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
10:27

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