Informe N. RPDMQ-TICS-2016-037
Quito, 28 de septiembre de 2016

30/09/2016
16h40

Para: Andrés Alberto Eguiguren Eguiguren
ADMINISTRADOR DEL CONTRATO No. 019-2014

Asunto: Segunda Revisión al Entregable E.61 "Declaración de Aplicabilidad de Controles"

Antecedentes:

Con fecha 15 de septiembre de 2016, el Consorcio MEB SEVENTEENMILE remite oficio No. CMS-RPQ-2016-112, mediante el cual se pronuncia al respecto de las observaciones realizadas por esta Comisión Técnica y que se les fue remitido mediante oficio No. RPDMQ-PROYMIRP-2016-0831D-OF de 31 de agosto de 2016.

Respecto a dicha contestación la Comisión Técnica manifiesta lo siguiente:

1.- Modificación de objetivo en Declaración de Aplicabilidad

> ***El objetivo del presente documento es bosquejar en una primera instancia qué controles son adecuados para implementar en el Registro de la Propiedad, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo facilitar la aprobación formal de la implementación de los controles mencionados.***

Dentro del contrato No. 019-2014 se encuentra el listado de bienes y servicios que el Consorcio MEB SEVENTEENMILE debe entregar al Registro de la Propiedad del Distrito Metropolitano de Quito, dentro del listado antes mencionado se encuentra el entregable "E. 68" que se trata de "Informe de Auditoría de certificación en ISO 27001", la Declaración de Aplicabilidad trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar **ISO/IEC 27001,** por lo que este entregable no puede ser "un bosquejo de primera instancia" debe ser el instrumento final mediante el cual se podrá realizar los controles previos a la Auditoria de certificación en ISO 27001.

2.- Mediante oficio No. RPDMQ-PROYMIRP-2016-0831D-OF de 31 de agosto de 2016 se solicita al Consorcio MEB SEVENTEENMILE que versión de ISO 27001 se ha utilizado como referencia para establecer los controles de la Declaración de Aplicabilidad. El Consorcio MEB SEVENTEENMILE ha aclarado que la versión utilizada es la del año 2013

3.- El Consorcio MEB SEVENTEENMILE indica: *"Se reitera que es necesarios se aprueben formalmente lo siguiente:"*

1. ***FICHAS DE CAPTURA DEL ACTIVOS DE INFORMACIÓN Y SUS VALORACIONES***

2. ***MODELO DE VALOR: Inventario de activos de información y sus valoraciones en las dimensiones de seguridad.***

[1]

Al ser necesario la aprobación tal como lo señala el consorcio se solicita se adjunte los respectivos documentos de respaldo, en los que se indique la aprobación de los numerales indicados.

4.- RIESGOS INHERENTES

Con respecto a riesgos inherentes el Consorcio MEB SEVENTEENMILE argumenta que: *"Es un documento ya entregado en TIC a los que está expuesto el Registro de la Propiedad por el solo hecho de usar tecnologías en la prestación de servicios ciudadanos"*.

Al respecto la Comisión Técnica solicita que se especifique si los "Riesgos Inherentes" son los que constan como Riesgos Intrínsecos en el entregable E.57, en qué fecha fue entregado y si este ya ha sido aprobado por la Comisión Técnica correspondiente y en qué fecha.

5.- RIESGOS RESIDUALES

Acerca de los Riesgos Residuales el Consorcio MEB SEVENTEENMILE manifiesta que dicho entregable ha sido "entregado en el momento oportuno al Registro de la Propiedad por parte del Consorcio"

Al igual que en el punto anterior la Comisión Técnica solicita al Consorcio se sirva indicar en qué fecha fue entregado el entregable E.58 y si este fue aprobado por la Comisión Técnica correspondiente y en qué fecha.

6.- DECLARACION DE APLICABILIDAD

Sobre la declaración de aplicabilidad mediante oficio No. RPDMQ-PROYMIRP-2016-0831D-OF de 31 de agosto de 2016 se solicitó al Consorcio que dentro de la Declaración de Aplicabilidad de Controles se complete la información en los campos: Justificación de elección/no elección, Objetivos de control y Estado.

