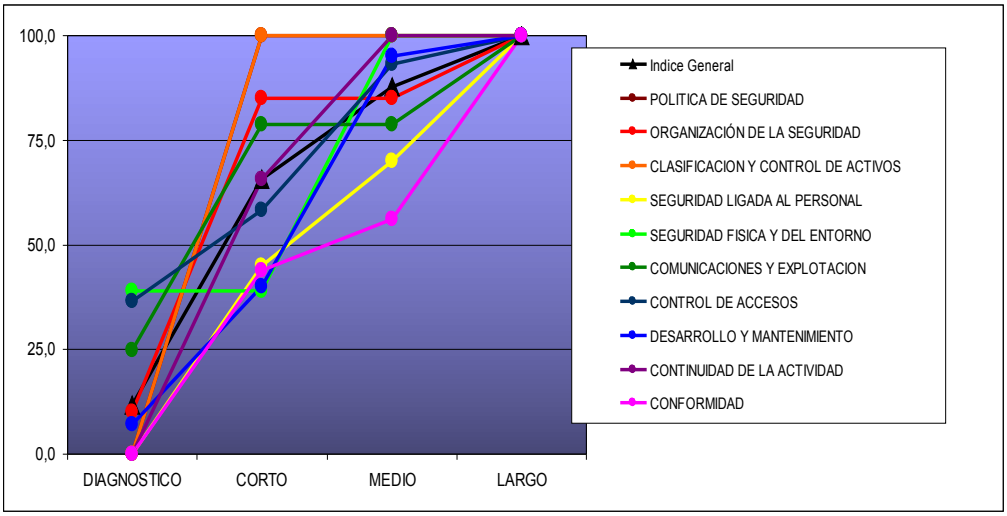

Ilustración 5. Vista Ejecutiva del Plan de Acción a Corto, Medio y Largo Plazo.

Facilidad de Reproducción

El proyecto puede reproducirse fácilmente en otras organizaciones públicas de tamaño semejante, contando con el apoyo de las máximas autoridades y por supuesto en empresas privadas con el apoyo de la Alta Dirección. En nuestro caso el Proyecto fue debidamente discutido y luego aprobado por los funcionarios correspondientes, como paso previo a su inclusión en una solicitud de financiamiento y la elevación para la aprobación del Intendente.

El apoyo de la más Alta Dirección debe considerarse un prerrequisito ya que si bien es una condición fuertemente resaltada en la aplicación de cualquier iniciativa de mejora, por Ej. en las que apuntan a la certificación de cumplimiento de normas o estándares, el tratamiento de activos intangibles, como en este caso, puede no resultar atractivo para quienes no visualizan claramente el aporte que hacen a la organización. De este modo iniciativas como las de este proyecto podrían abortarse prematuramente.

Los medios para llevarlo adelante pueden ser obtenidos desde afuera de la organización, si no están disponibles internamente, pues se trata de un proyecto que afecta activos muy sensibles a cualquier tipo de organización, sea pública o privada. De esta manera y considerando el nivel al que se encuentre posicionado, puede recurrirse a una fuente externa de financiamiento y a empresas o universidades con el know-how necesario para financiar como para formular el proyecto.

En cualquier caso la inversión necesaria no es significativa pues en este caso el presupuesto para el proyecto representó menos del diez por ciento del presupuesto anual de la DC, contando gastos en personal.

Ambiente de Hardware y Software

En cuanto a las derivaciones de implementación técnica que se desprenden del PM, el ambiente de hardware y software no tiene requerimientos particulares ya que puede emplearse equipamiento estándar disponible sea este de telecomunicaciones y/o hardware [ver Ilustración 6], por un lado y, por otro lado, software bajo licencia GNU o análogas para las soluciones de software.

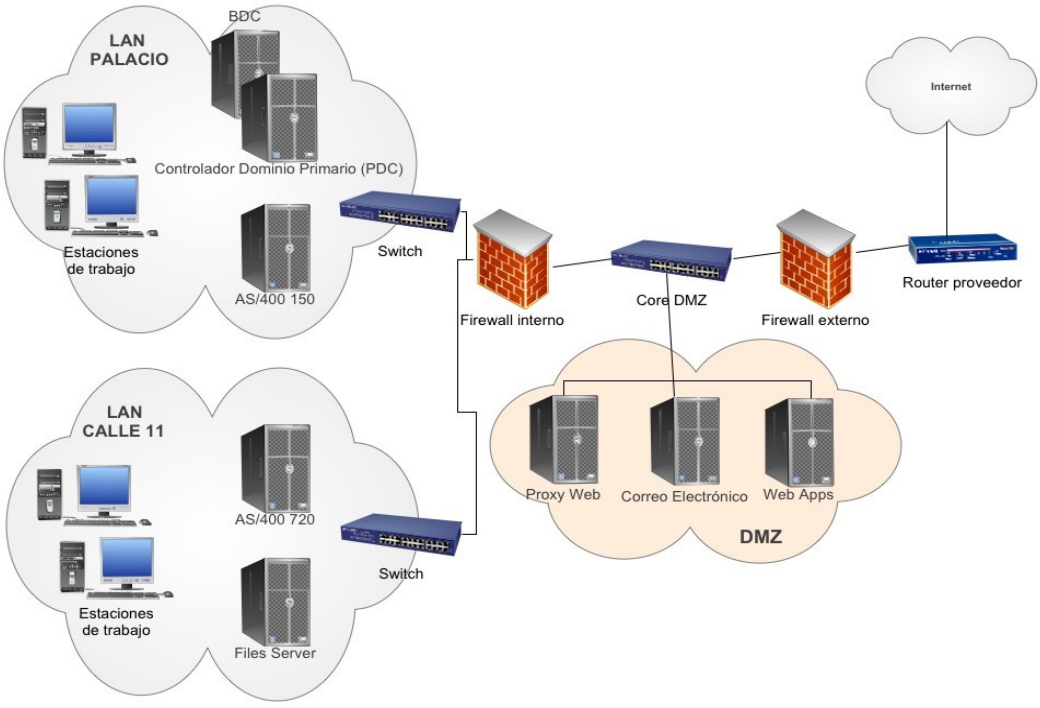

Ilustración 6. Hardware y Software para el esquema de Seguridad Perimetral y Filtrado

Para desarrollar parte de la solución de corto plazo se prevé la implementación de un único dispositivo de seguridad en una arquitectura de tipo screened-subnet que permita segmentar las redes en base a requerimientos particulares de seguridad en los accesos.
Para la implementación del dispositivo de seguridad se utilizará al sistema GNU/Linux como sistema operativo, más precisamente a Debian GNU/Linux por su compromiso con la calidad y con el software libre. Teniendo en cuenta la plataforma elegida, el producto recomendado para la implementación de los

mecanismos de seguridad y de infraestructura es Netfilter/Iptables. Netfilter/Iptables constituye el estándar de facto para el desarrollo de firewalls sobre plataformas GNU/Linux.
Esta herramienta cuenta con características destacadas para herramientas de este tipo entre las cuales puede nombrarse: Filtrado de paquetes, Network Address Translation, Mangling, Herramientas avanzadas de documentación de incidentes, etc.

Referencias

[1.] Consejo Federal de Ciencia y Tecnología del Ministerio de Ciencia, Tecnología en Innovación Productiva, sección Resultados de la Convocatoria 2008 para la operatoria Desarrollo Tecnológico Municipal. http://www.cofecyt.mincyt.gov.ar/convocatoria_detem_08.htm,

[2.] Programa Auditoria Ciudadana en General Pico, La Pampa, http://www.auditoriaciudadana.com.ar/index.php?option=com_content&view=article&id=126&Itemid=63

[3.] Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI) de la SUBSECRETARÍA DE GESTIÓN PÚBLICA de la JEFATURA DE GABINETES DE MINISTROS

[4.] IRAM-ISO/IEC 27001. Requisitos para los Sistemas de Gestión de Seguridad de la Información

[5.] BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, COMUNICACIÓN "A" 4609 Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información

[6.] Metodología de Análisis GAP ISO/IEC 17799:2005. Bacchuss, Seguridad de la Información. http://www.bacchuss.biz