20 de febrero de 2017

AIMC-014-2017

Licenciado
Edgar Mora Altamirano
Alcalde Municipal
Municipalidad de Curridabat

Estimado señor:

Asunto: Remisión del Informe AM-007-2016 "Valoración del marco de seguridad de información"

Para que proceda como corresponde se remite el Informe AM-007-2016, preparado por esta Auditoria, en el cual se consignan los resultados del estudio denominado "Valoración del marco de seguridad de información"

Cordialmente,

Original Firmado
Lic. Gonzalo Chacón Ch.
Auditor Interno

X

Municipalidad de Curridabat
ALCALDÍA MUNICIPAL
21 FEB 2017
RECIBIDO POR
24 p

Gonzalo Chacón Chacón
Auditor Interno

Adjunto: Lo indicado

C.c. Archivo
Copiador

20 de febrero de 2017

AIMC-015-2017

Señores
Concejo Municipal
Municipalidad de Curridabat

Estimados señores:

Asunto: Remisión del Informe AM-007-2016 "Valoración del marco de seguridad de información"

Para que se proceda como corresponde se remite el Informe AM-007-2016, preparado por esta Auditoria, en el cual se consignan los resultados del estudio denominado "Valoración del marco de seguridad de información"

Cordialmente,

Original Firmado
Lic. Gonzalo Chacón Ch.
Auditor Interno

X

Gonzalo Chacón Chacón
Auditor Interno

Adjunto: Lo indicado

C.c. Archivo
Copiador

Tel: 2216-5350 - Fax:(506)2272-0367 - Apdo. 17-2300 - e-mail: gonzalo.chacon@curridabat.go.cr

Auditoría Interna

Un servicio profesional comprometido con la objetividad y el servicio al cliente

MUNICIPALIDAD DE CURRIDABAT

INFORME AM-007-2016

Valoración del marco de seguridad de información

Realizado por:

MATI Wilber Ramírez Vindas

Supervisado por:

Lic. Gonzalo Chacón Chacón

Febrero 2017

INFORME DE AUDITORÍA

Valoración del marco de seguridad de información

Contenido

RESUMEN EJECUTIVO

Estudio - Valoración del Marco de Seguridad de Información

¿Qué se examinó?

En cumplimiento del plan anual de trabajo de la Auditoría para el período 2016, se realizó el estudio denominado "Valoración del Marco de Seguridad de Información", con el objetivo de evaluar el avance de implementación y puesta en marcha de los Procedimientos para el Marco de Seguridad Informática.

El estudio se realizó con el objetivo de determinar la naturaleza y alcance del Marco de Seguridad Informática (MSI) MC-SOP-011 versión 1.2 con fecha de emisión 29/02/2012 y su implementación en el periodo del estudio que abarca del 1 de enero de 2015 hasta el 31 de diciembre de 2015, periodo que se extendió cuando fue necesario considerar elementos más recientes.

Por la importancia que reviste para la institución y su relación directa con un el MSI se analizó la consideración de la Ley de Archivo (Ley 7202) y su direccionamiento, el contexto del Sistema de Control Interno en que se emite y opera el MSI y las condiciones de Gobierno que lo validan y sustentan; también se considera el esfuerzo de implementación y las inversiones realizadas que derivan de la implementación de dicho marco.

¿Por qué es importante?

La seguridad de la información y sus formas de presentación y representación constituye un elemento primordial para la organización y el MSI es el control directivo que direcciona su protección y aseguramiento.

La efectividad del control y los controles derivados depende del contexto institucional en que se articula, del esfuerzo de implementación y la forma en que integra los requerimientos de cumplimiento normativo y los elementos que tales normativas procuran proteger.

¿Qué se encontró?

Se encontró que el MSI no direcciona los aspectos relativos a gestión documental, firma digital y protección de la información en soporte digital, así como la gestión de los riesgos inherentes a tales actividades y el riesgo tecnológico. El instrumento requiere un

esfuerzo de actualización, mejora estructural e implementación supervisada que le permita evolucionar y mejorar producto de su aplicación práctica. El MSI debe direccionar aspectos relevantes de cumplimiento normativo -intencional-, de lo indicado por la CGR, la Ley de Archivo y la Ley General de Control Interno.

El MSI requiere estar sustentado en algún modelo de gestión de tecnologías de información (TI) que le sirva de referente metodológico y práctico (que le aporte estructura, conceptualización y prácticas de referencia).

La dinámica de control interno encontrada no favorece la adopción del MSI y el MSI no integra la perspectiva de control interno en su diseño, estructura e intención.

La gestión de la función de TI requiere intencionalidad y el Departamento de TI, apoyo para orientar su madurez y participación estratégica en la actividad sustantiva institucional.

¿Qué sigue?

Con el propósito de concretar oportunidades de mejora, se emiten recomendaciones para que el Alcalde Municipal genere las directrices de Gobierno de TI en materia de *Aseguramiento del Valor de TI, Riesgo Tecnológico, Seguridad de la Información y Gestión Documental.* Con estas directrices se recomienda a la Función de TI rediseñar el Marco de Seguridad de la Información, cuidando tanto la estructura y jerarquía de los controles –forma- como el direccionamiento de los aspectos relevantes y la integración de participantes clave –fondo-.

La implementación del MSI rediseñado requiere, sin embargo, que el Sistema de Control Interno (SCI) y el Sistema Específico de Valoración de Riesgo Institucional por lo que se recomienda a la Administración Superior dinamizar ambos sistemas.

1. *INTRODUCCIÓN*

El presente estudio se realiza de conformidad con las potestades que confiere el artículo N° 22 de la Ley General de Control Interno N°8292.

Lo que se persigue con el estudio es constatar la idoneidad del control directivo denominado "Marco de Seguridad Informática MC-SOP-011 versión 1.2" para direccionar la protección de la información, su impacto en el Sistema de Control Interno y el esfuerzo de implementación.

Siendo un control de alto nivel el "Marco de Seguridad Informática MC-SOP-011 versión 1.2" debe estar contextualizado en directrices, pronunciamientos y políticas de alcance institucional que orientan en materia de Tecnología de Información, Seguridad de la Información, Gestión Documental, Gestión de Riesgos y el cumplimiento normativo interno y externo.

1.1. Origen

Este estudio es de carácter tecnológico y se realizó de conformidad con lo señalado en el Plan Anual de Auditoría para el año 2016 el cual ha sido puesto en conocimiento del Concejo Municipal y comunicado a la Contraloría General de la República.

El estudio se realizó con fundamento en las competencias que le confieren a esta Auditoría Interna el artículo 22 de la Ley General de Control Interno.

1.2. Objetivo

El objetivo general del estudio consistió en valorar el Marco de Seguridad de Información (MSI), el grado de adopción de los controles indicados y la efectividad general de los mismos

Asimismo, se consideraron los siguientes objetivos relacionados:

a) Validación del cumplimiento de lo dispuesto por la Ley de Archivo y su reglamento, así como las directrices relacionadas respecto de las implicaciones en la seguridad de la información.

b) Consideraciones relativas al Sistema de Control Interno y la Implementación del MSI

c) Validación formal (según normativa y marcos referenciales) del Marco de Seguridad de Información (MSI) y sus componentes.

d) El gobierno de la función de TI

e) Análisis de las contrataciones, inversiones y adquisiciones en términos de cumplimiento de lo indicado en el MSI.

1.3. Alcance

El alcance del estudio comprendió la verificación del Marco de Seguridad Informática en la perspectiva de control directivo de alto nivel y su contexto, así como el esfuerzo de implementación o continuidad de la implementación (revisión del marco y su efectividad) para el periodo comprendido entre 1 de enero de 2015 hasta el 31 de diciembre de 2015.

El alcance comprendió, asimismo:

-El esfuerzo de implementación

-El marco (MSI) en la perspectiva de control y su anclaje en controles de nivel superior.

-Cumplimiento o atención de normativa vigente (Ley de archivo, Ley General de Control Interno, Ley de Firma Digital, entre otras).

-Contexto interno en materia de control interno (SCI) y SEVRI.

El estudio de Auditoría se ejecutó de conformidad con las "Normas para el Ejercicio de Auditoría Interna en el Sector Público" dictadas por la Contraloría General de la República (Resolución R-DC-119-2009)" y el "Normas Generales de Auditoría para el Sector Público (M-R-DC-64-2014).

1.4. Responsabilidad de la Administración y la Auditoría

La veracidad y exactitud de la información en la que se basó esta Auditoria para llegar a los resultados obtenidos en el presente informe, es responsabilidad de la Administración Activa.

La responsabilidad de esta Auditoría consiste en emitir una opinión sobre la efectividad del control denominado Marco de Seguridad Informática como control directivo en materia de Seguridad de la Información, su contexto como control de alto nivel, el direccionamiento de aspectos de cumplimiento, responsabilidades y responsables; así como el esfuerzo de implementación y articulación en sistemas activos tales como el Sistema de Control Interno y Sistema de Valoración de Riesgos.

1.5. Regulaciones de Control Interno

Las recomendaciones que derivan del presente estudio, deberán ser atendidas de conformidad con las regulaciones de la Ley General de Control Interno N° 8292, artículos 10, 12, 36, 37, 38 y 39 del 31 de julio de 2002.

1.6. Limitaciones al alcance

No se presentaron limitaciones durante el desarrollo del presente estudio.

1.7. Metodología Aplicada

El enfoque de análisis incluyó la revisión del contexto del control directivo "Marco de Seguridad de Información", esto es la forma en que se inserta en el Sistema de Control Interno y los controles de alto nivel que lo sustentan. Posteriormente se analizan los elementos que un control de esta naturaleza debe considerar: cumplimiento normativo, integración del esfuerzo de los responsables y sus responsabilidades y los controles derivados –necesarios para su implementación-.

Se analizó luego el Control Directivo en sí, esto es la estructura, el direccionamiento de los aspectos relevantes, el cumplimiento de los objetivos propuestos y las directrices de revisión estipuladas. En este análisis se incluye la consideración de lo indicado –en materia de seguridad- por las *Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)* emitidas por la Contraloría General de la República.

Por último, se revisaron las inversiones realizadas en el año 2015 a fin de determinar alguna relación con el Marco de Seguridad de Información o con algún esfuerzo identificable de implementación; sin embargo, se determinó que solo corresponden a

esfuerzos tendientes a mantener la infraestructura y atender requerimientos generales no asociados con el Marco.

