MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

# MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD PARA LOS GADS (GOBIERNOS AUTONOMOS DESCENTRALIZADOS) MUNICIPALES DEL ECUADOR CON BASE EN EL SISTEMA DE GESTIÓN DE INFORMACIÓN

**Propuesta de artículo presentado como requisito para la obtención del título:**

## Magíster en Auditoría de Tecnologías de la Información


**Por la estudiante:**
**Ingrid Fabiola CHICA CISNEROS**

**Bajo la dirección de:**
**Francisco Jospeh BOLAÑOS BURGOS.**



**Universidad Espíritu Santo**
**Maestría en Auditoría de Tecnología de la Información**
**Samborondón - Ecuador**
**Febrero del 2017**

# *Modelo de Defensa en Profundidad para los GADS (Gobiernos Autónomos Descentralizados) Municipales del Ecuador con base al Sistema de Gestión de Información.*

Model of defense in depth to the GADS municipal (decentralized autonomous governments) of the Ecuador based on the system of information management.

**Ingrid Fabiola CHICA CISNEROS**[1]
**Francisco Jospeh BOLAÑOS BURGOS**[2]

Resumen

El impacto de la tecnología, ha incidido notablemente en los procesos administrativos de los GADs municipales; sin embargo este impacto trae consigo nuevas amenazas a la seguridad de la información. El presente trabajo derivado de una investigación basada en las normativas, como: ISO 27001 y estándares como COBIT e ITIL además de aspectos organizativos y de sensibilización, plantea a través de fases un modelo de seguridad que conjuga la planificación estratégica de TI y la sensibilización en seguridad de la información, aspectos necesarios para disponer de innovación tecnológica y seguridad de la información en los municipios. Las fases del modelo propuesto al incluir temas organizativos y de sensibilización permiten la realización de un análisis estratégico para identificar el diagnóstico de la situación actual del municipio permitiendo conocer los aspectos necesarios para brindar seguridad de la información. Es necesario recalcar que la sensibilización debe estar presente en todas las fases del modelo propuesto, para conocer la importancia de mantener la seguridad de la información y de todas las actividades de TI. El modelo presentado, no entrega documentos desarrollados como procedimientos e instructivos, sino que sirve como un medio de orientación específica para que los municipios planteen las políticas y procedimientos de TI que consideren necesarios, sobre la base de sus presupuestos y la sensibilización de seguridad que existe en cada uno de ellos. A partir de la investigación realizada, se puede concluir que el modelo de seguridad propuesto permite una evaluación integral de TI y su efecto en el ámbito municipal, que lo constituye en una herramienta para facilitar la toma de decisiones desde el contexto de la gestión tecnológica.

Palabras clave: Modelo de Seguridad, Defensa en Profundidad, Seguridad de Información, Modelo de Defensa.

Abstract

The impact of the technology, has EFECT notably in them processes administrative of the GADs municipal; However, this impact brings with it new threats to the security of the information. This work derived from a research based on regulations, such: ISO 27001 and standards such as COBIT and ITIL as well as organizational aspects and awareness, raises a security model that combines the strategic it planning and awareness in security of the information, necessary for technological innovation and security of the information in the municipalities through phases. Them phases of the model proposed to the include themes organizational and of awareness allow the realization of an analysis strategic for identify the diagnostic of the situation current of the municipality allowing know them aspects necessary to provide security of the information. It is necessary to stress that awareness must be present at all stages of the proposed model, to know the importance of maintaining the security of the information and the activities of TI. The presented model, does not deliver documents developed as procedures and instructions, but it serves as a means of targeting that municipalities have the policies and procedures of TI deemed necessary, on the basis of their budgets and awareness of security that exists in each one of them. From the research, it concluded that proposed security model allows for a comprehensive evaluation of TI and its effect on the municipal level, which is a tool to facilitate decision making from the context of the technological management.

Key words: Model of security, Defense in depth, Security of information, Model of Defense.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail ichica@uees.edu.ec.
[2] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

## INTRODUCCIÓN

Información, es todo un conjunto de datos que posea valor para una organización (ISO 27000, 2016). Desde esta perspectiva, las tecnologías de la Información y comunicación se han constituido en la principal herramienta para la realización de las operaciones institucionales; es así que en las empresas públicas la tecnología ha generado un cambio en la forma de hacer gobierno; no solo en la administración sino en la necesidad de contar con políticas, procedimientos y servicios en línea, que acerque al ciudadano con su municipio (Grande, Ramilo, & Salvador, 2002).

Existe, una creciente dependencia de la información, por lo tanto la ausencia de un recurso o sistema de información provoca perturbaciones en el entorno personal o laboral (Milicevic & Goeken, 2011). Lo que ha provocado un crecimiento continuo del papel de la seguridad de la información, considerada el activo más valioso de la era digital, lo que conlleva que está siempre deba estar disponible para el usuario, generando que las infraestructuras tecnológicas tengan obligatoriamente que protegerse contra ataques cada vez más sofisticados (Balcerek, Frankowski, Kwiecién, Smutnicki, & Teodorczyk, 2012).

El aseguramiento de esta información y de los sistemas que lo procesan, es el principal objetivo de cualquier organización (ISO 27000, 2016); sin embargo, cada vez surgen más amenazas a las que está expuesta la información, siendo necesaria su protección a través de mecanismos y medidas eficientes, que incluyan tecnología y aspectos organizativos y personal, siendo este último el más importante (Merino & Cañizares, 2014).

La protección de la información es independiente del lugar de almacenamiento y se debe garantizar la disponibilidad de los servicios, mejorar la productividad y asegurar la continuidad de los procesos municipales, de acuerdo a lo establecido en las normativas legales que rigen el sector público (Neetha & Chandrasekar, 2014). La incorporación de controles de seguridad es fundamental en estas instituciones (Groat, Tront, & Marchany, 2012)

May, Hammerstein, Mattson, & Rush (2006) describen que la seguridad implementada debe ser concebida por capas para ofrecer protección integral. Secrétariat général de la défense nationale (2004) afirma que la implementación de un modelo de defensa en profundidad es una estrategia práctica que permite hacer frente a las potenciales vulnerabilidades. Estos controles sirven como directrices para evaluar la efectividad de los sistemas de información (Aguilera, 2010). No obstante, disponer de un mayor número de controles de seguridad, se vuelve cada vez más complejo, siendo necesario considerar un modelo de defensa en profundidad que contemple las mejores prácticas de seguridad de la información de acuerdo a las necesidades de cada municipio (Stytz, 2004).

Sin embargo, este modelo involucra la intervención de las máximas autoridades, para efectuar cambios en la cultura de seguridad de la información (Glendon & Stanton, 2000). Estos cambios conllevan la implementación de una estrategia de sensibilización que incluya la difusión de la importancia de la seguridad de la información en las organizaciones. (Bedón, Utrilla, & Ortega, 2012)

En este trabajo investigativo, se presenta un modelo de defensa en profundidad basado en el sistema de gestión de seguridad de la información a través de la integración de estándares y normas internacionales, involucrando aspectos organizativos y de sensibilización en seguridad de la información resaltando que el pilar principal, sobre el cual se fundamenta el modelo es la necesaria sensibilización, para concientizar a los directivos y empleados sobre el impacto de los riesgos, la necesidad de implementar controles y los beneficios que trae la protección de la información en las municipalidades.

De modo que el Modelo propuesto puede convertirse en un mecanismo de apoyo a las estrategias que deban asumir las autoridades municipales en pro de mejorar la seguridad de la información y de todos los procesos de TI, no solo permitiendo una evaluación integral de TI y su efecto en el ámbito municipal, sino también constituyéndose en una herramienta para la toma de decisiones desde el contexto de la gestión tecnológica.

## MARCO TEÓRICO

### Seguridad

De acuerdo al diccionario de la real academia de la lengua, seguridad es la cualidad de asegurar algo, es decir mantener su buen funcionamiento evitando que este falle o se violente. Matalobos (2009) indica que seguridad es la capacidad de resistir, con un nivel de confianza aceptable, los accidentes o acciones que puedan causar daño a un sistema u organización. Así mismo, Álvarez (2013) afirma que seguridad implica preservar los activos de atacantes, de desastres naturales, de condiciones ambientales adversas, de robo, y cualquier factor que afecte a un activo, considerando además las medidas necesarias para su protección.

### Seguridad de la Información

ISO 27001 (2016) define que la seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad así como de los sistemas implicados en los procedimientos de una organización. También Castillo, Caldera, Losavio, & Matteo (2006), ratifican que la seguridad representa la agrupación de disponibilidad, confidencialidad e integridad. Por otro lado, de acuerdo a (Ramió, 2006) la seguridad hace referencia a un conjunto de métodos y herramientas utilizados para proteger la información y los sistemas informáticos ante cualquier amenaza. De acuerdo a (Bertolín , 2008) define que la seguridad de la información implica la protección de los sistemas de información, redes y computadores, siendo un proceso que incluye aspectos tecnológicos, de gestión, humano, informático, económico y legal abarcando así aspectos físicos, del entorno y humano.

### Gestión de Seguridad de la Información

ISO 27000 (2016) menciona la Gestión de la Seguridad de la Información, es el proceso que permite definir, alcanzar y mantener los niveles apropiados de confidencialidad, integridad, disponibilidad y autenticidad de la información que necesita una organización para continuar sus operaciones. Por otro lado, Díaz, Alzórriz, Sancristóbal & Castro (2014) afirman que la gestión de seguridad de la información permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de una organización.

### Defensa en Profundidad

En el artículo de la conferencia realizada por Lippmann, Ingols, Scott, & Piwowarski (2006) se establece que la defensa en profundidad es una estrategia común que utiliza capas de protección para controlar los datos y otros recursos críticos. Por otro lado, Yaping, Jianhua, Yong, & Zengyu (2009) afirman que un modelo de defensa en profundidad no solo debe disponer de un método de prevención activa; sino que también debe mejorar la capacidad de detección y prevención, siendo necesario considerar un modelo de defensa en profundidad que contemple las mejores prácticas de seguridad de la información (Stytz, 2004).

### Auditoria de Seguridad

CNIS (2016) en su glosario establece que auditoria de la seguridad, consiste en la revisión de los sistemas para verificar la idoneidad de los controles, asegurar que se cumplan las políticas, procedimientos de seguridad establecidos, detectar errores y proponer modificaciones. Así mismo Chicano (2014) afirma que auditoria de seguridad es el análisis exhaustivo para identificar y describir las vulnerabilidades que

puedan presentarse en los sistemas informáticos, sin embargo esto se vuelve más complejo cuando no existe en un modelo de defensa en profundidad que este diseñado y que considere las características propias de una determinada organización (Slipper, McEwan, & Ifill, 2013)

**Estándares y Marcos de Referencia de Seguridad de la Información**

Burgos & Campos (2012) en su investigación establece que para una correcta administración de la seguridad de la información es necesario establecer y mantener acciones que busquen cumplir con los tres aspectos más importantes para la información como son: confidencialidad, integridad y disponibilidad. Desde esta perspectiva varias organizaciones internacionales han definido estándares y marcos de trabajo para apoyar el cumplimiento de los tres aspectos indicados anteriormente. En este sentido ISO 27001 y COBIT ayudan a definir lo que debería hacerse e ITIL proporciona como gestionar los servicios de TI (IT Governance Institute, 2012).

**ISO 27001: 2013**

SGSI es la abreviatura utilizada para referirse al Sistema de Gestión de la Seguridad de la Información y es el concepto sobre el que se construye la ISO 27001 (Ormella, 2016). De acuerdo al portal de la ISO 27001 (2013) esta norma internacional proporciona los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información siendo esta una decisión estratégica para la organización. Así mismo Calder (2011) establece que un sistema de gestión de la seguridad preserva la confidencialidad, integridad y disponibilidad de la información mediante un proceso de gestión de riesgos dando a los interesados confianza de que los riesgos se gestionan adecuadamente.

Enfatizando que para gestionar un sistema de gestión de la seguridad de la información se utiliza el ciclo PDCA - Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Este ciclo PDCA es un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo demostrando su aplicabilidad permitiendo el establecimiento de la mejora continua en las organizaciones (Fernández & Andrés , 2012).

ISO 27001 (2013) indica que un SGSI requiere que se establezca la política de seguridad de la información sirve como guía en los procesos que establezcan los siguientes ítems:

- El alcance que tendrá el SGSI sobre los procesos de la empresa.
- La política general de seguridad de la información
- La identificación y valoración de los activos de la información.
- Los riesgos a los cuales los activos identificados se encuentran expuestos.
- La selección de los controles para mitigar los riesgos que se han detectado.

Esta norma explica como diseñar un SGSI y establecer los controles de seguridad de acuerdo a las necesidades de una organización; sin embargo no especifica mediante que procedimientos se ponen en práctica (Gómez, 2012).

**COBIT (Control Objectives for Information and related Technology)**

IT Governance Institute (2012) define Los Objetivos de Control para la Información y la Tecnología Relacionada (COBIT) es un marco de referencia aceptado para el gobierno de TI que reúne las mejores prácticas y estándares internacionales, basado en procesos enfocados en la gestión de tecnologías de la información. Así mismo ISACA (2016) establece que COBIT 5 sirve para alinear la organización con las tendencias actuales sobre técnicas de gobierno y administración de TI para cubrir las necesidades de los interesados, está compuesto por cinco dominios (Vargas, 2015):

Evaluar, Orientar y Supervisar (EDM): este dominio establece los requerimientos para el gobierno de TI para alinearlos con la misión, metas y objetivos de la empresa. Que permitan asegurar la entrega de los beneficios, la optimización del riesgo, recursos y aseguren la transparencia hacia las partes interesadas.

Alinear, Planificar y Organizar (APO): este dominio es el encargado de la gestión de TI, que involucre la gestión estratégica y la arquitectura empresarial para gestionar la innovación, el portafolio, el presupuesto y costos, recursos humanos, relaciones, acuerdo de servicios, proveedores, la calidad, el riesgo y la seguridad. Para disponer de un sistema de seguridad de la información.

Construir, Adquirir e Implementar (BAI): dominio encargado de la gestión de programas, proyectos, definición de requisitos, gestión de soluciones que permitan generar un cambio organizativo.

Entregar, Dar Servicio y Soporte (DSS): dominio encargado de coordinar y ejecutar las actividades necesarias para entregar servicios de TI mantenimiento a la empresa en un nivel aceptable de riesgo de seguridad de la información. A través de la definición de controles para asegurar la información.

Supervisar, Evaluar y Valorar (MEA): es el dominio encargado de supervisar que todos los procesos se realicen de acuerdo al nivel acordado, evaluando el cumplimiento de los requisitos regulatorios establecidos en el entorno de control.

**ITIL (Information Technology Infrastructure Library)**

De acuerdo al IT Governance Institute (2012) ITIL es un marco de referencia que define procesos basados en las mejores prácticas para la gestión y soportes de servicios de TI, es aplicable a cualquier tipo de organización. Para Van, y otros (2008) consiste en una serie de publicaciones que proporcionan directrices sobre la calidad de los servicios y los procesos necesarios para soportarlos. Por su parte Figueroa (2012) indica que ITIL es una biblioteca de cinco libros de consulta basados en las mejores prácticas de organizaciones con éxito, proporciona un ciclo de vida de los servicios de TI.

Gómez (2012) indica que las cinco fases que conforman el ciclo de vida ITIL son:

Estrategia del Servicio: Tiene como objetivo proporcionar lineamientos para el diseño, desarrollo e implementación de la gestión de servicios de TI, sirviendo como guía dentro del modelo del ciclo de vida del servicio. Establece los siguientes procesos: gestión de niveles de servicio, gestión del catálogo de servicios, gestión de la disponibilidad, gestión de la seguridad de información, gestión de proveedores, gestión de la capacidad y gestión de la continuidad de los servicios de TI.

