OFICIO No. CMS-RPQ-2016-111

Quito D.M., 15 de septiembre de 2016

Señor ingeniero
Andrés Eguiguren
Administrador de Contrato
Registro de la Propiedad de Quito

Presente.-

15/09/2016
10:47

De mi consideración:

Dentro del marco contrato No. 19-2014 del proyecto de "MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO", entre los productos que se deben entregar del componente C.2 Modernización integral del RP, Subcomponente 7. Gestión de la Calidad y Seguridad de la Información - Implantación de ISO 9001 y 27001, se encuentra el entregable E.60 "Manual de procedimientos de controles".

Con Oficio No. CMS-RPQ-2016-098 del 18 de agosto de 2016 se realizó la entrega del entregable E60.

Con Oficio No. RPDMQ-PROYMIRP-2016-0831C-OF de 31 de agosto de 2016, se emiten las observaciones al entregable E60.

Respecto a las observaciones se señala lo siguiente:

La primera observación dice:

"Se trata de un compendio de definiciones generales, políticas enmarcadas en un historial general de temas de seguridad y control con una vaga referencia a procedimientos."

Respuesta: En el texto del entregable se insertó la TABLA 1 que se encuentra en el entregable.

Las definiciones del entregable E60 están basadas estrictamente en lo estipulado en las cláusulas de la norma ISO 27001:2013 y en el ANEXO A de la misma, en el que se definen los controles y sus objetivos. Véase el cruce representado en la **TABLA 1** en el que

se detalla para cada elemento del "Manual de Procedimientos de Controles" (columna izquierda) el respectivo numeral de la norma que se cumple con el mismo (columna derecha).

Los contenidos del entregable E60 son de carácter general, así como lo son las referencias a procedimientos en razón de que estos deben ser definidos y aprobados por las autoridades del Registro de la Propiedad, para lo cual es indispensable cumplir con las siguientes formalidades que aún no se cumplen y que en su momento han sido requeridas al RPDMQ:

1. Designación formal del Comité Directivo de Seguridad de la Información
2. Designación formal del Comité Operativo de Seguridad de la Información
3. Designación formal del responsable de seguridad de la información
4. Designación formal de los propietarios funcionales de los datos
5. Designación formal del responsable de seguridad de la información dentro de la unidad de Tecnologías de la Información
6. Asignación y aceptación formal de responsabilidades relacionadas con seguridad de la información de todo el personal del Registro de la Propiedad, incluidos directivos, técnicos y usuarios
7. Definiciones detalladas y aprobación de los procedimientos que se esbozan en el documento "Estructuras Organizacionales", en el que para cada uno constan las entradas , las salidas, los niveles de responsabilidad y rendición de cuentas, así como el alcance de cada proceso relacionado con las estructuras organizacionales del Registro de la Propiedad indispensables para implementar la norma ISO 27001:2013
8. Aprobación por parte de la alta dirección de los riesgos residuales, previas definiciones de apetencia y posiciones institucionales frente a los riesgos y asignación del presupuesto para el proyecto de seguridad de la información.
9. Validación y aprobación por parte del Comité Directivo de Seguridad de la Información de las valoraciones de impacto en los servicios en las dimensiones de seguridad DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD de la información levantadas en las fichas de captura de los activos de información.

Las formalidades detalladas en la lista anterior, es decir, la integración, alcance, objetivos, responsabilidades y procesos asociados con los comités están definidos en el documento entregado por el Consorcio y denominado ***"Estructuras Organizacionales de Seguridad de la Información"*** inserto en el "Manual de Procedimientos". Así mismo están detalladas las funciones y responsabilidades de las demás estructuras necesarias para implementar seguridad de la información con base en la norma ISO 27001:2013. Las formalidades y aspectos metodológicos que deben cumplirse para los

puntos 8 y 9 están detalladas en el documento que contiene el ***"Metodología de Evaluación y Tratamiento de los Riesgos"***

Entonces, como sustentación de la observación que dice que las definiciones dadas en el entregable E60 son de carácter general, debemos aclarar que, en la medida que se cumpla con las formalidades administrativas establecidas en dicho entregable, sobre todo en lo que tiene que ver con las "Estructuras Organizacionales", estas generalidades pasarán ser específicas. En suma, la falta de especificidad se debe a que aún no se cumplen las formalidades básicas, fundamentales, para la adopción de la norma ISO 27001:2013

Una vez que el Registro de la Propiedad cumpla con las formalidades arriba detalladas, las definiciones, procedimientos políticas y demás aspectos dejarán de ser generales y pasarán a ser específicos y concretos basados en una nueva realidad institucional, las mismas que revisten el carácter de indispensables para poder avanzar en el proceso de adopción de la norma ISO 27001:2013 y de alcanzar la certificación.

TABLA 1. Cruce de documentos insertos en el "Manual de Procedimientos" con estipulaciones de la ISO 27001:2013.

A efectos de alcanzar la certificación, el Registro de la Propiedad deberá tomar uno a uno los documentos detallados a continuación y analizarlos, ajustarlos, aprobarlos y formalizarlos. Se detallan dos columnas: La izquierda que contiene el nombre del documento, política, procedimiento entregado y la columna derecha que detalla la cláusula de la norma o el control del ANEXO que se cumple con la formalidad de la columna izquierda correspondiente.

Documentos necesarios para la implementación de la norma ISO/IEC 27001 e incluidos en el "Manual de Procedimientos"	***Referencia a la cláusula de la norma o al control del ANEXO A relacionado a cumplirse***
Parte 1: Obligatorios	
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)

Plan de tratamiento del riesgo	6.1.3 e), 6.2
Informe sobre evaluación y tratamiento de riesgos	8.2, 8.3
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4 *(ANEXO A)*
Inventario de activos	A.8.1.1 *(ANEXO A)*
Uso aceptable de los activos	A.8.1.3 *(ANEXO A)*
Política de control de acceso	A.9.1.1 *(ANEXO A)*
Procedimientos operativos para gestión de TI	A.12.1.1 *(ANEXO A)*
Principios de ingeniería para sistema seguro	A.14.2.5 *(ANEXO A)*
Política de seguridad para proveedores	A.15.1.1 *(ANEXO A)*
Procedimiento para gestión de incidentes	A.16.1.5 *(ANEXO A)*
Procedimientos de la continuidad del negocio	A.17.1.2 *(ANEXO A)*
Requisitos legales, normativos y contractuales	A.18.1.1 *(ANEXO A)*

Otros no incluidos en el Manual por ser productos de la posterior implementación del mismo.	***Referencia a la cláusula de la norma o al control del ANEXO A relacionado***
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por parte de la dirección	9.3
Resultados de acciones correctivas	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3 *(ANEXO A)*

Parte 2: Documentos de uso común no estipulados explícitamente en la norma pero necesarios y de uso común incluidos	***Referencia a la cláusula de la norma o al control del ANEXO A relacionado***
Procedimiento para control de documentos	7.5

Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1
Política Trae tu propio dispositivo (BYOD)	A.6.2.1 *(ANEXO A)*
Política sobre dispositivos móviles y tele-trabajo	A.6.2.1 *(ANEXO A)*
Política de clasificación de la información	A.8.2.1, A.8.2.2, A.8.2.3 *(ANEXO A)*
Política de claves	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Política de eliminación y destrucción	A.8.3.2, A.11.2.7 *(ANEXO A)*
Procedimiento para trabajo en áreas seguras	A.11.1.5 *(ANEXO A)*
Política de pantalla y escritorio limpio	A.11.2.9 *(ANEXO A)*
Política de gestión de cambio	A.12.1.2, A.14.2.4 *(ANEXO A)*
Política de creación de copias de seguridad	A.12.3.1 *(ANEXO A)*
Política de transferencia de la información	A.13.2.1, A.13.2.2, A.13.2.3 *(ANEXO A)*

La segunda observación dice:

"La funcionalidad y lectura del mencionado manual de procedimientos de control o entregable E60, no facilita su entendimiento y aplicabilidad, ya que no menciona ningún tipo de procedimientos de control, existen tablas o cuadros, sin explicación a que se refieren."

Respuesta:

En primer lugar podemos decir que a esta observación también aplica la respuesta de la observación 1 y con la inserción de la TABLA 1 en el texto del entregable se aclara el rol de cada documento en relación con el cumplimiento de la norma ISO 27001:2013, que es el objetivo del entregable E60.

Cada uno de los documentos incluidos en el Manual de Procedimientos obedece a una estructura estandarizada en función de los requisitos de la norma ISO 27001:2013, es así que cada uno de los documentos que integran el Manual incluye un primer numeral que contiene el objetivo, el alcance y los destinatarios del documento respectivo. Respecto a la

mención al procedimiento de control aceptamos que faltaba esa indicación. En la TABLA 1 de la respuesta 1 la primera observación se supera esa omisión y así se determina qué cláusula de la ISO 27001:2013 se está cubriendo o qué control u objetivo de control se satisface. Los procedimientos de control relacionados con cada cláusula o punto del ANEXO A de la norma son de competencia del personal designado por el Registro de la Propiedad como responsable de la implementación de la norma, la gestión de los riesgos y su tratamiento para lo cual se facilitan las definiciones en el documento con la metodología de tratamiento de riesgos.

