

*[Handwritten signature]*  
9/03/2017  
11h30

Memorando N.- RPDMQ-TICS-2017-027-M

Quito, D.M., 09 de Marzo del 2017

**PARA:** Andrés Eguiguren  
**GERENTE DEL PROYECTO DE MODERNIZACION INTEGRAL DEL RPDMQ  
ADMINISTRADOR DEL CONTRATO 019-2014**

**ASUNTO:** Tercera revisión al entregable E.61 "Declaración de Aplicabilidad de controles"

- Mediante memorando RPDMQ DESPACHO 2016-079 del 10 de agosto del 2016, el Registrador de la Propiedad (E) Pablo Falconí, designa a Luz Verónica Flor, José Taípe y Oswaldo José Paz y Miño como miembros de la Comisión Técnica a Cargo de la Recepción parcial del Entregable E.61 del contrato No.019-2014.
- Mediante Oficio No. CMS-RPQ-2016-099 de fecha 18 de agosto del 2016, el consorcio MEB SEVENTEENMILE presenta al Administrador de Contrato No. 019-2014, Ing. Andres Eguiguren, el entregable E.61 "Declaración de Aplicabilidad de Controles".
- Mediante correo electrónico del 24 de agosto del 2016 el Administrador del Contrato informa a los miembros de la comisión, que el Entregable E.61 se encuentra para su revisión en: \\srv100filerp01\modernizacion\$\ENTREGABLES-Consortio\55\_E-61\_DECLARACION\_DE\_APLICABILIDAD\_DE\_CONTROLES
- Mediante Informe N.-RPDMQ-TICS-2016-029, del 30 de agosto del 2016 la Comisión Técnica emite un informe dirigido al Administrador del Contrato No. 019-2014, con las observaciones al entregable E.61.
- Con fecha 21 de septiembre del 2016 se recibió vía email la solicitud de revisión del denominado "Entregable E.61 Ajustado", en el email se indica que se revise la versión ajustada en: \\srv100filerp01\modernizacion\$\ENTREGABLES-Consortio\55\_E-61\_DECLARACION\_DE\_APLICABILIDAD\_DE\_CONTROLES\Entregable\_Ajustado. Además señala revisar el documento CMS-RPQ-2016-112 que contiene la respuesta dada por el consorcio a las observaciones del entregable del Contrato No. 019-2014.
- Mediante Informe N.-RPDMQ-TICS-2016-037, del 28 de septiembre del 2016 la Comisión Técnica designada procedió a emitir un informe al Administrador de Contrato No. 019-2014, con las observaciones sobre la segunda revisión al entregable E.61.

- Con fecha 26 de octubre del 2016, el Administrador de Contrato No. 019-2014, Ing. Andrés Eguiguren vía correo electrónico, da a conocer un Acta de Reunión de Trabajo de los Entregables, en donde se indica:  
*"En reunión de trabajo entre el RPDMQ, Consorcio y Fiscalización se determinó el alcance que deben tener los entregables relacionados con tecnología E30 E31 E60 E62 E61 E63 E55 E56 E59 E32 E65 E66"*.
- Con fecha 13 de diciembre del 2016, se firma en contrato complementario No. 003-2016, relacionado al Código de Proceso LICBS-002-RDMQ-2014: "MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO", en donde en la cláusula sexta de plazos se indica que: " ... aprobó una prórroga de plazo de hasta 4 meses, contados a partir de la fecha de la terminación del contrato principal...", pero no se ha encontrado ninguna referencia específica sobre el entregable E61.
- Mediante correo electrónico enviado del 17 de febrero del 2017, por el Administrador del Contrato No. 019-2014, informa a los miembros de la comisión que deben realizar la revisión de una nueva versión del entregable E61, cuya documentación se encuentra ubicada para su revisión en:  
 \\srv100filerp01\modernizacion\$\ENTREGABLES-Consorcio\55\_E-61\_DECLARACION\_DE\_APLICABILIDAD\_DE\_CONTROLES\Entregable\_Ajustado2
- Mediante Memorando N.-RPDMQ-PROYMIRP-2017-0308B-M de fecha 08 de marzo del 2017 el Administrador de Contrato No. 019-2014, Ing. Andres Eguiguren, informa a los miembros de la comisión técnica sobre el entregable E.61, que el día 31 de enero del 2017 se notificó al Proveedor del contrato No. 019-2014, sobre el OFICIO: DEMPILERPQ-00134-2017, donde se informa sobre avance de 11 productos, entre los cuales se encuentra el entregable E61: "Declaración de aplicabilidad de controles".  
 En el OFICIO: DEMPILERPQ-00134-2017, en relación al entregable E61, indica que:

*"Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento"*

*"CONCLUSIÓN CON RESPECTO AL PRODUCTO: No se recomienda su aceptación hasta que las observaciones hayan sido acogidas"*

### **Análisis**

Como miembros de la comisión técnica designados para la recepción del Entregable E61, se procede a revisar la documentación presentada y a detallar las siguientes observaciones:

Al comparar el contenido del entregable E61 en esta tercera revisión con el contenido del entregable realizado en la segunda revisión, se puede observar que



el único cambio realizado es la Fecha de 15/08/2015 por 15/02/2017 ubicado en el encabezado de cada página cómo se indica en las imágenes siguientes.

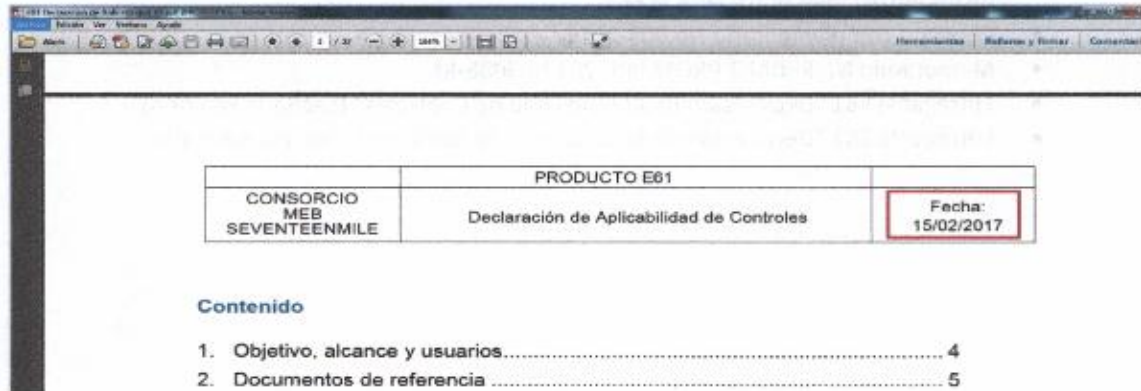


Imagen 1: Documento Tercera Revisión \\Srv100filep01/modernizacion\ENTREGABLES-Consorcio\55\_E-61\_DECLARACION\_DE\_APLICABILIDAD\_DE\_CONTROLES\Entregable\_Ajustado2\E61 Declaracion de Aplicabilidad V3.pdf

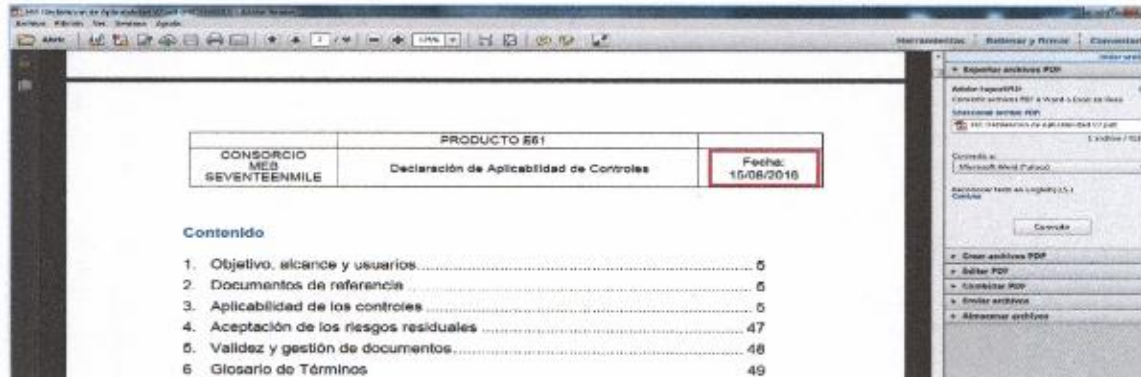


Imagen 2: Documento Segunda Revisión ubicada en la ruta \\Srv100filep01/modernizacion\ENTREGABLES-Consorcio\55\_E-61\_DECLARACION\_DE\_APLICABILIDAD\_DE\_CONTROLES\Entregable\_Ajustado\E61 Declaracion de Aplicabilidad V2.pdf

### Conclusiones

Hasta el momento existen observaciones no subsanadas en esta tercera revisión del entregable E.61, por lo que el entregable se encuentra observado.

  
**Luz Verónica Fior Solís**  
 MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E61 CONTRATO Nº 019-2014 RPDMQ

  
**José Rodolfo Taípe Guaño**  
 MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E61 CONTRATO Nº 019-2014 RPDMQ

  
**Oswaldo José Paz y Miño Ramón**  
 MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E61 CONTRATO Nº 019-2014 RPDMQ

**Anexos**

- Emails sobre notificación para revisión del entregable E61.
- Email sobre reunión de trabajo entre el RPDMQ, Consorcio y Fiscalización en relación al alcance de los entregables entre ellos el E61.
- Contrato complementario No.003-2016
- Memorando N.- RPDMQ-PROYMIRP-2017-0308B-M
- Entregable E61 "Declaración de Aplicabilidad de Controles" (Segunda Revisión)
- Entregable E61 "Declaración de Aplicabilidad de Controles" (Tercera Revisión)



**De:** Andrés Alberto Eguiguren Eguiguren  
**Enviado el:** miércoles, 24 de agosto de 2016 8:54  
**Para:** Jose Rodolfo Taipe Guaño; Luz Veronica Flor Solis; Oswaldo Jose Paz y Miño Ramon  
**Asunto:** Entregable E.61

Estimados

Como miembros de la comisión técnica designados para la recepción del Entregable E.61 pueden revisarlo en:

\\srv100filerp01\modernizacion\$\ENTREGABLES-Consorcio\55 E-61 DECLARACION DE APLICABILIDAD DE CONTROLES

Saludos,



Andrés Eguiguren  
Gerente del Proyecto de  
Modernización Integral del RPDMQ  
Administrador del Contrato 019-2014  
**REGISTRO DE LA PROPIEDAD DMQ**  
Ulloa N31-10 y Murgeón  
Telf.: 3988170 Ext. 29671  
Celular: 0996032128  
[andres.eguiguren@quito.gob.ec](mailto:andres.eguiguren@quito.gob.ec)

AVISO DE CONFIDENCIALIDAD: La información contenida en este e-mail es confidencial y sólo puede ser utilizada por el individuo o la entidad a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo a su origen para comunicar la recepción equivocada y borre inmediatamente el mensaje y cualquier adjunto recibido. MIDMQ no asume responsabilidad sobre la información, opiniones o criterios contenidos en este e-mail que no estén relacionados con negocios o actividades comerciales o funciones de su remitente.

**De:** Andrés Alberto Eguiguren Eguiguren  
**Enviado el:** miércoles, 21 de septiembre de 2016 10:28  
**Para:** Jose Rodolfo Taipe Guaño; Luz Veronica Flor Solis; Oswaldo Jose Paz y Mino Ramon  
**Asunto:** RE: Entregable E.61 Ajustado

Estimados

Como miembros de la comisión técnica designados para la recepción del Entregable E.61 pueden revisar la versión ajustada en:

[\\srv100filerp01\modernizacion\\$\ENTREGABLES-Consorcio\55 E-61 DECLARACION DE APLICABILIDAD DE CONTROLES\Entregable Ajustado](#)

Por favor revisar el documento CMS-RPQ-2016-112-Entregable E61 que contiene la respuesta dada por el consorcio a las observaciones del Entregable.

Saludos,



Andrés Eguiguren  
Gerente del Proyecto de  
Modernización Integral del RPDMQ  
Administrador del Contrato 019-2014  
**REGISTRO DE LA PROPIEDAD DMQ**  
Ulloa N31-10 y Murgeón  
Telf.: 3988170 Ext. 29671  
Celular: 0996032128  
[andres.eguiguren@quito.gob.ec](mailto:andres.eguiguren@quito.gob.ec)

AVISO DE CONFIDENCIALIDAD: La información contenida en este e-mail es confidencial y sólo puede ser utilizada por el individuo o la entidad a la cual esta dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo a su origen para comunicar la recepción equivocada y borre inmediatamente el mensaje y cualquier adjunto recibido. MDMQ no asume responsabilidad sobre la información, opiniones o criterios contenidos en este e-mail que no estén relacionados con negocios o actividades comerciales o funciones de su remitente.



**De:** Andrés Alberto Eguiguren Eguiguren  
**Enviado el:** viernes, 17 de febrero de 2017 10:24  
**Para:** Jose Rodolfo Taípe Gúaño; Luz Veronica Flor Solis; Oswaldo Jose Paz y Mino Ramon  
**Asunto:** Entregable E.61 Ajustado

Estimados

Como miembros de la comisión técnica designados para la recepción del Entregable E.61 pueden revisar la versión ajustada en:

[\\srv100filerp01\modernizacion\\$\ENTREGABLES-Consorcio\55 E-61 DECLARACION DE APLICABILIDAD DE CONTROLES\Entregable Ajustado2](\\srv100filerp01\modernizacion$\ENTREGABLES-Consorcio\55 E-61 DECLARACION DE APLICABILIDAD DE CONTROLES\Entregable Ajustado2)

Saludos,



Andrés Eguiguren  
Gerente del Proyecto de  
Modernización Integral del RPDMQ  
Administrador del Contrato 019-2014  
**REGISTRO DE LA PROPIEDAD DMQ**  
Ulloa N31-10 y Murgeón  
Telf.: 3988170 Ext. 29671  
Celular: 0996032128  
[andres.eguiguren@quito.gob.ec](mailto:andres.eguiguren@quito.gob.ec)

AVISO DE CONFIDENCIALIDAD: La información contenida en este e-mail es confidencial y sólo puede ser utilizada por el individuo o la entidad a la cual esta dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo a su origen para comunicar la recepción equivocada y borre inmediatamente el mensaje y cualquier adjunto recibido. MDMQ no asume responsabilidad sobre la información, opiniones o criterios contenidos en este e-mail que no estén relacionados con negocios o actividades comerciales o funciones de su remitente.

**De:** Andrés Alberto Eguiguren Eguiguren  
**Enviado el:** miércoles, 26 de octubre de 2016 16:03  
**Para:** Carlos Rafael Paredes LLerena; Cesar Patricio Espin Mora; Darwin Anibal Garzon Carrion; Doris Capucine Ochoa Ramirez; José Eduardo Báez Pérez; Jose Rodolfo Taipe Guaño; Miguel Angel Palacios Giler; Wilson Raul Vela Gomez; Cesar Antonio Lopez Viteri; Cesar Patricio Espin Mora; Daniel Ricardo Sierra Chiriboga; Oswaldo Jose Paz y Mino Ramon; Johanna del Rosario Maldonado Alvarado; David Alejandro Salazar Estevez  
**Asunto:** RV: Acta de Reunion de Trabajo de los Entregables  
**Datos adjuntos:** RPDMQ-PROYMIRP-2016-0927A-ARTP-Definicion alcance y estructura E30 E31 E60 E62 E61 E63 E55 E56 E59 E32 E65 E66.pdf  
**Importancia:** Alta

Estimados

En reunión de trabajo entre el RPDMQ, Consorcio y Fiscalización se determinó el alcance que deben tener los entregables relacionados con tecnología E30 E31 E60 E62 E61 E63 E55 E56 E59 E32 E65 E66

Adjunto les envío el Acta de Reunión firmada por los asistentes.

Este alcance ayudará a la revisión de dichos entregables.

Posteriormente les enviaré copia de dicha acta en respuesta a los memos entregados.

Saludos,



Andrés Eguiguren  
Gerente del Proyecto de  
Modernización Integral del RPDMQ  
Administrador del Contrato 019-2014  
**REGISTRO DE LA PROPIEDAD DMQ**  
Ulloa N31-10 y Murgeón  
Telf.: 3988170 Ext. 29671  
Celular: 0996032128  
[andres.eguiguren@quito.gob.ec](mailto:andres.eguiguren@quito.gob.ec)

**AVISO DE CONFIDENCIALIDAD:** La información contenida en este e-mail es confidencial y sólo puede ser utilizada por el individuo o la entidad a la cual esta dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo a su origen para comunicar la recepción equivocada y borre inmediatamente el mensaje y cualquier adjunto recibido. MDMQ no asume responsabilidad sobre la información, opiniones o criterios contenidos en este e-mail que no estén relacionados con negocios o actividades comerciales o funciones de su remitente.





**Acta de Reunión de Trabajo N.- RPDMQ-PROYMIRP-2016-0927A-ARTP**

**FECHA:** 27 de septiembre de 2016

**PROYECTO:** Modernizar de Manera Integral el Registro de la Propiedad del Distrito Metropolitano (Contrato No. 019-2014)

**ASUNTO:** Definición de alcance y estructura de entregables E.30, E.31, E.60, E.62, E.61, E.63, E.55, E.56, E.59, E.32, E.65, E.66

**LUGAR:** Sala 4to piso del RPDMQ

**HORA:** 10:00 – 13:00

**1. PARTICIPANTES**

No.	NOMBRE / sigla	FIRMA	INSTITUCIÓN / AREA	CARGO / ROL
1	Andrés Eguiguren /AE		RPDMQ	Administrador de Contrato 019-2014 Modernización Integral
2	Byron Paredes / BP		Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE	Lider del Proyecto
3	Patricio Espín / PE		RPDMQ	Asesor de Informática
4	Paola Pullas / PP		Empresa FISCALIZADORA	Delegado técnico

**2. TEMAS TRATADOS**

DESCRIPCIÓN DEL TEMA
1   Análisis de entregables E.30, E.31, E.60, E.62, E.61, E.63, E.55, E.56, E.59, E.32, E.65, E.66

**3. COMPROMISOS**

DESCRIPCIÓN DEL COMPROMISO	RESPONSABLE	FECHA MAXIMA
1		

**4. TEMAS PENDIENTES**

TEMA PENDIENTE	FECHA PARA TRATARLO
1	

**5. LINEAMIENTOS DE ACUERDOS ESTABLECIDOS**





REGISTRO DE LA PROPIEDAD

ACTA REUNIÓN DE TRABAJO PROYECTO

ALCANCE DE LOS ENTREGABLES

E.30	Informe técnico de los servicios web.	<ul style="list-style-type: none"><li>▪ Arquitectura de servicios web: debe tener un mapa que permita saber con cuales entidades interactúa el RPDMQ ya sea para consumir o publicar servicios.</li><li>▪ Listado de servicios web consumidos</li><li>▪ Listado de servicios web ofrecidos</li><li>▪ Funcionalidad de cada servicio web identificando que está publicando cada servicio y como se consume cada servicio..</li><li>▪ Estructura detallada del servicio web con parámetros de entrada y salida requeridos por cada servicio</li><li>▪ Información que se generará para terceros que no consumen servicios web. Listado de entidades y la forma de entregar la información.</li></ul>
E.31	Manual de usuario de servicios de la sede electrónica y plan de comunicación para ciudadanos	<p>Manual de usuario de los servicios de sede electrónica y plan de comunicación para ciudadanos debe contener:</p> <ul style="list-style-type: none"><li>▪ Listado de servicios que ofrece la sede electrónica</li><li>▪ Procedimiento de creación de usuarios</li><li>▪ Por cada servicio listado se debe entregar un flujo de utilización del servicio/funcionalidad</li><li>▪ Plan de comunicación en base a los productos ya entregados de planificación de comunicación.</li></ul>

