# EVALUACIÓN TÉCNICA DE SEGURIDADES DEL DATA CENTER DEL MUNICIPIO DE QUITO SEGÚN LAS NORMAS ISO/IEC 27001:2005 SGSI E ISO/IEC 27002:2005.

Ing. Diego Santiago Aguirre Freire, Ing. Jhon Carlos Palacios Cruz
Unidad de Gestión de Postgrados; Escuela Politécnica del Ejército, Sangolquí, Ecuador

**Resumen:**

El MDMQ maneja información sensible de la ciudadanía, como lo es la información catastral, licencias metropolitanas, pagos de impuestos prediales, declaración de patente ente otros. Dicha información es crítica la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en el Data Center, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad.

El presente trabajo se orienta a la evaluación técnica informática para determinar el cumplimiento de las normas y estándares internacionales que establecen un GAP de la gestión de seguridad de la información, según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. Cabe señalar que dicho trabajo, se desarrollará mediante una investigación documental - descriptiva, para la recolección de la información se empleará técnicas de investigación de campo de fuentes primarias, como son la observancia y la entrevista; y secundarias como son documentos y libros dicha información, será analizada y evaluada, mediante lo cual, se determinará el cumplimiento o no de los lineamientos según la norma ISO/IEC 27002:2005, con el fin de identificar vulnerabilidades de seguridad en el de todos los elementos que se encuentran en Data Center y recomendar se establezcan políticas de seguridad de la información y se implemente controles para el manejo de riesgos, monitoreo y revisión del desempeño y efectividad del Data Center, considerando el mejoramiento continuo de la seguridad de la información.

## Palabras claves

**Activo** Definido como un bien que tenga o genere valor y sea necesario para la organización.

**Disponibilidad**Es garantizar el acceso a la información por personal autorizado, en el momento que lo necesiten.

**Confidencialidad de la Información** Es garantizar que solo las personas dueñas de la información tengan acceso a ella.

**Trazabilidad**Es garantizar que se mantenga un registro o una bitácora en los que se almacenaran los cambios realizados a la información, quien los ejecutó y en qué momento.

**Autenticidad**Es garantizar la identidad del usuario que genera la información.

**Sistema de gestión de la seguridad de la información (SGSI)**Define como una organización limita, desarrolla, e implanta un SGSI basado en el modelo PDCA y este comprende el Anexo A donde están descritos los controles de seguridad de la información, fundamentales que son importantes para reducir y minimizar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información.

**Auditoria**Emitir un criterio profesional sobre un objetivo sometido a análisis presentando la realidad de cumplimiento para las que ha sido concebida.

**Auditoria Informática**Sebasa en el principio de evaluar de forma sistemática y objetiva, es un parte integral de la Auditoria, en fin es definir el uso adecuado y como son utilizados los recurso informáticos.

**Hallazgo**Es el resultado relevante que obtiene de la evaluación un determinado a un control.

**Política** Es una guía donde se encuentran publicadas normas o estándares para la toma de decisiones establecidos por parte de la alta gerencia.

**Proceso**Conjunto de pasos que se encuentran dados o mencionados en un políticas y estándares de la organización.

**Procedimiento**Metodología para ejecutar un conjunto de pasos que permita realizar un trabajo de forma organizada.

**Riesgo**Es una vulnerabilidad de que ocurra o no un daño en perjuicio de la organización.

**Abstract:**

The MDMQ handles sensitive information from the public, such as cadastral information, metropolitan licenses, property tax payments, patent statement among others. Such information is critical that it is hosted on servers and storage systems located in the data center, so it is necessary that its confidentiality, integrity and availability is guaranteed.

This paper is oriented to computer technical evaluation to determine compliance with international norms and standards that establish a GAP management information security according to ISO / IEC 27001:2005 ISMS and ISO / IEC 27002:2005 standards. It should be noted that this work will be developed through documentary research - descriptive , for the collection of information from field research techniques will be used primary sources , such as enforcement and interview, and secondary documents such as books and such information will be analyzed and evaluated , whereby the fulfillment or not of the guidelines will be determined according to ISO / IEC 27002:2005 standard, in order to identify security vulnerabilities in all the elements found in Data Center and recommend policy information security controls are established and risk management , monitoring and

review of performance and effectiveness of the data Center is implemented, considering the continuous improvement of safety.

**Key words**

**Active.** Defined as a well that has or creates value and necessary to the organization.

**Availability**Ensure access to information by authorized, when they need it.

**Confidentiality of Information**Is to ensure that only the owners of the information people have access to it.

**Traceability** Is to ensure that a record or diary in which changes to the information, who executed them and when they were stored is maintained.

**Authenticity** Is to ensure the user's identity information generated.

**Management System of Information Security (SGSI)**Defined as an organization limits , develops, and implements an SGSI based on the PDCA model and this includes Appendix A which controls information security , fundamental that are important to reduce and minimize the risks to confidentiality, integrity, and are described availability information .

**Auditing**Issue a professional judgment on a subject to analysis by presenting the reality of performance for which it was conceived goal.

**Computer Auditing**It is based on the principle of systematically evaluate and objectively, is an integral part of the audit, it is in order to define the appropriate use and are used as computer resource.

**Find** It is the important result obtained from the evaluation to a particular control.

**Policy** It is a guide where you will find published standards or standards for decision-making established by senior management.

**Process**Set of steps that are given or referred to in policies and standards of the organization.

**Procedure** Methodology to perform a set of steps that allows for organized work.

**Risk** It is a vulnerability that occurs or no harm to the detriment of the organization.

**Secciones**

## I. Introducción

El proceso de evaluación posee un ciclo de vida que tiene como inicio el identificar los objetivos de la organización o negocio, los activos de información y los sistemas o recursos de información que tengan y manipulen información de vital importancia como es hardware, software, base de datos, redes, instalaciones, personas, etc.

Una vez identificados los activos de información sensible o critica, se realiza una evaluación de riesgos para identificar las amenazas y poder determinar la probabilidad de ocurrencia, como el fin de dimensionar el impacto resultante y sus respectivas medidas para la mitigación de las amenazas hasta llegar a un nivel aceptable para la organización.

## II. Metodología

El presente trabajo se ha realizado a través de una metodología basada en riesgos, utilizando métodos de investigación de fuentes primarias como son encuestas, entrevistas y observación.

Para evitar emitir criterios sin fundamentos es necesario utilizar técnicas y las fuentes de información disponibles las cuales se detalla a continuación:

- Registros anteriores
- Experiencias relevantes
- Prácticas  y experiencias de la organización
- Opiniones y juicios de especialistas y expertos

Las técnicas pueden incluir:

- Entrevistas estructuradas con expertos en el área de interés
- Evaluaciones individuales utilizando cuestionarios
- Uso de árboles de fallas y árboles de eventos

La etapa de mitigación del riesgo se identifican los controles para mitigar los riesgos identificados, los controles son medidas para la mitigación del riesgo que tratan de conseguir como resultado prevenir, reducir y en los mejores de los casos eliminar la probabilidad de que el evento ocurra, detectar la ocurrencia y minimizar el impacto o transferir el riesgo.

La evaluación de los controles es uno de los pasos principales al que se debe dar la importancia necesario ya que se lo realiza mediante un análisis costo - beneficio hasta obtener el riesgo un nivel aceptable  por parte de la gerencia y esto se analiza de la siguiente forma:

- El costo del control comparado con el beneficio de minimizar el riesgo
- La tolerancia a riesgos de la gerencia de aceptación de la amenaza

La siguiente etapa es la última y se la conoce como monitoreo de los niveles de desempeño de los riesgos gestionados cuando se procede con cambios que son relevantes y significativos.

Estos tienen procesos de verificación que son:

- Evaluación de riesgos
- Mitigación de riesgos
- Reevaluación de riesgos

Aplicado esto podemos volver a identificar si los riesgos están en un nivel aceptable para la gerencia. (AS/NZS 4360:1999, pág. 13)

## III. Evaluación, resultados y discusión

La seguridad y el resguardo de la información llevada de una manera adecuada protegen de una gran variedad de amenazas que se presentar día a día y estos procesos se los realiza con el fin de asegurar la continuidad del negocio, minimizando el impacto ya que en estos procesos se encuentra la Direccione Metropolitana Informática.

En la evaluación de los controles de la ISO 27001:2005 SGSI se sugiere que se adopte un modelo de mejoramiento continuo para el Data Center como es:

- Sistema de Gestión de la Seguridad de Información (SGSI), que comprende:
  - Responsabilidad de la Dirección
  - Control de documentos y registros
  - Auditorías Internas
  - Análisis Crítico
  - Mejora del SGSI

Los resultados obtenidos en el análisis de la evaluación de los controles que posee la Dirección Metropolitana de Informática en su Data Center y los controles establecidos por la ISO 27002:2005 se concluye que el 92.24% posee de cumplimiento total o parcial de dichos controles y el 6.76% faltante de estos controles de lo que indica esta norma.


## IV. Trabajos relacionados

Empresas establecidas en el Ecuador se han certificado con la norma ISO/IEC 27001:2005 SGSI:

TELCONET empresa de provisión de servicios de comunicación de video, voz y datos en el año 2008. TELCONET mantiene certificaciones a nivel empresarial ISO/IEC 27001:2005 SGSI en Sistemas de Seguridad de la Información.

Telefónica Movistar Ecuador, empresa que en febrero de 2011 recibió la certificación del "Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001:2005 SGSI", otorgado por la Asociación Española de Normalización y Certificación (AENOR). Esta certificación "tiene relación con la provisión y soporte del servicio de datos fijos e internet dedicado para el segmento de grandes empresas" (...), (Movistar, 2011),

## V. Conclusiones y trabajo futuro

Por el análisis realizado podemos concluir que el Municipiodel Distrito Metropolitano de Quito y sobre todo la Dirección Metropolitana de Informática se encuentran dando pasos agigantados en la parte tecnológica,anteriormente no tenía políticas para la ejecución

de procesos y manejo de información pero en los últimos años ha tomado fuerza la seguridad de la información, considerándola como algo vital y de gran importancia para el resguardo de sistemas e información sensible que se maneja.

La Dirección Metropolitana de Informática se encuentra en un proceso de transición para la creación, aplicación y evaluación de procesos de seguridad, lo cuales de vital importancia y brinda un valor agregado al buen desarrollo y desempeño de la dirección.

El objetivo de este trabajo es que sea el puntal para iniciar con los cimientos para la elaboración del Sistema de Gestión de la Seguridad en el MDMQ, según la normas 27001 y 27002.

En base al presente trabajo se debería establecer políticas y normas de seguridad, implementando los controles que no cumplen o faltantes y volver a evaluarlos en una nueva auditoría donde se revisen el cumplimiento de los mismos para poder tener un buen desarrollo y contar con procedimientos seguros en la organización.

**Agradecimiento**

Se agradece a las autoridades y en especial al Director Metropolitano de Informática Ingeniero Jefferson Capelo por la apertura y el apoyo brindado en la recolección de información sobre las seguridades, manejo de procesos implantados en esta Dirección.

**Referencias Bibliográficas**

aglone3. (Julio de 2012). *Responsabilidad sobre los activos*. Obtenido de Responsabilidad sobre los activos: https://iso27002.wiki.zoho.com/7-1-Responsabilidad-sobre-los-activos.html.

aglone3. (Julio de 2012). *Seguridad Física y del Entorno*. Obtenido de Seguridad Física y del Entorno: https://iso27002.wiki.zoho.com/9-1-%C3%81reas-seguras.html.

aglone3. (Julio de 2013). *Adquisición, Desarrollo y Mantenimiento de Sistemas de Información*. Obtenido de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: https://iso27002.wiki.zoho.com/12-1-Requisitos-de-seguridad-de-los-sistemas.html

aglone3. (Julio de 2013). *Identificación de la legislación aplicable*. Obtenido de Identificación de la legislación aplicable: https://iso27002.wiki.zoho.com/15-1-1-Identificaci%C3%B3n-de-la-legislaci%C3%B3n-aplicable.html

aglone3. (Julio de 2013). *Organización Interna*. Obtenido de Organización Interna: https://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html.

aglone3. (Julio de 2013). *Política de seguridad de la información*. Obtenido de Política de seguridad de la información: https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html.

aglone3. (Julio de 2013). *Procedimientos y responsabilidades de operación*. Obtenido de Procedimientos y responsabilidades de operación: https://iso27002.wiki.zoho.com/10-1-Procedimientos-y-responsabilidades-de-operaciC3%B3n.html.

aglone3. (Julio de 2013). *Proceso de la gestión de continuidad del negocio*. Obtenido de Proceso de la gestión de continuidad del negocio: https://iso27002.wiki.zoho.com/14-1-1-Proceso-de-la-gesti%C3%B3n-de-continuidad-del-negocio.html.

aglone3. (Julio de 2013). *Requerimientos de negocio para el control de accesos*. Obtenido de Requerimientos de negocio para el control de accesos: https://iso27002.wiki.zoho.com/11-1-Requerimientos-de-negocio-para-el-control-de-accesos.html

aglone3. (Julio de 2013). *Seguridad en la definición del trabajo y los recursos*. Obtenido de Seguridad en la definición del trabajo y los recursos: https://iso27002.wiki.zoho.com/8-1-Seguridad-en-la-definici%C3%B3n-del-trabajo-y-los-recursos.html.

AS/NZS 4360(1999). (1999). *Estándar australiano administración de riesgos.*

Departamento de Comunicación. (Agosto de 2013). *ValdezAlbizu informa Banco Central obtiene certificación ISO 27001*. Obtenido de ValdezAlbizu informa Banco Central obtiene certificación ISO 27001: http://www.bancentral.gov.do/notas_del_bc.asp?a=bc2012-05-30.

Estándar internacional ISO/IEC. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información- Requerimientos.*

Estándar internacional ISO/IEC17799 - 27002. (2005). *ecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.*

Estándar internacional ISO/IEC27001. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requerimientos.*

ISO 31000. (2009). *Gestión de riesgo– principios y guías.*

Quezada. (2012). *Base de datos. Recuperado*. Obtenido de Base de datos. Recuperado: http://es.scribd.com/doc/119813298/Telconet.

Quito, M. d. (2011). *Plan de desarrollo 2012 - 2022.* Quito.