OFICIO No. CMS-RPQ-2015-157

Quito D.M., 3 de diciembre de 2015

Señor
Marcelo Carrera Riquetti
Administrador de Contrato
Registro de la Propiedad de Quito

3-dic-2015
14:15

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", Componente 2 "Modernización integral del RP", Subcomponente 7. Gestión de la Calidad y Seguridad de la Información - Implantación de ISO 9001 y 27001, el Consorcio Archivos Digitales Mebseventeenmile (Consorcio) inicio la ejecución de actividades de este componente desde el mes julio de 2015.

Entre las actividades relacionadas con la certificación ISO 27001 se encuentra la estructura organizacional de la seguridad de la información, cuya norma ISO 27001:2013 respecto a las estructuras organizacionales, roles y responsabilidades indica: "…

5.3 Roles, autoridades y responsabilidades de la organización dice:

La alta gerencia deberá garantizar que se asignen y comuniquen las responsabilidades y autoridad para los roles relacionados con la seguridad de la información.
La alta dirección deberá asignar la responsabilidad y autoridad para:

a) Garantizar que el Sistema de Gestión de Seguridad de la Información se adapte a los requisitos de esta norma internacional: e
b) Informar acerca del desempeño del Sistema de Gestión de Seguridad de la Información a la alta gerencia.
NOTA: La alta gerencia también asignará responsabilidades y autoridad para informar acerca del desempeño del Sistema de Seguridad de la Información dentro de la organización."

En cumplimiento de la citada cláusula, es necesario asignar las estructuras organizacionales que garanticen el cumplimiento de la norma en miras a la certificación.

A continuación se detallan las estructuras, roles, responsabilidades y alcance de control necesarias, que solicito gestione desde ya su creación al interior del Registro, con la finalidad de iniciar los pasos previos al certificado ISO:

1. Comité Ejecutivo de Seguridad y Riesgos
2. Comité Directivo de Seguridad de la Información
3. Oficial de Seguridad[1]
4. Gerente de Seguridad de la Información (puede ser el jefe de la Unidad de TI o el responsable de alguna de las áreas internas a TI)[2].
5. Propietarios funcionales de la información

1. ACERCA DEL COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS

Este Comité de alto nivel ejecutivo es el responsable de la toma de decisiones el Registro de la Propiedad relacionadas con la valoración, optimización, el control, el financiamiento y el monitoreo de los riesgos de diverso origen, en este caso de los tecnológicos.

El objetivo final es que el Registro de la Propiedad logre alcanzar sus objetivos estratégicos, ya que este alcance está directa y totalmente relacionado con la óptima utilización de los servicios y sistemas tecnológicos y su seguridad.

Se detallan a continuación tablas que describen su composición, alcance, ámbito, responsabilidades y niveles de autoridad.

Comité Ejecutivo de Seguridad y Riesgos: Conformación	
Rol	**Descripción**
Oficial de Seguridad de la Información	Asesora al Comité en aspectos específicos del seguridad de la información
Directivos de las áreas funcionales del Registro de la Propiedad	Representan los intereses de las áreas en el planteamiento de la estrategia de seguridad de la información
Propietarios de los procesos del Registro de la Propiedad	- Tienen a cargo los servicios del Registro de la Propiedad que son usuarios de tecnología. - Comunican las iniciativas y actividades del Registro de la Propiedad que puedan tener impacto en la seguridad de la

[1] Responsable Institucional de la Seguridad de la Información.
[2] Es el ejecutor de políticas de seguridad de la información, en el ámbito de seguridad de la información, debe responder al Jefe de Seguridad de la información

	información, así como del impacto que las prácticas de seguridad tenga en los usuarios de los servicios de TI. - Deben tener una buena comprensión de las necesidades de seguridad desde el punto de vista operativo del Registro de la Propiedad, los impactos y costos.
Auditoría Interna. Personal a cargo del cumplimiento de regulaciones.	Pueden estar de manera ocasional o permanente en el Comité dando sus puntos de vista especializados sobre temas de auditoría y cumplimiento relacionados con la seguridad de la información. Informan acerca del cumplimiento relacionado con el tratamiento de los riesgos.
Representante del área legal del registro de la Propiedad	Asesora en aspectos legales relacionados con la seguridad de la información. Ejemplo, propiedad intelectual, delitos informáticos, legislación aplicable. Su presencia puede ser ocasional cuando las circunstancias lo ameriten.
Responsable de la gestión de riesgos	Su presencia debe ser de manera ocasional cuando se requiera asesoría especializada sobre riesgos de TI. Por ejemplo ante la implementación de estrategias tecnológicas como "cloud computing", tecnologías móviles, virtualización, etc. Si no existe esta función se debe analizar su implementación o bien dejarla al jefe de la Unidad de TI.

NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS	
PRÁCTICA PROCESO	**NIVEL DE INVOLUCRACIÓN**
Asesoramiento acerca de la estrategia de seguridad de la información definida por el Comité Directivo de Seguridad de la Información.	Responsable
Establecer los niveles de tolerancia al riesgo	Rinde cuentas
Definir e implementar las estrategias de evaluación y respuesta a los riesgos.	Rinde cuentas
Revisar las valoraciones y los perfiles de riesgo	Rinde cuentas

2. ACERCA DEL COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN

Este Comité es el encargado del aseguramiento que se sigan las buenas prácticas de seguridad de la información. Tiene la competencia de que la seguridad de la información se aplique de manera efectiva y consistente en todo el ámbito del Registro de la Propiedad.

COMPOSICIÓN DEL COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN	
Rol	**Descripción**
Oficial de Seguridad de la Información	- Preside el Comité y es el enlace con Comité Ejecutivo de Seguridad y Riesgos - Es el responsable general de la seguridad de la información del Registro de la Propiedad. - Comunica el diseño, la implementación y el monitoreo de las prácticas de seguridad de la información.
Propietarios funcionales de la información.	- Son los encargados de los procesos o aplicaciones del Registro de la Propiedad que dependen de TI. - Responsables de evaluar y comunicar acerca de las iniciativas del Registro de la Propiedad que impacten la seguridad de la información y sus procesos. - Deben tener una comprensión clara de los riesgos operativos y de los costos y beneficios de los requerimientos específicos de seguridad de la información de sus respectivas áreas.
Responsable de la Unidad de TICs	- Reporta acerca del estado en general de los aspectos relacionados con la seguridad de la información: - Cumplimiento de políticas y responsabilidades de seguridad de la información del personal de TI. - Afectaciones posibles de la seguridad debida a cambios en las infraestructuras tecnológicas. En al ámbito de su competencia es quien tiene la responsabilidad de la implementación en la plataforma y en la organización de TI las políticas y sistemas de seguridad de la información y monitoreo de su efectividad.
Representantes de las funciones especializadas del Registro de la Propiedad que tengan relación con seguridad de la información	- Traen iniciativas de seguridad desde sus ángulos de especialidad cuando éstas sean relevantes, por ejemplo, desde el punto de vista de los recursos humanos, auditoria interna, departamento legal, oficina de proyectos, Dirección de informática del Municipio de Quito, etc. - Pueden estar en el Comité de manera ocasional ante eventos relevantes coyunturales de la estrategia del Registro de la Propiedad, o bien pueden estar asignados de manera permanente, como el caso de Auditoría Interna, con el fin de que informen al Comité acerca del cumplimiento del tratamiento de los riesgos.

COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad	
Mandato	Aseguramiento que se sigan las buenas prácticas de seguridad de la información. Es quien tiene la competencia de que la seguridad de la información se aplique de manera efectiva y consistente en todo el ámbito del Registro de la Propiedad.
Principios operacionales	- El presidente es el Oficial de Seguridad de la Información. - Se reúne con una regularidad predefinida y cuando las necesidades lo ameriten. Debe aumentarse la frecuencia de reuniones durante eventos específicos del desarrollo de la estrategia del Registro de la Propiedad en la que sean necesarias definiciones y medidas específicas de seguridad, o bien cuando haya necesidades emergentes de seguridad de la información. - Se permite la delegación o presencia de personas que sustituyan a los titulares, pero no se debe abusar de esta facilidad. - La membresía a este Comité se debe limitar a un pequeño grupo de líderes tácticos o estratégicos con el fin de asegurar una adecuada comunicación bidireccional y toma de decisiones. Se puede invitar a otros líderes cuando así lo ameriten las circunstancias. - Se deben elaborar, aprobar, firmar y archivar actas de todas las reuniones. -
Alcance del control	El Comité responde por la toma de decisiones acerca de seguridad de la información del Registro de la Propiedad.
Nivel de autoridad y de decisiones	Responde por las decisiones de seguridad de la información del Registro de la Propiedad en apoyo de las decisiones estratégicas del Comité Ejecutivo de Seguridad y Riesgos
Derechos de delegación	Este Comité es el responsable final de la estrategia de diseño e implementación del programa de seguridad de la información y no puede delegar esta responsabilidad.
Escala de autoridad	Todos los temas deben ser escalados al más alto ejecutivo involucrado del equipo responsable de seguridad de la información (Comité Ejecutivo de Seguridad y Riesgos). Las estrategias de gestión de los riesgos se deben escalar al Comité Ejecutivo de Seguridad y Riesgos para su aprobación.