[1] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles V2, Producto E.61, 19 Septiembre 2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si	⇧	⇧	Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI Si es necesario, el [cargo] define responsabilidades adicionales	⇧

Tabla 1: Aplicabilidad de controles[2]

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si			Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI Si es necesario, el [cargo] define responsabilidades adicionales	
A.6.1.2	Segregación de deberes	Si			Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra	

Tabla 2: Aplicabilidad de controles[3]

Siendo este un servicio que consta dentro del contrato No. 019-2014, y que el Consorcio para poder realizarlo ha podido recabar la información que permite entregar dicha Declaración de Aplicabilidad de Controles y es mas permite al Consorcio afirmar que:

"A juicio del Consorcio y de acuerdo a las observaciones del quehacer institucional, de su dependencia en tecnologías y de las actividades que desarrolla la Unidad de TIC, se considera que todos los controles son aplicables y que por lo tanto deben ser implementados."

[2] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016
[3] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles V2, Producto E.61, 19 Septiembre 2016

La Comisión Técnica insiste en que el Consorcio MEB SEVENTEENMILE complete la información en los campos: Justificación de elección/no elección, Objetivos de control y Estado.

7.- OTROS DOCUMENTOS

El Consorcio MEB SEVENTEENMILE presenta como resumen de respuesta a las observaciones presentadas sobre el entregable E61 lo siguiente:

> ***Es necesario que el Registro de la Propiedad cumpla las formalidades establecidas en la norma ISO 27001:2013 y recogidas en el documento entregado llamado "Manual de Procedimientos de Controles", de manera especial en el que tiene que ver con las "Estructuras Organizacionales", en el que se detallan los lineamientos dados por el Consorcio en cuanto lo que tiene que realizar el Registro de la Propiedad para adoptar la implementación de la norma ISO 27001:2013 y alcanzar la certificación en la misma en concordancia con el Proyecto de Modernización".***

El Consorcio no puede argumentar que el Registro de la Propiedad debe cumplir con formalidades recogidas en el documento entregado llamado "Manual de Procedimiento de Controles", cuando este documento como bien menciona el Consorcio dentro del oficio No. CMS-RPQ-2016-112, se encuentra actualmente observado por parte de la Comisión Técnica correspondiente.

CONCLUSIÓN

En virtud de las observaciones presentadas en este documento y las indicadas en el informe N.- RPDMQ-TICS-2016-029 del 30 de agosto del 2016 que aún no han sido en su totalidad subsanadas, la comisión técnica no puede aceptar a satisfacción el entregable E.61 "Declaración de Aplicabilidad de Controles" hasta que cumpla las observaciones realizadas en este informa.

José Rodolfo Taipe Guaño
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

Luz Verónica Flor Solís
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

Oswaldo José Paz y Miño Ramón
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

OFICIO No. CMS-RPQ-2016-112

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
10:17

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.61 "Declaración de Aplicabilidad de Controles".

Con Oficio No. CMS-RPQ-2016-099 del 18 de agosto de 2016 se realizó la entrega del entregable E61.

Con Oficio No. RPDMQ-PROYMIRP-2016-0831D-OF de 31 de agosto de 2016, se emiten las observaciones al entregable E61.

Respecto a las observaciones se señala lo siguiente:

Se inserta un texto explicativo en el entregable en relación con las observaciones al mismo que tienen que ver con las aprobaciones previas que son necesarias toda vez en que se centran en el hecho de que hay una secuencia de documentos previos.

El texto inserto cambia el punto de objetivos quedando de la siguiente manera:

> ***El objetivo del presente documento es bosquejar en una primera instancia qué controles son adecuados para implementar en el Registro de la Propiedad, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo facilitar la aprobación formal de la implementación de los controles mencionados.***
>
> ***Se reitera que es necesario se aprueben formalmente lo siguiente:***
>
> 1. ***FICHAS DE CAPTURA DEL ACTIVOS DE INFORMACIÓN Y SUS VALORACIONES***

2. ***MODELO DE VALOR: Inventario de activos de información y sus valoraciones en las dimensiones de seguridad.***
3. ***MODELO DE RIESGOS INHERENTES***
4. ***MODELO DE RIESGOS RESIDUALES***
5. ***METODOLOGÍA DE TRATAMIENTO DE LOS RIESGOS***

Se observa que se explicite a qué versión de la norma se refiere el documento, se ha incluido en todos los documentos anteriores y las explicaciones que la versión de la norma es ISO 27001:2013.

Hay una secuencia lógica, un paso lógico de un documento a otro documento, para cada una de los cuales, efectivamente, faltan las debidas formalidades expresadas en la respuesta a las tres primeras observaciones hechas al producto E60 Manual de Procedimientos de Controles. La secuencia es la siguiente y el detalle de las formalidades que deben ser cumplidas por el Registro de la Propiedad en cada paso se detalla a continuación:

1) FICHAS DE CAPTURA DE ACTIVOS DE INFORMACIÓN

Se diseñó y entregó en su momento a la unidad de TIC del Registro de la Propiedad una serie de fichas de captura (en formato EXCEL), para cada tipo activo de información del Registro de la Propiedad de acuerdo a una catalogación estándar que los divide en los siguientes tipos: Los servicios y sistemas informáticos, los equipos informáticos, los equipos auxiliares, las base de datos o archivos de datos, las aplicaciones y sistemas de información, las instalaciones físicas, los equipos auxiliares y las personas.

Para cada una de ellas se determina una tipificación que permite evaluar sus vulnerabilidades respecto a los riesgos que conlleva para las dimensiones de seguridad que son: DISPONIBILIDAD, INTEGRIDAD, CONFIDENCIALIDAD, TRAZABILIDAD Y AUTENTICIDAD y una valoración de los respectivos impactos negativos que causaría al Registro de la Propiedad una falla en cada una de esas dimensiones para cada uno de los activos.

Estas fichas de captura configuran un detalle del estado actual en cuanto a los riesgos operativos de carácter tecnológico que enfrenta el Registro de la Propiedad y permite establecer las necesidades de salvaguardas o controles de seguridad exigidos en la norma ISO 27001:2013.

Como ya se anotó en las respuestas a las observaciones al entregable E60, la información contenida en las fichas de captura de los activos de información deben ser validadas de manera acorde con las formalidades ***que aún no se han cumplido y que deben cumplirse para llegar a la determinación objetiva, real y formalmente expresada de la situación actual.***

Una vez más es necesario recalcar que el Consorcio, ha insistido de manera permanente y desde el inicio mismo del proyecto, en la necesidad de cumplir las formalidades establecidas en la norma como única forma de acercarse a la certificación en la norma ISO 27001:2013, para lo cual ha emitido y entregado los documentos necesarios y la capacitación adecuada.

2) MODELO DE VALOR (con base en las FICHAS DE CONTROL).

Este documento entregado es el modelo que comprende no solamente el inventario de activos de información que maneja la unidad de TIC's del Registro de la Propiedad sino las valoraciones de impacto en las dimensiones de seguridad que se debe realizar de manera oficial mediante las formalidades que están pendientes y que se detallan en respuesta a las primeras tres observaciones hechas al entregable E60. Las realizan los propietarios de los datos con la coordinación del Oficial de Seguridad y el responsable de TIC´s del Registro de la Propiedad.

La metodología para estas valoraciones y la herramienta informática para realizarlas fue facilitada por el Consorcio en razón de la imposibilidad de adquirir la respectiva licencia argumentada por el Registro de la Propiedad.

La metodología de llenado de las fichas de captura de los activos de información (véase documento MODELO DE VALOR entregado por el Consorcio) fue explicada a los funcionarios designados del Registro de la Propiedad, no obstante, al no estar formalizadas y aprobadas las estructuras organizacionales de acuerdo al documento entregado por el consorcio no existe el debido proceso de elaboración, discusión, aprobación y divulgación de los documentos y sus definiciones.

Luego de alcanzar unos documentos formalizados, discutidos y aprobados por las instancias permanentes se elaboran los siguientes documentos de la secuencia:

3) RIESGOS INHERENTES

Es un documento ya entregado que contiene el detalle de todos los riesgos operativos de origen en TIC a los que está expuesto el Registro de la Propiedad por el solo hecho de usar tecnologías en la prestación de sus servicios ciudadanos. Este detalle de riesgos inherentes (o potenciales), que deben ser presentados a los comités que aún no están conformados, los cuales a su vez deben dar su aprobación. Se trata de los riesgos que existen de manera potencial por el hecho de utilizar tecnologías de información en la prestación de los servicios institucionales.

La evaluación de estos riesgos tiene dos componentes: El primero es la valoración de los impactos (recogida en las fichas de captura de cada activo de información) y el segundo es la probabilidad de ocurrencia, que viene dada por la herramienta automatizada que se ha utilizado, datos que a su vez se basan en buenas prácticas internacionales.

Para cada activo de información se detalla un valor de riesgo en cada una de las dimensiones pertinentes según el tipo de activo. Los activos esenciales son LOS DATOS Y LOS SERVICIOS. Los datos reciben valoraciones en las dimensiones de INTEGRIDAD y de CONFIDENCIALIDAD y los servicios en las dimensiones de DISPONIBILIDAD y en las necesidades de TRAZABILIDAD (posibilidad de seguir una pista de quienes utilizan los servicios y de qué manera) y de la AUTENTICIDAD (posibilidad y necesidad de conocer de manera fehaciente si quien se conecta a un servicio es quien dice ser o no).

4) RIESGOS RESIDUALES

El cuarto elemento en la cadena de productos es el de riesgos residuales, documento entregado en el momento oportuno al Registro de la Propiedad por parte del Consorcio.

Los riesgos residuales son aquéllos que permanecen luego de la aplicación de controles. Deben ser aprobados por los comités, y aquellos que estén por fuera de los rangos de aceptabilidad que se definan deben recibir el tratamiento establecido en la estrategia que se adopte para ellos en función del costo beneficio y los recursos disponibles.

Tal como se explica en el documento entregado y comprendido en el Manual de Procedimientos llamado "Metodología de Evaluación y Tratamiento de los Riesgos", existen varias formalidades que deben ser cumplidas para llegar a una lista definitiva de riesgos residuales según la política que adopten los altos directivos del Registro de la Propiedad acorde con la apetencia y umbrales de riesgos que definan como los necesarios en función de las estrategias y los presupuestos.

Para llegar a esta definición se requiere un trabajo previo de planificación de seguridad en el que se recojan los recursos disponibles al momento, los objetivos de seguridad y los tiempos disponibles para alcanzarlos.

5) DECLARACIÓN DE APLICABILIDAD

Este quinto documento entregado registra los controles que sean aplicables para el registro de la Propiedad.

Se debe tomar en cuenta que la norma ISO 27001:2013 dice que si se excluyere alguna de las cláusulas de ésta no se puede asegurar conformidad con su cumplimiento. Además, el Registro de la Propiedad realiza todas las actividades de su competencia mediante la utilización de servicios tecnológicos, tanto los relacionados con hardware, software básico

y aplicaciones, telecomunicaciones, redes, soporte a usuarios, por lo que son aplicables todos los controles estipulados en el ANEXO A de la norma.

Este documento entonces debe comprender una lista de todos los controles estipulados en la norma ISO 27001:2013 en la que se señale su aplicabilidad total.

Si existiese algún control de los estipulados en la norma ISO 27001:2013, que el Registro de la Propiedad considerase "NO APLICABLE", así debería declararlo y explicar las causas de no aplicabilidad. A juicio del Consorcio y de acuerdo a las observaciones del quehacer institucional, de su dependencia en tecnologías y de las actividades que desarrolla la Unidad de TIC, se considera que todos los controles son aplicables y que por lo tanto deben ser implementados.

Este documento debe recoger además, las estrategias que se van a utilizar para la implementación de los controles, definiciones que debe hacer el Registro de la Propiedad en función de los recursos disponibles para el efecto. Debe ser aprobado por las instancias organizacionales definidas como responsables según las recomendaciones dadas al Registro de la Propiedad en el documento "Manual de Procedimientos", de manera principal en la parte relativa a Estructuras Organizacionales, roles y responsabilidades de seguridad de la información. Formalidad que aún no se ha realizado.

6) OTROS DOCUMENTOS

En el Manual de Procedimientos entregado se detallan una serie amplia de documentos, políticas, procedimientos y estructuras que se deben implementar para alcanzar la certificación en la norma. Estas implementaciones comienzan con las formalidades que aún no se han dado y sin las cuales cualquier esfuerzo de certificación es vano.

Como resumen de respuesta a las observaciones del entregable E61 Declaración de Aplicabilidad, podemos decir:

Es necesario que el Registro de la Propiedad cumpla las formalidades establecidas en la norma ISO 27001:2013 y recogidas en el documento entregado llamado "Manual de Procedimientos de Controles", de manera especial en el que tiene que ver con las "Estructuras Organizacionales", en el que se detallan los lineamientos dados por el Consorcio en cuanto lo que tiene que realizar el Registro de la Propiedad para adoptar la implementación de la norma ISO 27001:2013 y alcanzar la certificación en la misma en concordancia con el Proyecto de Modernización".

Es necesario aclarar que los productos finales requeridos para la certificación ***son resultados de procesos institucionales que aún no existen y que deben ser establecidos.*** El Consorcio ha emitido una guías y lineamientos metodológicos y técnicos para que la institución pueda llegar a tener esos productos a la luz de lo que dice la norma y de

experiencias en otras entidades. Es de alta importancia que cumplan paso a paso y una a una las formalidades, lo que dará paso a alcanzar la certificación, es un trabajo interno e indelegable del RPDMQ. El Consorcio cumple con lo que le corresponde: orientar, acompañar, asesorar, facilitar el trabajo, que es lo que hace y seguirá haciendo.

Los pasos, a grandes rasgos son los siguientes:

1. Conformación y formalización institucional del Comité ***Directivo*** de Seguridad de la Información (acorde a lineamientos dados por el Consorcio) y reunión inicial en la que se conozcan los documentos emitidos por el mencionado Consorcio y se disponga la implementación de las demás estructuras organizacionales, las políticas y procedimientos señalados en los respectivos documentos.
2. Conformación y formalización institucional del Comité ***Operativo*** de Seguridad de la Información y reunión inicial en la que se conozcan en detalle los documentos emitidos por el Consorcio y se ejecute la implementación y se alcance la aprobación de las demás estructuras organizacionales, de las políticas y de los procedimientos señalados por el Consorcio. Seguir lineamientos documentados por el Consorcio (detalladas a continuación). La conformación de este Comité deberá ser aprobada por el Comité Directivo señalado en el punto 1.
3. El Comité Operativo deberá conocer y aprobar, así como someter a la aprobación del Comité Directivo, el esquema de roles, responsabilidades y procedimientos recogidos en el documento denominado Estructuras Organizacionales de Seguridad de la Información. Este es un trabajo detallado en el que uno a uno se debe analizar, evaluar y ajustar cada uno de los alrededor de 30 documentos que recopilan el quehacer indispensable para la certificación en la norma. Es importante la designación de los Propietarios de los Datos, rol en el que se basan las definiciones detalladas de seguridad de la información recogidas en las fichas de captura que sirven a su vez como punto de partida para todas las definiciones institucionales relativas a seguridad de la información.
4. Se debe designar de manera formal al responsable de seguridad de la información de la institución. Este cargo se ha dado en llamar Oficial de Seguridad de la Información y su perfil, nivel de responsabilidad, alcance du sus funciones están dadas en el documento Estructuras Organizacionales. Este funcionario debe recibir la capacitación necesaria para el ejercicio de sus funciones y debe recibir la delegación necesaria para ejercer sus atribuciones.
5. Debe formalizarse la utilización de una herramienta automatizada para el análisis y tratamiento de los riesgos de TIC. El Consorcio ha recomendado y facilitado el uso de una herramienta de su propiedad y el Registro de la Propiedad debe adoptar esta o cualquier herramienta que considere se ajuste a sus necesidades. Se deben adquirir licencias empresariales de la herramienta escogida y capacitar al Oficial de Seguridad y al responsable de TIC en el uso de la misma.

Con la formalización de las estructuras organizacionales y el establecimiento de los niveles de responsabilidad y rendición de cuentas según lo recomendado en la documentación entregada por el Consorcio al Registro de la Propiedad estarán sentadas las bases para iniciar el proyecto de certificación en la norma ISO 27001:2013.

Con la designación del Oficial de Seguridad de la Información y la adquisición y capacitación en el uso de la herramienta de análisis y gestión de riesgos y con el apoyo y supervisión esquematizado en los párrafo anteriores, así como con la dotación de todos los recursos necesarios para implementar el plan de seguridad de la información el Registro de la Propiedad estará encaminado de manera definitiva hacia la certificación.

En virtud de lo anterior, adjunto al presente se servirá encontrar un CD de datos con el entregable E.61 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

Informe N.-RPDMQ-TICS-2016-029

Quito, 30 de agosto del 2016

Para: Andrés Alberto Eguiguren Eguiguren
ADMINISTRADOR DEL CONTRATO No. 019-2014

31/08/2016
17h00

Antecedentes:

Mediante Memorando No. RPDMQ DESPACHO-2016-079 de fecha 10 de Agosto del 2016 se nos asigno como MIEMBROS DE LA COMISIÓN TÉCNICA A CARGO DE LA RECEPCIÓN PARCIAL DEL ENTREGABLE E.61 DEL CONTRATO NO. 019-2014, PARA MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO.

Documentos Recibidos:

Se reciben dos documentos digitales en formato PDF los mismos que se encuentran publicados en el servidor del repositorio compartido de entregables de Modernización \\Srv100filerp01\modernizacion$\ENTREGABLES-Consorcio

1.- Oficio_CMS-RPQ-2016-099_Entregable_E61.pdf

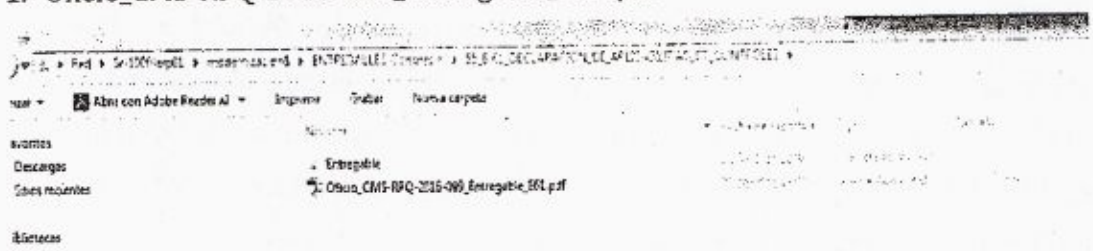

Figura 1: Oficio_CMS-RPQ-2016-099_Entregable_E61[1]

[1] Imagen realizada del repositorio compartido de entregables de Modernización \\Srv100filerp01\modernizacion$\ENTREGABLES-Consorcio\55_E-61_DECLARACION_DE_APLICABILIDAD_DE_CONTROLES

2.- E61 Declaración de Aplicabilidad.pdf

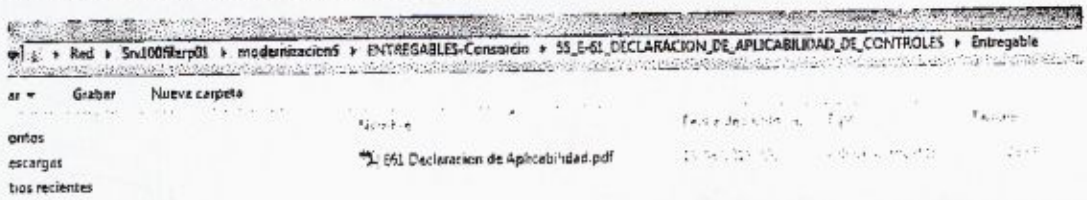

Figura 2: E61 Declaración de Aplicabilidad.pdf[2]

Análisis al entregable E.61:

1.- Dentro de los objetivos que establece el CONSORCIO MEB SEVENTEENMILE en la Declaración de Aplicabilidad de Controles manifiesta que busca:

"Definir qué controles son adecuados para implementar en el Registro de la Propiedad, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y facilitar la aprobación formal de la implementación de los controles mencionados"[3]

Para llegar a este objetivo es necesario que se encuentren establecidos varios puntos previos analizados, revisados y aprobados, siendo los más básicos una evaluación de riesgos (Intrínsecos y residuales) y posteriormente un Plan de Tratamiento de Riesgos.

Dentro del Contrato No. 19-2014 que tiene como objeto "Modernizar de manera integral el Registro de la Propiedad del Distrito Metropolitano de Quito" Dentro de la Cláusula Tercera y Cuarta se encuentra establecido el subcomponente 6 denominado "Gestión de la Calidad y Seguridad de la Información" se incluyen los entregables E.57, E.58 y E.59 que son Informe de Riesgos Intrínsecos, Informe de Riesgos Residuales y Plan de Tratamiento de Riesgos respectivamente.

[2] Imagen realizada del repositorio compartido de entregables de Modernización \\Srv100filerp01\modernizacion$\ENTREGABLES-Consorcio\55_E-61_DECLARACION_DE_APLICABILIDAD_DE_CONTROLES\Entregable

[3] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016

Actualmente dichos entregables se encuentran en fase de revisión por parte de las Comisiones Técnicas designadas por el Registro de Propiedad del Distrito Metropolitano de Quito encontrándose en revisión de ajuste los Entregables E.57[4] y E.58[5] desde el dieciocho de agosto de dos mil dieciséis mientras que el entregable E.59[6] se halla en revisión desde esa misma fecha, por lo que se puede establecer que estos no han sido aprobados, al no existir estos requisitos no es posible determinar ningún tipo de control aplicable.