Diseño del Servicio: Se encarga del diseño o modificación de servicio y de los procesos necesarios para apoyarlo en su introducción en el entorno real. Establece los siguientes procesos: Gestión de Eventos, Gestión de Incidentes, Gestión de Solicitudes del Servicio, Gestión de Problemas y Gestión de Accesos.

Transición del Servicio: Tiene como objetivo coordinar los cambios en los servicios y procesos de gestión de servicios de TI para que sean realizados de manera coordinada, mejorando el impacto en la producción e incrementando la satisfacción del usuario. Planeación y soporte en la transición, gestión de cambios, gestión de activos de servicio y de configuraciones, gestión de liberaciones e implementación, validación del servicio y pruebas, evaluación y gestión del conocimiento.

Operaciones del Servicio: Su objetivo es la gestión continua de la tecnología que se emplea para entregar y soportar los servicios gestionando los servicios destinados al usuario y clientes dentro de los niveles de servicio establecidos. Establece los siguientes procesos: Gestión de Eentos, Gestión de Incidentes,

Gestión de Solicitudes del Servicio, Gestión de Problemas y Gestión de Accesos.

Mejora continua: Su objetivo es mejorar continuamente los servicios para garantizar que estos respondan a las necesidades del negocio, identificando oportunidades de mejora para los procesos, servicios y actividades de cada una de las fases del ciclo de vida del servicio.

**Cultura de Seguridad de la Información**

En la Tesis doctoral de Veiga (2008) define que la cultura de seguridad de la información es el conjunto de supuestos, creencias, valores y conocimientos que empleados y partes interesadas utilizan para interactuar con sistemas y procedimientos, esta interacción se ve reflejada en la manera en que se realizan las cosas en una organización para proteger sus activos de información. Por su parte (Schlienger & Teufel (2003) afirman que la cultura de seguridad de la información abarca todas las medidas socio-culturales que apoyan las medidas de seguridad, por lo tanto la seguridad de la información se convierte en un aspecto natural en las actividades diarias de cada empleado. Además puede ser considerada como los patrones de conductas en una organización que contribuyen a la protección de cualquier tipo de información (Dhillon, 1995). Van (2000) añade que la cultura de seguridad de la información debe apoyar las políticas de seguridad de la información, procedimientos, métodos y responsabilidad en una organización, de tal manera que la seguridad de la información se convierta en un aspecto natural de las actividades diarias de todos los empleados de una organización.

**Sensibilización en Seguridad de la Información**

Oxfort (2017), define que la sensibilización es hacer que una persona se dé cuenta de la importancia o el valor de una cosa. Desde esta perspectiva Burgos & Campos (2012), establecen que la Sensibilización en seguridad de la información, permite a que las organizaciones conozcan sobre la importancia de mantener la seguridad de la información y el resguardo de todas las actividades de TI. Así mismo Bedón, Utrilla, & Ortega (2012) mencionan que en la implementación de proyectos de seguridad de información que involucre análisis de riesgos, es fundamental la participación de la alta dirección, siendo necesario disponer de un programa de sensibilización a través de la difusión de documentación relacionada.

**Modelo de Seguridad**

Gómez (2007) establece que un modelo de seguridad de la información es un diseño que promueve la utilización de mecanismos efectivos y sólidos para la definición e implementación de controles. Sirviendo como directriz para evaluar los sistemas de información en las organizaciones (Aguilera, 2010).

Milicevic & Goeken (2011) en su investigación establece que un modelo de seguridad de una empresa debe relacionarse e integrarse con modelos como COBIT, ITIL, ISO 27001. Esta vinculación permitirá contar como una herramienta útil que los integre para diseñar un modelo que se adapte a la naturaleza de la organización.

**Propósito de un Modelo de Seguridad en las Organizaciones**

López & Quezada (2006), establecen que los modelos de seguridad en las organizaciones proporcionan un adecuado nivel de protección de los activos de información. Burgos & Campos (2012), en cambio plantean un modelo para facilitar la obtención de un adecuado nivel de riesgo de TIC que permita disminuir o evitar las fallas en los activos de información. En la investigación realizada por (Milicevic & Goeken (2011), examina un metamodelo de la seguridad de la información en base a la norma ISO 27001, que permitan aprovechar los beneficios en los procesos de negocios basados en TI. (Shengjian , Haiyan, & Fengni, 2013), propone un modelo de monitorización dinámica, detección de intrusos,

alerta en tiempo real y seguimiento, lo que lo convierte en un guía práctica para la alerta de la seguridad de red.

**METODOLOGÍA.**

Para el desarrollo del modelo objeto de este estudio, se contemplaron aspectos organizativos y propios de TI, con especial énfasis en la sensibilización en seguridad de la información, pues considera que las autoridades de los municipios no están debidamente sensibilizados en los riesgos que trae la no aplicación de medidas y controles, lo cual se evidencia en la poca importancia para asignar los debidos recursos y la inversión necesaria para adoptar las medidas de seguridad que se apliquen.

De forma general y después de haber analizado estándares, normas, marcos de referencia y diferentes investigaciones se identificó que no existen modelos de defensa en profundidad para los GADs municipales.

Siendo necesario para la construcción del modelo propuesto la consideración de normas y estándares vigentes, que faciliten una mejor gestión de la información que permitan integrar el modelo propuesto con prácticas líderes como ITIL, ISO y COBIT. El resultado del modelo permitirá establecer lineamientos para el establecimiento de políticas y controles internos que minimicen los riesgos en los GADs municipales.

En el presente trabajo, se están vinculando modelos formales para proporcionar fundamentación teórica en dominios diferentes en gobierno de TI en general y seguridad en particular. La construcción de un modelo implica que estos puedan utilizarse de varias formas, convirtiéndose en un apoyo metodológico de acuerdo a las necesidades organizativas.

Desde este enfoque, se propone un modelo de defensa en profundidad, que facilite la valoración de la efectividad de las TI, en todos los procesos que se desarrollan a nivel municipal y proporcione resultados que apoyen a las máximas autoridades a tomar decisiones sobre la importancia de proteger todas las actividades de TI, manteniendo así la seguridad de la información. Lo cual requiere sensibilizar a los usuarios en la importancia de mantener la seguridad de la información por tanto es necesario capacitarlos sobre los riesgos que conllevan la no utilización de controles de seguridad en los municipios. Pues son ellos la línea crítica de protección y aseguramiento de la información, más allá de sanciones y multas que se puedan implementar es necesario mantener una sensibilización en seguridad de la información en la municipalidad, para definir las creencias, acciones y comportamientos que los empleados asocian con la seguridad de la información. Entender lo que significa la apropiación, el cumplimiento y la concienciación como factores claves de la sensibilización en seguridad de la información demanda asumir el reto del empleado desde el contexto organizacional y como se interesa en las necesidad de protección de la información de la municipalidad ( ITInsecurity , 2017).

**Modelo de Defensa en Profundidad para los GADS Municipales con base al Sistema de Gestión de la Información**

Antes de iniciar la explicación del modelo propuesto, y para mayor comprensión del mismo, es necesario abarcar dos aspectos fundamentes: el primero, identificar el principal problema en los GADs municipales, y por último, pero no menos importante, el nivel de complejidad de la seguridad de la información en los municipios.

**Principal Problema en los GADs Municipales**

Para identificar el principal problema existente en los GADs municipales, se realizó una encuesta para determinar el grado de importancia que tiene la seguridad de la información en los municipios considerando los tres aspectos fundamentales para disponer de seguridad como son: confidencialidad, integridad y disponibilidad. A partir del análisis de estos parámetros, se puede establecer que el principal problema en los

GADs Municipales del Ecuador, es la falta de sensibilización en seguridad de la información.

Centrándonos en el contexto de que la sensibilización en seguridad de la información abarca la forma de actuar y de pensar de las máximas autoridades y empleados en temas de tecnologías de la información, la falta de sensibilización en los municipios se ve reflejada en la falta de disponibilidad presupuestaria y la correspondiente asignación de recursos. Considerando el reducido presupuesto que estos administran, y los cambios administrativos que se realizan.

Lo que conlleva que los mayores esfuerzos sean realizados por profesionales informáticos que en general desarrollan múltiples labores como análisis, seguridad básica, programación, soporte técnicos, etc., lo cual ocasiona que no exista un uso eficiente de todos los aspectos de seguridad (Burgos & Campos, 2012). Lo que conlleva a considerar a la seguridad como un gasto, más no como inversión que permita aumentar valor agregado a los municipios.

**Niveles de complejidad de la Seguridad de la Información**

Para establecer los niveles de complejidad de seguridad de la información en los municipios, se ha considerado aspectos organizativos y de tecnología de la información. Lo que conlleva a identificar los procesos administrativos que se ejecutan en los municipios, y que serán parte del análisis de la seguridad de la información.

En la investigación desarrollada por Alnatheer (2012) se establecen tres factores que constituyen una cultura de seguridad de la información como son: la apropiación, la concienciación y el cumplimiento como se muestra en la Figura 1. La apropiación es la expresión de hacernos responsable de nuestras acciones respecto a la seguridad de la información, la concienciación busca que los empleados se hagan conscientes de los riesgos y amenazas frente a la protección de la información y por último el cumplimiento es la adherencia a las políticas, procedimientos y prácticas establecidas.


**Figura 1.** Factores que constituyen una cultura profesional
**Fuente:** (Alnatheer, 2012)

Considerando los tres factores establecidos en la investigación realizada por Alnatheer (2012) y a partir del análisis efectuado a los GADs Municipales en tema de Seguridad de la información, se definen 3 niveles de complejidad de seguridad de la información como son: sensibilización, gestión y operación como se muestra en la Figura 2.

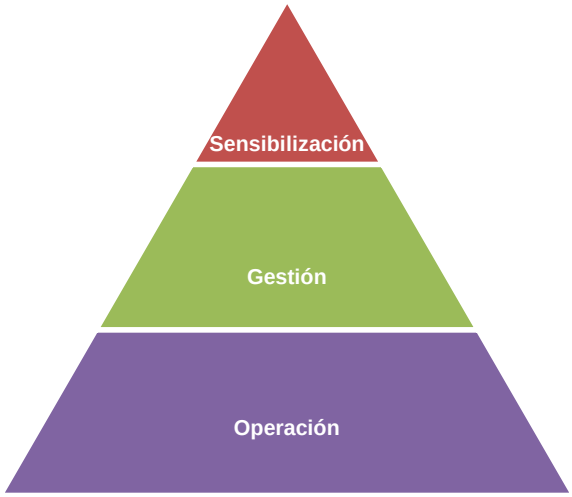


**Figura 2.** Niveles de Complejidad de Seguridad de la Información
**Fuente:** GADs Municipales del Ecuador

Siendo necesario conceptualizar cada uno de los términos utilizados en la determinación del nivel de complejidad.

**Sensibilización:** busca que las máximas autoridades y empleados se hagan conscientes de los riesgos y amenazas que conlleva no utilizar controles de seguridad, así también entiendan el impacto y los beneficios de hacer uso de adecuadas directrices y procedimientos para proporcionar seguridad de la información, cuanto mayor sea el grado de sensibilización mayor será la importancia que se le dé a la gestión de la información y por ende la correspondiente disponibilidad presupuestaria.

**Gestión:** está relacionada con la alineación estratégica institucional al modelo de seguridad, siendo necesario que los municipios dispongan de procedimientos y directrices a seguir para disponer de adecuados mecanismos que permitan brindar seguridad a la información de los GADs Municipales. Involucra además la intervención de las máximas autoridades municipales para el entendimiento de la seguridad de la información respecto a la importancia de la protección de la información. En este sentido todo lo relacionado con políticas, procedimientos y prácticas alrededor de la seguridad de la información debe integrarse con aspectos organizativos, para que la protección de la información no sea algo adicional, sino algo propio de la organización municipal.

**Operación:** este nivel se encarga de verificar la correcta ejecución de procedimientos y directrices establecidas. Además permite verificar la efectividad de los controles implementados para disponer de seguridad en los GAD Municipales, los cuales son sujetos a auditorias y cumplimiento con el fin de conocer el nivel de inobservancia de los municipios en temas de seguridad de la información. En definitiva la seguridad de la información no debe ser considerada como un “costo”, sino como una “inversión” que se anticipe a los riesgos y asegure la continuidad de las operaciones municipales.

Los niveles de complejidad de la seguridad de la información en los municipios, dependen de la sensibilización. Entender la sensibilización desde el contexto organizacional conlleva asumir el reto de comprender la realidad propia de cada individuo y como desde su perspectiva se interesa en las necesidades de protección de la información.

Considerando que la planificación estratégica en seguridad de la información mejora siempre y cuando los lineamientos institucionales tengan un grado aceptable de sensibilización, es necesario aumentar la importancia que los directivos y empleados le den a la seguridad de la información. Esta importancia en los municipios se logra con una adecuada gestión que permita la inclusión de programas de sensibilización en temas de seguridad de la información, que permitan una adecuada protección de la información municipal.

**Construcción del modelo para Defensa en Profundidad para los GADS Municipales con base al Sistema de Gestión de la Información**

Para la construcción del modelo que permita evaluar de forma integral la seguridad de la información, se consideró los estándares ITIL, ISO 27001 y COBIT, porque posibilitan y soportan:

- Una mejor gestión de TI
- Un gobierno eficaz de las actividades de TI.
- Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas, lo que es necesario para que todos sepan lo que hay que hacer (IT Governance Institute, 2008; IT Governance Institute, 2012)

Precisamente estos estándares tienen un capítulo destinado a sensibilización, porque lo consideran importante para una adecuada gestión de la seguridad de la información. Proporcionando además un marco de acción donde se evalúan los criterios de información como seguridad y calidad, permitiendo auditar los recursos que comprenden la tecnología de la información, mediante la evaluación de los procesos involucrados, identificando los riesgos a los que se ve expuesta una organización, para así establecer los controles respectivos para gestionarlos o eliminarlos.

Tomando como referencia que el principal problema en los GADs municipales, es la falta de sensibilización en seguridad de la información, se pone especial interés, en tratar de aumentar la percepción que tienen las personas, en torno a temas de seguridad de la información. A través de la sensibilización que será el aspecto fundamental a considerarse en la construcción del modelo.

Lo que implica que esta etapa deba estar presente, durante todas las fases del modelo, porque permite entregar información constante relacionada con la importancia de mantener la seguridad de la información y todas las actividades de TI que esta conlleve.

**Descripción del modelo para la defensa en profundidad para los GADs Municipales con base al sistema de gestión de la información.**

El modelo SGSI (Sistema de Gestión de Seguridad de la Información), es el conjunto de políticas para la seguridad de la información; sin embargo después de analizar los estándares y normas de seguridad de la información, se puede concluir que no existe un modelo para ser aplicado en los GADs municipales, sobre todo cuando éstas no se han involucrado en procesos relacionados con normas de Gestión de Seguridad de la Información.

En base a las buenas prácticas de seguridad de la información, se presenta el siguiente modelo formal, que se sustenta en un conjunto de actividades que deben ser abarcadas para lograr un adecuado nivel de seguridad de información en los municipios.

Considerando los parámetros establecidos en el nivel de complejidad de seguridad de la información y teniendo en cuenta los principales elementos incluidos en las normas y estándares internacionales, se establece el presente modelo de defensa en profundidad, que se muestra en la Figura 3, como resultado del análisis realizado a los GADS municipales; este modelo abarca aspectos organizativos como la planificación estratégica, el diagnóstico de nivel de complejidad, hasta aspectos propios de TI como, la integración y alineación de controles, el plan de acción, la evaluación y auditorias y la sensibilización en seguridad de la información.