1.8. Comunicación de Resultados

El pasado 13 de febrero de 2017, la Auditoría Interna, mediante una reunión denominada "conferencia final" dio a conocer a la Alcaldía y al encargado del departamento de Tecnología de Información, funcionarios de la Administración, los resultados a los cuales se llegó en el desarrollo del estudio, así como las conclusiones y las recomendaciones que a criterio de esta Auditoría deberían girarse.

Tomando en consideración que los funcionarios antes mencionados avalaron lo expuesto, se sometió a consenso los plazos de cumplimiento de las referidas recomendaciones.

Se confeccionó además un documento denominado "Acta de Validación" en el cual se detallan los principales aspectos del estudio y los plazos de cumplimiento de las recomendaciones acordados.

Por parte de la Auditoría expusieron el presente informe Wilber Ramírez V., Auditor Analista y Lic. Gonzalo Chacón Chacón, Auditor Interno.

2. RESULTADOS

A continuación, se presentan los resultados del estudio de auditoría. Asimismo, con fundamento en los resultados obtenidos, así como en las potestades conferidas en la Ley General de Control Interno artículos 12 inciso c) y artículo 36, se emiten recomendaciones a la entidad auditada, en virtud de las circunstancias encontradas, para mejorar los controles internos, la eficiencia operativa y los resultados institucionales en cada uno de los resultados en que aplique.

2.1 Gestión documental y protección de la información

De un control de alto nivel -como el Marco de Seguridad Informática- se espera un claro direccionamiento de los aspectos normativos tales como gestión documental (Archivo), firma digital, simplificación de trámites, y protección frente al tratamiento de los datos personales. También se espera la atención de los temas de fondo de estas

regulaciones. Sin embargo, para cumplir esta expectativa dicho control requiere que estén, previamente definidos, controles directivos (políticas, directrices, etc.), los cuales –en el alcance de este estudio- y según la información aportada, se concluye que no han sido desarrollados. Resultado, entonces, que los controles derivados y el direccionamiento de los procesos, carecen de asidero en el Sistema de Control Interno y de los elementos de gobernanza necesarios.

El análisis del *Marco de Seguridad Informática* y la *Directriz para el uso de Internet y Correo Electrónico* en su versión 1.2, permite concluir que este control directivo carece de asidero formal, en controles de alto nivel, que direccionen los aspectos relativos a:

1. Generación de valor en el uso de Tecnología de Información (lo que la Municipalidad espera de este recurso crítico, en términos de visión de largo plazo y estrategia).
2. Seguridad de la información, esto es la naturaleza de la información que se recibe, procesa, resguarda y descarta; así como la intención de la administración en términos de su protección.
3. La gestión documental interna, esto es, la atención de un proceso transversal a la actividad sustantiva y los procesos de apoyo, a la vez que su orquestación en tecnología de información.
4. La atención formal al documento en soporte digital y su validez como elemento de gestión y trámite.
5. Atención a los lineamientos respecto de la reducción del exceso de requisitos y trámites, esto es, la oportunidad del análisis de simplificación de procesos. En particular de aquellos que habilitan los servicios al munícipe y el apoyo tecnológico requerido.
6. La restante normativa que tiene impacto en los procesos y los servicios tecnológicos tales como la normativa y directrices emitidas por la Contraloría General de la República.
7. Los riesgos inherentes a todos estos aspectos y en particular, el riesgo tecnológico.

En este contexto la Función de TI no logra direccionar los aspectos relativos a Gestión Documental, tales como firma digital y protección de la información en soporte digital.

Los ***trámites*** -flujos de trabajo para la atención del munícipe- generan una serie de documentos que se agrupan en ***expedientes***, en este punto no es posible determinar los elementos que garanticen la salvaguarda de la información –de los expedientes-, ante la ausencia de una definición concreta de responsabilidades y de los responsables; lo que no permite clarificar el proceso, su articulación institucional y los requerimientos de soporte tecnológico.

Se procuró determinar a los involucrados, sus responsabilidades y los requerimientos en materia de TI; sin embargo, los principales involucrados –Centro de Información y Documentación, Plataforma de Servicios, Departamento de TI- no están suficientemente separados en términos de sus funciones y del espacio físico- toda vez que no se tiene una clara integración alrededor de una visión común, respecto de la importancia de la Gestión Documental Institucional.

Si bien se direcciona el cumplimiento –transaccional- con Archivo Nacional y sus requerimientos, la Gestión Documental -y su concepción como proceso transversal- requiere definición y formalización, así como protagonismo y empoderamiento, que se traduzca en espacio de maniobra para los responsables directos.

En el MSI no se atiende los temas relativos a Ley de Archivo (las implicaciones a lo interno), y la Gestión Documental, en tanto no disponen de un marco de gestión claro -con asignación de responsabilidades y responsables concretos- y los controles directivos que garanticen la gestión interna de documentación, trámites y archivos de gestión.

La atención a la normativa en relación con la Gestión Documental (Archivo), Firma Digital, Simplificación de Trámites y Protección frente al tratamiento de los datos personales, requiere la definición a lo interno de los mecanismos de direccionamiento formal en términos de la dirección, el alcance, las responsabilidades y los responsables. Las siguientes son las directrices que requieren atención en esta materia, a saber:

Archivo y Gestión documental.

La Seguridad de la Información tiene diferentes perspectivas y una de ellas es la ***protección del documento*** –en soporte físico o digital- en este sentido la Ley 7202 – artículo 39- y su reglamento, apuntan a la definición de un proceso interno de Gestión Documental que garantice –razonablemente- la protección de la información.

El artículo 60, de la ley antes citada, establece el rol de coordinación -del Archivo Central Institucional- tanto a lo interno como hacia la organización, asegurando que se generan y establecen los lineamientos de gestión acordes al contexto particular. La separación de los archivos de gestión y del archivo central se establece en el artículo 62 del reglamento a la Ley 7202.

Subyace en la ley 7202 y su reglamento la definición de un proceso de ***trámite*** que corresponde a los servicios prestados al munícipe por parte de la Municipalidad y que requieren atención expedita (y, por tanto, una oportunidad en materia de simplificación de trámites). Este proceso genera un volumen significativo de documentos, cuya agrupación conforma un expediente; este periodo de pre-archivalía, en que el

documento se construye con soporte digital y luego se convierte en documento físico -para agregar evidencia de recibo- es una etapa crítica, tanto por la importancia operativa del documento como por su mutabilidad, según evoluciona el trámite. Es en esta etapa en que el soporte tecnológico cumple su función primordial de resguardo, archivo y respaldo y es susceptible al análisis en procura de simplificación del trámite.

Firma digital

En su fase de documento digital el ***documento*** tiene igual valor que el documento físico y la firma digital tiene igual validez que la física (rúbrica); así establecido por la ley 8454 (30 de agosto de 2005) –artículo 3-. Esta condición evita la impresión y conversión del documento a un formato que soporte la rúbrica, sello y marcas de tiempo.

Sobre este tenor se pronuncia la Directriz 29-2007 del 14/11/2007 emitida por la Junta Administrativa del Archivo Nacional la cual regula la gestión de artefactos documentales en formato digital y su tratamiento, así como la coordinación entre los responsables de los distintos medios de representación (soporte) de la información institucional. El *Apartado I,* incisos 2 y 3, en Materia de Gestión de Documentos estipulan:

> 2) Debe existir una coordinación interdisciplinaria entre los archivistas, administradores e informáticos, en el diseño y desarrollo de aplicaciones informáticas que respondan a necesidades reales de información.
>
> 3) Los responsables en materia de gestión documental deben:
>
> a) Establecer las políticas y los procedimientos institucionales para la creación, organización, utilización y conservación de los documentos en soporte electrónico, y estas deben ser de acatamiento obligatorio;
>
> b) Regular el uso del correo electrónico y de otras herramientas informáticas, de acuerdo con las políticas y los procedimientos institucionales para la creación, organización, utilización y conservación de los documentos.

La gestión de la seguridad de la información en términos de confidencialidad, integridad y disponibilidad suponen, adicionalmente, requerimientos especiales de archivo (conservación), formalidad (niveles) y responsabilidad (definición de responsables: propiedad, tratamiento informático, etc.)

Simplificación de trámites

En este sentido la ley 8220 - *Ley de protección al ciudadano del exceso de requisitos y trámites administrativos*- direcciona la importancia de mantener un proceso formal de análisis que evidencia la oportunidad de simplificación. También direcciona lo relativo a la gestión de la información (coordinación institucional e inter institucional,

artículo 8) y la definición del trámite (hoja de control, código de acceso y seguimiento -artículo 5-). Estos criterios aplican a la creación y mantenimiento de los servicios y sistemas de información y su funcionamiento integrado y conectado con otras entidades gubernamentales.

Tratamiento de datos personales

Respecto de la *Protección de la persona frente a al tratamiento de sus datos personales,* según se consigna en la Ley 8454, artículo 10 refuerza la responsabilidad de la gestión adecuada de las bases de datos -la definición de medidas organizacionales, técnicas y físicas- para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a dicha ley.

Innovación y desarrollo tecnológico

En lo relativo al soporte de los procesos institucionales en servicios tecnológicos, se debe mantener una perspectiva de mejora continua y de innovación, consignado en la Ley 7169 –Ley de promoción del desarrollo científico y tecnológico. En particular el artículo 4, inciso K establece: "Impulsar la incorporación selectiva de la tecnología moderna en la administración pública, a fin de agilizar y actualizar permanentemente los servicios públicos, en el marco de una reforma administrativa, para lograr la modernización del aparato estatal costarricense, en procura de mejores niveles de eficiencia."

Gobernanza de TI y Riesgos

Según el artículo 17 del Código Municipal y el Manual Básico de Organización y Funcionamiento [29/02/2012], corresponde al Alcalde Municipal (titular de la Alcaldía Municipal) "Instaurar los manuales de organización, de clases de puestos, de evaluación del desempeño y cualquier otro para el buen desarrollo de la organización..."

La gestión de riesgos de nivel institucional, a cargo de la Contraloría de Servicios y un Comité de Riesgos Institucional -según el Reglamento de Control Interno (LA GACETA Nro. 55 del 19 de marzo de 2014)-, que establece la creación de una Comisión de Control Interno (CECI) con sesiones de trabajo al menos mensuales y la generación de directrices para mejorar el SCI; un proceso de autoevaluación anual (con el requerido soporte documental) y la definición de medidas correctivas y preventivas; la definición de una Guía de Autoevaluación y su registro formal (documental, archivo); y, la implementación de un Sistema Específico de Valoración del Riesgo (igual al CECI).

No se tienen los controles directivos de alto nivel que atiendan los aspectos críticos (Gestión Documental, Firma Digital, Simplificación de Trámites y Protección frente al tratamiento de los datos personales, etc.). En este contexto la creación e implementación de un Marco de Seguridad Informática (MSI) resulta compleja y desarticulada, toda vez que dicho control no logra convertirse –en sí mismo- en una directriz integradora del esfuerzo de gobernanza y atender aspectos específicos. En ese sentido el control se debate en la pretensión de direccionar aspectos de alto nivel de abstracción y las especificidades de la delimitación de operaciones concretas.

A falta de dirección –gobierno- de la función de TI, la gestión documental y la seguridad de la información, cada responsable directo se acoge a su criterio, visión y perspectiva de cumplimiento normativo inmediato según su mejor intención. Los involucrados indirectos a falta de definición de responsabilidades se involucran al mínimo.

En este escenario se crea el MSI –una excelente intención con limitada capacidad de impactar y modelar la cultura organizacional-, sin un plan de implementación que permita monitorear su adopción y asegurar su madurez en el tiempo, en primera instancia por falta de asidero en la gobernanza intencional y en segunda, a falta de estructura, profundidad y manejo del nivel de abstracción del discurso según los aspectos direccionados.

La Gestión Documental (Centro de Información y Documentación), por su parte, procura el cumplimiento de sus responsabilidades inmediatas y la salvaguarda de la documentación, en un escenario de protagonismo y convocatoria muy reducido.

2.2 El MSI requiere un esfuerzo de actualización

La revisión detallada del MSI permitió determinar que éste carece de anclaje en controles directivos que orienten y definan la gobernanza de TI (Política de TI institucional, Política de Gestión de Riesgos, Sistema de Control Interno, Sistema de Gestión Documental, etc.). El control en sí mismo no puede atender ese direccionamiento y aportar controles detallados.

El MSI no aporta controles derivados cuyo detalle facilite una implementación operativa adecuada de los controles. La implementación e impacto no es observable en el tiempo, a falta de planificación y objetivos concretos –medibles y con trazabilidad hacia esfuerzos definidos-. En pocos casos se encontró que los controles y su impacto resultan observables directamente en la práctica.

El MSI no cuenta con un plan de implementación intencional con ejercicios de difusión y divulgación medibles o mecanismos de supervisión y monitoreo de su aplicación.

El objetivo general –esbozado en el documento mismo- "*Ser un lineamiento organizacional para concientizar a cada uno de sus miembros sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la entidad*" y los objetivos específicos no se concretan con la implementación del MSI, lo que le resta valor como instrumento de gestión, fiscalización y fortalecimiento de la cultura de protección a la información en la Institución.

El MSI debe direccionar los elementos requeridos por la ***Norma 1.4 Gestión de la Seguridad de la Información***, De las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE). Se espera que dicho instrumento indique, al menos:

a) El propósito del Marco de Control en términos de gobernanza e intención de la administración superior.
b) El alcance del Marco -institucional-
c) Las expectativas de la administración en términos de la intención del control (lo que necesita ser controlado y porqué)
d) Roles y responsabilidades (institucional) y
e) Las metodologías, marcos referenciales, normativas aplicables
f) El cumplimiento normativo externo e interno.

El referente directamente relacionado –en términos normativos- que constituye un criterio de valoración, son las Normas técnicas para la gestión y el control de las tecnologías de Información (N-2-2007-CO-DFOE) en particular las siguientes normas:

Capítulo I Normas de aplicación general

1.1 Marco estratégico de TI

1.3 Gestión de riesgos

1.4 Gestión de la seguridad de la información

1.4.1 Implementación de un marco de seguridad de la información

1.4.2 Compromiso del personal con la seguridad de la información

1.4.3 Seguridad física y ambiental

1.4.4 Seguridad en las operaciones y comunicaciones

1.4.5 Control de acceso

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura. 1.4.7 Continuidad de los servicios de TI

Capítulo III Implementación de tecnologías de información

3.1 Consideraciones generales de la implementación de TI.

Las normas proponen una estructura -y niveles de granularidad de los controles- intencional, de forma que una definición integral de la estrategia de TI permite contextualizar la gestión de riegos y ambos marcos permiten articular la gestión de la seguridad en detalle (ítem 1.4) el ítem 3.1 apoya las consideraciones de implementación.

Esta condición particular del MSI es causada por la necesidad coyuntural de regular y fiscalizar aspectos operativos y transaccionales relacionados con la gestión de los recursos informáticos –correo, contraseñas, dispositivos de almacenamiento- y limitar el uso del servicio de navegación web y acceso a redes sociales. Sin embargo, en el discurso y la redacción del instrumento se deja entrever la pretensión de ser un control directivo de mayor nivel.

Las condiciones analizadas tienen el efecto de restar efectividad al control directivo, resultando que:

- El MSI direcciona aspectos concretos y deja el vacío sobre aspectos relevantes de cumplimiento normativo, definición de responsabilidades, coordinación de las actividades entre los principales interesados, gestión de riesgos y dirección de TI.
- El MSI no formaliza el cumplimiento específico de *Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)* pero deja la impresión de atender el tema y cierra el espacio de discusión para esfuerzos e iniciativas en esta dirección.
- La Función de TI no dispone de un instrumento normativo que le permita ajustar sus propios controles (reglamentos, metodologías, procedimientos, operaciones, etc.) y prácticas de gestión (gestión basada en servicios, contingencia y continuidad).

2.3 Dinámica de Control Interno

La dinámica de Control Interno encontrada no favorece la adopción del MSI y el MSI no integra la perspectiva de Control Interno en su diseño y estructura.

Entendido el Sistema de Control Interno (SCI) como una "*serie de acciones ejecutadas por la administración activa diseñadas para proporcionar seguridad en la consecución de los objetivos ...*" -y siendo que este sistema tiene alcance institucional- tal sistema y su dinámica son el contexto necesario para la definición de controles en una función crítica, como resulta ser, la función de TI.

Igual caso, asociado con el SCI, se encontró en la valoración del riesgo, que requiere un marco institucional contextualizado en el Sistema Específico de Valoración del Riesgo Institucional (SEVRI).

La sinergia y dinámica generada por ambos sistemas (Control Interno y Gestión de Riesgos) contextualizan el esfuerzo de asegurar la información. Este es el contexto en que se debe articular el Marco de Seguridad Informática (MSI).

Aunque se tiene claridad de los elementos de gestión más relevantes (jerárquicos y funcionales: Alcaldía y Finanzas) la participación de las áreas usuarias ocurre orgánicamente -como opuesto a intencionalmente- y las prioridades se discuten con la administración superior. La gestión del control interno ocurre como producto de la buena intención de la administración de TI, si bien no se direcciona su reforzamiento y la aplicación de prácticas sugeridas de control interno.

Según la Ley General de Control Interno N°8292 en el Artículo 8° "... se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos (...)" y, en el artículo 14:

> "En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:
>
> a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.
>
> b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.
>
> c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.

d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar."

Artículo 17" Entiéndase por seguimiento del sistema de control interno las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo".

Y artículo 18 "Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.

En el mismo tenor las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) la norma 1.1 indica "El jerarca y los titulares subordinados, según sus competencias, deben emprender las medidas pertinentes para contar con un SCI, conformado por una serie de acciones diseñadas y ejecutadas por la administración activa para proporcionar una seguridad razonable en la consecución de los objetivos organizacionales."

La norma 1.4 "La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias."

La norma 1.5 "Responsabilidad de los funcionarios sobre el SCI. De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de manera oportuna, efectiva y con observancia a las regulaciones aplicables, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI."

Bajo esta perspectiva el MSI debe referenciar, direccionar y agregar componentes a las diferentes dimensiones del SCI. Esto es, el ambiente de control se refuerza promoviendo e implementando prácticas deseadas y la cultura de seguridad de la información; la valoración del riesgo adquiere relevancia y la metodología específica para la Gestión del Riesgo Tecnológico se diseña considerando la gestión de riesgos institucional; las actividades de control son los controles específicos –o la mezcla de controles necesaria- para proteger los diferentes elementos críticos. Así la información fluye en los canales de comunicación y con el monitoreo oportuno el sistema se enriquece, madura y se fija en la cultura organizacional.

El escenario anterior se explica ante el hecho de que las actividades de monitoreo, del Sistema de Control Interno, no conducen a dinamizar los procesos de control y los

órganos de gobierno encargados -Comisión de Control Interno y SEVRI- han disminuido la periodicidad de sus sesiones de trabajo.

El hecho de no estar contextualizado en un Sistema de Control Interno dinámico y la necesidad coyuntural de fiscalizar elementos específicos de seguridad (de nivel operativo) conduce a diseñar un MSI que no se integra con dicho sistema y, por tanto, no direcciona la inserción del mismo en el sistema. A pesar de constituir un compendio de controles (directivos, operativos, preventivos) no se diseña ni se implementa en el contexto del Sistema de Control Interno y por tanto su intencionalidad sobre elementos específicos del ambiente de control interno no se direcciona apropiadamente, igual caso ocurre en lo relativo a la valoración del riesgo, actividades de control y monitoreo –componentes vitales del sistema de control interno-.

Lo anterior se explica por el hecho de que es la implementación del MSI el que, finalmente, impactará el ambiente de control; son las actividades de capacitación, promoción de mejores prácticas y concienciación de la importancia de la protección de la información las que conducirán a mejorar el ambiente de control y gestionar los riesgos. Sin embargo, el esfuerzo de implementación del MSI no es suficiente para generar cambios identificables atribuibles al MSI.

2.4 Intencionalidad en la Gestión de Tecnología de Información

El Departamento de TI no tiene el protagonismo y la convocatoria requerida para emitir un control directivo de alto nivel, sin el amparo de los elementos de gobierno (directrices, políticas, etc.), los órganos de gobierno (comités, comisiones, etc.), la dirección orientadora en la estrategia y gobernanza en materia de TI.

Sin embargo, en el contexto de sus atribuciones el departamento de TI elabora el Marco de Seguridad Informática; la Administración superior lo aprueba y emite la directriz para su cumplimiento en el año 2012, en oficio AMC-037-06-2012, el cual requiere el cumplimiento del control asociado "Reglamento para el uso del Correo Electrónico e Internet - Aprobado en oficio AMC-134-2012".

La Comisión de TI cumple un valioso papel en el seguimiento y monitoreo del gerenciamiento (administración) de TI. Sin embargo, -sin restar mérito a lo realizado hasta ahora- se pospone la atención de los temas de gobierno de TI y de aspectos relevantes (de mayor nivel de abstracción) y el pronunciamiento en temas de fondo tales como:

1. Responsabilidad de la Función de TI (institucional) y direccionar los aspectos de definición de responsabilidades de todas las áreas y niveles participantes (Administración Superior, Comisiones, Unidades funcionales, etc.)
2. Alineamiento estratégico con la actividad sustantiva y evolución hacia la prestación de servicios dejando atrás la perspectiva de unidad técnica de soporte.
3. Gestión de la adquisición oportuna, en tiempo y direccionada por los requerimientos futuros y -cada vez menos- por los requerimientos pasados o actuales (gestión oportuna de la capacidad).
4. Monitoreo del desempeño -de la participación en actividad sustantiva, de habilidades para participar y calidad del servicio prestado, creación de conocimiento y apropiación del conocimiento creado 'fuera' del ámbito institucional.
5. Cumplimiento de la legislación, normativa y regulaciones. La gestión de TI tiene un fuerte componente de fiscalización -del uso apropiado de TI y de las prácticas de seguridad y la gestión con terceros-.
6. Del comportamiento humano respecto de la tecnología -promoviendo el desarrollo humano, de competencias y condiciones individuales para movilizar la generación de valor en la orquestación tecnológica.
7. Gestión de los riesgos y el control Interno -dos aspectos críticos para la organización y que se 'ocultan' tras equipos y términos de la juerga tecnológica.

Estos aspectos requieren ser direccionados intencionalmente y con la perspectiva de futuro, de superación de la brecha respecto de un profundo entendimiento de las condiciones actuales.

Las estructuras de gobierno son críticas para apoyar a la función de TI, la Comisión de Informática que realiza una función de supervisión debe incorporar la perspectiva de fortalecimiento de la función de TI, de gestión de riesgos y de empoderamiento en la actividad sustantiva apoyando y proponiendo la innovación.

La administración superior -naturalmente- delega en el Departamento de TI la gestión de los asuntos relativos a la orquestación tecnológica. Así indicado por el Artículo 17, inciso b) del Código Municipal "Delegar las funciones encomendadas por esta ley…".

El departamento de TI por su parte recibe el mandato de la administración superior ratificado por el Manual Básico de Organización y Funcionamiento (Setiembre 2008), que define entre las actividades del Proceso de Servicios Informáticos la responsabilidad de "Coordinar y articular en forma adecuada y oportuna las políticas

municipales en materia de informática en conjunto con las áreas, unidades e instancias municipales".

Adicionalmente este documento le confiere atributos suficientes para emitir controles directivos de alcance institucional, -se indican solo las relevantes en este contexto-:

- Coordinar y articular en forma adecuada y oportuna las políticas municipales en materia de informática en conjunto con las áreas, unidades e instancias municipales.

- Investigación y avance tecnológico en estrategias de proyectos informáticos que afecten la gestión del negocio y la proyección del mismo.

- Informar e Involucrar a los usuarios sobre nuevas iniciativas y proyectos que involucren el uso de las tecnologías de información o en aquellos en las que la tecnología podría convertirse en una herramienta de utilidad y crecimiento.

- Informar, asesorar y recomendar lo pertinente sobre las reformas, modificaciones y avances en informática; sistemas y equipos de cómputo a los funcionarios de las áreas, unidades e instancias municipales.

Este espacio de maniobra resulta suficiente para realizar la gestión adecuada de TI toda vez que la coordinación con los restantes elementos de gobierno y la integración con la administración superior, siguen siendo vitales para concretar dicha gestión en procura de alinear su tarea con la visión institucional.

Esta situación se origina ante el hecho de que la gestión de la función de TI requiere intencionalidad y el Departamento de TI requiere apoyo para orientar su madurez y participación estratégica en la actividad sustantiva institucional. Si no se potencia al departamento y se desarrollan –intencionalmente- sus competencias se mantiene la tendencia al soporte, al apoyo a los procesos administrativos –más conocidos y normalizados- en detrimento del apoyo y contribución en la actividad sustantiva.

Cuando la función de TI no logra –a lo interno- apoyar los requerimientos de innovación tecnológica y la incorporación de dicha innovación en la generación de valor al munícipe; dicho proceso ocurre a lo externo de la institución –contratación externa, desarrollo externo. En tales casos el conocimiento generado debe integrarse rápidamente en el conjunto de habilidades del departamento y de ahí apoyar a los

procesos de negocio (principalmente de la actividad sustantiva). Esto es, incorporar en la institución el conocimiento generado, de forma que se entienda el alineamiento con la visión y la estrategia, el impacto en los procesos de negocio subyacentes y la forma en que la tecnología (aplicaciones e infraestructura) deben modificarse para incorporar la evolución tecnológica.

El efecto de generar innovación, desarrollo y conocimiento tecnológico fuera del contexto institucional es el aumento en el riesgo de no incorporarlo naturalmente en la institución y dinamizarla, de forma que se pierde la oportunidad de coadyuvar la madurez organizacional y sus estructuras orgánicas.

La consecuencia de integrar la innovación tecnológica -en la orquestación de los servicios al munícipe- por la vía de la tercerización del esfuerzo produce resultados rápidos y victorias que sirven de ejemplo sobre cómo hacer mejor las cosas. Estos resultados –el conocimiento generado- debe integrarse en los procesos institucionales, crear las habilidades pertinentes en la función de TI y promover la infraestructura y las herramientas de orquestación tecnológica requeridas. De otra forma el esfuerzo no obtiene asidero institucional -en la visión, misión, procesos, servicios tecnológicos, infraestructura y herramientas; en ese orden. El conocimiento se queda a lo externo, las capacidades generadas no logran integrarse en los procesos internos y la oportunidad de mejora se diluye en el tiempo y se pierde inevitablemente.

3. CONCLUSIÓN GENERAL

Este despacho considera que realizada la revisión del Marco de Seguridad Informática y su contexto al día 3 de febrero de 2017 los hallazgos, las debilidades de control interno y las condiciones de implementación de dicho control no permiten tener una seguridad razonable, respecto de la gobernanza de la seguridad de la información y la efectividad de los controles derivados.

Por lo tanto, la opinión general es que la gobernanza de tecnología de información y los controles directivos en materia de seguridad de la información requieren mejoras sustanciales.

4. RECOMENDACIONES

De conformidad con las competencias asignadas en el artículo 12 de la "Ley General de Control Interno, Nº 8292, que señala entre los deberes del jerarca y los titulares subordinados, analizar e implementar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan, se emiten las siguientes recomendaciones, las cuales deberán estar debidamente cumplidas en los plazos conferidos para tales efectos y que cuentan a partir de la fecha de recibo de este informe.

Para el cumplimiento de las recomendaciones, deberán dictarse lineamientos claros y específicos y designar puntualmente los responsables de ponerlos en práctica, por lo que estas instrucciones deberán emitirse por escrito y comunicarse formalmente, así como definir los plazos razonables para su implementación, de manera que la administración activa pueda establecer las responsabilidades respectivas en caso del no cumplimiento de éstas.

Además, el órgano o funcionario a quién se gira la recomendación es el responsable de su cumplimiento, por lo cual deberá realizar las acciones pertinentes para verificar que los funcionarios subordinados a quienes se designen su instauración, cumplan con lo ordenado dentro del plazo que se les otorgó.

Esta Auditoría se reserva la posibilidad de verificar, mediante los medios que considere pertinentes, la efectiva implementación de las recomendaciones emitidas, así como de valorar la aplicación de los procedimientos administrativos que correspondan, en caso de incumplimiento injustificado de tales recomendaciones.

4.1. Al Concejo Municipal

a) Dotar de los recursos necesarios para atender los requerimientos identificados en el presente informe.

4.2. A la Alcaldía Municipal

a) Remitir a este Despacho, en el plazo de quince días contados a partir de la fecha de recibo de ese documento, el cronograma de actividades para dar cumplimiento a cada una de las recomendaciones emitidas en el presente informe.

b) Para que un plazo de seis meses se formalicen los controles directivos que orienten –en términos estratégicos y de visión de largo plazo- y definan las

responsabilidades y los responsables, así como la implementación, monitoreo y control de los aspectos críticos que resultan insuficientemente direccionados por el Marco de Seguridad Informática, a saber:

- Generación de valor en el uso y adopción de Tecnología de Información.
- Seguridad de la información.
- El proceso de Gestión Documental como un proceso transversal a la actividad sustantiva y los procesos de apoyo, a la vez que su orquestación en Tecnología de Información.
- La atención formal al documento en soporte digital y su validez como elemento de gestión y trámite.
- Exceso de requisitos y trámites, esto es, la oportunidad del análisis de simplificación de procesos.
- La restante normativa que tiene impacto en los procesos y los servicios tecnológicos.
- Los riesgos inherentes a todos estos aspectos y, en particular, el riesgo tecnológico.

c) Para que, de forma inmediata, proceda a dinamizar –empoderar y dar seguimiento- al Sistema de Control Interno y al Sistema Específico de Valoración de Riesgos, de forma que estos coadyuven la gestión de TI y le aporten un marco de gestión integral e informar en un plazo de tres meses respecto de las gestiones realizadas y sus resultados.

d) Presentar el cronograma de implementación del MSI definiendo los mecanismos de monitoreo y control oportuno; en el contexto de la dinámica del Sistema de Control Interno a que se refiere el ítem c).

e) Para que de forma inmediata se determine en todos los esfuerzos de evolución tecnológica en curso (adquisición de tecnología, innovación tecnológica, desarrollo de nuevas capacidades basadas en tecnología, etc.) y se consigne como parte del proyecto o iniciativa:

- El alineamiento estratégico y la contribución a la generación de valor al munícipe y el cumplimiento de los objetivos institucionales.
- El impacto en los procesos institucionales– las modificaciones que requieren, las responsabilidades y la natural resistencia al cambio.
- las implicaciones en la orquestación tecnológica requerida (impacto en aplicaciones, infraestructura, competencias internas del departamento, y gestión de la información).
- Los mecanismos de transferencia del conocimiento y desarrollo de habilidades internas cuando se trate de esfuerzos con participación de terceros.

4.2 Al Departamento de Tecnología de Información

a) Para que en el plazo de tres meses posteriores al cumplimiento del ítem b) de las recomendaciones de este informe –dirigidas a la Alcaldía-, replantee el MSI de forma que esté contextualizado en tales directrices de alto nivel.

b) Para que paralelamente al ítem a) –anterior-, reformule el MSI cuidando su estructura, nivel de abstracción y el direccionamiento hacia los responsables institucionales de los requerimientos de participación y coordinación.

MATI. Wilber Ramírez Vindas
Auditor Analista

Lic. Gonzalo Chacón Chacón
Auditor Interno