NIVEL DE INVOLUCRACIÓN DEL COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN (Responsabilidades y rendición de cuentas)	
Definición y comunicación de la estrategia de seguridad de la información en alineamiento con la estrategia del Registro de la Propiedad.	Rinde cuentas
Investigación, definición y documentación de los requerimientos de seguridad de la información	Rinde cuentas
Validación de los requerimientos de seguridad de la información con las partes interesadas , los responsables operativos del Registro de la Propiedad y con los encargados de la implementación técnica	Rinde cuentas
Desarrollo de políticas y procedimientos de seguridad de la información	Rinde cuentas
Desarrollo del plan de seguridad de la información que identifique el ambiente de seguridad de la información y las actividades a ser implementadas por el equipo del proyecto para la protección de los activos de información del Registro de la Propiedad.	Rinde cuentas
Aseguramiento de que el impacto potencial de los cambios es evaluado	Rinde cuentas
Recopilación y análisis de los datos de desempeño y cumplimiento relativos a seguridad de la información y gestión de los riesgos tecnológicos	Rinde cuentas
Determinación, acuerdo y comunicación de las funciones y responsabilidades del Oficial de Seguridad.	Rinde cuentas
Promoción de la función de seguridad de la información en todas las instancias del Registro de la Propiedad y potencialmente fuera, en ámbitos como la Dirección de Informática del Municipio.	Rinde cuentas
Apoyo con iniciativas a los esfuerzos de continuidad de servicios en todo el ámbito del Registro de la Propiedad	Rinde cuentas

COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN; ENTRADAS Y SALIDAS A LA FUNCIÓN			
ENTRADA	**DE**	**SALIDA**	**A**
Planificación Estratégica del Registro de la Propiedad.	Alta Dirección	Estrategia y programa de seguridad de la información	Comité Ejecutivo de Seguridad y Riesgos. Propietarios de la información, dueños de los procesos
Niveles de aceptación de riesgos	Comité Ejecutivo de Seguridad y Riesgos	Perfil de riesgos de la información	Comité Ejecutivo de Seguridad y Riesgos
Proyectos institucionales	Propietarios de los procesos		
Reportes de Auditoria Interna	Auditoría Interna		

3. ACERCA DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad	
ÁREA	**CARACTERÍSTICAS**
Mandato	Responsabilidad general del programa de seguridad de la información del Registro de la Propiedad
Principios operacionales y habilidades	Debe reportar al responsable de la Unidad de TIC Es el enlace entre el área ejecutiva y el programa de seguridad de la información. Debe coordinar y comunicarse muy de cerca con todos los estamentos institucionales interesados en el buen funcionamiento del Registro de la Propiedad para tratar adecuadamente las necesidades de protección de la información. Además el Oficial de Seguridad debe: - Tener una comprensión precisa de la visión estratégica del Registro de la Propiedad. - Tener buenas habilidades para comunicar. - Ser hábil en la construcción de excelentes relaciones con las personas relevantes del Registro de la Propiedad. - Tener la capacidad de traducir los objetivos del Registro de la Propiedad en requerimientos de seguridad de la información.
Ámbito de Control	- Sistema de Gestión de Seguridad de la Información (SGSI). - Tratamiento de los riesgos de seguridad de la información.
Nivel de Autoridad y de decisiones	- Tiene a su cargo todas las decisiones necesarias para implementar y actualizar la estrategia de seguridad de la información. - Debe rendir cuentas y aprobar decisiones importantes e seguridad de la información como parte del Comité de Seguridad de la Información.
Qué delega	Debe delegar tareas de seguridad de la información a directivos y otras personas del Registro de la Propiedad.
Escala de autoridad	- Jefe inmediato - Comité Directivo de Seguridad de la Información

NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	
PRÁCTICA PROCESO	**NIVEL DE INVOLUCRACIÓN**
Identificación y comunicación de las amenazas de seguridad y riesgos en general, de los comportamientos deseables consistentes para superarlas y de los cambios que deben implementarse para tratar estos temas.	Rinde cuentas
Aseguramiento de que los aspectos ambientales y de las instalaciones de procesamiento cumplen con requerimientos de seguridad de la información.	Rinde cuentas
Protección contra software dañino	Rinde cuentas
Gestión de la seguridad de la red	Rinde cuentas
Gestión de identidades y control de accesos	Rinde cuentas
Gestión de acceso físico a los activos de TI	Rinde cuantas
Monitoreo de la infraestructura por eventos de seguridad de la información	Rinde cuentas
Proposición de acciones necesarias para el mejoramiento de la efectividad y la eficiencia de las funciones de seguridad de la información, por ejemplo: capacitación del personal de seguridad de la información, documentación, estandarización y automatización de los procesos, las tecnologías y las aplicaciones de seguridad.	Rinde cuentas
Monitoreo de la gestión de riesgos tecnológicos	Responsable
Definición y divulgación de la estrategia de seguridad de la información, que debe estar alineada con la estrategia del Registro de la Propiedad.	Responsable
Investigación, definición y documentación de los requerimientos de seguridad de la información	Responsable
Validación de los requerimientos de seguridad de la información con los interesados, dueños de los procesos y con el personal de implementación técnica	Responsable
Desarrollo de políticas y procesos de seguridad de la información	Responsable
Definición e implementación de las estrategias de evaluación y respuesta a riesgos tecnológicos y cooperación con el responsable de riesgos para la administración de éstos.	Responsable
Aseguramiento de la evaluación del impacto potencial de los cambios	Responsable
Recopilación y análisis de los datos de desempeño y cumplimiento relativos a seguridad de la información y gestión de los riesgos tecnológicos	Responsable

ENTRADAS Y SALIDAS A LA FUNCIÓN DEL OFICIAL DE SEGURIDAD			
Entrada	**De**	**Salida**	**A**
Tolerancia al riesgo	Comité Ejecutivo de Seguridad y Riesgos	Estrategia de Seguridad de la Información Políticas, estándares y procedimientos	Registro de la Propiedad Comité Ejecutivo de Seguridad y Riesgos
Disposiciones y mandatos regulatorios	Externo (reguladores)		
Estrategia del Registro de la Propiedad y de su unidad de TIC	Registro de la Propiedad / Unidad de TICs		
Reportes de Auditoría	Auditoría	Plan de remediación de observaciones de Auditoría de TI	Auditoria

4. ACERCA DEL GERENTE DE SEGURIDAD DE LA INFORMACIÓN

GERENTE DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad	
ÁREA	**CARACTERÍSTICAS**
Mandato	Responsabilidad general de la gestión de la seguridad de la información del Registro de la Propiedad
Principios operacionales y habilidades	- Reporta al Oficial de Seguridad de la Información y al Jefe de la Unidad de TI
Ámbito de Control	Seguridad de la información en: - Aplicaciones - Infraestructura de TI. Gestión de accesos Gestión y tratamiento de incidentes Gestión de riesgos Programa de concienciación en seguridad de la información Indicadores de seguridad de TI Gestión de proveedores de seguridad de la información.
Nivel de Autoridad y de decisiones	Autoridad general en la toma de decisiones sobre las prácticas de seguridad de la información de su dominio.
Qué delega	Debe delegar tareas de seguridad de la información a directivos y otras personas del Registro de la Propiedad, ejemplo: Buenas prácticas, cumplimiento de políticas, definiciones de seguridad operativas, custodia de datos.
	Escala los temas al Oficial de Seguridad. *Se debe analizar objetivamente para el caso del Registro de la Propiedad si este rol debe ser realizado por una persona adicional o bien puede ser*

Escala de autoridad	*ocupado por el Jefe de la Unidad de TI. Hay ventajas y desventajas de cada enfoque, pero las principales consideraciones deben ser:* - *El tiempo que requieren estas tareas* - *Las competencias y habilidades* - *En cierta forma la incompatibilidad de los dos roles* *No es recomendable que sea el mismo Oficial de Seguridad, ya que al ser un ejecutor de la estrategia diseñada puede en un momento dado ser juez y parte.*

NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL GERENTE DE SEGURIDAD DE LA INFORMACIÓN	
PRÁCTICA PROCESO	**NIVEL DE INVOLUCRACIÓN**
Desarrollo y comunicación de la visión unificada al equipo de seguridad de la información. Esta visión está alineada con la visión del Registro de la Propiedad.	Responsable
Asignación de los recursos humanos de seguridad de la información acorde a los requerimientos del registro de la Propiedad.	Responsable
Realización de las actividades conducentes a la valoración de los riesgos de la información y definición del perfil de riesgos para los activos de información.	Responsable
Administración de roles, responsabilidades, privilegios de acceso y niveles de autoridad respecto a seguridad de la información.	Responsable
Desarrollo del plan de seguridad de la información que identifique el ambiente de seguridad de la información y los controles a ser implementados por el equipo del proyecto para proteger los activos de información del registro de la Propiedad. Monitorea, ajusta y mejora estos controles.	Responsable
Identificación y comunicación de puntos específicos del plan de seguridad, comportamientos deseables, y los cambios necesarios para tratar estos puntos.	Responsable
Identificación de formas de desarrollar y mejorar la efectividad y eficiencia de la función de seguridad de la información. Por ejemplo con actividades de capacitación al personal de seguridad de la información, documentación de los procesos, las tecnologías y las aplicaciones y la estandarización y automatización de procesos de seguridad de la información.	Responsable
Aseguramiento de que los aspectos ambientales y de las instalaciones de procesamiento cumplen con requerimientos de seguridad de la información.	Responsable
Recopilación y análisis de los datos de desempeño y cumplimiento relativos a seguridad de la información y gestión de los riesgos tecnológicos. Indicadores de seguridad de la información.	Responsable

ENTRADAS Y SALIDAS A LA FUNCIÓN DE GERENTE DE SEGURIDAD DE LA INFORMACIÓN			
Entrada	**De**	**Salida**	**A**
Tolerancia al riesgo	Comité Ejecutivo de Seguridad y Riesgos	Diseño, implementación y planes de mejora de las prácticas de seguridad de la información	Usuarios y prestatarios de los servicios y sistemas de información del Registro de la Propiedad.
Disposiciones y mandatos regulatorios	Externo (reguladores)		
Estrategia del Registro de la Propiedad y de su unidad de TIC	Registro de la Propiedad / Unidad de TICs		
Reportes de Auditoría	Auditoría	Valoraciones periódicas de los riesgos de seguridad de la información y pruebas de las prácticas y contramedidas de seguridad de la información	Oficial de Seguridad de la Información. Directivos de unidades operativas del Registro de la Propiedad
Estrategia de Seguridad de la Información	Comité Directivo de Seguridad de la Información	Reportes del estado de implementación de la seguridad de la información	Oficial de Seguridad de la Información
Configuración, arquitectura y planificación de la infraestructura de TI	Unidad de TIC del Registro de la Propiedad o de la Dirección de Informática del Municipio.		
Políticas, estándares y procedimientos de seguridad de la información	Oficial de Seguridad y Comité Directivo de Seguridad		

NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS	
PRÁCTICA PROCESO	**NIVEL DE INVOLUCRACIÓN**
Asesoramiento acerca de la estrategia de seguridad de la información definida por el Comité Directivo de Seguridad de la Información.	Responsable
Establecer los niveles de tolerancia al riesgo	Rinde cuentas
Definir e implementar las estrategias de evaluación y respuesta a los riesgos.	Rinde cuentas
Revisar las valoraciones y los perfiles de riesgo	Rinde cuentas

5. ACERCA DEL ROL DE PROPIETARIO FUNCIONAL DE LA INFORMACIÓN

Los propietarios funcionales de la información son los responsables de los procesos el Registro de la Propiedad y actúan como enlace entre la institución y la función de seguridad de la información.

Deben tener una muy buena comprensión de los flujos de información y los procesos institucionales y el uso de aplicaciones específicas y los servicios de TI que facilitan sus actividades operativas. Conocen las necesidades de clasificación y de protección de la información. Los jefes departamentales son las personas que posiblemente mejor cumplan este rol.

En los ámbitos de su competencia estas personas son las que tienen a su cargo:

- La asignación derechos de acceso a los datos de su propiedad
- Las definiciones de criticidad y sensibilidad de los datos de su propiedad.
- La definición de las características funcionales de las aplicaciones sobre los datos de su propiedad.

NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUANTAS DE LOS PROPIETARIOS FUNCIONALES DE LA INFORMACIÓN	
PRÁCTICA PROCESO	**NIVEL DE INVOLUCRACIÓN**
Comunicar, coordinar y asesorar en los aspectos relacionados las definiciones necesarias en la de gestión de riesgos de seguridad de la información	Responsable
Reportar los cambios en la estrategia o en los procesos del registro de la Propiedad: nuevos productos, nuevos servicios.	Responsable
Revisar las valoraciones y perfiles de riesgo en su ámbito de competencia.	Responsable

Atentamente,

Byron Paredes Buitrón
GERENTE DE PROYECTO
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE