1

EL VALOR DE LA INFORMACIÓN CIUDADANA. SEGURIDAD INFORMÁTICA Y GESTIÓN MUNICIPAL.

Rodrigo Martorell P[1].
Fernanda Huacarán[2].

RESUMEN

En el presente artículo, se aborda el tema de la seguridad informática en la gestión municipal mediante el análisis de los resultados de una reciente encuesta aplicada a 186 municipios a lo largo del país, para conocer sus realidades en cuanto al uso y manejo de las TI. Los resultados muestran que si bien se ha masificado la implementación de las TI, no existe una gestión adecuada y que se requiere fortalecer la seguridad informática. Junto con exponer los principales resultados del estudio, se discute acerca de la importancia de valorizar la información y contar con planes de introducción y uso de la TI que efectivamente contribuyan a la gestión municipal.

Palabras clave: Tecnologías de la Información (TI), Sistemas de Seguridad de la Información (SSI), Municipios Inteligentes, Ciudadano Inteligente, Plan de Continuidad Operacional.

ABSTRACT

In the present article, addresses the issue of computer security in municipal management by analyzing the results of a recent survey of 186 municipalities throughout the country, to know their realities in the use and management of IT. The results show that although the implementation of IT is widespread, there is no proper management and to strengthen information security requires. Along with exposing the main results of the study, discusses the importance of give value of the information and have plans for the introduction and use of IT to effectively contribute to municipal management.

Keywords: Information Technology (IT) Information Systems Security (ISS), Municipalities Intelligent, Smart Citizen, Operational Continuity Plan.

1 Ingeniero Civil Industrial, Ms. en Informática y MBA, Universidad Mayor. Gerente Técnico y Desarrollo TIC, CAS-Chile.
2 Geógrafa, Pontificia Universidad Católica de Chile.

INTRODUCCIÓN

La integración de los servicios informáticos facilita y fomenta el trabajo conjunto entre diferentes áreas de una organización, independiente de la distancia física en la que se encuentren. Estos servicios se desarrollan a través de las tecnologías de la información (TI), cuyo uso se ha masificado tanto en el mundo privado como público, constituyendo una herramienta fundamental en la sociedad actual. En el ámbito municipal, la implementación y el desarrollo de las TI es una realidad, lo que no garantiza por sí solo, de manera inmediata ni a largo plazo, la obtención de resultados óptimos.

TI al servicio municipal

Se entiende como tecnologías de la información (TI) aquellas herramientas y métodos empleados para reunir, almacenar, manipular o distribuir información, de manera tal que contribuyan a la toma de decisiones (Bologna y Walsh, 1997). Este punto es crucial para comprender la importancia de potenciar la utilización de las TI en los municipios. Bien gestionadas, éstas permiten realizar una administración eficiente, optimizando procesos internos y externos que faciliten las relaciones con los ciudadanos.

Frente a esta realidad, cabe considerar algunos aspectos para alcanzar un nivel adecuado de modernización municipal. Dada la gran diversidad territorial que abarcan, los municipios cuentan con condiciones disímiles para asumir los desafíos de gestión que corresponden al gobierno local. Por otra parte, es fundamental mejorar la calidad de la gestión, plantearlo como un punto prioritario en la política municipal, lo cual se logra a través de la acreditación de servicios municipales y capacitaciones a sus funcionarios. A su vez, el Gobierno Central debiese buscar las condiciones para traspasar algunas de sus competencias, a fin de alcanzar mayor autonomía municipal (SUBDERE, 2008).

El Instituto Chileno de Estudios Municipales publicó el 2006 un estudio sobre la aplicación de las tecnologías de la información en el ámbito de la Reforma Municipal (ICHEM, 2006). Allí se sostenía que el desafío para los municipios que disponían de sitios web era doble: por una parte, debían ampliar su presencia en internet y por otra, potenciar y masificar los servicios en línea, como mecanismos facilitadores de la gestión moderna del municipio.

Habiendo comprendido esto, los municipios en Chile se han integrado rápidamente a esta dinámica. En el estudio mencionado, se concluyó que el 98% de las municipalidades encuestadas indicaron contar con acceso a Internet, mientras un 2% no contaba con acceso a la red en sus recintos. Sin embargo, el acceso a Internet es el primer paso para la modernización municipal y no da cuenta de la alta disparidad en los niveles de digitalización de la gestión. En general, en la actualidad las páginas web municipales ofrecen al ciudadano la posibilidad de interacción, sin embargo, menos del 12% ofrece los servicios básicos que califican para la existencia de un E-Government (Gobierno electrónico). Más grave aún, no alcanzan el 3% aquellas municipalidades que ofrecen servicios de participación ciudadana a través de Internet (Cetiuc, 2010).

El valor de la información

La utilización de las TI en los servicios públicos adquiere relevancia frente a activos de gran valor, como es el caso de la información y amenazas que se ciernen en torno de ésta, como por ejemplo, la entrega de certificados con datos adulterados y las caídas del servicio cuando se realizan pagos en línea o se filtra información personal. De materializarse este tipo de amenazas, se expone al servicio público y al ciudadano a un impacto previsible y cuyos posibles efectos necesitan ser cuantificados.