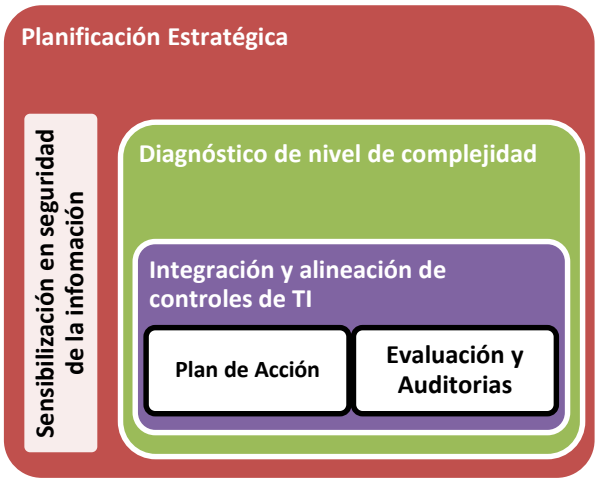


**Figura 3.** Modelo de Seguridad de Defensa en Profundidad de los GADs Municipales con base en el Sistema de Gestión de la Información

**Fuente:** GADs Municipales del Ecuador

En la figura 3, se muestra el modelo de forma esquemática. Este esquema agrupa y resume todas las actividades; sin embargo muchas de ellas conllevan a un ciclo de mejora continua. Permitiendo a las fases del modelo articularse adecuadamente al cumplimiento de los objetivos organizacionales.

Las actividades propuestas, forman un ciclo de vida del proceso de seguridad de información

dependiendo de cada GAD Municipal y del estado en que se encuentre respecto a temas de gestión de la seguridad de la información. A continuación se presenta la descripción de cada una de las fases y actividades que se consideran necesarias para brindar seguridad de defensa en profundidad:

**Planificación Estratégica de TI:** En esta fase se define el alcance de los Proyectos tecnológicos a ser ejecutados, se establecen tareas, metas, plazos de ejecución, presupuesto, personal, capacitación, entre otros recursos necesarios para brindar defensa en profundidad a los GADs Municipales. Implica además la verificación de políticas de seguridad y la alineación de Seguridad de la Información, en base a las normas y procedimientos vigentes que regulan el sector público en temas de TI, específicamente las normas 410 Tecnologías de la Información, emitidas por la Contraloría General del Estado y Reglamento para el Control de Bienes del Sector Público.

Que permitan, preservar la confidencialidad, integridad y disponibilidad de la información, formando un conjunto de mejores prácticas enfocadas en controlar y supervisar las tecnologías de la información.

**Diagnóstico de nivel de complejidad de los servicios de TI:** En esta fase, se pretende identificar el estado actual de la gestión de la seguridad en los GADs Municipales con respecto a temas de confidencialidad, integridad y disponibilidad de la información. Se considerará la estructura interna, procesos, infraestructura, comunicaciones, los requerimientos legales y regulatorios.

**Integración y Alineación de Controles de TI:** En esta etapa, se diseñan y definen los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisiones o auditorias del modelo. En base al Sistema de Gestión de la Seguridad, corresponde además realizar un análisis de riesgo que permita evaluar todos los potenciales peligros en los cuales se pueden ver involucrado los activos de información de los GADs Municipales que impactan en la seguridad de la información.

**Evaluación y Auditoria:** En esta etapa se debe realizar evaluaciones para el cumplimiento de auditoria, ya sea esta interna o externa, permitiendo verificar el cumplimiento de las normativas y reglamentos en temas de TI. Además se debe realizar, preparar y desarrollar la revisión que avale que todos los procesos de TI se están cumpliendo y llevando a cabo adecuadamente. A través de evidencias que permitan verificar de manera adecuada que todos los registros de TI para todos sus procesos y controles estén disponibles para cualquier tipo de revisión.

Se complementa esta etapa con la elaboración de informes, sobre el proceso de revisión que derivarán en actividades de mejorar el modelo, permitiendo la revisión por parte del concejo cantonal y la elaboración de acciones correctivas necesarias.

**Planes de Acción:** En esta etapa, es necesaria la aplicación de planes de acción conforme a los plazos y actividades establecidos en el proceso de auditoría. Estos planes de acción pueden incluir la revisión y ajuste de todas las actividades que involucren la seguridad de la información, ya sea a nivel de procesos de seguridad, normas, políticas o cualquier actividad identificada en el proceso de auditoría.

**Sensibilización en seguridad de la información:** Es la capa principal del modelo, permite concientizar a los GADs municipales sobre la importancia de mantener seguridad de la información, lo que permite recibir el apoyo y los recursos necesarios; no obstante la sensibilización en los GADs Municipales debe ser tratada mediante charlas y capacitaciones que involucren a todo el personal, pues son ellos, los principales actores para mantener la seguridad de la información.

Esta etapa debe permanecer constante, en todas las fases del modelo, porque permite entregar

información a la municipalidad sobre la importancia de mantener la seguridad de la información y de todas las actividades de TI, lo que permitirá recibir el apoyo de las máximas autoridades de la municipalidad y disponer de una adecuada gestión de seguridad de la información.

## ANÁLISIS DE RESULTADOS

Una vez realizado el proceso de búsqueda en las bases de datos y literatura relevante en torno a temas de SGSI y modelos de seguridad, se analizó la literatura recopilada dando como resultado la determinación del modelo que se adapte a la estructura de los GADs Municipales, tomando como referencia los estándares y normas internacionales. Este análisis permitió además, la elaboración del marco teórico del presente trabajo.

Para establecer la estructura del modelo, se realizaron encuestas a los actores involucrados, donde se logró obtener los requerimientos funcionales del modelo y se identificaron los aspectos generales relacionadas con la seguridad de la información en los municipios.

### Análisis de la encuesta realizada a los Directores y Jefes de Tecnología de la Información de los GAD Municipales

La cantidad total de encuesta fue 25. La mayoría de encuestados, son funcionarios que han trabajo en los municipios no menos de 3 años. Lo que ha influido en que los resultados tengan una perspectiva centrada en la seguridad de la información y al cumplimiento de las leyes y normas que rigen el sector público en temas de TI.

En la Figura 4 se muestra las preguntas formuladas en las encuestas realizadas, la mayoría de respuestas fueron contestadas en línea. Cuando esto no fue posible, el cuestionario fue contestado durante las entrevistas en persona.

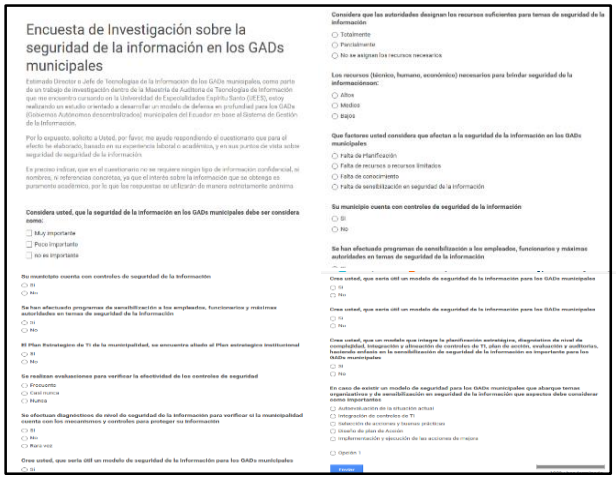


**Figura 4.** Encuesta realizada a los 25 directos y jefes de tecnología de la información de los GAD Municipales
**Fuente:** GADs municipales del Ecuador

Para identificar el departamento o unidad a la que depende la función de seguridad de la información en los GADs municipales, se realizó una encuesta dirigida a 25 funcionarios municipales. Los resultados obtenidos se muestran en la Figura 5.

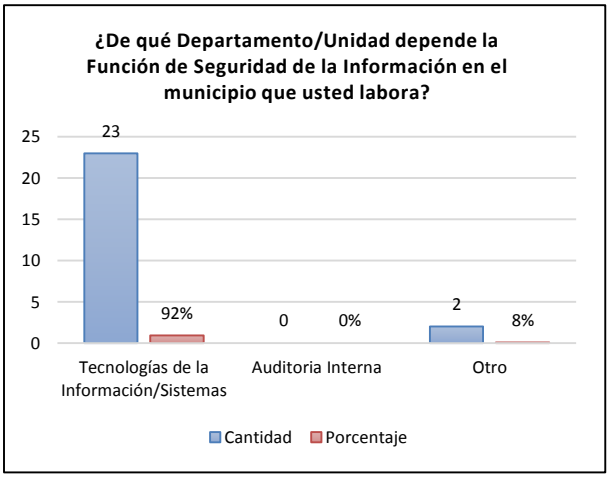


**Figura 5.** Departamento que depende la función de seguridad de la información en los GADs municipales
**Fuente:** GADs Municipales del Ecuador

De los resultados obtenidos, el 92% de los GADs municipales encuestados manifestaron que las actividades de seguridad de la información

dependen de la Unidad de Tecnologías de la Información. Por otra parte, un 2% manifiesta que esta actividad es responsabilidad de otras unidades dentro de la municipalidad.

Entre los factores que afectan la seguridad de la información en los GADs municipales, los resultados indican que el mayor de ellos es la falta de sensibilización en seguridad de la información con un 72%, seguido de la falta de recursos con un 30% y la falta de políticas de seguridad con un 18%, como se muestra en la Figura 6.

Desde el punto de vista organizacional, se evidencia que el principal problema es la sensibilización en seguridad de la información, lo que impide disponer de adecuados niveles de seguridad de la información, evidenciada por la falta de mecanismos de seguridad, desde el punto de vista de inversión, se evidencia la falta de recursos económicos, debido a que los municipios manejan recursos limitados, sumado a la percepción de que seguridad es una gasto y no una inversión. Dificultando disponer de una adecuada planificación que involucre una estrategia de seguridad de la información alineada con los objetivos institucionales en los GADs Municipales.

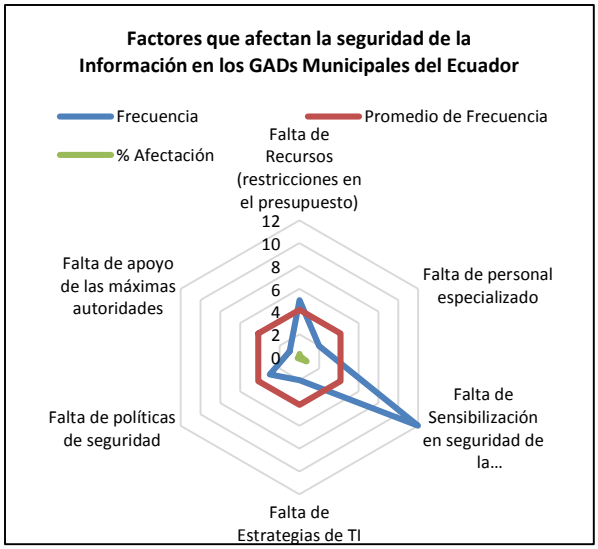


**Figura 6.** Factores que afectan la seguridad de la Información en los GADs municipales
**Fuente:** GADs Municipales del Ecuador

Cabe rescatar que en el análisis efectuado, las municipalidades como instituciones gubernamental tienen claramente definidos los aspectos legales y regulatorios que rigen el sector público, en temas de seguridad de la información, como es el caso de las normas de control interno para las entidades, Organismos del Sector Público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, específicamente la norma 410 – Tecnologías de la Información, así como también la ley orgánica del servicio público y el Esquema gubernamental de seguridad de la Información EGSI

En la Figura 7. Se muestra que los GADs municipales en su mayoría no efectúan diagnósticos de nivel de seguridad de la información, las medidas que se toman son de carácter reactivo, se cuentan con algunos procedimientos de seguridad de la información; sin embargo no se encuentran documentados, lo que ocasiona que no se gestionen los recursos necesarios.

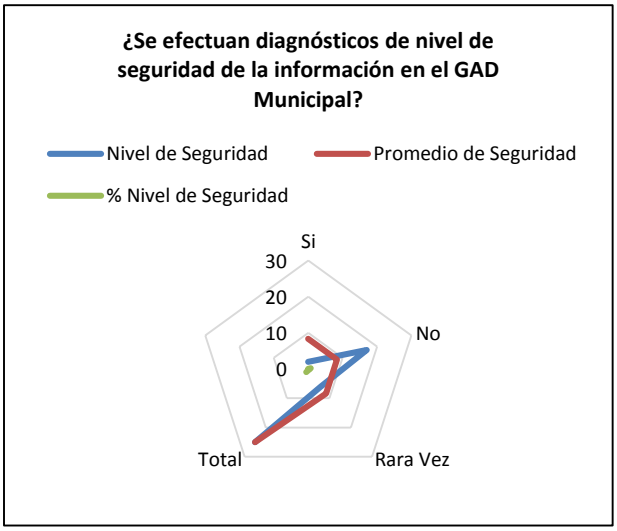


**Figura 7.** Evaluación de la existencia de nivel de diagnóstico de seguridad de la información
**Fuente:** GADs Municipales del Ecuador

Los resultados mostrados en la Figura 7, establecen la evaluación que se realiza en los municipios en temas de seguridad de la

información. Es así que el 68% de los municipios no efectúa diagnósticos para identificar el nivel de seguridad de la información, solo un 8% realiza un análisis empírico para identificar los posibles problemas de seguridad existentes. Esto depende muchas veces de su presupuesto y la sensibilización de seguridad que existe en cada uno de ellos.

Por su parte, uno de los aspectos importantes considerados en la encuesta, está relacionado con la importancia de la utilización de un modelo de defensa en profundidad para los GADs municipales. Como se observa en la Figura 8.

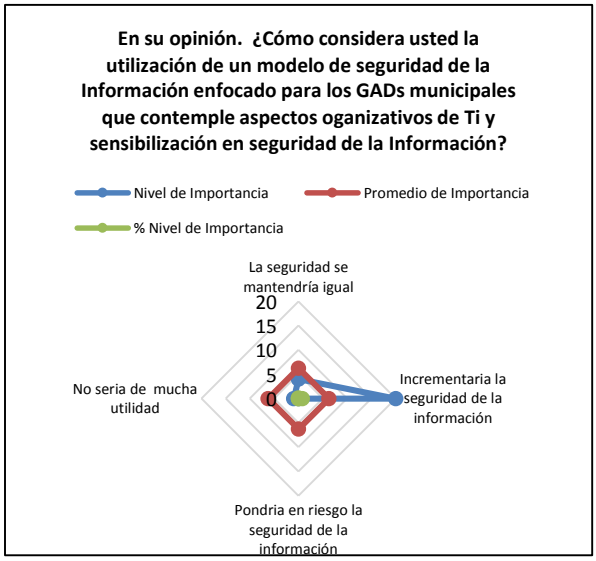


**Figura 8.** Utilización de un modelo de defensa en profundidad para los GADs municipales
**Fuente:** GADs Municipales

De los resultados obtenidos, el 80% de los GADs municipales encuestados consideraron que un modelo de seguridad de la información que contemple aspectos organizativos de TI y de sensibilización, incrementaría la seguridad de la información. Por otra parte, un 4% manifiesta que no sería de mucha utilidad, porque esto depende de su presupuesto y la sensibilización de seguridad de información que existe en cada uno de ellos.

Al consultar a los GADs municipales sobre los aspectos que consideran importantes en el modelo propuesto, respondieron que la autoevaluación de la situación actual es el aspecto de mayor relevancia con un 32%, seguido del diseño del plan de acción con un 20%, la integración de controles de TI, selección de acciones y buenas prácticas, así como la implementación y ejecución de acción con un 12% cada una como se muestra en la Figura 9.

Esto puede explicarse considerando que existen municipios que no disponen de Plan de Contingencia, Plan Estratégico de TI, así como la inexistencia de políticas procedimientos de seguridad definidos y documentados o en su defecto no se encuentran actualizados.

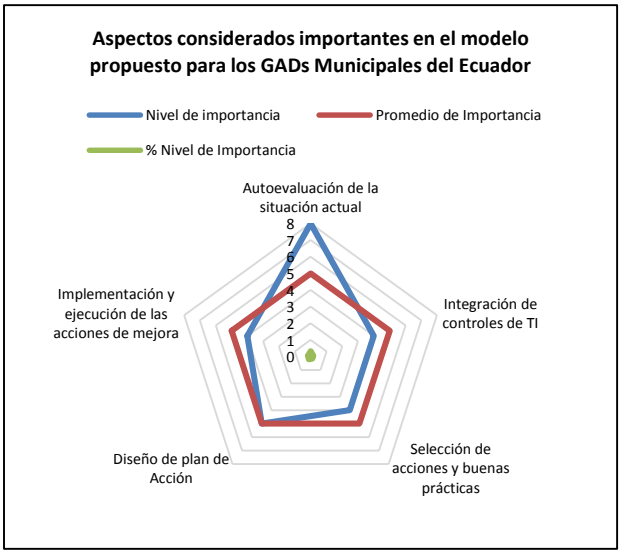


**Figura 9.** Aspectos importantes del modelo de defensa en profundidad para los GADs municipales
**Fuente:** GADs Municipales

En el gráfico 10, se puede apreciar la evaluación detallada de la Importancia de las fases del Modelo de Defensa en Profundidad de los GADs municipales, donde se corrobora que la sensibilización de seguridad de la información, es el fase más importante dentro del modelo propuesto, es necesario destacar que los resultados obtenidos en la encuesta evidencian la falta de asignación de recursos, derivado de

las restricciones en el presupuesto municipal lo que ocasiona poca inversión.

De los resultados obtenidos en la Figura 10, el 24% de los municipios indican que la sensibilización de seguridad de la información es la fase más importante del modelo, seguido del diagnóstico del nivel de complejidad con un 20%, así como la planificación estratégica de TI, integración y alineación de controles, plan de acción, evaluación y auditoria son también fases importantes dentro del modelo con un 12% cada una.

De ahí que el modelo presentado sirve como un medio de orientación específica para que los municipios planteen las políticas y procedimientos de TI que consideren necesarios, sobre la base de sus presupuestos y la sensibilización de seguridad que existe en cada uno de ellos.

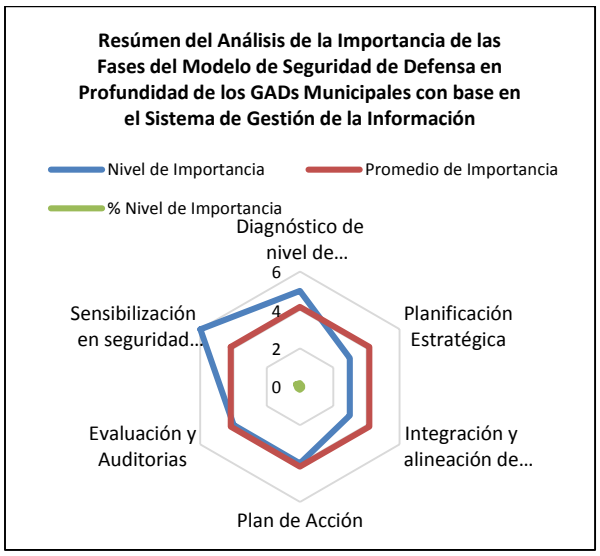


**Figura 10.** Evaluación detallada de la Importancia de las fases del Modelo de Defensa en Profundidad de los GADs municipales
**Fuente:** GADs Municipales

Los resultados obtenidos del análisis efectuado a las municipalidades sobre seguridad de la información, reflejan el análisis de los aspectos organizativos y de sensibilización en temas de TI, que permitirán a los GADs municipales disponer de una adecuada sensibilización en seguridad de la información. Es importante mencionar que una adecuada sensibilización en seguridad es necesaria para concientizar a las máximas autoridades municipales sobre el impacto de los riesgos, la necesidad de implementar controles y los beneficios que trae la protección de la información en las municipalidades para garantizar una correcta gestión de la información.

## CONCLUSIONES

La creciente dependencia de la información en las municipalidades, enfrenta a nuevos retos en donde salvaguardar la privacidad, confidencialidad y disponibilidad de la información se hace más arduo, y la preparación ante la ocurrencia de eventos se vuelve necesaria. De ahí que exista la necesidad de incorporar estándares y normas internacionales que brinden una gestión segura de la información, a través de la incorporación de buenas prácticas de seguridad de la información.

En la presente investigación, se ha realizado el Análisis de las prácticas líderes en seguridad así como de aspectos organizativos y de sensibilización de TI en los GADs municipales del Ecuador, lo que ha determinado que no existe un modelo que se adapte a los municipios.

Por lo tanto se propone un modelo de defensa en profundidad que integre aspectos organizativos de TI y sensibilización de seguridad de la información, considerando este último como el pilar fundamental para tener seguridad de la información en las municipalidades, porque permite concientizar a las máximas autoridades sobre el impacto de los riesgos y la necesidad de implementar controles para proteger la información de los GADs municipales.

De ahí que el Modelo propuesto pueda convertirse en un mecanismo de apoyo a las estrategias que deben asumir las autoridades municipales en pro de mejorar la seguridad de la información y de todos los procesos de TI, no solo permitiendo una evaluación integral y su efecto en el ámbito municipal, sino también

constituyéndose en una herramienta para la toma de decisiones en el contexto de la gestión tecnológica permitiendo que las fases del modelo se articulen, integren y contemplen un conjunto de actividades que estén ligadas, mediante la secuencia de actividades necesarias para brindar defensa en profundidad.

De manera que la estructura que presenta el modelo se basa en la implementación práctica de las actividades que permiten brindar seguridad, en base a sus propias necesidades, lineamientos y perspectivas, considerando el presupuesto y la sensibilización de seguridad de la información de cada municipio, así mismo por su presentación sencilla puede ser fácilmente interpretado y relacionado con las actividades que realizan los municipios, de manera que se logre asegurar la información en base a la realidad de las TIC que dispongan.

No obstante para la implementación correcta del modelo es necesario conocer las funciones, tareas y actividades propias de los GADs municipales para ajustarlas a cada una de las fases del modelo propuesto, de modo que puede ser considerado como base para el establecimiento de Gobierno de TI en los GADs municipales, además la particularidad del modelo que se presenta reside en su aspecto operativo y práctico que requiere de una adecuada sensibilización sobre el impacto de los riesgos, siendo fundamental que las máximas autoridades entiendan los beneficios que trae la protección de la información en las municipalidades, a fin de disponer de una adecuada cultura de seguridad a través de la sensibilización.

Por lo tanto el modelo considera una estructura de tres fases, tomando como referencia los niveles de complejidad de seguridad de la información de los GADs Municipales como son: sensibilización, gestión y operación. Y los convierte en fases de planificación estratégica, diagnóstico de nivel de complejidad, integración y alineación de controles, plan de acción, evaluación y auditorias y sensibilización en seguridad de la información, garantizando una correcta gestión de la información. No obstante, el modelo propuesto no entrega documentos desarrollados como procedimientos e instructivos, sino que sienta sus bases para su desarrollo, esto se justifica en que cada municipio tiene su presupuesto asignado y su sensibilización en seguridad de la información.

Es necesario enfatizar que la planificación estratégica de TI en los municipios mejora siempre y cuando los lineamientos de Planificación, Organización, Dirección y Control estén en un nivel alto de sensibilización, lo que permitirá que el diagnóstico de TI, sea más efectivo desde el contexto de la gestión tecnológica. Sin embargo, este modelo puede ser perfeccionado y modificado en el futuro, considerando que su estructura puede ser mejorada y adaptada de acuerdo a los cambios en las normativas y regulaciones que rigen el sector público, permitiendo una implicación de TI en los procesos administrativos de los GADs municipales.

**Referencias Bibliográficas**

ITInsecurity . (20 de enero de 2017). Cultura organizacional de seguridad de la información. Factores clave, relaciones relevantes e impactos organizacionales. Obtenido de http://insecurityit.blogspot.com/2014/01/B-organizacional-de-seguridad-de.html

Aguilera, P. (2010). Seguridad Informática. Editex.

Alnatheer. (7 de enero de 2012). Understanding and measuring information security culture in developing countries: Case of Saudi Arabia. Unpublished Doctoral Thesis. Queensland University of Technology. Obtenido de http://eprints.qut.edu.au/64070/1/Mohammed_Al_Nat

Álvarez, A. (2013). Evaluación de la seguridad de los Sistemas Informáticos: políticas, estándares y análisis de riesgos.

AME Guayas. (2016).

Asociación de Muninicipalidades del Ecuador. (2016). Ecuador.

Balcerek, B., Frankowski, G., Kwiecién, A., Smutnicki, A., & Teodorczyk, M. (2012). Security best practices: applying defense-in-depth strategy to protect the NGI_PL. Springer Berlin Heidelberg., 128-141.

Bedón, M., Utrilla, J., & Ortega, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. IV Congreso Internacional de Computación y Telecomunicaciones, (págs. 1-7).

Bertolín , J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Madrid: Editorial Paraninfo.

Burgos, J., & Campos, P. (2012). Modelo para seguridad de la Información en TIC. Universidad del Bío - Bío, 1-20.

Calder, A. (2011). Implementing information security based on ISO 27001/ISO 27002. Van Haren.

Castillo, I., Caldera, R., Losavio, F., & Matteo, A. (2006). Caracterización de Sistemas Fiables basada en un modelo estándar de calidad. XXXII Conferencia Latinoamericana de Informática. Chile: Center for Web Research (CWR).

Chen, D. (2012). Data Security and Privacy Protection Issues in Cloud Computing. IEEE, 647 - 651.

Chicano, E. (2014). Auditoría de Seguridad Informática. Málaga: ic.

CNIS. (13 de diciembre de 2016). Glosario Seguridad. Obtenido de http://www.cnis.es/glosario-seguridad/

Dhillon. (1995). Interpreting the Management of Information Systems Security.

Díaz, G., Alzórriz, I., Sancristóbal, E., & Castro, M. (2014). Procesos y herramientas para la seguridad de redes. Madrid: UNED.

ESET Security Report. (2015). ESET Security Report, Latinoamérica 2015.

Fernández, L., & Andrés , A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Asociación Española de Normalización y Certificación. AENOR.

Figueroa, N. (2012). ITIL V3¿ Por dónde empezar. Buenos Aires.

Fiscalía General del Estado. (13 de 06 de 2015). Los Delitos Informáticos van desde el fraude hasta el espionaje. Obtenido de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

GAD Municipal de Balao. (s.f.).

Glendon, A., & Stanton, N. (2000). Perspectives on safety culture. Safety Science. SciELO - Scientific Electronic Library Online, 193-214.

Gómez. (2012). Implantación de los procesos de gestión de incidentes y gestión de problemas según ITIL v3. 0 en el área de tecnologías de la información de una entidad financiera.

Gómez, Á. (2007). Enciclopedia de la seguridad informática. México.

Grande, I., Ramilo, M., & Salvador, M. (2002). La necesidad de teoría (s) sobre gobierno electrónico. Una propuesta Integradora. . XVI Concurso de ensayos y monografías del CLAD sobre reforma del estado y modernización de la administración pública, 1-52.

Groat, S., Tront, J., & Marchany, R. (2012). Advancing the defense in depth model. System of Systems Engineering (SoSE), 2012 7th International Conference on. IEEE, 285 - 290.

ISACA. (10 de diciembre de 2016). COBIT5-and-InfoSec-Spanish. Obtenido de http://www.isaca.org/cobit5

ISO 27000. (25 de noviembre de 2016). Sistema de Gestión de la Seguridad de la Información. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27001. (16 de enero de 2013). ISO 27001: 2013. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO 27001. (2013). ISO 27001:2013. Information technology – Security.

IT Governance Institute. (2008). Alineando Cobit 4.1, ITIL v3 y ISO 27002 en beneficio de negocio. Un reporte para gestión del ITGI y la OGC. Obtenido de https://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

IT Governance Institute. (2012). CobiT 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. Un reporte para gestión del ITGI y la OGC. Obtenido de http://www. ISACA. com/. IT Governance Institute.

ITIL. (10 de diciembre de 2016). ITIL Books. Obtenido de https://www.itil.org.uk/

Laudon, J., & Laudon, K. (2004). Sistemas de información gerencial: administración de la empresa digital. México: Pearson.

Lippmann, R., Ingols, K., Scott, C., & Piwowarski, K. (2006). Validating and restoring defense in depth using attack graphs.

López, M., & Quezada, C. (2006). Fundamentos de seguridad informática. Mexico.

Matalobos, J. (2009). Análisis de Riesgos de Seguridad de la Información.

May, C., Hammerstein, J., Mattson, J., & Rush, K. (2006). Defense in Depth: Foundations for Secure and Resilient IT Enterprises. Carnegie Mellon University, 1- 369.

Merino , C., & Cañizares, R. (2014). Auditoría de Sistemas de Gestión de Seguridad de la Información. FC Editorial.

Milicevic, D., & Goeken, M. (2011). Application of Models in Information Security Management. Research Challenges in Information Science (RCIS), 1-6.

Neetha, X., & Chandrasekar. (2014). Cloud computing data security for personal health record by using attribute based encryption. International Journal of Information, Business & Management.

Ormella, C. (05 de diciembre de 2016). Normas ISO de Seguridad de la Información. Obtenido de http://www.criptored.upm.es/guiateoria/gt_m327a.htm

Oxfort. (18 de enero de 2017). Obtenido de https://es.oxforddictionaries.com/definicion/sensibilizar

Ramió, J. (2006). Seguridad Informática y Criptografía., Versión 4.1. Libro Electónico.

Schlienger, & Teufel. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture.

Secrétariat général de la défense nationale. (19 de julio de 2004). La defensa en profundidad aplicada a los sistemas de información. Obtenido de http://www.ssi.gouv.fr/archive/es/confian

za/documents/methods/mementodep-V1.1_es.pdf

Shengjian , L., Haiyan, Y., & Fengni, W. (2013). Design of network security early-warning system based on network defense in depth model. IEEE, 355-359.

Slipper, D., McEwan, A., & Ifill, W. (2013). Modelling and analysing Defence-in-Depth in Arming Systems. IEEE, 6.

Stytz, M. (2004). Considering defense in depth for software applications. IEEE, 72-75.

UTR 5 AME. (s.f.).

Van, J., Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van, A., & Verheijen, T. (2008). Foundations of IT Service Management Based on ITILFoundations of IT Service Management Based on ITIL.

Vargas, J. (2015). Diseño de un plan de gestión de seguridades de la información para Instituciones Públicas Ecuatorianas. Riobamba.

Veiga, D. (2008). Cultivating and Assessing Information Security. Obtenido de http://repository.up.ac.za/dspace/bitstream/handle/2263/24117/Complete.pdf?sequence=4&isAllowed=y

Von. (200). Information Security - The Third Wave?. Computer & Security.

Yaping , J., Jianhua, Z., Yong , G., & Zengyu , C. (2009). A Method of In-Depth-Defense for Network Security Based on Immunity Principles. IEEE, 4.