Es importante señalar que la Comisión Técnica no está de acuerdo que en este entregable E.61 se deba aprobar riesgos residuales si estos no han sido determinados y deben ser aprobados por la Comisión Técnica que esta designada para el entregable E.58

"La Declaración de Aplicabilidad se desarrolla luego del tratamiento de riesgos, que a su vez es la actividad posterior a una evaluación de riesgos. El tratamiento tiene como objetivo la definición de las acciones a realizar para **mitigar** aquellos riesgos que han sido identificados y analizados.

Existen varias opciones de tratamiento, aunque de manera general se pueden agrupar en las siguientes categorías:

- **Mitigar.** Consiste en implementar algún control que reduzca el riesgo.
- **Transferir.** Ocurre cuando se delega la acción de mitigación a un tercero.
- **Aceptar.** Se presenta cuando el impacto generado por un riesgo es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo.

[4] OFICIO No. CMS-RPQ-2016-095
[5] OFICIO No. CMS-RPQ-2016-096
[6] OFICIO No. CMS-RPQ-2016-097

Una vez que se han definido las opciones de tratamiento para los riesgos, la organización debe aplicar medidas de seguridad, es decir, decidir de qué manera serán mitigados los riesgos. Es en este punto cuando se desarrolla un SoA, el documento donde se registran los controles de seguridad que son **aplicables** (necesarios) y si éstos se encuentran operando o todavía no."7

2.- Dentro de los documentos de referencia establecidos por el CONSORCIO MEB SEVENTEENMILE en el entregable E.61 se indica que se utilizó:

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos

La comisión considera que no se puede tomar como referencia documentada Política de Seguridad de la Información, Metodología de Evaluación y Tratamiento de Riesgos e Informe de evaluación y tratamiento de riesgos, que como lo determina el contrato **No. 19-2014** se encuentran descritas en el cronograma de entregables E.57 E.58 y E.59, que como se señaló anteriormente todavía no se encuentran aprobados por las respectivas Comisiones Técnicas designadas.

Es importante establecer la versión de la Norma ISO/IEC 27001 que se está utilizando como referencia, debido a que de versión a versión se indican diferente número de controles.

---

[7] http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

3.- Acerca de la Aplicabilidad de los Controles el CONSORCIO MEB SEVENTEENMILE manifiesta que "Son aplicables todos los controles del Anexo A de la norma ISO 27001"[8]. No se puede determinar que controles pueden aplicarse ya que como se menciona reiteradamente no constan informes que sustenten la necesidad de utilizar ciertos controles, por cuanto no existen las debidas aprobaciones de los entregables antes mencionados.

Dentro de la **Declaración De La Aplicabilidad De Controles** entregadas por el CONSORCIO MEB SEVENTEENMILE se evidencia que la información constante en la tabla no es completa, en los siguientes campos: Justificación de elección, Objetivos de control y Estado.

ID	Controles según la norma ISO/IEC 27001	Aplica (Si/No)	Justificación de elección / no elección	Objetivos de control	Método de implementación	Estado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si			Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI Si es necesario, el [cargo] define responsabilidades adicionales	

Tabla 1: Aplicabilidad de controles[9]

[8] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016
[9] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016

La COMISIÓN TÉCNICA considera que conforme a la tabla 1 se debe adjuntar: Políticas, Planes, Procedimientos y todos los documentos relacionados con la columna de **métodos de implementación** (debidamente aprobados)

Teniendo en cuenta que las Políticas, Planes, Procedimientos y todos los documentos relacionados se encuentran contenidos en el entregable E.60 "Manual de Procedimiento de Controles"[10] el que fue entregado el 18/08/2016 por el CONSORCIO MEB SEVENTEENMILE al Administrador de Contrato No.19-2014, el entregable hasta el momento se encuentra en proceso de revisión por la Comisión Técnica designada por el Registro de Propiedad del Distrito Metropolitano de Quito.

4.- Dentro del numeral cuatro en la página 46 del documento entregado por el CONSORCIO MEB SEVENTEENMILE referente a Aceptación de los riesgos residuales manifiestan que:

"Debido a que no se han podido reducir todos los riesgos en el proceso de gestión de riesgos, por medio de la presente se aceptan todos los siguientes riesgos residuales:

1. Todos los riesgos con valor 0, 1 ó 2.

2. Los riesgos que no pudieron ser reducidos a los niveles mencionados en el punto anterior luego de la aplicación de los controles, de acuerdo con el siguiente cuadro:"[11]

[Completar el cuadro con datos de todos los riesgos específicos que no son aceptables; utilizar el Cuadro de tratamiento de riesgos para tomar los datos].

Nro.	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Nuevo impacto	Nueva probabilidad	Riesgo residual

[10] Ruta compartida de entregables de Modernización, \\Srv100fileip01\modernizacion$\ENTREGABLES-Consorcio\59_E-60_MANUAL_DE_PROCEDIMIENTOS_CONTROLES, OFICIO No. CMS-RPQ-2016-098

[11] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016

Al respecto la Comisión Técnica manifiesta su desacuerdo, el CONSORCIO MEB SEVENTEENMILE no puede determinar lo señalado en el párrafo entre comillas, pues forma parte del entregable E.58 que no ha sido aceptado y que se encuentra en proceso de revisión de ajuste, tampoco fundamenta la razón de porque "no se han podido reducir todos los riesgos en el proceso de gestión de riesgos"[12]

5. – Existen algunos controles en el cuadro del entregable E.61 que el **métodos de implementación** esta descrito de manera muy general. Describir el cómo se lo implementara.

		Si			(Política del uso de controles criptográficos)	
A.10.1.2	Gestión clave	Si				
A.11	Seguridad física y del entorno					
A.11.1	Áreas seguras	Si				
		Si			Las áreas con información sensible están protegidas [describir cómo: con puertas, etc.]	
A.11.1.1	Perímetro de seguridad física	Si			El acceso a las áreas seguras del RDP deben estar controladas [describir cómo: tarjetas de acceso, entrada principal con guardia, etc.]	
A.11.1.2	Controles de entrada físicos					

Tabla 2: Aplicabilidad de Controles extraido del Entregable E.61

6.- Agregar glosario de términos al Entregable E.61

[12] CONSORCIO WEB SEVENTEENMILE, Declaración de aplicabilidad de controles, Producto E.61, Agosto 2016

Conclusiones:

Por todo lo expuesto anteriormente esta Comisión Técnica no puede aceptar a satisfacción el entregable E.61 hasta que se cumplan con las observaciones realizadas en este informe.

José Rodolfo Taipe Guaño
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61 CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

Luz Verónica Flor Solís
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61 CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

Oswaldo José Paz y Miño Ramón
MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61 CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ

Anexos

OFICIO No. CMS-RPQ-2016-095

OFICIO No. CMS-RPQ-2016-096

OFICIO No. CMS-RPQ-2016-097

OFICIO No. CMS-RPQ-2016-098

OFICIO No. CMS-RPQ-2016-095

Quito D.M., 18 de agosto de 2016

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

17/08/2016
11h00

Presente.-

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.57 "Informe de Riesgos Intrínsecos".

Con oficio No. RPDMQ-PROYMIRP-2016-0803A del 3 de agosto de 2016, comunica respecto a las observaciones realizadas al entregable.

En cumplimiento de lo requerido, adjunto se servirá encontrar un CD de datos con el entregable E.57 "Informe de Riesgos Intrínsecos" ajustado de acuerdo a las observaciones planteadas en las que se incluye el informe de pre-auditoria como diagnóstico inicial conforme a las reuniones previas mantenidas.

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

Atentamente,

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE

OFICIO No. CMS-RPQ-2016-096

Quito D.M., 18 de agosto de 2016

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

18/08/2016
11h00

Presente.-

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.58 "Informe de Riesgos Residuales".

Con oficio No. RPDMQ-PROYMIRP-2016-0803A del 3 de agosto de 2016, comunica respecto a las observaciones realizadas al entregable.

En cumplimiento de lo requerido, adjunto se servirá encontrar un CD de datos con el entregable E.58 "Informe de Riesgos Residuales" ajustado de acuerdo a las observaciones planteadas.

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

Atentamente,

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE

OFICIO No. CMS-RPQ-2016-097

Quito D.M.. 18 de agosto de 2016

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

18/08/2016
11h00

Presente.-

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.59 "Plan de Tratamiento de Riesgos".

En cumplimiento del cronograma del proyecto, adjunto al presente se servirá encontrar un CD de datos con el entregable E.59 "Plan de Tratamiento de Riesgos".

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

Atentamente,

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE

OFICIO No. CMS-RPQ-2016-098

Quito D.M., 18 de agosto de 2016

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

18/08/2016
11h00

Presente.-

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".

En cumplimiento del cronograma del proyecto, adjunto al presente se servirá encontrar un CD de datos con el entregable E.60 "Manual de procedimientos de controles".

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

Atentamente,

Byron Paredes Baitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE