QUITO
REGISTRO DE LA PROPIEDAD

Memorando N.- RPDMQ-TICS-2016-255-M

Quito, D.M., 30 de septiembre del 2016

PARA: Ing. Andrés Eguiguren
ADMINISTRATIDOR DEL CONTRATO NO. 19-2014

ASUNTO: Revisión Entregable E.56

30/09/2016 16h10

Antecedentes

Mediante Memorando No. RPDMQ-DESPACHO-2016-097 del 13 de septiembre de 2016 fuimos designados como parte de la comisión técnica a cargo de la recepción parcial del Entregable E56 denominado: Documento de Políticas de Seguridad de la Información, del Contrato No. 019-2014.

Mediante Memorando N.- RPDMQ-TICS-2016-250-M, dirigido al administrador del contrato No. 019-2014, se solicito la información sobre alcance del entregable E.56 y la relación con otros entregables, del cual hasta el momento no se ha tenido contestación, que es indispensable para la recepción del entregable.

Además se solicita información sobre la asignación formal de los Comites y Oficial de seguridad.

En base a lo expuesto, se comunica que el entregable se encuentra observado, para la aceptación es necesario que se corrija y subsane las observaciones presentadas en el informe adjunto N.- RPDMQ-TICS-2016-043-IN

Sin otro particular por el momento, aprovecho la oportunidad para reiterarle mis más altos sentimientos de consideración y estima.

Atentamente

Wilson Raúl Vela Gómez	Daniel Ricardo Sierra Chiriboga
MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E56 CONTRATO No. 019-2014 RPDMQ	

Adjunto: Informe N.- RPDMQ-TICS-2016-043-IN

QUITO
REGISTRO DE LA PROPIEDAD

Informe N.- RPDMQ-TICS-2016-043-IN
DM Quito, 30 de septiembre 2016

Observaciones sobre E56 Documento de Políticas de Seguridad de la Información del Contrato No. 019 – 2014

ANTECEDENTES

Mediante Memorando No. RPDMQ-DESPACHO-2016-097del 13 de septiembre de 2016 se designa la comisión de entrega-recepción parcial del Entregable E56 denominado: "Documento de Políticas de Seguridad de la Información" que corresponde al subcomponente 6 "Gestión de la Calidad y Seguridad de la Información", del Contrato No. 019-2014, para modernizar de manera Integral el Registro de Propiedad del Distrito Metropolitano de Quito, en base a lo cual se ha realizado la revisión del documento entregado al Registro de la Propiedad de dicho entregable, y se presentan las observaciones que constan en el área de Análisis de este documento.

ANÁLISIS

1. Con respecto al punto "1. Antecedentes, objetivo, alcance y usuarios "no se encuentra lo que indica el título como: objetivos, alcance y usuarios; estos deberían tener títulos independientes para cada tema. En la siguiente imagen se señalan varias observaciones:
   1.1. En el literal b) del punto 1., se encuentra que este documento se basa en conocimiento preliminar de "riesgos operativos", indicar cuáles son los riesgos operativos en los que se basan o en su defecto el documento de referencia.

> b) Se basa en el conocimiento preliminar de los riesgos operativos de procedencia en las tecnologías de la información y las comunicaciones. Por lo tanto, en cuanto dichos riesgos sean determinados y aceptados por las instancias institucionales cuyas formalidades están pendientes, esta política deberá ser ajustada. No obstante, existe la certeza de que todos los aspectos contemplados en la misma con aplicables a la realidad del Registro

Gráfico 1: Extracto de documento E56 - Documento de Políticas de Seguridad de la Información.pdf

   1.2. De acuerdo al texto del literal b) las formalizaciones están pendientes. Aclarar por qué se dice que existe una "certeza" de que todos los aspectos contemplados son aplicables a la realidad del Registro.
   1.3. En la serie de documentos previos que se detallan los literales i, ii, iii, iv. Indicar donde se los puede encontrar o cuáles son los documentos de referencia exactos en base al punto "4. Documentos de Referencia".

1.4. En el literal c) indica que estos aspectos están en las páginas de 6 a la 12. Se debe especificar exactamente en qué puntos y no en que páginas se encuentra esos aspectos.

2. En el punto "2. Justificativos" se visualiza un texto que dice "La Oficina de Seguridad de la Información". Verificar si está bien este nombre que se indica que después se lo llamará solo OSI.

3. En el punto "3. Objetivos" se define que...para cumplir los objetivos el Sistema de Seguridad de la Información (SGSI) se basa en los activos de información... Indicar el documento que contenga esta información.

4. En el punto "4. Terminología....." se debe mejorar la definición de sus términos en especial sobre Disponibilidad que es un factor importante en el SGSI, para prestar un servicio permanente.

5. En el punto "6. Gestión de la Seguridad de la Información", en el título "Requisitos de seguridad de la información" Indicar la lista de requisitos contractuales y legales o el documento de referencia.

   En el título "Controles de seguridad de la información" Indicar si los controles seleccionados corresponden a algún entregable.