Respecto a las tablas o cuadros que observan como que no tienen explicación: Cada uno de los documentos tiene un esquema estandarizado que incluye un par de tablas para la identificación del documento y otra para el historial de modificaciones. Hay otras tablas o cuadros que son formalidades que deben ser llenadas con las definiciones que se vayan dando en el Registro de la Propiedad y cuyo nombre de las columnas especifica de qué se trata.

Para una mayor comprensión de los entregables es indispensable que las personas involucradas en su análisis y evaluación así como en su implementación conozcan el texto de la norma ISO 27001:2013, para lo cual en su debido momento y de manera oportuna se les indicó a los representantes del Registro de la Propiedad que adquirieran el texto de la norma en el INEN y la socializaran. Es necesario que los funcionarios que emiten las observaciones conozcan de la norma, el Consorcio ejecutó un taller al respecto y se indicó fuentes y sitios en dónde se puede obtener el detalle de la norma, estos conocimientos demandan una especialidad en la gestión de riesgos, por lo recomendamos la lectura de la norma ISO, que va a ayudar a comprender todos los entregables.

Por lo anterior sugerimos: ***Mantener una sesión de trabajo del personal directivo del Consorcio con las personas encargadas de revisar y emitir las observaciones por parte del Registro de la Propiedad con el objeto de aclarar los términos del entregable a la luz de la norma. Este documento pretende orientar a los directivos en los argumentos a exponer.***

La tercera observación dice:

"No se especifican los procedimientos por etapas enmarcadas en la necesidad de cada área que forma parte del Registro de la propiedad y el proyecto de modernización"

Respuesta: se inserta el siguiente texto dentro del numeral Objetivos y Alcance:

> ***"En lo concerniente la norma ISO 27001:2013 y al respectivo componente de Seguridad de la Información dentro del Proyecto de Modernización, las necesidades de cada una de las áreas relacionadas con el tema de seguridad de la información están recogidas en las FICHAS DE CAPTURA de los activos de información, realizadas de manera provisional por el Registro de la Propiedad (provisional en virtud de que falta cumplir formalidades en cuanto al esquema de responsabilidades, estructuras organizacionales y demás formalizaciones necesarias pendientes de realizar)."***

Las formalidades pendientes están detalladas en la respuesta a la primera observación que serán las que le den validez y el carácter de definitivo y orgánico a las valoraciones de impactos).

Con el levantamiento de tales fichas se cumple el primer procedimiento y se alcanzan las definiciones de necesidades de seguridad de cada área, ya que las valoraciones de impactos se dan por parte de los propietarios de los servicios y los datos para cada una de las dimensiones de seguridad de la información: DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, TRAZABILIDAD Y AUTENTICIDAD. Esto está recogido en el documento Modelo de Valor del dominio a certificar entregado por el Consorcio, elaborado utilizando una herramienta informática.

Las fichas de captura contienen las necesidades de cada área en cuanto a seguridad de la información ya que en éstas fichas se recogen las valoraciones de impacto en cada una de las dimensiones de seguridad de los activos de información esenciales, como son los DATOS y los SERVICIOS.

Esas valoraciones permiten determinar la situación actual en cuanto a seguridad de la información y se reflejan en el modelo que valora los riesgos inherentes tal como se detalla en el entregable E57.

Los siguientes procedimientos están detallados en la "Metodología de Evaluación y Tratamiento de los Riesgos" y básicamente son:

- Determinación y aprobación de riesgos residuales
- Definición y aprobación de la Declaración de aplicabilidad de controles
- Definición de salvaguardas y de la estrategia de seguridad aprobada por los respectivos Comités
- Elaboración y Aprobación del Plan de Seguridad de la Información, su calendario y presupuesto y asignación de recursos humanos
- Implementación del Plan.

- Elaboración y aprobación del procedimiento de mejoramiento continuo que adoptará el Registro de la Propiedad.

Como resumen de la respuesta a esta observación se debe anotar lo siguiente:

El primer procedimiento que se debe realizar para establecer las necesidades de cada área en lo concerniente a seguridad de la información en el marco del proyecto de Modernización está dado y se ha ejecutado mediante el llenado de las FICHAS DE CAPTURA en las que se detallan los activos de información del dominio a certificar y sus respectivas valoraciones de impacto por fallas en las dimensiones de seguridad. Esto constituye el punto de partida para los demás procesos relativos a la seguridad detallados más arriba.

Es necesario formalizar, analizar y aprobar por parte de los respectivos comités de seguridad del Registro de la Propiedad, las valoraciones dadas en las fichas de captura.

La cuarta observación dice:

"Se pudo determinar que gran parte del entregable en mención es copia textual de un proyecto de tesis que se encuentra en: Fuente: advisera.com/wp-content/uploads//sites/5/2015/06/Plan_del_Protecto_ES.docx ."

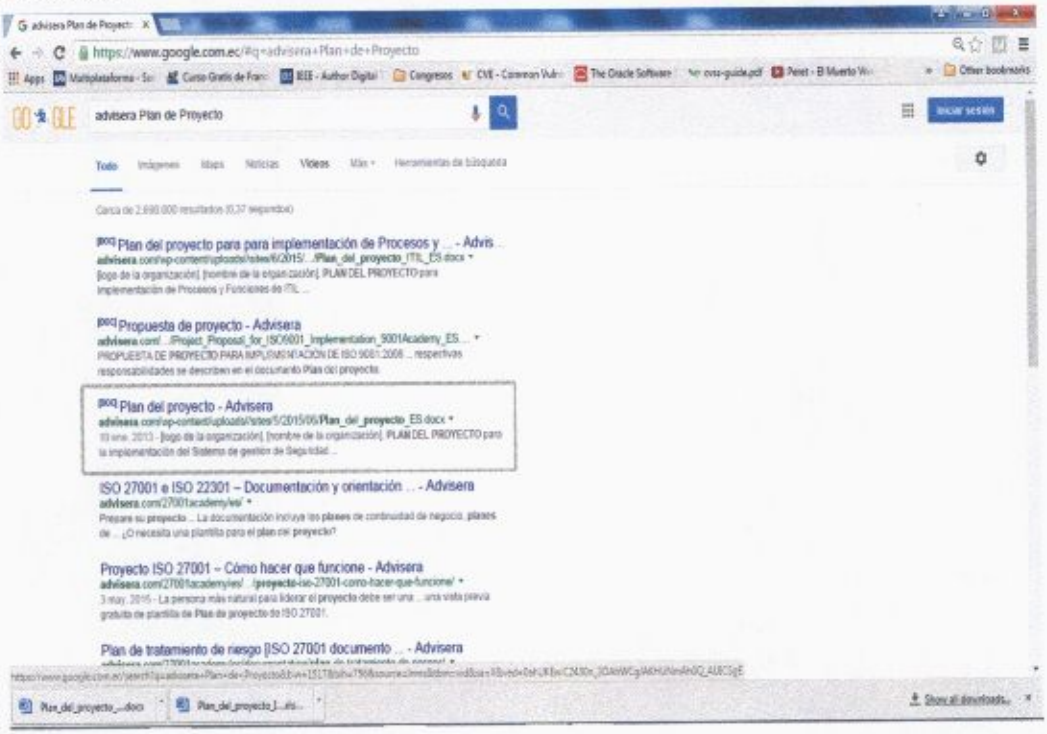
Respuesta: NO se inserta nada respecto a esta observación dentro del texto, ya que no aplica la observación.

Uno de los documentos que comprende el Manual entregado, efectivamente, es el "Plan de Proyecto". La referencia al sitio web indicada en las observación no corresponde a un proyecto de grado, sino a una página del sitio de la empresa **ADVISERA** en el sitio web http://www.advisera.com.

Debo hacer notar que la empresa ADVISERA, especialista de talla mundial en servicios y productos para la implementación y certificación en diversas normas ISO como la 27001:2013, ofrece al público sin costo alguno el texto en formato WORD denominado "Plan de Proyecto" en el que utiliza un esquema general de documento que cumple lo exigido por la norma ISO 27001:2013. Es una recopilación hecha por expertos internacionales basada estrictamente en las definiciones estandarizadas por ISO para sistemas de gestión, tales como la de seguridad de la información 27001 y la de calidad 9001. El documento no tiene ni "copyright" ni ninguna restricción para su uso. Lo puede bajar cualquier persona con solo registrar su nombre y una dirección de correo sin costo y sin limitaciones de uso ya que no es más que un esquema o "templete" de documento muy utilizado por expertos de todo el mundo (hay en inglés y en español). Se debe tomar en

cuenta que no es otra cosa que un modelo genérico de texto cuyo valor agregado y especificidad se alcanza en cada institución cuando se analiza, se complementa y formaliza con sus propias realidades que, en el caso del Registro de la Propiedad, se darán una vez se cumpla con las formalidades detalladas en respuesta a la primera observación. Mientras tanto el documento no tiene valor. El Consorcio lo entrega al Registro de la Propiedad como una propuesta de texto a completar con las especificidades de su propia realidad, lo que se ha hecho es una adaptación al contexto organizacional y a sus realidad interna.

Debemos reiterar que no se trata de una copia de una tesis de grado como se afirma equivocadamente (el URL dado no corresponde a ninguna tesis sino al sitio oficial de ADVISERA en el que se puede descargar el documento), como puede verse la captura de pantalla adjunta.



En virtud de lo anterior, adjunto al presente se servirá encontrar un CD de datos con el entregable E.60 ajustado.

Por la atención que preste al presente, le anticipo mi sincero agradecimiento.

Atentamente,

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE