


OFICIO No. CMS-RPQ-2016-131

Quito D.M., 5 de octubre de 2016

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


5/10/2016
10h30

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 las actividades que ejecuta el Consorcio Archivos Digitales MEB Seventeenmile (Consortio) se encuentran las relacionadas al C.2 Modernización integral del RP, Subcomponente 7. Gestión de la Calidad y Seguridad de la Información - Implantación de ISO 9001 y 27001.

De conformidad con la planificación vigente, las actividades relacionadas al entregable E.66 “Informe de auditoría interna del SGSI” están relacionadas con la planificación de la auditoría interna y acompañamiento en ejecución.

En virtud de lo anterior, a continuación se describen los procedimientos de Auditoría Interna que el RPDMQ deberá seguir, en estos se incluye la planificación:

Objetivo, alcance y usuarios

El objetivo de este procedimiento es describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son [miembros de la alta gerencia] del Registro de la Propiedad y los auditores internos o los expertos designados.

Documentos de referencia
Norma ISO/IEC 27001, punto 9,2

Auditoría interna

Objetivo de la auditoría interna

El objetivo de la auditoría interna es determinar si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGSI concuerdan con las normas ISO 27001, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

Planificación de la auditoría interna

El [cargo] aprueba un programa anual de auditorías internas, redactado como se detalla en la Plantilla 1, anexo en CD al presente para facilitar al proceso de planificación.

Se deben realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance del SGSI. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la gerencia.

El Programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

- Momento de la auditoría (especificando fechas o el mes en el que está planificada la auditoría).
- Alcance de la auditoría (departamentos, procesos, puntos de la norma, etc.).
- Criterio de auditoría (normas, disposiciones legales, documentación interna, obligaciones contractuales y/o normas corporativas).
- Métodos de la auditoría (revisión de documentación, entrevistas con empleados, revisión de registros, de sistemas informáticos, etc.).
- Quién realizará la auditoría (si será más de un auditor, especificar quién será el auditor líder).

Se debe llevar un registro de las auditorías realizadas en el Programa anual de auditoría interna.

Designación de auditores internos

El [cargo] debe designar a los auditores internos.

Un auditor interno puede ser alguien del Registro de la Propiedad o una persona externa independiente al SGSI.

Los criterios para la designación de los auditores son:

- Que conozca las normas ISO/IEC 27001.
- Que esté familiarizado sobre técnicas de auditoría sobre sistemas de gestión.
- Que sepa cómo funcionan las tecnologías de la información y de la comunicación como para estar familiarizado con el objetivo de los sistemas individuales y también con los impactos sobre procedimientos de seguridad y/o continuidad del negocio.
- Que sean independientes de las personas involucradas en la gestión del SGSI

Se debe seleccionar a los auditores internos de tal forma de garantizar objetividad e imparcialidad; es decir, de evitar el conflicto de intereses, ya que los auditores no pueden auditar su propio trabajo.

Se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 27001.

Realización de auditorías internas individuales

Las personas responsables de las auditorías internas individuales están identificadas en el programa anual de auditoría interna. Si una auditoría es realizada por un equipo de varios auditores, la persona responsable de la auditoría es aquella que está indicada como líder de equipo de auditoría.

Durante la realización de una auditoría interna se deben tener en cuenta los siguientes puntos:

- El criterio establecido en el programa anual de auditoría interna.
- Los resultados de auditorías internas o externas anteriores, si las hubiere.
- Los resultados de la evaluación de riesgos, de la implementación de controles, del análisis de impacto en los negocios, etc.
- Lista de apoyo de auditoría interna;

Se deben documentar los siguientes elementos como resultado de la auditoría interna:

- Informa de auditoría interna, debe ser enviado al [cargo]
- Las posibles medidas correctivas deben ser documentadas en el Formulario para medidas correctivas, de acuerdo a lo establecido en el Procedimiento para medidas correctivas.

Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Programa anual de auditoría interna (en formato electrónico)	Computador del [cargo]	[cargo]	Solamente el [cargo] y el auditor interno pueden ingresar datos y modificaciones al Programa anual de auditoría interna.	Los programas son almacenados por el plazo de 3 años.
Informe de auditoría interna (en formato electrónico)	Computadores del auditor interno y del [cargo]	Auditor interno	Los informes son almacenados en versiones de sólo lectura.	Los informes son guardados por un período de 3 años.
Lista de apoyo de auditoría interna (completada durante la auditoría interna)	Computador del auditor interno	Auditor interno	La lista de apoyo se guarda como sólo lectura.	La lista de apoyo es almacenada por el plazo de 3 años.

Solamente el [cargo] puede otorgar a otros empleados el derecho de acceso al Programa anual de auditoría interna, al Informe de auditoría interna y a la Lista de apoyo de auditoría interna.

Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas identificadas durante la auditoría.
- Cantidad de acciones correctivas identificadas durante la auditoría de certificación realizada luego de la auditoría interna.
- Si la frecuencia de auditorías internas coincide con el Programa anual de auditoría interna.

En virtud de lo antes indicado, el proceso de auditoría del RPDMQ se deberá ejecutar el 11 y 12 de octubre; y, el acompañamiento del Consorcio se realizará en los horarios que determine el RPDMQ.

Por la atención brindada, le anticipo mi agradecimiento.

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE

Adj: CD de datos con

- Plantilla 1: Programa anual de auditoría interna
- Plantilla 2: Informe de auditoría interna
- Plantilla 3: Lista de apoyo de auditoría interna