6. Se observa que en el documento se refieren a los dominios de la ISO 27001-2013, en el punto "8. Validez y gestión de documentos" se realiza una lista de estos dominios, pero no están todos los que se mencionan en la norma, como se ve en la siguiente imagen:

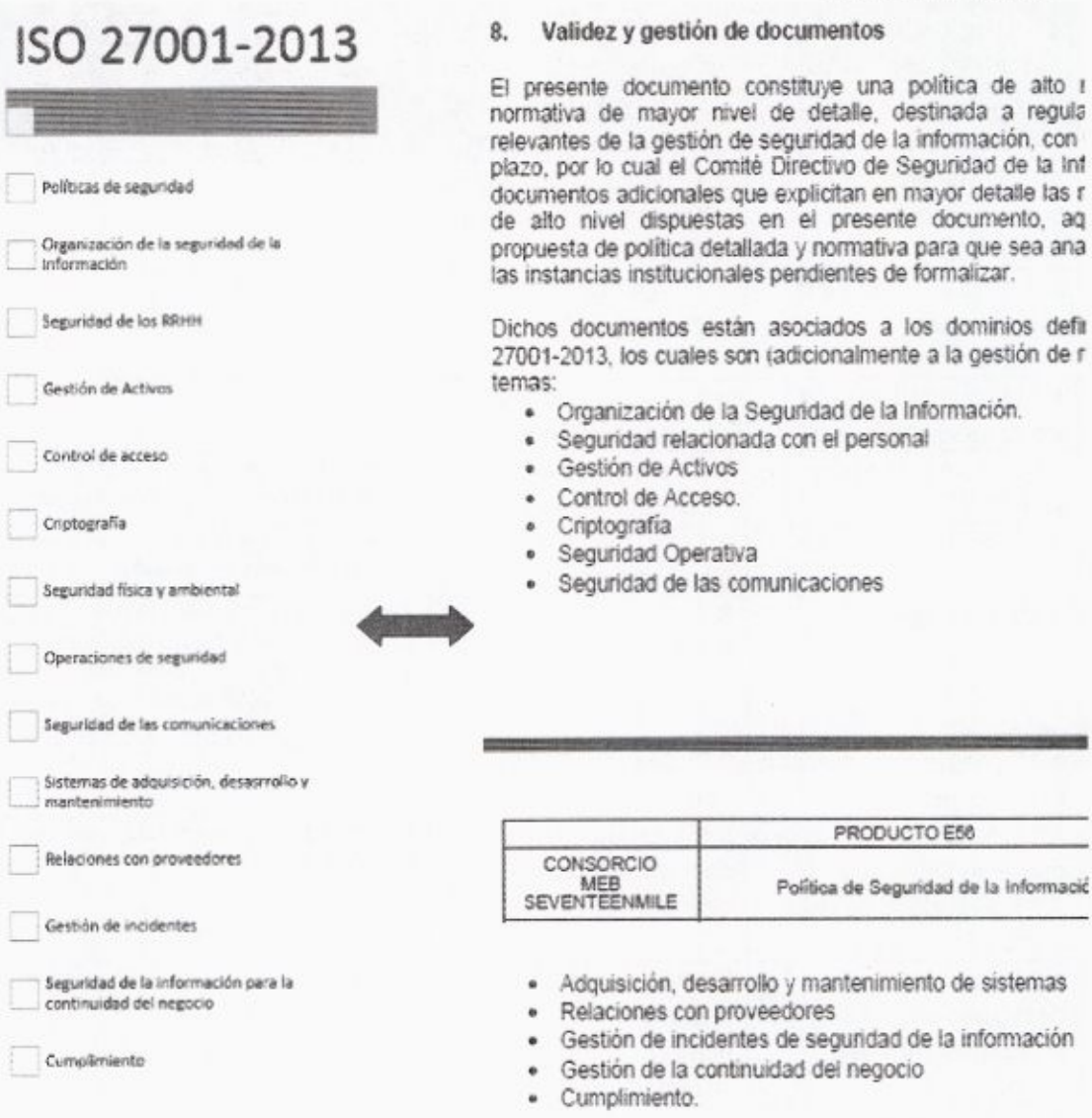

Gráfico 2: Extracto de documento E56 - Documento de Políticas de Seguridad de la Información.pdf Comparando con los Dominios Norma ISO 27001-2013

7. Revisando los anexos de la norma ISO 27001 – 2013, se evidencia que al comparar con el punto "9. Propuesta de Política Detallada y Normativa de seguridad de la Información" del documento entregable E56:"Documento de Políticas de Seguridad de la Información", no todos los puntos de control de los anexos están en el punto nueve. En la siguiente tabla se compara e indica cuales controles de la norma, no están en el entregable:

COMPARACIÓN DOMINIOS ISO 27001-2013 CON DOMINIOS DEL ENTREGABLE E56		
Norma ISO 27001-2013	E56 "Documento de Políticas de Seguridad de la Información"	Observaciones
A.5: Políticas de Seguridad de la información	9.1 Política de seguridad y normativa asociada a la 27001:2013	
A.6: Organización de la seguridad de la información	9.2 Organización de la seguridad de la información	
A.7: Seguridad ligada a los recursos humanos	9.4 La seguridad y los recursos humanos	
A.8: Administración de activos	9.3 Gestión de activos de la información	Indicar el documento o entregable al que hace referencia sobre los activos de información.
A.9: Control de Acceso	9.7 Controles de acceso a la información	No menciona ningún procedimiento de control, se debe ampliar esta información.
A.10: Criptografía	9.8.... 9.8.3...	Existe poca información sobre criptografía en punto 9.8 del documento de políticas de seguridad, pero se debe mejorar con más propuestas de políticas poniendo este punto en un dominio propio como indica la norma.
A.11: Seguridad física y del ambiente	9.5 Seguridad física y ambiental	
A.12: Seguridad de las operaciones	9.6 Gestión de las comunicaciones y de las operaciones	Ampliar las políticas en estos dominios para los controles.
A.13: Seguridad de las comunicaciones		
A.14: Adquisición, desarrollo y mantenimiento del sistema	9.8 Adquisición, desarrollo y mantenimiento de sistemas de información	Ampliar las políticas en este dominio para los diferentes controles.
A.15: Relaciones con el proveedor	No existe información de este dominio	No hay políticas escritas en base a este dominio de la norma, tener en cuenta que si existen proveedores que realizan mantenimientos y otras actividades.
A.16: Gestión de incidentes de seguridad de la información	9.9 Administración de incidentes de seguridad de la información.	
A.17: Aspectos de seguridad de la información en la gestión de continuidad del negocio.	9.10 Administración de la continuidad de servicios	Para la continuidad de servicios es importante mencionar políticas sobre redundancia para cumplir con los requisitos de disponibilidad, y no hay ningún párrafo que habla sobre este tema.
A.18: Cumplimiento	9.11 Cumplimiento de normas	

Tabla 1: Comparación Dominios ISO 27001-2013 Con Dominios Del Entregable E56

Se solicita que se completen los dominios de la Tabla 1, para asegurarse que se está tratando todos los puntos que requiere la norma.

Estos puntos deben coincidir con los que indica la norma 27001-2013.

8. En el punto "9. Propuesta de Política Detallada y Normativa de Seguridad de la Información" se solicita que revisen y corrijan la redacción, que genera confusión, en la siguiente imagen:

> Esta propuesta de normativa deberá ser revisada por las diversas instancias organizacionales que están pendientes de formalizar para que analicen el documento y lo ajusten en función de los riesgos residuales e emitan y aprobación

Gráfico 3: Extracto de documento E56 - Documento de Políticas de Seguridad de la Información.pdf

9. En distintos párrafos del punto "9.1.1 Gestión de Riesgos" se observa que se refieren a distintos numerales como 1.3 y 1.10 los cuales no fueron encontrados en el documento entregable "E56. Documento de Políticas de Seguridad de la Informacion.pdf". Favor especificar en qué puntos exactos están esas referencias pero revisando que coincidan los datos.
10. Revisar la redacción del texto del punto "9.3.1.3"
11. Revisar la redacción del texto del punto "9.6.1.2"
12. Se observa que en ciertos títulos está escrita la palabra "Administración" y en otros está la palabra "Gestión". Se solicita que esas palabras se cambien por la palabra "Gestión". En la siguiente imagen se indica una de las palabras que hay que cambiar:

> **9.7.2 Administración de los accesos de usuarios**

Gráfico 4: Extracto de documento E56 - Documento de Políticas de Seguridad de la Información.pdf

13. Sobre el punto "9.6.2.4" especificar la dependencia a la que hace referencia sobre los servicios y sus SLA´s.
14. Se observa en el punto "9.6.6.4", se solicita ampliar las políticas en este punto para un mejor entendimiento.
15. En el punto "9.7.1.1", se solicita ampliar los requerimientos de políticas de requerimientos de control de acceso.
16. En el punto "9.7.2.1", se solicita mejorar la redacción.
17. En el punto "9.7.3", se solicita ampliar y enfocar las políticas hacia el uso de información de autenticación secreta.
18. Revisar la redacción del punto "9.9.1.2"

CONCLUSIONES.

En base a las observaciones expuestas en la parte de análisis de este Informe, el entregable *E56–Documento de Políticas de Seguridad de la Informacion.pdf,* se encuentra observado con los siguientes puntos:

- Especificar el alcance, objetivos, antecedentes del documento de políticas de seguridad de la información.
- Especificar todo acerca de las referencias o documentos en los cuales se basan para la creación del documento de propuesta de políticas.
- Revisar la ortográfica, redacción y todo texto que pueda afectar el entendimiento del documento.

Para aceptar la recepción de dicho documento, debe corregirse y subsanarse las observaciones presentadas por los miembros de la comisión.

Elaborado por:

Wilson Raúl Vela Gómez	Daniel Ricardo Sierra Chiriboga
MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E56 CONTRATO No. 019-2014 RPDMQ	