OFICIO No. CMS-RPQ-2016-113

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.62 "Cuadro de Mando de Seguridad de la Información".

Con Oficio No. CMS-RPQ-2016-100 del 19 de agosto de 2016 se realizó la entrega del entregable E62.

Con Oficio No. RPDMQ-PROYMIRP-2016-0902B-OF de 2 de septiembre de 2016, se emiten las observaciones al entregable E62.

Respecto a las observaciones se señala lo siguiente:

Las primeras dos observaciones se refieren a que no hay información en los cuadros iniciales: Son cuadros que identifican al documento dentro del sistema de seguridad en producción. He procedido a colocar los datos explicativos de qué es lo que debe ir y la razón por la que no se puede llenar todavía. Básicamente son datos que se deben llenar a partir del conocimiento, ajustes y puesta en producción del documento. Por el momento es un modelo de documento previo, propuesto en el marco de lo que estipula la norma ISO 27001:2013.

Para acoger la tercera observación se dejó explícito y claro que el SGSI depende del Registro de la Propiedad y no de TIC's.

La cuarta observación pide que se puntualice ***"los nombres de quienes integran el directorio del SGSI"***. En respuesta se aclara que a lo que se refiere el punto observado no

es a "los miembros del Directorio del SGSI", sino a los miembros de la alta dirección del Registro de la Propiedad y se insertaron los cargos que de acuerdo con el organigrama publicado en el sitio web del Registro de la Propiedad constituyen dichas altas autoridades.

Ni la norma ni el entregable se refieren en ninguna parte al concepto de Directorio del SGSI. A lo que si se refiere el entregable en este punto es a los ***miembros del equipo de proyecto del SGSI*** y su rol en el SGSI. En el texto insertado ahora aclara que éstos deberán ser designados por el Comité Directivo de Seguridad de la Información cuando éste entre en funcionamiento de acuerdo con lineamientos dados en el Manual de Procedimientos y en particular en el documento denominado "Estructuras Organizacionales de Seguridad de la Información".

La quinta observación dice que se aclare ***"el contenido de cada una de las dimensiones de seguridad"*** y que éstas ***"deben estar explícitas y aprobadas en entregables anteriores"***
Para sustentar esta inquietud se ha insertado en el respectivo texto la aclaración de que las dimensiones de seguridad están explicadas en el glosario de términos que se ha adjuntado a los entregables E58 y E60, además deben tomar en cuenta que esas dimensiones de seguridad fueron suficientemente aclaradas con personal de TIC's del Registro de la Propiedad toda vez que en las FICHAS DE CAPTURA DE ACTIVOS DE INFORMACIÓN se incluyeron valoraciones a cada una de estas dimensiones en todos los activos declarados por el Registro de la Propiedad. En cuanto a que deben ser aprobados previamente se aclara que el Registro de la Propiedad ya ha emitido unas observaciones a estos dos entregables y se están recogiendo.

La sexta observación pide que se aclaren las razones por las cuales "Modelo de Valor" y el "punto 9.1 de la norma ISO 27001:2013" son incluidos en la parte denominada Documentos de Referencia.
Se hacen las aclaraciones del caso y se inserta el texto relevante de la norma. Se aclara que los dos documentos de referencia son claves para elaborar el cuadro de mando.

La séptima observación expresa inquietud con respecto a la siguiente afirmación hecha en el entregable (resaltada en rojo: Transcribo del entregable:

"...

Estos indicadores deben ser gestionados adecuadamente para lo que deben disponer de las estructuras organizacionales, el esquema de responsabilidades y los procesos que permitan configurar una estrategia de medición consistente con los objetivos estratégicos. No se puede hablar de un buen servicio si de manera permanente "se cae el Sistema" y los usuarios no pueden realizar sus trámites registrales. Si existiese alguna falla importante de cualquier servicio crítico para la misión, este hecho debería ser conocido de manera inmediata por las autoridades, quienes dispondrán la

respectiva investigación de las causas y el planteamiento de las soluciones idóneas. Para ello es que se necesita un Cuadro de Mando de Seguridad de la Información."

La manifiesta preocupación surge porque toman la frase como si fuera una afirmación de una realidad que está ocurriendo, lo cual no es así, puesto que estamos en una fase inicial y no se tiene evidencias de lo que ocurre. Es un ejemplo, nada más que ilustra un posible escenario que amerita la adopción de un cuadro de mando. Para solventar la inquietud se ha puesto todo el párrafo en modo condicional, indicando que se trata de una situación hipotética que podría ocurrir.

La octava observación pregunta por qué se escogieron los servicios que constan en la siguiente tabla :

SERVICIO	***DIMENSION Y VALORACIÓN*** ***PERIODO DE EVALUACIÓN: Del ___ al _____***						***NIVEL DE APROBACIÓN***
	DISPONIBILIDAD (%)		***INTEGRIDAD***		***CONFIDENCIALIDAD***		
	ESPERADO	***ALCANZADO***	***ESPERADO***	***ALCANZADO***	***ESPERADO***	***ALCANZADO***	
Servicios Ciudadanos	***99.8***	***99.8***	***99.5***	***99.6***	***99.4***	***99.4***	
Elaboración de Inscripciones (actas)	***99.8***	***99.5***	***99.1***	***99.0***	***99.8***	***99.5***	
Elaboración de Certificados	***99.8***	***99.4***	***99.3***	***99.2***	***99.8***	***99.7***	
Consultas de Actas y Certificados	***99.8***	***99.6***	***99.7***	***99.0***	***99.8***	***99.4***	
Indicadores de desempeño (Cumplimiento de controles de la norma)	***Este indicador se calcula con base en el cumplimiento de los controles de la ISO 27001 detallados en la hoja Desempeno de este libro. Se realiza el promedio simple del número de controles que están implementados según los aspectos de dicha norma.***						

RESPUESTA:

Se escogieron esos servicios con base en el organigrama oficial del registro de la propiedad en el que se determina cuáles son los procesos agregadores de valor, los de gobierno y los de soporte y apoyo, estos servicios se siguen manteniendo en el nuevo manual de procesos y de ser el caso podrán ser actualizados cuando se aprueben los productos relacionados a gestión de procesos.

La idea de un cuadro de mando no es monitorear absolutamente todos los servicios, sino los principales de los procesos de agregación de valor y de gobierno, que son los que están propuestos. No se debe congestionar un cuadro de mando con aspectos que pueden ser tratados en instancias diferentes.

Se pone un párrafo aclaratorio en el texto del entregable para sustentar esta observación.

La novena observación dice que ***"se debe anexar el Manual de Procedimientos"***

RESPUESTA:

El Manual de Procedimientos es el entregable E60.

La décima observación tiene que ver con la integración del Comité de Seguridad. Se ha respondido insertando el siguiente párrafo aclaratorio:

> ***"Todas las estructuras organizacionales indispensables para implementar el sistema de gestión de seguridad de la información están detalladas y justificadas en el "Manual de Procedimientos de Controles", concretamente en uno de sus documentos integrantes llamado "Estructuras Organizacionales de Seguridad de la Información" entregado y en fase de análisis y emisión de observaciones. En ese documento están detallados los integrantes de cada uno de los comités, sus responsabilidades, ámbito de acción, y los procesos asociados con tales comités. Están por formalizarse y ponerse en producción todas las estructuras propuestas. Se remite a la revisión del mencionado documento para todos los detalles."***

La undécima observación dice:

"Puntualizar los principios de cantidad y tiempo de la mano de la política de seguridad"

RESPUESTA: se inserta en el texto una nota aclaratoria respecto a la política de seguridad de la información según las siguientes consideraciones:

En el ***"Manual de Procedimientos de Controles"*** existe en documento con una propuesta de ***"Política de Seguridad de la Información"***, basada estrictamente en el ANEXO A de la norma ISO 27001:2013.

Esta propuesta debe ser revisada por los respectivos comités y ajustada al resultado final de las formalidades pendientes relativas a la aprobación de los riesgos. Una política de seguridad se fundamenta en el análisis de los riesgos y su objetivo es permitir alcanzar los

niveles de seguridad que se propongan en función de la estrategia institucional y los recursos disponibles, para todo lo cual es indispensable el cumplimiento de las formalidades pendientes detalladas en las respuestas a los entregables E60 y E61.

La observación número 12 se refiere a que ***"no existe firma de responsabilidad"***

El espacio reservado para nombre y firma al que se refiere la observación corresponde a quien firme el documento propuesto. No han tomado en cuenta que es una propuesta de documento y deberá ser firmado por quien en su momento sea designado como responsable de acuerdo con las formalidades que aún están pendientes.

En respuesta a esto se insertó una indicación en ese sentido en el entregable.

La observación número 13, que consta en el punto 4 del oficio de observaciones llamado Metodología, dice:

> ***"En el documento no existe métodos de investigación, en el caso de haberlo no se detalla la fuente para su verificación y autenticidad del mismo"***

RESPUESTA:

Supongo que esto tiene que ver con la observación cuarta del entregable E60 ya respondida, observación que 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 ."

Este documento entregable E62 no es un trabajo de investigación, más bien es un documento de buenas prácticas y estándares internacionales de uso general y extendido, cuyos formatos y contenidos tiene una estructura determinada en la norma y utilizada por entidades de todo el mundo. Cosa similar ocurre cuando una organización implementa ITIL, por ejemplo, en ese marco de trabajo se encuentran modelos estándares de documentos, procesos, etc. que se utilizan en todo el mundo "customizándolos". Que es lo que se está haciendo en el RPDMQ mediante la utilización de modelos de documentos publicados por empresas especializadas en este tipo de sistemas de gestión.

Son "templetes" de documentos contextualizados con base en la realidad específica de una entidad, en este caso del Registro de la Propiedad.

Cada documento comprende textos de dos categorías:

1. Textos estándares "de cajón" que van en todos los documentos (caso similar, por ejemplo, a un contrato de compra-venta o de arrendamiento estandarizado, sin rellenar). Estos textos son comunes en función de lo que exige la norma.
2. Texto contextualizado según la entidad a la que se aplique y que se basa en definiciones particulares del registro de la Propiedad. Nosotros lo que hemos hecho es contextualizar esos contenidos hasta donde es posible de acuerdo a la realidad del Registro de la Propiedad, su estructura, sus objetivos, sus sistemas de información, sus recursos tecnológicos, etc. Las demás cosas que no se han colocado obedecen a definiciones que aún no se han formalizado.

Véase la respuesta a la mencionada observación 4 del E60.

No se insertó nada a este respecto en el documento por que no viene al caso la observación ya que no es una investigación sino una aplicación de una norma internacional y un marco de gobierno de seguridad de la información.

En virtud de lo anterior, adjunto al presente se servirá encontrar un CD de datos con el entregable E.62 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