En este sentido, una correcta gestión municipal de las TI permitiría resguardar la información frente a hechos administrativos o informáticos como los señalados. Con el propósito de hacer frente a estas amenazas, constantes, es fundamental considerar y evaluar la Seguridad de la Información, anticiparse a los futuros impactos y prever las respuestas a dar en caso de producirse una situación de contingencia.

PROBLEMÁTICA

La importancia que otorga la ciudadanía al rol de los municipios radica en que éstos son un espacio clave, donde acontece el primer nivel de acercamiento con las instituciones democráticas. Actualmente, la percepción ciudadana de la gestión municipal dista mucho de ser positiva; por el contrario, ésta demanda profesionalismo de los funcionarios municipales (INAP, 2012). Nos encontramos frente a Ciudadanos Inteligentes que reclaman Municipios Inteligentes (Pahlka, 2012).

Un ciudadano del Municipio Inteligente aspira a interactuar con una plataforma virtual mediante herramientas proporcionadas por la administración local, que le permita satisfacer sus necesidades y/o resolver sus problemas. De tal manera, dicha plataforma proporcionaría oportunidades a la comunidad de generar valor mediante el uso de las nuevas aplicaciones disponibles. De esta forma, un municipio que gestiona eficientemente las TI permitiría a sus vecinos: obtener información comunal relevante, descargar documentos municipales en línea, realizar el pago de servicios como derechos de aseo o permisos de circulación, o incluso, permitiría ubicar puntos sensibles de tráfico desde un celular inteligente. El nuevo ciudadano, al cual llamaremos Ciudadano Inteligente, está totalmente conectado, evalúa las acciones y servicios que recibe, y que definen en gran medida su calidad de vida, exigiendo una gestión eficiente.

Rol del Ciudadano Inteligente en la realidad municipal

Para comprender la realidad nacional de gestión de las TI, es necesario identificar quién demanda el servicio – Ciudadano Inteligente- , y quién entrega dicho servicio. En este último punto es necesario detenerse.

Existen diferencias considerables en el desarrollo de las TI entre el mundo público y el privado. En el ámbito tecnológico, el sector público se encuentra retrasado, ya que en el último tiempo se ha enfocado en consumir tecnología, dejando de lado la gestión y la seguridad de la misma. El sector privado, en tanto, luego de adquirir tecnologías y desarrollar un plan de gestión de las mismas, se encuentra asegurando la información y las tecnologías asociadas al manejo de éstas.

Ilustración n°1. Desarrollo del servicio de Tecnología de la Información Municipal.

Fuente: Elaboración propia.

En la búsqueda de resolver las demandas ciudadanas, el municipio ha optado por establecer una alianza con el mundo privado, el que posee mayor experiencia en la entrega de los servicios asociados a las TI y, además, comprende de mejor manera los requerimientos del usuario. Es en este punto donde el ciudadano, bajo la mirada municipal, pasa de ser vecino a usuario, el cual tiene preferencias, expectativas y conocimientos sobre los servicios que demanda.

Mientras un Ciudadano Inteligente demanda calidad en la gestión de servicios municipales y la municipalidad se mantiene al margen de estos requerimientos, el ciudadano pasa a ser únicamente un usuario, en tanto que la municipalidad no logra mejorar la calidad de vida de sus habitantes, es decir, en cuanto ciudadano.

Seguridad de la información y normativa chilena

En este escenario, cabe preguntarse quién finalmente responde al ciudadano (vecino-usuario) cada vez que se deja de prestar un servicio, o se ve amenazada la seguridad de la información municipal disponible. Tal como se planteaba con anterioridad, los gobiernos locales se han orientado a la adquisición de infraestructura (equipamientos y servicios) sin un análisis previo, tercerizando de alguna manera el servicio y traspasando con ello a las empresas privadas la responsabilidad del servicio contratado. En función del cumplimiento de las formalidades contractuales, las empresas han potenciado y mejorado sus procesos, encontrándose obligadas a aplicar un sistema de gestión de la seguridad de la información, lo cual favorece la optimización de su trabajo y a la vez, constituye un resguardo frente a las multas por incumplimientos de los contratos.

Para el sector privado es comprensible identificar que el principal problema en esta relación que establecen con las municipalidades es el desconocimiento de los funcionarios públicos de las operaciones necesarias para satisfacer al ciudadano actual, las que, dada su complejidad, son cada vez más difíciles de abordar.

El tema de los recursos humanos (RRHH) de las municipalidades no es menor, ya que el capital intelectual que hoy está presente en las entidades públicas, en términos cuantitativos y cualitativos, no es suficiente para satisfacer las necesidades de un mercado en continua evolución. Para incorporar capital humano de mayor nivel de conocimiento a la administración pública se necesita motivarlo. Independiente de los recursos asignados a la contratación de personal, existen normativas y lineamientos para el manejo de información municipal (Dipres, 2012).

Con el fin de resguardar la información en los distintos órganos del Estado, se publicaron, desde el año 2004, una serie de decretos supremos referidos al Gobierno Electrónico, en el marco del programa de mejoramiento de la gestión (PMG). Uno de esos fue el Decreto Supremo N° 83 de 2005, que planteó un código de prácticas para la gestión de la seguridad

de la información. Dos años más tarde, el Ministerio del Interior detectó algunas falencias en su aplicación en las instituciones del sector público, tales como las siguientes:

1. Aplicaciones y sistemas informáticos con configuración inadecuada.
2. Sitios web de gobierno implementados deficitariamente y con vulnerabilidades conocidas.
3. Redes informáticas institucionales con debilidades en sus mecanismos de control de acceso y de regulación del tráfico de datos.
4. Problemas de continuidad operacional frente a incidentes de índole recurrente, tales como los cortes de energía eléctrica.
5. Inexistencia de políticas de seguridad institucionales.

Para enfrentar estos problemas se incluyó, desde el año 2010, el Sistema de Seguridad de la Información (SSI) en el Programa de Mejoramiento de la Gestión (en el marco de la ley N° 19.553). A su vez, durante el 2012 se complementa el mencionado DS N° 83 con la Norma chilena ISO 27001, la cual se erige como el referente normativo del sector.

El objetivo del SSI es "lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información" (Dipres, 2012b).

Es decir, el SSI entrega la posibilidad de disminuir en forma significativa el impacto de los diferentes riesgos e inseguridades a los que están sometidos los activos de información, tanto dentro de la propia organización como desde fuera de ella. Cuando se habla del conjunto de activos de información institucional, el SSI se refiere a los documentos en papel, bases de datos, sistemas y software de aplicación, equipos informáticos, redes de transmisión de datos, soportes de almacenamiento y otros elementos de infraestructura.

Para implementar un Sistema de Seguridad de la Información municipal, es fundamental la existencia de un Comité de Seguridad de la Información (CSI), que sea responsable de su desarrollo y supervisión. Es responsabilidad de éste "ejecutar los procedimientos y estándares que se desprenden de las políticas de seguridad de la información, proponer estrategias y soluciones específicas para la implantación de los controles necesarios para implementar las políticas de seguridad establecidas" (Dipres, 2012).

El CSI idealmente debe estar integrado por los siguientes funcionarios:

a) Jefe de Operaciones o Tecnologías de Información.
b) Jefe de Recursos Humanos.
c) Encargado de Calidad.
d) Encargado de Riesgos.
e) Asesor Jurídico (abogado de la Institución).
f) Jefes de Áreas Funcionales o encargados de procesos, si corresponde.
g) Encargado de Seguridad de la Información (ESI).

Si la institución prescinde de estos funcionarios, y sobre todo de un encargado de seguridad de los activos de la información, se expone a la institución a diversas amenazas.

Para enfrentar las amenazas, es imprescindible contar con un Plan de Continuidad Operacional, que permita da una respuesta adecuada de la institución ante situaciones de contingencia, sin afectar la continuidad de algunos procesos relevantes. Dentro de este plan es fundamental contar con un procedimiento de Gestión de Incidentes, acotado y conocido por el personal encargado.

Para resguardar la integridad de la información se debe, por tanto, contar con un tratamiento adecuado de las amenazas y conocerlas de antemano. En términos generales, y para efectos de este estudio, se consideraron algunos tratamientos básicos de la información, tales como respaldos y sistemas de protección interna.

En relación a los respaldos, estos pueden realizarse o no bajo un procedimiento definido con anterioridad y varían según los tipos de soporte físico en que se encuentran, además de su ubicación. Si bien la sola existencia de respaldos es un hecho positivo, de poco servirá respaldar información en un cd, pendrive, o cloud computing, si no se tiene acceso a dicha información o se ha comprobado que es íntegra. Aun contando con un servidor centralizado, si la entidad se halla frente a una amenaza que afecta la integridad de su infraestructura (tales como robos, incendios o terremotos), éste no servirá, a menos que exista un servidor externo de respaldo.

METODOLOGÍA

Para evaluar la realidad nacional respecto de la seguridad informática, el ICHEM realizó el Estudio Nacional sobre Seguridad Informática y respaldo de la Información en las Municipalidades Chilenas, a comienzos de 2013, que abordó los siguientes puntos:

1. Perdida en la continuidad del funcionamiento municipal por fallas en el servicio (Internet, software, robo de información, etc.).
2. Registro de pérdidas de información.
3. Existencia de algún sistema de protección en la red interna.
4. Existencia de personal dedicado a la Seguridad de la Información.
5. Existencia de normas de creación de contraseñas.
6. Existencia de un Plan de Continuidad de Negocio (o Plan de Continuidad de Operaciones).
7. Existencia de procedimientos de Gestión de Incidentes.
8. Métodos de actualización de sistemas operativos y software.
9. Ocurrencia de Incidentes de Seguridad de la Información asociada a los Servicios prestados por la municipalidad.
10. Existencia de Copias de Respaldo de la Información.
11. Existencia de Plan de Respaldo de la Información.
12. Responsabilidad de los Respaldos de Información
13. Tipos de Soporte para Respaldo de Información.

El universo de este estudio se realizó con criterio censal, por tanto fueron contactadas las 335 municipalidades para que respondieran a cuestionario enviado. Contestaron favorablemente 186 municipalidades, a través de sus encargados de informática, o sea, el 55,5%. El levantamiento de la información se realizó durante el mes de enero de 2013.

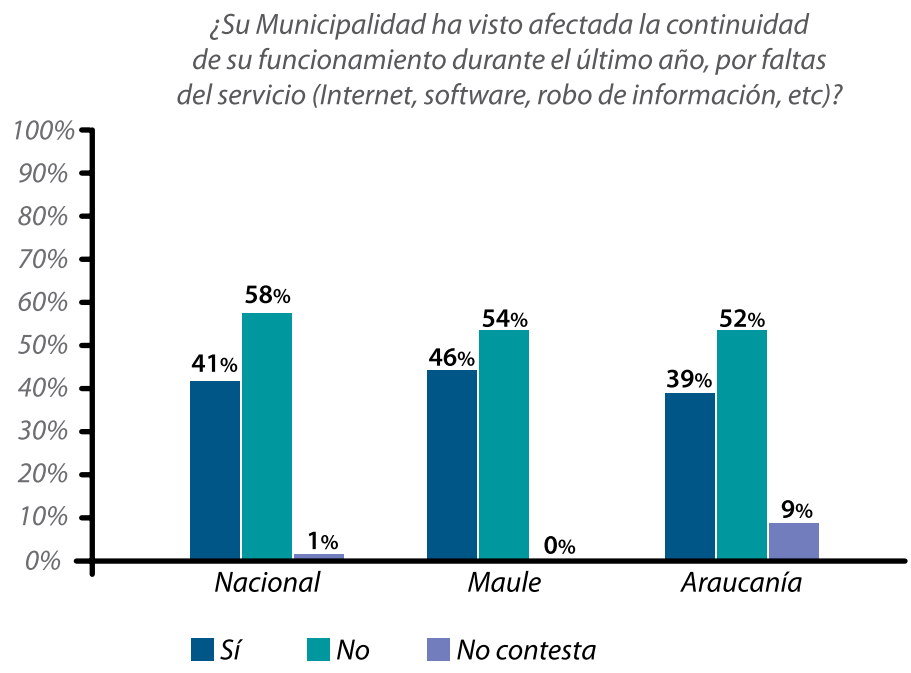
Como medio de contraste con los resultados a nivel nacional, utilizaremos los datos de las regiones del Maule y la Araucanía. En dos casos, las regiones del Maule y La Araucanía, las respuestas al cuestionario fueron 26 (de 30) y 23 (de 32) municipalidades, respectivamente.

RESULTADOS

A nivel nacional se puede observar que el 41% de los municipios que contestaron la encuesta se han visto afectados por fallas generales en su servicio informático (problemas de conectividad con Internet y funcionamiento de los softwares).

En la región del Maule esta cifra sube al 46% de las municipalidades y en la región de la Araucanía, los municipios afectados alcanzan al 39%.

Gráfico n°1. Porcentaje de municipalidades con fallas en el servicio informático, año 2012.

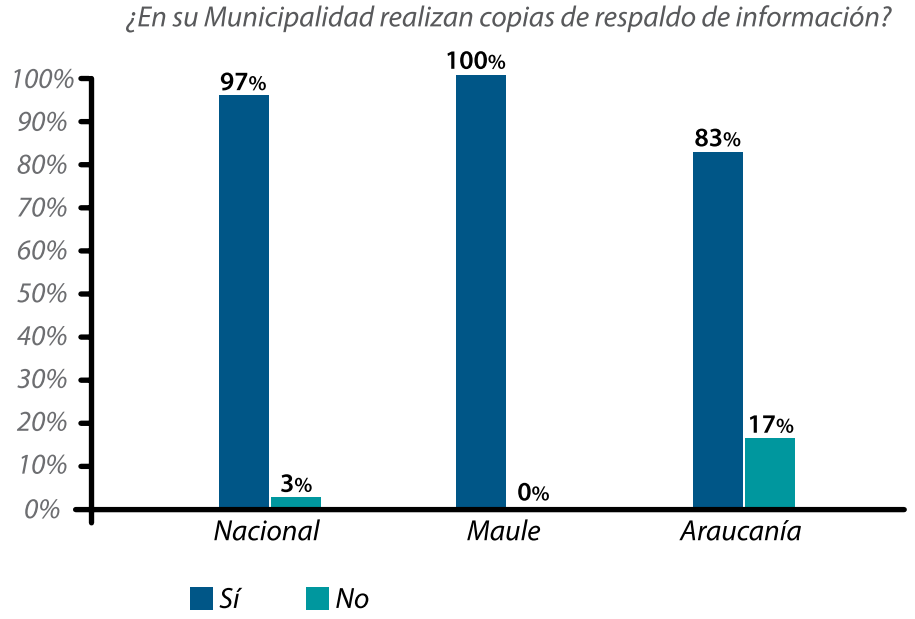


Fuente: Elaboración propia en base a ICHEM 2013.

Sin embargo, el problema de seguridad de la información, frente robos o ataques no aparece como un asunto relevante para las municipalidades de Chile. Esto porque, solamente un 4% declara haber sufrido este tipo de eventualidades (0% en el Maule, y 9% en La Araucanía), en los últimos 6 meses.

De otro lado, la gran mayoría de las municipalidades cuenta con planes para el respaldo de información (el 95% de las municipalidades los tiene). Al mismo tiempo, ellas declaran que ejecutan efectivamente estos respaldos (el 97% de las municipalidades respalda su información).

