DEMPILE S.A.
Compañía Consultora Técnica

OFICIO: DEMPILE-RPQ-00134-2016
Quito, 23 de diciembre de 2016

Señor ingeniero
Patricio Espín
ADMINISTRADOR DEL
CONTRATO NO. 005-2015
REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO
Presente.

De mi consideración,

Ref.: Se informa sobre avance de productos

En atención a sus Oficio No. RPDMQ-PROYMIRP-2016-1205A-OF y RPDMQ-PROYMIRP-2016-1212C-OF de 5 de diciembre de 2016 y 12 de diciembre de 2016 respectivamente, manifestamos:

1. ANTECEDENTES

Lo solicitado, **no corresponde a unINFORME OFICIAL DE PRODUCTOS** previsto dentro de nuestro contrato pues esta Fiscalización no ha sido notificada formalmente con la última versión, en cada caso, entregada por el Consorcio contratista.

La información puesta a consideración de Dempile S.A. corresponde a 11 productos como se detalla en el Oficio en referencia. El informe solicitado de los entregables puestos en consideración de Dempile S.A., se recoge a continuación.

Si bien es cierto que el contrato está vigente, el retraso en la presentación de productos ha sido directa responsabilidad del Consorcio contratista. Esta Fiscalización ha venido realizando las alertas correspondientes desde hace tiempo atrás.

2. EVALUACIÓN DEL CONTENIDO DE LOS PRODUCTOS PUESTOS A CONSIDERACIÓN DE FISCALIZACIÓN

E.57: Informe de los riesgos intrínsecos del Registro de la Propiedad en razón de uso de nuevas tecnologías de la información y las comunicaciones

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar revisada, caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- Como introducción al documento debe colocarse:

  - Diagnóstico inicial del RPQ.
  - Una sección que indique la metodología a seguirse para la evaluación y tratamiento del riesgo
  - Una sección en donde se indique técnicas para evitar y minimizar los riesgos encontrados.

- El documento desde la página 31 hasta la 209 está compuesta principalmente de los anexos que deben especificar y justificar:

  - Herramienta con la que se obtuvo esa información.
  - Validar la información del anexo, esto es, funcionarios de RPQ deben firmar la información levantada para considerarse como válida.
  - Procedimiento que se utilizó para la recolección de información, esto para poder seguir el mismo esquema para los procesos futuros de actualización de información obtenida. Esto permitiría que RPQ simplemente actualice y versione las fichas inicialmente recolectadas y no se tenga que ingresar la información nuevamente desde cero.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.58: Informe de los riesgos residuales del Registro de la Propiedad en razón de uso de nuevas tecnologías de la información y las comunicaciones

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar revisada, caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- Como introducción al documento debe colocarse:

  - Diagnóstico inicial del RPQ.
  - Una sección que indique la metodología a seguirse para la evaluación y tratamiento del riesgo

- Una sección en donde se indique técnicas para evitar y minimizar los riesgos encontrados.

- El documento desde la página 31 hasta la 209 está compuesta principalmente de los anexos que deben especificar y justificar:

  - Herramienta con la que se obtuvo esa información.
  - Validar la información del anexo, esto es, funcionarios de RPQ deben firmar la información levantada para considerarse como válida.
  - Procedimiento que se utilizó para la recolección de información, esto para poder seguir el mismo esquema para los procesos futuros de actualización de información obtenida. Esto permitiría que RPQ simplemente actualice y versione las fichas inicialmente recolectadas y no se tenga que ingresar la información nuevamente desde cero.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.60: Manual de procedimientos de controles

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar validada caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- Si bien el documento es un manual se solicita incorporar:

  - Firmas de aceptación del manual por parte de RPQ
  - Incorporar en los formatos propuestos particularidades propias de RPQ es decir aterrizar la propuesta de lo genérico al caso puntual RPQ.

- El documento hace referencia a entregables anteriores que aún no cuenta con validación del RPQ por lo que este entregable no es sustentable en tanto entregables previos no sean aceptados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.62: Cuadro de mando de seguridad de la información

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar validada caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- En la sección OBJETIVOS, ALCANCE Y USUARIOS se hace referencia a unidades institucionales, procesos de gobierno, agregación de valor y de soporte y apoyo pero no se hace referencia al documento donde se puede validar esta información.

- Se hace referencia a entregables previos no validados ni aprobados como el Modelo de Valor y las Fichas de Captura de Activos de Información. No puede hacerse referencia a esa información cuando no ha sido aprobada

- Se hace referencia al organigrama oficial del Registro de Propiedad pero no se anexa el documento para su validación.

- En la sección INDICADORES se coloca un cuadro con indicadores como: servicios ciudadanos, elaboración de inscripciones, elaboración de certificados, consultas de actas y certificados. Fiscalización considera que no son los únicos indicadores que deben constar en esta sección y que se deben levantar indicadores por proceso que conste en el Alcance de la implementación del sistema de gestión. Adicionalmente debe anexarse un documento de trabajo en el cual conste bajo que criterio se escogió los indicadores y la aprobación del RPQ de aceptación de los indicadores.

- En el Anexo del documento se encuentra una matriz de indicadores de desempeño, se debe indicar la aplicabilidad y forma de uso de estos indicadores por parte de RPQ y la periodicidad de evaluación

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.61: Declaración de aplicabilidad de controles

Observaciones encontradas:

- En relación a este documento se solicita anexar una prueba de que existió una reunión de consenso con RPQ para validar la matriz, caso contrario esta matriz podría tomarse como apreciaciones del Consorcio sin sustento en mesas de trabajo.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.63: Manual de procedimientos del SGSI

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar validada caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- Si bien el documento es un manual se solicita incorporar:
  - Firmas de aceptación del manual por parte de RPQ
  - Incorporar en los formatos propuestos particularidades propias de RPQ es decir aterrizar la propuesta de lo genérico al caso puntual RPQ

- El documento hace referencia a entregables anteriores que aún no cuenta con validación del RPQ por lo que este entregable no es sustentable en tanto entregables previos no sean aceptados.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.55: Documento del alcance del sistema de gestión de seguridad de la información

Observaciones encontradas:

- En la sección DOCUMENTOS DE REFERENCIA especificar como los documentos tienen relación con el entregable y adjuntar mediante Anexo dichos documentos. En el caso de documentos específicos como:

  - Documento de Plan de Proyecto para la implementación de la norma ISO 27001 adjuntar como Anexo el plan de proyecto de implementación "aprobado" por RPQ.
  - Regulaciones y procedimientos internos aplicables a la entidad listar las regulaciones a las que hace referencia, no se puede citar de manera genérica.
  - Modelo de Valor, Modelo de Salvaguardas, Modelo de Procedimientos entregar los modelos "aprobados" por RPQ

- En la sección PROCESOS Y SERVICIOS se hace mención a:
    - La matriz de competencias institucional, adjuntar mediante anexo dicha matriz; la misma deberá ser validada y aceptada por el RPQ.
    - En esta misma sección se habla de los procesos cubiertos para el alcance del SGSI pero se debe adjuntar el documento de procesos definitivo "aprobado" por el RPQ para determinar si los procesos a los que se hace referencia en este alcance son correctos

- En la sección UNIDADES ORGANIZATIVAS se lista las unidades que intervendrán pero no se hace referencia a ningún documento oficial del RPQ en donde se pueda validar que esas unidades forman parte de la entidad, incluso existe una observación del personal de RPQ en relación al informe en donde indica que se hace referencia a una unidad que no consta en la página del RPQ.

