

Memorando No. RPDMQ-PROYMIRP-2016-0114A-M

Quito, D.M., 14 de Enero del 2016

**PARA:** Fátima Rodríguez  
DIRECCIÓN INSCRIPCIONES RPDMQ

Paúl Tamayo  
DIRECCIÓN INSCRIPCIONES RPDMQ

Freddy Herrera  
DIRECCIÓN CERTIFICACIONES RPDMQ

Mario Andrade  
DIRECCIÓN CERTIFICACIONES RPDMQ

José Luis Aucancela  
DIRECCIÓN ARCHIVO RPDMQ

David León  
DIRECCIÓN ARCHIVO RPDMQ

Agustín Vásconez  
DIRECCIÓN ASESORÍA Y CONTROL JURÍDICO RPDMQ

Ana María Castrillón  
DIRECCIÓN ASESORÍA Y CONTROL JURÍDICO RPDMQ

Andrés Eguiguren  
ASESORÍA INFORMÁTICA RPDMQ

Doris Ochoa  
TICS RPDMQ

Marcelo Cornejo  
SERVICIOS CIUDADANOS RPDMQ

Verónica Tobar  
SERVICIOS CIUDADANOS RPDMQ

María Eugenia Velasco  
PLANIFICACIÓN RPDMQ

Wladimir Alban  
PLANIFICACIÓN RPDMQ

Diana Pachacama  
DIRECCIÓN ADMINISTRATIVA FINANCIERA (DAF) RPDMQ

*Fátima Rodríguez*

*Paúl Tamayo*

*Freddy Herrera*

*Mario Andrade*

*José Luis Aucancela*

*David León*

*Andrés Eguiguren*

*Marcelo Cornejo*

*María Eugenia Velasco*

*Wladimir Alban*

*Diana Pachacama*

080384946 14/01/2016

14-1-2016  
11:45

14-01-2016.

14-01-2016. 11:50

14.01.15  
11:31 *Carsten Juncos*

14-1-2016.

14/01/2016  
11h30

Recibido  
14/01/2016  
11:35.

14/01/2016 11:40AM.

14/01/2016 11:36.

14/01/2016 11:36

14/01/2016 / 11:33

14/01/2016

**ASUNTO:** Delegación para Grupos y Cargos requeridos para ISO 27001.

Con oficio No. CMS-RPQ-2015-157, el Consorcio expresa como requerimiento al RPDMQ lo siguiente:

"A continuación se detallan las estructuras, roles, responsabilidades y alcance de control necesarias, que solicita 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**
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).**
5. **Propietarios funcionales de la información".**

Con memorando No. RPDMQ-PROYMIRP-2015-1228C-M, se presenta al Sr. Registrador de la Propiedad (E) la propuesta en la cual, con base en la gestión efectuada en la ejecución del proyecto de Modernización Integral del RPDMQ para el ámbito relacionado con ISO 27001, se indica una propuesta para conformación de Grupos a conformar y Cargos a Designar en relación a lo requerido para ISO 27001.

Con sumilla del Sr. Registrador suscrita el 07 de enero de 2016, en memorando No. RPDMQ-PLAN-2016-55-M, se indica "proceder a... notificar por escrito a funcionarios".

Con base en lo anteriormente expuesto y realizando análisis final de designación, me permito describirles las delegaciones RPDMQ establecidas para la conformación de Grupos y Cargos vinculados a la gestión ISO 27001:

| EQUIPO RPDMQ / CARGO RPDMQ                      | ROL   | DELEGACIÓN RPDMQ  |
|---|---|---|
| COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS         | Oficial Seguridad de la Información RPDMQ   | Coordinador/a TICs  |
|   | Directivos de las áreas funcionales de la Gestión Registral del RPDMQ   | Director/a Inscripciones  |
|   |   | Director/a Certificaciones  |
|   |   | Director/a Archivo  |
|   | Propietarios de procesos del RPDMQ  | Responsable Planificación   |
|   |   | Responsable SSCC  |
|   | Auditoría interna (personal a cargo del cumplimiento de regulaciones).  | Técnico/a de Planificación  |
| Agente de Control Gestión Registral             |   |   |
| Representante del área legal del RPDMQ          | Técnico/a de Asesoría y Control Jurídico  |   |
| Responsable de gestión de riesgos TI            | Asesor/a de Informática   |   |
| COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN | Oficial Seguridad de la Información   | Coordinador/a TICs  |
|   | Propietarios funcionales  | Directivos de la Dirección de Inscripciones, Dirección de Certificaciones, Dirección de Archivo, Dirección de Asesoría y Control Jurídico, Servicios Ciudadanos RPQ |
|   |   | Asesor/a de Informática   |
|   | Responsable de la Unidad de TIC's   | Asesor/a de Informática   |
|   | Representantes de las funciones especializadas del Registro de la Propiedad que tengan relación con seguridad de la información | Agentes de Control Gestión Registral  |
| Delegado/a de DAF (gestión de Recaudaciones)    |   |   |
| Técnico/a de Asesoría y Control Jurídico        |   |   |
| Técnico/o de Planificación                      |   |   |
| OFICIAL DE SEGURIDAD                            | Responsable Institucional de la Seguridad de la Información de la Gestión Registral del RPDMQ                                   | Coordinador/a TICs  |
| GERENTE DE SEGURIDAD DE LA INFORMACIÓN          | Gestión de la seguridad de la información de la Gestión Registral del RPDMQ   | Asesor/a de Informática   |
| PROPIETARIOS FUNCIONALES DE LA INFORMACIÓN      | Propietarios funcionales de la información de la Gestión Registral del RPDMQ  | Director/a Inscripciones<br>Director/a Certificaciones<br>Director/a Archivo<br>Responsable SSCC<br>Director/a Asesoría y Control Jurídico                          |

A continuación describo listado de los funcionarios específicos relacionados con las delegaciones RPDMQ:

| DELEGACIÓN RPDMQ                         | FUNCIONARIO/A RPDMQ   |
|--|-----------------------|
| Director/a Inscripciones                 | FÁTIMA RODRÍGUEZ      |
| Director/a Certificaciones               | FREDDY HERRERA        |
| Director/a Archivo                       | JOSÉ LUÍS AUCANCELA   |
| Director/a Asesoría y Control Jurídico   | AGUSTÍN VÁSCONEZ      |
| Asesor/a de Informática                  | ANDRÉS EGUIGUREN      |
| Responsable SSCC                         | MARCELO CORNEJO       |
| Responsable Planificación                | MARÍA EUGENIA VELASCO |
| Coordinador/a TICs                       | DORIS OCHOA           |
| Delegada/o de DAF                        | DIANA PACHACAMA       |
| Técnico/a de Planificación               | WLADIMIR ALBAN        |
| Técnico/a de Asesoría y Control Jurídico | ANA MARÍA CASTRILLÓN  |
| Agente de Control Inscripciones          | PAÚL TAMAYO           |
| Agente de Control Certificaciones        | MARIO ANDRADE         |
| Agente de Control Archivo                | DAVID LEÓN            |
| Agente de Control Servicios Ciudadanos   | VERÓNICA TOBAR        |

Para una mejor comprensión sobre las funciones a cumplir, en los siguientes cuadros se describen el alcance de los roles designados:

#### COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS:

| 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             | <ul style="list-style-type: none"> <li>- Tienen a cargo los servicios del Registro de la Propiedad que son usuarios de tecnología.</li> <li>- Comunican las iniciativas y actividades del Registro de la Propiedad que puedan tener impacto en la seguridad de la información, así como del impacto que las prácticas de seguridad tenga en los usuarios de los servicios de TI.</li> <li>- 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.</li> </ul> |
| 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.   |

#### COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN:

| ROL                                    | DESCRIPCIÓN  |
|--|--|
| Oficial de Seguridad de la Información | <ul style="list-style-type: none"> <li>- Preside el Comité y es el enlace con Comité Ejecutivo de Seguridad y Riesgos</li> <li>- Es el responsable general de la seguridad de la información del Registro de la Propiedad.</li> <li>- Comunica el diseño, la implementación y el monitoreo de las prácticas de seguridad de la información.</li> </ul> |

| ROL   | DESCRIPCIÓN  |
|---|--|
| Propietarios funcionales de la información.   | <ul style="list-style-type: none"> <li>- Son los encargados de los procesos o aplicaciones del Registro de la Propiedad que dependen de TI.</li> <li>- Responsables de evaluar y comunicar acerca de las iniciativas del Registro de la Propiedad que impacten la seguridad de la información y sus procesos.</li> <li>- 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.</li> </ul>  |
| Responsable de la Unidad de TICs  | <ul style="list-style-type: none"> <li>- Reporta acerca del estado en general de los aspectos relacionados con la seguridad de la información:</li> <li>- Cumplimiento de políticas y responsabilidades de seguridad de la información del personal de TI.</li> <li>- Afectaciones posibles de la seguridad debida a cambios en las infraestructuras tecnológicas.</li> </ul> <p>En el 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.</p>  |
| Representantes de las funciones especializadas del Registro de la Propiedad que tengan relación con seguridad de la información | <ul style="list-style-type: none"> <li>- Traen iniciativas de seguridad desde sus ángulos de especialidad cuando éstas sean relevantes, por ejemplo, desde el punto de vista de los recursos humanos, auditoría interna, departamento legal, oficina de proyectos, Dirección de informática del Municipio de Quito, etc.</li> <li>- 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.</li> </ul> |

#### OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:

| ÁREA                                   | CARACTERÍSTICAS  |
|--|--|
| Mandato                                | Responsabilidad general del programa de seguridad de la información del Registro de la Propiedad   |
| Principios operacionales y habilidades | <p>Debe reportar al responsable de la Unidad de TIC</p> <p>Es el enlace entre el área ejecutiva y el programa de seguridad de la información.</p> <p>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.</p> <p>Además el Oficial de Seguridad debe:</p> <ul style="list-style-type: none"> <li>- Tener una comprensión precisa de la visión estratégica del Registro de la Propiedad.</li> <li>- Tener buenas habilidades para comunicar.</li> <li>- Ser hábil en la construcción de excelentes relaciones con las personas relevantes del Registro de la Propiedad.</li> <li>- Tener la capacidad de traducir los objetivos del Registro de la Propiedad en requerimientos de seguridad de la información.</li> </ul> |
| Ámbito de Control                      | <ul style="list-style-type: none"> <li>- Sistema de Gestión de Seguridad de la Información (SGSI).</li> <li>- Tratamiento de los riesgos de seguridad de la información.</li> </ul>  |
| Nivel de Autoridad y de decisiones     | <ul style="list-style-type: none"> <li>- Tiene a su cargo todas las decisiones necesarias para implementar y actualizar la estrategia de seguridad de la información.</li> <li>- Debe rendir cuentas y aprobar decisiones importantes e seguridad de la Información como parte del Comité de Seguridad de la Información.</li> </ul>   |
| Qué delega                             | Debe delegar tareas de seguridad de la información a directivos y otras personas del Registro de la Propiedad.   |
| Escala de autoridad                    | <ul style="list-style-type: none"> <li>- Jefe inmediato</li> <li>- Comité Directivo de Seguridad de la Información</li> </ul>  |

#### GERENTE DE SEGURIDAD DE LA INFORMACIÓN:

| ÁREA    | CARACTERÍSTICAS  |
|---------|--|
| Mandato | Responsabilidad general de la gestión de la seguridad de la información del Registro de la Propiedad |

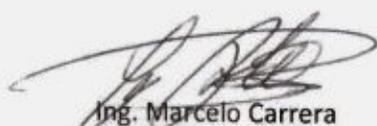
| ÁREA                                   | CARACTERÍSTICAS   |
|--|---|
| Principios operacionales y habilidades | Reporta al Oficial de Seguridad de la Información y al Jefe de la Unidad de TI  |
| Ámbito de Control                      | Seguridad de la información en:<br>- Aplicaciones<br>- Infraestructura de TI.<br>Gestión de accesos<br>Gestión y tratamiento de incidentes<br>Gestión de riesgos<br>Programa de concienciación en seguridad de la información<br>Indicadores de seguridad de TI<br>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 de autoridad                    | Escala los temas al Oficial de Seguridad.<br><br><i>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 ocupado por el Jefe de la Unidad de TI. Hay ventajas y desventajas de cada enfoque, pero las principales consideraciones deben ser:</i> <ul style="list-style-type: none"> <li>- El tiempo que requieren estas tareas</li> <li>- Las competencias y habilidades</li> <li>- En cierta forma la incompatibilidad de los dos roles</li> </ul> <i>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.</i> |

### PROPIETARIO FUNCIONAL DE LA INFORMACIÓN:

| ÁREA                  | CARACTERÍSTICAS  |
|-----------------------|--|
| Alcance               | Los propietarios funcionales de la información son los responsables de los procesos del Registro de la Propiedad y actúan como enlace entre la institución y la función de seguridad de la información.  |
| Destreza              | 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. |
| Ámbito de competencia | <ul style="list-style-type: none"> <li>- La asignación derechos de acceso a los datos de su propiedad</li> <li>- Las definiciones de criticidad y sensibilidad de los datos de su propiedad.</li> <li>- La definición de las características funcionales de las aplicaciones sobre los datos de su propiedad</li> </ul>  |

Para consultar información sobre alcance de responsabilidades de los grupos y cargos, relacionados con ISO 27001, pueden ver el oficio No. CMS-RPQ-2015-157.

Atentamente:



Ing. Marcelo Carrera

**GERENTE DE PROYECTO MODERNIZACIÓN INTEGRAL RPDMQ**

**ADMINISTRADOR DE CONTRATO No. 019-2014**

**REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO**

ANEXO: Copia oficio No. CMS-RPQ-2015-157  
Copia memo No. RPDMQ-PROYMIRP-2015-1228C-M  
Copia Fe Erratar que corrige error de edición en mem No. RPDMQ-PROYMIRP-2015-1228C-M  
Copia memo No. RPDMQ-PLAN-2016-55-M con sumilla del Sr. Registrador (E)

CC: Pablo Falconí  
Andrés Eguiguren

Registrador de la Propiedad (E)  
Administrador de Contrato No. 005-2015 (Fiscalización)

*[Handwritten signature]* 14/01/2016  
11:30

MCarrera/

**QUITO**  
REGISTRO DE LA PROPIEDAD  
**DESPACHO REGISTRADOR**  
Recibido por: *M. Ricci E*  
Fecha: *14/ Ene / 2016*  
Hora: *12:00*

*[Handwritten signature]*

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 (Consortio) 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<sup>1</sup>
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)<sup>2</sup>.
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.

| <b>Comité Ejecutivo de Seguridad y Riesgos: Conformación</b>     |  |
|--|--|
| <b>Rol</b>   | <b>Descripción</b>   |
| 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        | <ul style="list-style-type: none"> <li>- Tienen a cargo los servicios del Registro de la Propiedad que son usuarios de tecnología.</li> <li>- Comunican las iniciativas y actividades del Registro de la Propiedad que puedan tener impacto en la seguridad de la</li> </ul> |

<sup>1</sup> Responsable Institucional de la Seguridad de la Información.

<sup>2</sup> 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

|   |   |
|---|---|
|   | <p>información, así como del impacto que las prácticas de seguridad tenga en los usuarios de los servicios de TI.</p> <ul style="list-style-type: none"> <li>- 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.</li> </ul>                |
| 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. |

| <b>NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS</b>                                  |                               |
|---|-------------------------------|
| <b>PRÁCTICA PROCESO</b>   | <b>NIVEL DE INVOLUCRACIÓN</b> |
| 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.

| <b>COMPOSICIÓN DEL COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN</b>  |  |
|---|--|
| <b>Rol</b>  | <b>Descripción</b>   |
| Oficial de Seguridad de la Información  | <ul style="list-style-type: none"> <li>- Preside el Comité y es el enlace con Comité Ejecutivo de Seguridad y Riesgos</li> <li>- Es el responsable general de la seguridad de la información del Registro de la Propiedad.</li> <li>- Comunica el diseño, la implementación y el monitoreo de las prácticas de seguridad de la información.</li> </ul>   |
| Propietarios funcionales de la información.   | <ul style="list-style-type: none"> <li>- Son los encargados de los procesos o aplicaciones del Registro de la Propiedad que dependen de TI.</li> <li>- Responsables de evaluar y comunicar acerca de las iniciativas del Registro de la Propiedad que impacten la seguridad de la información y sus procesos.</li> <li>- 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.</li> </ul>  |
| Responsable de la Unidad de TICs  | <ul style="list-style-type: none"> <li>- Reporta acerca del estado en general de los aspectos relacionados con la seguridad de la información:</li> <li>- Cumplimiento de políticas y responsabilidades de seguridad de la información del personal de TI.</li> <li>- Afectaciones posibles de la seguridad debida a cambios en las infraestructuras tecnológicas.</li> </ul> <p>En el 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.</p>  |
| Representantes de las funciones especializadas del Registro de la Propiedad que tengan relación con seguridad de la información | <ul style="list-style-type: none"> <li>- Traen iniciativas de seguridad desde sus ángulos de especialidad cuando éstas sean relevantes, por ejemplo, desde el punto de vista de los recursos humanos, auditoría interna, departamento legal, oficina de proyectos, Dirección de informática del Municipio de Quito, etc.</li> <li>- 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.</li> </ul> |

| <b>COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad</b> |  |
|--|--|
| Mandato  | Aseguramiento que se sigan las buenas prácticas de seguridad de la información.<br>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   | <ul style="list-style-type: none"> <li>- El presidente es el Oficial de Seguridad de la Información.</li> <li>- 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.</li> <li>- Se permite la delegación o presencia de personas que sustituyan a los titulares, pero no se debe abusar de esta facilidad.</li> <li>- 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.</li> <li>- Se deben elaborar, aprobar, firmar y archivar actas de todas las reuniones.</li> </ul> |
| 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).<br>Las estrategias de gestión de los riesgos se deben escalar al Comité Ejecutivo de Seguridad y Riesgos para su aprobación.  |

| <b>NIVEL DE INVOLUCRACIÓN DEL COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN (Responsabilidades y rendición de cuentas)</b>  |               |
|---|---------------|
| 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 |

| <b>COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN; ENTRADAS Y SALIDAS A LA FUNCIÓN</b> |   |  |   |
|---|---|--|---|
| <b>ENTRADA</b>  | <b>DE</b>                               | <b>SALIDA</b>  | <b>A</b>  |
| 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 Auditoría Interna   | Auditoría Interna                       |  |   |

**3. ACERCA DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**

| <b>OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad</b> |  |
|---|--|
| <b>ÁREA</b>   | <b>CARACTERÍSTICAS</b>   |
| Mandato   | Responsabilidad general del programa de seguridad de la información del Registro de la Propiedad   |
| Principios operacionales y habilidades  | <p>Debe reportar al responsable de la Unidad de TIC</p> <p>Es el enlace entre el área ejecutiva y el programa de seguridad de la información.</p> <p>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.</p> <p>Además el Oficial de Seguridad debe:</p> <ul style="list-style-type: none"> <li>- Tener una comprensión precisa de la visión estratégica del Registro de la Propiedad.</li> <li>- Tener buenas habilidades para comunicar.</li> <li>- Ser hábil en la construcción de excelentes relaciones con las personas relevantes del Registro de la Propiedad.</li> <li>- Tener la capacidad de traducir los objetivos del Registro de la Propiedad en requerimientos de seguridad de la información.</li> </ul> |
| Ambito de Control   | <ul style="list-style-type: none"> <li>- Sistema de Gestión de Seguridad de la Información (SGSI).</li> <li>- Tratamiento de los riesgos de seguridad de la información.</li> </ul>  |
| Nivel de Autoridad y de decisiones  | <ul style="list-style-type: none"> <li>- Tiene a su cargo todas las decisiones necesarias para implementar y actualizar la estrategia de seguridad de la información.</li> <li>- Debe rendir cuentas y aprobar decisiones importantes e seguridad de la información como parte del Comité de Seguridad de la Información.</li> </ul>   |
| Qué delega  | Debe delegar tareas de seguridad de la información a directivos y otras personas del Registro de la Propiedad.   |
| Escala de autoridad   | <ul style="list-style-type: none"> <li>- Jefe inmediato</li> <li>- Comité Directivo de Seguridad de la Información</li> </ul>  |

| <b>NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN</b>   |                               |
|---|-------------------------------|
| <b>PRÁCTICA PROCESO</b>   | <b>NIVEL DE INVOLUCRACIÓN</b> |
| 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 cuentas                 |
| 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                   |

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

**4. ACERCA DEL GERENTE DE SEGURIDAD DE LA INFORMACIÓN**

| <b>GERENTE DE SEGURIDAD DE LA INFORMACIÓN: Mandato, principios operacionales y habilidades, alcance de control y nivel de autoridad</b> |   |
|---|---|
| <b>AREA</b>   | <b>CARACTERÍSTICAS</b>  |
| 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:<br>- Aplicaciones<br>- Infraestructura de TI.<br>Gestión de accesos<br>Gestión y tratamiento de incidentes<br>Gestión de riesgos<br>Programa de concienciación en seguridad de la información<br>Indicadores de seguridad de TI<br>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.<br><br><i>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</i>  |

|                            |  |
|----------------------------|--|
| <p>Escala de autoridad</p> | <p><i>ocupado por el Jefe de la Unidad de TI. Hay ventajas y desventajas de cada enfoque, pero las principales consideraciones deben ser:</i></p> <ul style="list-style-type: none"> <li>- <i>El tiempo que requieren estas tareas</i></li> <li>- <i>Las competencias y habilidades</i></li> <li>- <i>En cierta forma la incompatibilidad de los dos roles</i></li> </ul> <p><i>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.</i></p> |
|----------------------------|--|

| <p><b>NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL GERENTE DE SEGURIDAD DE LA INFORMACIÓN</b></p>   |                                      |
|--|--------------------------------------|
| <p><b>PRÁCTICA PROCESO</b></p>   | <p><b>NIVEL DE INVOLUCRACIÓN</b></p> |
| <p>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.</p>  | <p>Responsable</p>                   |
| <p>Asignación de los recursos humanos de seguridad de la información acorde a los requerimientos del registro de la Propiedad.</p>   | <p>Responsable</p>                   |
| <p>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.</p>   | <p>Responsable</p>                   |
| <p>Administración de roles, responsabilidades, privilegios de acceso y niveles de autoridad respecto a seguridad de la información.</p>  | <p>Responsable</p>                   |
| <p>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.<br/>Monitorea, ajusta y mejora estos controles.</p>   | <p>Responsable</p>                   |
| <p>Identificación y comunicación de puntos específicos del plan de seguridad, comportamientos deseables, y los cambios necesarios para tratar estos puntos.</p>  | <p>Responsable</p>                   |
| <p>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.</p> | <p>Responsable</p>                   |
| <p>Aseguramiento de que los aspectos ambientales y de las instalaciones de procesamiento cumplen con requerimientos de seguridad de la información.</p>  | <p>Responsable</p>                   |
| <p>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.</p>   | <p>Responsable</p>                   |

| <b>ENTRADAS Y SALIDAS A LA FUNCIÓN DE GERENTE DE SEGURIDAD DE LA INFORMACIÓN</b> |  |   |   |
|--|--|---|---|
| <b>Entrada</b>   | <b>De</b>  | <b>Salida</b>   | <b>A</b>  |
| 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.<br><br>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                                       |   |   |

| <b>NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DEL COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS</b>                                  |                               |
|---|-------------------------------|
| <b>PRÁCTICA PROCESO</b>   | <b>NIVEL DE INVOLUCRACIÓN</b> |
| 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.

| <b>NIVELES DE RESPONSABILIDAD Y RENDICIÓN DE CUANTAS DE LOS PROPIETARIOS FUNCIONALES DE LA INFORMACIÓN</b>  |                               |
|---|-------------------------------|
| <b>PRÁCTICA PROCESO</b>   | <b>NIVEL DE INVOLUCRACIÓN</b> |
| 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**

**QUITO**  
REGISTRO DE LA PROPIEDAD

**DESPACHO REGISTRADOR**

Recibido por: M. Pizarro

Fecha: 28/12/2015

Hora: 16:21

**REGISTRO DE LA PROPIEDAD**



Memorando No. RPDMQ-PROYMIRP-2015-1228C-M

Quito, D.M., 28 de Diciembre del 2015

**PARA:** Pablo Falconi Castillo  
**REGISTRADOR DE LA PROPIEDAD (E)**  
**DISTRITO METROPOLITANO DE QUITO**

**ASUNTO:** Solicitud Conformación Equipo Coordinador RPDMQ, y Designación Responsables para Gestión del Cambio y Seguridad de la Información solicitados por Consorcio.

En relación a la sumilla del 27 de noviembre de 2015, suscrita en memorando No. RPDMQ-PROYMIRP-2015-1127A-M, en el cual manifiesta no estar de acuerdo con la propuesta y solicita por correo electrónico revisión y comentarios a Asesoría y a Planificación; me permito informarle que con fecha 02 y 03 de diciembre de 2015, mediante correo electrónico se realizó gestión de depuración de la propuesta, según observaciones de mejora remitidos. El 03 de diciembre de 2015 se emitió correo electrónico a Asesoría, con copia a Planificación y a usted, adjuntando la matriz depurada con la Propuesta para Conformación del Equipo Coordinador RPDMQ; desde ese momento no se ha recibido comentario adicional alguno de la propuesta depurada. En vista de lo expuesto, solicito se designe a quien corresponda la gestión para designación y conformación del EQUIPO COORDINADOR RPDMQ.

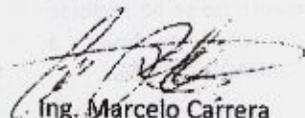
Adicionalmente, el Consorcio emitió oficio No. CMS-RPQ-2015-156 en el cual solicitan al RPDMQ "indique los responsables designados por el Registrador para la Gestión del Cambio", y también emitió oficio No. CMS-RPQ-2015-157 en el cual solicitan al RPDMQ la designación y conformación de equipos / cargo orientados a cumplir con lo que determina la norma de certificación ISO 27001 (en este oficio, consta el alcance de cada equipo / cargo).

Considerando la propuesta depurada para conformación del Equipo Coordinador RPDMQ y los pedidos del Consorcio; a continuación, para su consideración y designación a quien corresponda para su canalización a la brevedad posible, emito propuesta (salvo su mejor criterio) orientada a la conformación / delegación de equipos y cargos para GESTIÓN DEL CAMBIO y GRUPOS ORGÁNICOS DE ISO 27001:

| EQUIPO RPDMQ / CARGO RPDMQ              | DELEGACIÓN RPDMQ   | OBSERVACIÓN  |
|---|--|--|
| CONTRAPARTE PARA GESTIÓN DEL CAMBIO     | Responsable Comunicación<br>Asesor SSCC – Interinstitucional | ROL: El Consorcio es unidad asesora en lineamientos para Gestión del Cambio.<br>ROL: El RPDMQ es unidad ejecutora de la Estrategia del Cambio. |
| COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS | Coordinador/a TICs   | ROL: Oficial Seguridad de la Información   |
|   | Director/a Inscripciones                                     | ROL: Directivos de las áreas funcionales del RPDMQ   |
|   | Director/a Certificaciones                                   |  |
|   | Director/a Archivo   |  |
|   | Responsable Planificación                                    | ROL: Propietarios de procesos del RPDMQ  |
|   | Responsable SSCC   |  |
|   | Equipo de Planificación                                      | ROL: Auditoría Interna (personal a cargo del cumplimiento de regulaciones).  |
|   | Asesores de Control Registral                                |  |
|   | Técnica/o de Asesoría y Control Jurídico                     | ROL: Representante del área legal del RPDMQ  |
| Asesor/a de Informática                 | ROL: Responsable de gestión de riesgos TI                    |  |

| EQUIPO RPDMQ / CARGO RPDMQ                      | DELEGACIÓN RPDMQ                         | OBSERVACIÓN  |
|---|--|--|
| COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN | Coordinador/a TICs                       | ROL: Oficial Seguridad de la Información   |
|   | Director/a Inscripciones                 | ROL: Propietarios funcionales de la información  |
|   | Director/a Certificaciones               |  |
|   | Director/a Archivo                       |  |
|   | Responsable SSCC                         |  |
|   | Asesor de Informática                    | ROL: Responsable de la Unidad de TIC's   |
|   | Asesores de Control Registral            | ROL: Representantes de las funciones especializadas del Registro de la Propiedad que tengan relación con seguridad de la información |
|   | Técnica/o de Asesoría y Control Jurídico |  |
|   | Delegada/o de DAF                        |  |
| Delegada/o de Planificación                     |  |  |
| GERENTE DE SEGURIDAD DE LA INFORMACIÓN          | Director/a de Archivo                    | ROL: Gestión de la seguridad de la información del RPDMQ   |

Atentamente:



Ing. Marcelo Carrera

**GERENTE DE PROYECTO MODERNIZACIÓN INTEGRAL RPDMQ**

**ADMINISTRADOR DE CONTRATO No. 019-2014**

**REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO**

- ANEXO: Copia de oficio No. RPDMQ-PROYMIRP-2015-1127A-M con sumilla del 27-nov-2015  
 Copia de correo electrónico emitido por el Sr. Registrador el 27-nov-2015  
 Copia de correo electrónico que se emitió el 3-dic-2015 con propuesta depurada  
 Copia impresa de Propuesta Depurada para EQUIPO COORDINADOR RPDMQ  
 Copia de oficio No. CMS-RPQ-2015-156 con pedido Responsables RPDMQ para Gestión del Cambio  
 Copia de oficio No. CMS-RPQ-2015-157 con información aclaratoria de equipos /cargos para ISO 27001

CC: Andrés Eguiguren Administrador de Contrato No. 005-2015 (Fiscalización)

MCarrera/

**QUITO**  
 SERVICIO DE LA INFORMACIÓN  
**TECNOLOGÍA DE LA INFORMACIÓN  
 Y COMUNICACIONES**  
 Recibido por El Ch.  
 Fecha: 21/12/2015 Hora: 16:19

REGISTRO DE LA PROPIEDAD

Proceso de Licitación LICBS-RPDMQ-002-2014 cuyo objeto es "Modernizar de manera integral el Registro de la Propiedad del Distrito Metropolitano de Quito"  
Contrato No. 19-2014

FE DE ERRATAS

Doctor  
Pablo Falconí Castillo  
REGISTRADOR DE LA PROPIEDAD (E)  
DISTRITO METROPOLITANO DE QUITO  
En su despacho.-

Del memorando No. RPDMQ-PROYMIRP-2015-1228C-M, del 28 de diciembre del 2015, con Asunto: "Solicitud Conformación Equipo Coordinador RPDMQ, y Designación Responsables para Gestión del Cambio y Seguridad de la Información solicitados por Consorcio", se hace constar que se ha detectado error de texto en la matriz de delegación propuesta, en la sección "COMITÉ EJECUTIVO DE SEGURIDAD Y RIESGOS" (8va línea de la columna "DELEGACIÓN RPDMQ") y en la sección "COMITÉ DIRECTIVO DE SEGURIDAD DE LA INFORMACIÓN" (7ma línea de la columna "DELEGACIÓN RPDMQ"), siendo la siguiente errata u error en el mencionado memorando:

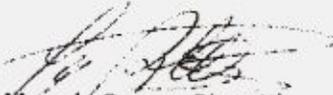
"Asesores de Control Registral"

Debe sustituirse por

"Agentes de Control Registral"

No habiendo ningún otro punto que tratar, es aprobada por el Administrador del Contrato, para constancia de lo actuado y en señal de conformidad suscribe la Fe de Erratas.

Dado en, Quito el 31 de diciembre de 2015.

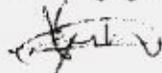
  
Marceló Carrera Riquetti

ADMINISTRADOR DEL CONTATO No. 019-2014

REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO

ANEXO: Copia Oficio No. RPDMQ-PROYMIRP-2015-1228C-M

CC: Andrés Eguiguren Administrador de Contrato No. 005-2015 (Fiscalización)

  
31/12/2015  
12:27



Memorando No. RPDMQ-PLAN-2016-55-M

Quito, D.M., 07 de Enero del 2016

**PARA:** Pablo Falconí Castillo  
REGISTRADOR DE LA PROPIEDAD (E)

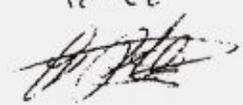
**DE:** María Eugenia Velasco  
ASESORA DE PLANIFICACIÓN

**ASUNTO:** Solicitud conformación de equipo de coordinación

MARCELO CARRERA: PROCEDER A CONFIRMAR  
A CONSEJO Y NOTIFICAR  
POR ESCRITO A FUNCIONARIOS  
02/01/2016  
P.S.F.

En relación al Memorando RPDMQ-PROYMIRP-2015-1228 remitido el 28 de diciembre del 2015 y Fe Erratas del 31 de diciembre del 2015 en el cual están efectuando la propuesta para la conformación del Equipo Coordinador del RPDMQ, para lo cual esta Unidad está de acuerdo con la delegación para:

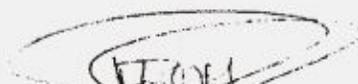
- Contrapartes para gestión del cambio
- Comité ejecutivo de seguridad y riesgos
- Comité directivo de seguridad de la información
- Gerente de seguridad de la información

Recibido en  
08 de enero 2016  
10:00  


Es importante mencionar que esta delegación no tendrá la figura de reemplazo - back up o por excepción; en el caso que uno de los delegados no pueda asistir a reuniones planificadas deberá notificar por escrito a dichos comités o reuniones.

Particular que comunico para los fines consiguientes.

Atentamente,

  
María Eugenia Velasco  
ASESORA DE PLANIFICACIÓN

  
Recibido por:.....  
Fecha:.....  
Hora:.....