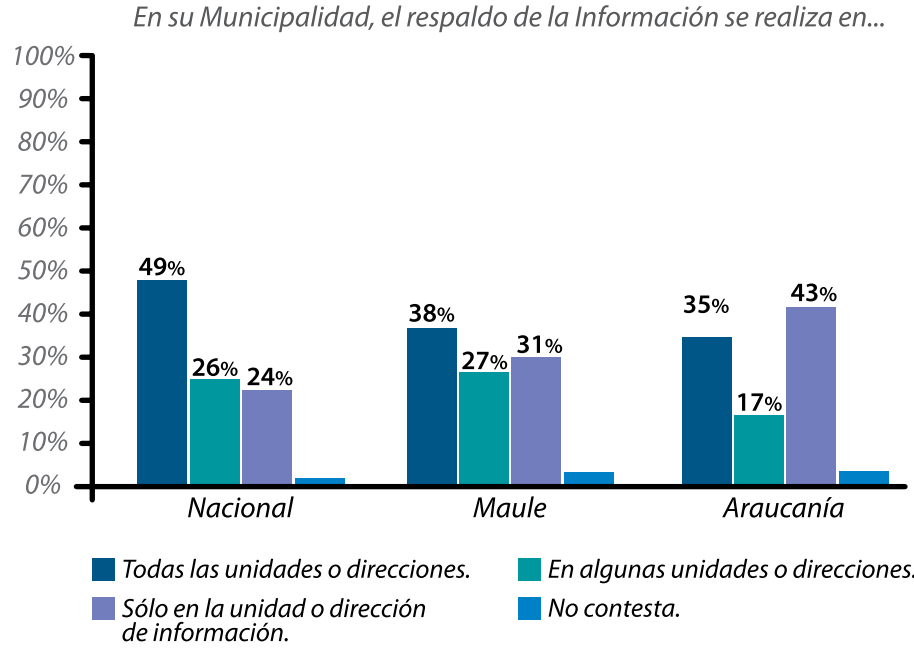
Gráfico n°2. Porcentaje de municipalidades que respalda la información digitalizada.



Fuente: Elaboración propia en base a ICHEM 2013.

Cabe mencionar que el respaldo de información es realizado por las municipalidades de manera no centralizada, en cada una de las direcciones municipales. Solamente en un 24% de las municipalidades, la Unidad de Informática concentra este respaldo de la información.

Gráfico n°3. Porcentaje de unidades municipales responsables de respaldar la información.

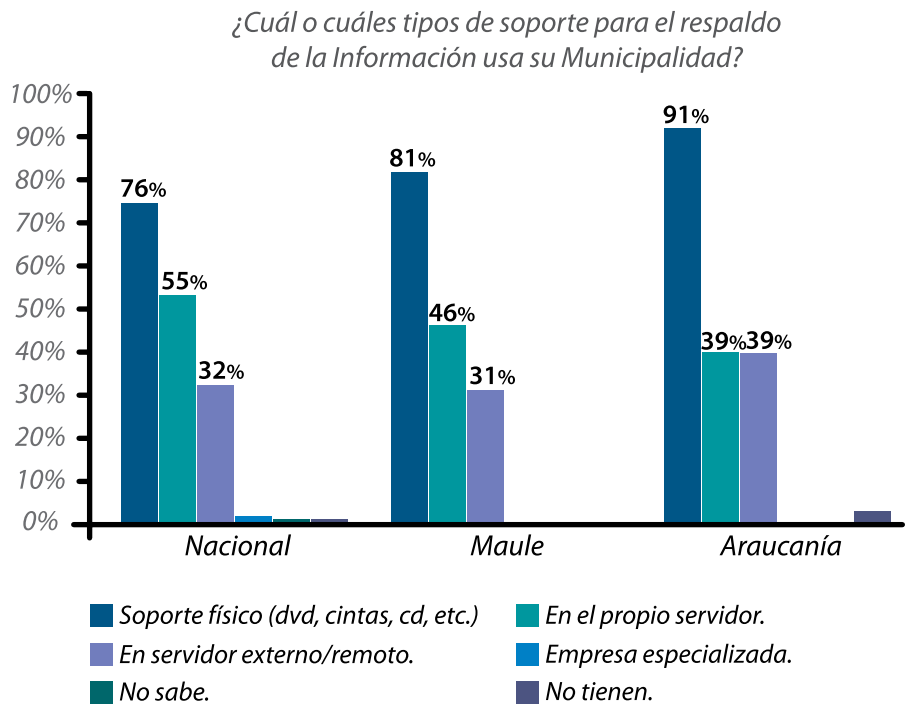


Fuente: Elaboración propia en base a ICHEM 2013.

Pese a lo anterior, en general la unidad responsable del respaldo de información es la Unidad de Informática (un 83% de las municipalidades del país, así lo declara), mientras que sólo un 3% declara que no hay responsabilidades asociadas. Por lo tanto, en la mayoría de las municipalidades chilenas la responsabilidad del respaldo de información recae en la Unidad de Informática, aunque dichos respaldos no se encuentran centralizados en esta unidad.

Al consultar respecto a los soportes de información, la mayoría de las municipalidades cuenta con soportes físicos (disco duro, pendrive, DVD, etc.), mientras que otras herramientas de respaldo como servidores y nubes de información *(cloud computing)*, definitivamente no se utilizan. Es necesario distinguir el uso de servidores remotos, de los que se ubican al interior de la municipalidad (32% y 55% respectivamente), ya que en caso de incidentes como robos, incendios, inundaciones o terremotos, solo el servidor remoto constituye un real respaldo de la información.

Gráfico n°4. Tipos de soportes usados para respaldar la información a nivel municipal.

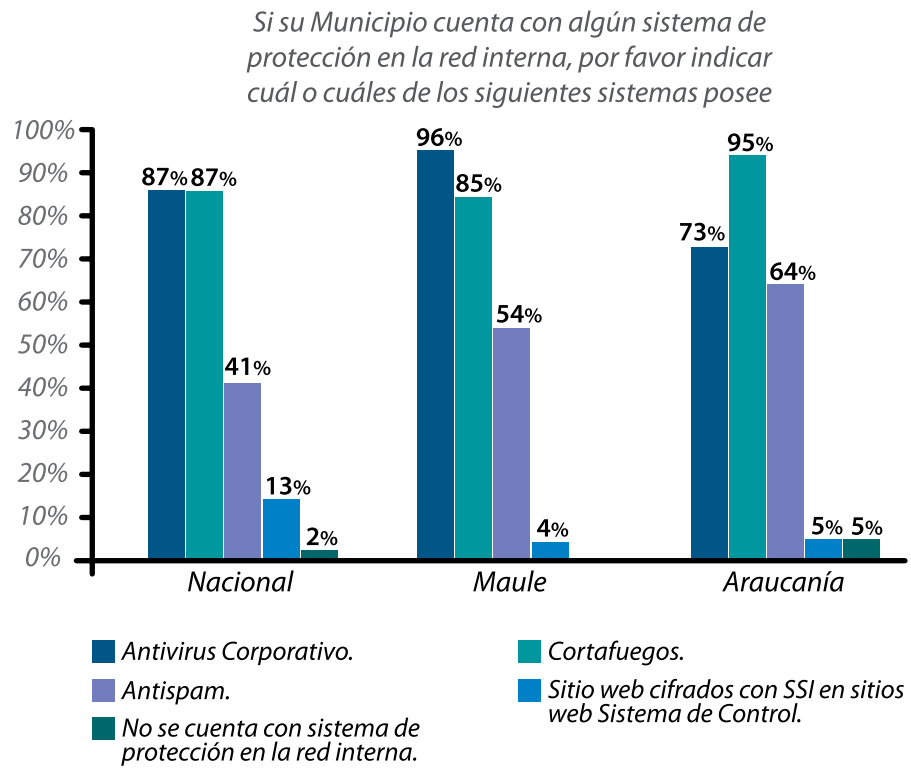


Fuente: Elaboración propia en base a ICHEM 2013.

En relación a la pérdida de información, solamente el 11% de las municipalidades ha sufrido pérdidas significativas (cifra que es prácticamente idéntica en las regiones del Maule, 12% y La Araucanía, 13%), lo cual se encontraría directamente relacionado a la escasa relevancia que se le da a la seguridad de la información.

Lo anterior dice relación con el extendido uso que hacen las municipalidades de sistemas de protección como el antivirus y el cortafuego, ya que el 87% de éstas usan alguno de esos tipos de protección, mientras que 2% no cuenta con ellos. Esto refleja confianza en los sistemas de protección interna en las municipalidades.

Gráfico n°5. Sistema de protección interna del sistema informático municipal.



Fuente: Elaboración propia en base a ICHEM 2013.

Sin embargo, y pese a que prácticamente todas las municipalidades tienen página web, solo un 13% declaró tener sistemas de protección de sus sitios web (sitio web cifrado con SSL).

Si se considera que las municipalidades en su mayoría realizan respaldos de información, éstas cuentan con sistemas de protección interna y registran una escasa cantidad de fallas de sistema informático. En ese marco, llama la atención que solo un 68% declare tener funcionarios dedicados a la seguridad informática. Este porcentaje es aún menor en La Araucanía, donde alcanza el 61%.

Asimismo, solamente un 57% de las municipalidades tiene una política de entrega y administración de contraseñas de resguardo de la información, y poco menos de la mitad (49%) tiene planes de continuidad para seguir funcionando ante fallas y pérdidas de información. Vale decir, si bien las municipalidades no muestran grandes pérdidas de información, una de cada dos no tiene planes de contingencia para enfrentar este tipo de situaciones y casi un tercio tampoco cuenta con funcionarios dedicados a la seguridad informática.

CONCLUSIONES

La instauración de las tecnologías de la información (TI) al servicio del ciudadano -vecino-, es un hecho y una necesidad que debe ser abordada con celeridad. Más aún si se considera que la realidad municipal -en relación al uso y desarrollo de las TI-, requiere una evolución que se ajuste a las demandas del ciudadano actual.

Hoy día los ciudadanos son demandantes de servicios de calidad, en un contexto de competencia entre municipios. Los ciudadanos buscan la mejor manera de satisfacer sus necesidades, demandando en el municipio A lo que no existe en el B, y buscando en C lo que no encuentra en A y B. Así, se establece una competencia entre los municipios, en una dinámica de movilidad de los servicios que apunta a la entrega de un servicio eficiente. Dicho servicio, hoy por hoy, se puede entregar o mejorar, en gran medida, mediante el apoyo tecnológico y su correcta gestión. Está comprobado que la inversión en tecnología a lo largo del tiempo, lleva al municipio a maximizar la participación ciudadana y a mejorar la calidad de la atención, si pone al centro de la atención al mismo ciudadano (Estéves, 2005).

Siendo los municipios instituciones eminentemente políticas, la necesidad de valorar los activos de información en la gestión municipal, es importante debido a su incidencia en las dimensiones política, económica y social. La entrega de un servicio deficiente afecta directamente la calidad de vida del ciudadano (valor social);

tiene repercusiones políticas cuando significa perder votos (valor político); y sin duda es relevante cada vez que se deja de percibir ingresos, por ejemplo, por recaudación de permisos de circulación (valor económico).

De esta forma, el rol de los municipios es fundamental para la ciudadanía; y sobre todo para el nuevo Ciudadano Inteligente, que posee expectativas y aspiraciones.

¿SSI: Cuestión de Recursos?

Ciertamente la adquisición de tecnologías está en función de los recursos que dispone el municipio. Acerca de este punto, no existe discusión sobre las enormes disparidades entre municipalidades, que se observa a nivel nacional. Sin embargo, esta lógica funciona en el acceso a las tecnologías en cuanto a volumen, infraestructura y recursos humanos; no así en la gestión ni aseguramiento de la información. Es decir, en términos de Gobierno electrónico, los municipios de mayores recursos llevan la delantera en la adquisición de tecnologías, pero no necesariamente gestionan de mejor manera la seguridad de la información.

De esta forma, un municipio con mayores recursos podría implementar servicios tales como pago en línea de Patentes Comerciales o Permiso de Circulación, pero si en momentos de alta demanda éstos estuvieran fuera de servicio, no servirán de nada. A nivel nacional no se registran diferencias entre municipios de mayores o menores recursos en relación con el respaldo de información o la existencia de Planes de Continuidad Operacional, ya que en este sentido el retraso municipal es generalizado.

SSI en las municipalidades de Chile

El que exista tanto la legislación como la normativa para la Gestión de la Seguridad de la Información, a la luz de los resultados de la encuesta, no parece ser un tema prioritario en la agenda municipal, ya que un 40% de los municipios no cumple con la normativa (DS N° 83) que exige entre los aspectos más importantes:

a) Un jefe de seguridad informático.
b) Un comité de seguridad.
c) Plan de Continuidad Operacional.

Lo anterior conlleva sanciones administrativas, a cargo de la Contraloría General de la República que, al parecer, son exiguas.

Si se considera que: un tercio de los municipios no cuenta con funcionarios dedicados a la seguridad informática; que el 41% afirma haber sido afectado por fallas de continuidad de servicio, lo que implica que en más de alguna oportunidad los servicios de alta demanda no se han logrado entregar, por falta de un Plan de Continuidad Operacional o construcción de SLA (Service Level Agreement) con un proveedor; y que el 48% de los municipios no cuenta con un plan que permita levantar los servicios de manera eficiente al momento de una caída de servidores o una falla de infraestructura; tiene sentido pensar que siendo un tema importante, no es prioritario. Esto ocurre aun cuando se ha complementado el DS N° 83 con

la norma chilena ISO 27001. Frente a la inexistencia de políticas de reacción, en caso de fallas, la herramienta más utilizada es la improvisación.

En relación a lo anterior, la mayor falencia es el desconocimiento de las obligaciones del municipio en relación a la ley. Se ignora, dentro de la misma institución, dónde se debe concentrar y administrar la información; ello, pese a que la mayoría declara que los respaldos se realizan de forma no centralizada pero bajo la responsabilidad de la Unidad de Informática. La ignorancia en este sentido, y por tanto, la falta de planificación, ponen en riesgo los datos de los ciudadanos, con lo que se corre el peligro de que disminuya cada vez más la credibilidad de la institución. Este hecho se complejiza al considerar que en muchos casos la provisión y administración de las TI se han externalizado, pasando a ser tema de la empresa que presta el servicio, en vez de la municipalidad que lo ofrece.

Al aumentar las exigencias en las prestaciones de servicio por parte del ciudadano, la empresa que asegura la disponibilidad de las TI busca optimizar el servicio, alejándose cada vez más del funcionario público para la atención del usuario. Las empresas gestionan y disponen las TI en función del usuario, pasando por alto un hecho crucial: "Las personas no son consumidores, son ciudadanos. Y la municipalidad no es una empresa" (Flores, 2012).

Tal como se lo mencionara más arriba, para enfrentar las amenazas se deben conocer y cuantificar sus impactos, pero, si no existe una valoración de la información no se enfrentarán las amenazas hasta que éstas sean un problema inminente. Con tal nivel de exposición a las amenazas, aumenta el foco en los respaldos de información. De lo que se puede deducir que no existe una comprensión real de este procedimiento, ni se asimila el trasfondo de la acción de respaldar o la necesidad de contar con un plan de acción en caso de alguna eventualidad. Siendo Chile un país amenazado contantemente por fenómenos naturales de diversa índole, no se comprende la indiferencia hacia tener una alternativa real en caso de desastres.