- En la sección REDES E INFRAESTRUCTURA de TI se tiene las siguientes observaciones:

    - Se presenta un listado de usuarios por unidad debe indicarse de donde se obtuvo esta información y si el número de usuarios es constante o variable en el tiempo. En el caso de que se variable que cambio se espera para los siguientes 5 años. Deberá entonces presentarse un documento de levantamiento de información.
    - Se hace referencia a servicios compartidos pero no se indica de donde se obtuvo esta información. Deberá entonces presentarse un documento de levantamiento de información.
    - Se hace referencia a los programas que soportan los procesos registrales pero solo se menciona al SISREG y SIREL, si se hace referencia a esto deberá colocarse el listado de todos los programas del RPQ y su relación de dependencia, etc.
    - El ISO 27001 deberá ser implementado cuando el SIREL esté en funcionamiento al 100% por lo que no debería haber referencias a que el sistema está en pruebas.
    - Se presenta un gráfico de arquitectura de red. Este gráfico deberá tener coherencia con el documento de arquitectura de sistemas que es parte de los solicitado por RPQ y Fiscalización al Consorcio y al cual debe hacerse referencia en este documento cuando se presente gráficos de arquitectura.

- En la sección COMENTARIOS SOBRE EL ALCANCE:

    - Se hace referencia a servicios del municipio y servicios de terceros debe anexarse documentos que permitan determinar de donde se sacó ese listado de servicios para validación.
    - Debe adjuntarse el documento de niveles de servicio para validación.

- En la sección VALIDEZ Y GESTIÓN DE DOCUMENTOS:

  - Se presenta una fecha de validez que indicaría que el documento revisado por fiscalización ya no tiene validez.
  - Se indica que el oficial de seguridad es el responsable de dar mantenimiento al documento e indicar el mecanismo de actualización pero se considera que esto debe ser incluido y no hacer referencia a la responsabilidad del oficial, esto es, debe incluirse un texto que indique bajo que condiciones se actualiza el documento, cual es el nombre del oficial, etc., como se presenta actualmente da la idea de que el documento es una guía no actualizada ni trabajada en conjunto con el oficial de seguridad.

- En la sección ANEXO:

  - Se evidencia que los activos de información fueron levantados mediante fichas que indica que no han sido aprobadas, es mandatorio adjuntar las fichas aprobadas caso contrario el listado es inservible.

  - Se indica que la fecha de levantamiento es de 2015 con actualización Agosto de 2016 esto debe entregarse actualizado a la fecha y sobre todo con la inclusión de todos los componentes a la fecha en que los sistemas nuevos salgan a producción, cualquier levantamiento intermedio es informativo y se considera no definitivo

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.56: Propuesta de una política de seguridad de la información

Observaciones encontradas:

- En la sección HISTORIAL DE MODIFICACIONES se indica que las formalizaciones del documento están pendientes esto daría a entender que el documento no ha sido aprobado por funcionarios del RPQ. Se debe aclarar este punto.

- En la sección ANTECEDENTES se indica que lo expuesto es una propuesta y que no ha sido validada en una mesa de trabajo con RPQ pero se asume o se tiene la "certeza" de que lo que se expone podría aplicar a la realidad del RPQ, esto debe validarse puesto que el documento definitivo no puede estar basado en "certezas" y no se puede

asumir que lo propuesto va a ser adoptado por RPQ si este no lo ha aprobado. Así mismo adjuntar como anexo los documentos a los que se hace referencia como:

- Fichas de captura
- Alcance del SGSI
- Riesgos inherentes
- Riesgos residuales

- En la sección OBJETIVOS se indica que se debe identificar los activos de información para los procesos de negocio y procesos de soporte, pero a continuación se lista las "actividades esenciales" y solo se menciona el proceso de inscripción y certificación. Cuando se hace referencia a procesos se debe:

  - Hacer primero referencia al manual definitivo de procesos de RPQ para validar que los procesos constan en el manual.
  - Los procesos que acá se nombren deben tener coherencia con los procesos objeto del alcance en el Entregable E55.
  - El momento de listar actividades esenciales deberá listarse las actividades esenciales para todos los procesos involucrados según el alcance y no solo para algunos de ellos

- En la sección TERMINOLOGÍA validar el término disponibilidad, se indica en el documento que es el acceso a la información por personas autorizadas pero creemos que la definición está equivocada. De la misma manera esta sección debe contar con la aprobación de una mesa de trabajo con RPQ y anexarse el documento resultante.

- En la sección 9.1.3 se hace referencia al numeral 1.3 pero no se encuentra ese numeral en el documento.

- En la sección 9.1.8 se hace referencia al numeral 1.10 pero no se encuentra ese numeral en el documento.

- Literal 9.2.1.5 es parte del literal anterior y no un nuevo literal para dar consistencia a la lectura.

- Corregir el literal 9.7.2.1: …"Es recomendable aplicar principios básicos de seguridad tales como conceder privilegios de acceso a la información con base en al necesidad de conocer y de mínimos privilegios" . Se solicita explicar que es la necesidad de conocer y cuáles serían los mínimos privilegios. Se recomienda también mejorar la redacción del literal.

- El literal 9.7.3 es genérico aterrizar a la realidad del registro y las responsabilidades del usuario en el manejo de información y confidencialidad así como también en el tratamiento del archivo físico asociado, y el uso de dispositivos de almacenamiento externo al interior y fuera del RPQ.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.59: Metodología de análisis/evaluación y plan de tratamiento de los riesgos de Registro de Propiedad

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, se pide que la documentación entregada debe estar validada caso contrario es difícil entregar un criterio sobre información que no ha sido verificada por RPQ.

- Como introducción al documento debe colocarse:

  - Diagnóstico inicial del RPQ.
  - Una sección que indique la metodología a seguirse para la evaluación y tratamiento del riesgo
  - Una sección en donde se indique técnicas para evitar y minimizar los riesgos encontrados

- Se entendería que los entregables 57, 58 y 59 tienen un diferente enfoque a pesar de ellos las secciones que se detallan a continuación se repiten textualmente por lo que solo cambiarían los anexos. Se pide corregir esto, los documentos no pueden ser iguales en texto:

  - Naturaleza de los riesgos (a pesar de que los entregables 57,58 y 59 son distintos siempre se coloca el mismo texto de naturaleza de los riesgos)
  - El papel de la alta gerencia en la gestión de los riesgos
  - Modelo de gestión de riesgos

- Si bien el documento presenta una recomendación para el proceso de evaluación de riesgos deben anexarse actas de sesiones de trabajo en donde personal de RPQ valida esta información y está de acuerdo con la clasificación y supuestos propuestos.

- Al encontrarse un tercer entregable con el mismo texto copiado una y otra vez se recomienda a RPQ invalidar los tres entregables y solicitar al Consorcio la redacción de nuevos textos aterrizados a cada tema en este caso riesgos residuales, intrínsecos y operativos.

- El entregable hace referencia a un estado en el cual los sistemas core no han salido a producción. Los informes de ISO 27001 deben apuntar a un estado en que todos los sistemas hayan sido implementados

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

E.65: Documentación de material de capacitación "Seguridad de la información" y evidencia de participación en la capacitación

Observaciones encontradas:

- Se recomienda a RPQ pedir la inclusión de la duración de las capacitaciones puesto que esto no consta ni en el texto del documento, ni en el registro de asistencia.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: El RPQ debe exigir el cumplimiento de la recomendación.

E.66: Informe de auditoría interna del SGSI

Observaciones encontradas:

- Este informe de auditoría interna puede ser considerado como un ejercicio inicial de preparación, no como el informe definitivo para la entrega puesto que los sistemas core de RPQ ni siquiera han salido a producción y la ejecución de este informe debería darse cuando todos los sistemas estén operando al 100%. Se recomienda entonces a RPQ esperar para la aceptación de este entregable a que SIREL esté en funcionamiento.

CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación.

Atentamente,

Dr. Leonardo Sempértegui O.
PRESIDENTE
DEMPILE S.A.

Abg. Marcelo Dávila Martínez
LÍDER DEL EQUIPO DE FISCALIZACIÓN