En términos de procedimientos, solo el 30% de los municipios realiza un respaldo de forma correcta, es decir, separa la información que existe en el municipio y la ubica afuera, en un servidor externo. La mayoría de los municipios no está cumpliendo con la norma básica de respaldar la información en zona segura. A pesar de la importancia que reviste el tema, menos del 5% de las municipalidades realizan un respaldo centralizado de estaciones de trabajo.

Contar con respaldos adecuados, tampoco es un tema de recursos, ya que existe tecnología de bajo costo que permite almacenar información de toda las operaciones municipales, a través de herramientas que permiten realizar estos procedimientos de forma automática y sin requerir esfuerzos mayores de las estaciones de trabajo.

Queda de manifiesto que lo esencial es destinar el tiempo necesario para la implementación de un Plan de Continuidad Operacional y con ello adoptar una correcta evaluación de riesgos, que permita mantener un sistema de respaldo adecuado a la valoración de los activos de información que mantiene el municipio.

RECOMENDACIONES

Tal como se ha desarrollado a lo largo del artículo, la importancia del uso de las TI como herramienta al servicio municipal, es fundamental. Sin embargo, se requiere un manejo adecuado de la información, a partir de la valorización de la misma.

Que dicha información se encuentre íntegra, confidencial, y disponible para los procesos institucionales relevantes, y que junto a ello se asegure la continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información, es el foco de la labor municipal en este ámbito.

Entender la labor municipal en el contexto actual, es el paso previo para revitalizar la institución. Ello se puede lograr a través de: una inducción al tema; realización de capacitaciones adecuadas a los funcionarios; asignando responsabilidades claras y específicas; elaboración de un plan estratégico –que incluya el aspecto comunicacional- acerca de las amenazas a las que están expuestas las TI y los protocolos de reacción; y con sistemas preventivos estables, que permitan la continuidad operativa en todo momento de los servicios TI.

Fortalecer la imagen municipal es una tarea que implica la puesta en valor de ésta como institución y de los servicios que presta a la comunidad. Para potenciar la imagen municipal se requiere, por una parte, dar valor agregado a la experiencia municipal; y por otra, instaurar y fomentar en sus habitantes, el sentido de territorialidad y empoderamiento del espacio habitado. En este sentido, las TI en cuanto herramientas al servicio municipal, colaboran en gran medida, si se encuentran correctamente gestionadas.

REFERENCIAS

Bologna, J. & Walsh, A. M. (1997). The Accountant´s Handbook of Information Technology. New Jersey: John Wiley and Sons.

Cetiuc. (2010). Niveles de digitalización en los Municipios 2008-2010. Centro de Estudios de Tecnologías de la Información. Descargado el 28 de marzo de 2013, de: http://www.cetiuc.cl/estudios/otros

Dipres. (2012). Guía metodológica 2012. Programa de mejoramiento de la gestión y Metas de eficiencia institucional - Sistema de seguridad de la información. Dirección de Presupuestos, Ministerio de Hacienda. Santiago de Chile.

Dipres. (2012b). Documento Técnico: Programa de Mejoramiento de la Gestión (PMG). Año 2012. Programa Marco Básico. Dirección de Presupuestos, Ministerio de Hacienda. Santiago de Chile.

Estéves, José (2005). "Análisis del desarrollo del gobierno electrónico municipal en España. En IE Working Paper, 29 de noviembre de 2005. Consultado el 16 de marzo de 2013, disponible en http://latienda.ie.edu/working_papers_economia/WPE05-32.pdf

Flores, D. (2012). ¿Gerencia o Gobierno?: Lecciones de las municipales. La Segunda Digital, 31 de octubre de 2012. Descargado el 28 de marzo de 2013, de http://www.la2da.cl/Pages/NewsDetail.aspx?dt=2012-10-31&PaginaId=11&bodyid=0

ICHEM. (2006). "Aplicación de las tecnologías de la información en los municipios chilenos; Propuestas para estudiar su aplicación en el ámbito de la Reforma Municipal", Santiago: ICHEM.

ICHEM (2013). Estudio Nacional sobre Seguridad Informática y respaldo de la Información en las Municipalidades Chilenas, Santiago: ICHEM.

INAP. (2012). Instituto de Asuntos Públicos y Asociación Chilena de Municipalidades firman convenio de colaboración. Instituto de Asuntos Públicos, Universidad de Chile,13 de diciembre de 2012. Descargado el 27 de marzo de 2013, de: http://www.uchile.cl/noticias/87646/inap-capacitara-a-funcionarios-municipales-para-mejor-atencion

Pahlka, J. (2012). Coding a better government. Using IT to Establish an Automated and Transparent Governance System. TED Coversations, Marzo de 2012. Recuperado el 20 de marzo de 2013, de: http://www.ted.com/talks/jennifer_pahlka_coding_a_better_government.html

Subdere. (2008). Presidenta recibió a alcaldes de todo el país en La Moneda. Subsecretaría de Desarrollo Regional, Ministerio del Interior, 12 de diciembre de 2012. Descargado el 28 de marzo de 2013, de: http://www.subdere.gov.cl/sala-de-prensa/presidenta-recibi%C3%B3-alcaldes-de-todo-el-pa%C3%ADs-en-la-moneda