2



<p>E.60</p>	<p>Manual de procedimientos de controles.</p>	<p>Procedimiento para control de documentos y registros.</p> <p>Plan del proyecto para la implementación del sistema de gestión de seguridad de la información</p> <p>Procedimiento para identificación de requisitos</p> <p>Documento sobre el alcance del SGSI</p> <p>Política de seguridad de la información</p> <p>Metodología de evaluación y tratamiento de riesgos</p> <p>Declaración de aplicabilidad</p> <p>Plan de tratamiento del riesgo</p> <p>Política sobre dispositivos móviles y tele-trabajo</p> <p>Política trae tu propio dispositivo (BYOD)</p> <p>Declaración de aceptación de los Documentos del sistema de gestión de seguridad de la información</p> <p>Declaración de confidencialidad</p> <p>Política de Clasificación de la Información</p> <p>Política de uso aceptable</p> <p>Política de claves</p> <p>Política de control de acceso</p> <p>Política del uso de controles criptográficos</p> <p>Política de eliminación y destrucción</p> <p>Política de pantalla y escritorio limpio</p> <p>Procedimientos para trabajo en áreas seguras</p> <p>Política de creación de copias de seguridad</p> <p>Política de gestión de cambio</p> <p>Procedimientos operativos para tecnología de la información y de la</p>
-------------	---	--



		<p>comunicación</p> <p>Política de transferencia de la información</p> <p>Política de desarrollo seguro</p> <p>Política de seguridad para proveedores</p> <p>Procedimiento para gestión de incidentes</p> <p>Plan de recuperación ante desastres</p> <p>Plan de capacitación y concienciación</p> <p>Procedimiento para auditoría interna</p> <p>Minutas de revisión por parte de la dirección</p> <p>Procedimiento para medidas correctivas</p> <p>Estructuras organizacionales de seguridad de la información</p> <p>Debe contener la Tabla de relación de documentos con la norma ISO 27001</p>
E.61	Declaración de Aplicabilidad de Controles	<p>Aplicabilidad de los controles. Justificativo de si es aplicable o no el control.</p> <p>Aceptación de los riesgos residuales</p> <p>Validez y gestión de documentos.</p> <p>Los objetivos de control van en el Entregable E.60 en cada documento.</p> <p>Debe estar acorde a la norma.</p>

ACTA REUNIÓN DE TRABAJO PROYECTO

E.62	Cuadro de Mando de la Seguridad de la Información.	<p>Definición del Cuadro de Mando del SGSI</p> <p>Objetivos del Cuadro de Mando del SGSI</p> <p>Indicadores</p> <p>Actividades de medición</p> <p>Estrategia de medición</p> <p>Revisión</p> <p>Matrices de Indicadores</p> <p>Acciones correctivas: implementar la mejora y optimizar los incumplimientos que se encuentren en la revisión.</p> <p>Debe estar acorde a la norma.</p>
------	--	---

A S P  
/ /



<p>E.63</p>	<p>Manual de procedimientos SGSI</p>	<p>Proceso de implementación del SGSI</p> <p>Objetivo</p> <p>Resultados</p> <p>Plazos</p> <p>Organización</p> <p>Principales riesgos del proceso</p> <p>Herramientas para implementación del proceso y generación de informes</p> <p>Anexos:</p> <ul style="list-style-type: none"> <li>• Procedimiento para control de documentos y registros</li> <li>• Procedimiento para identificación de requisitos</li> <li>• Documento sobre el alcance del SGSI</li> <li>• Política de seguridad de la información</li> <li>• Metodología de evaluación y tratamiento de riesgos</li> <li>• Cuadro de Evaluación de Riesgos</li> <li>• Cuadro de Tratamiento de los Riesgos</li> <li>• Formulario – Informe sobre evaluación y tratamiento de riesgos</li> <li>• Declaración de aplicabilidad</li> <li>• Procedimiento para auditoría interna</li> <li>• Procedimiento para medidas correctivas</li> <li>• Formulario para minutas de revisión por parte de la dirección</li> <li>• Plan de tratamiento del riesgo</li> </ul> <p>Clasificar por nivel los anexos:</p> <ul style="list-style-type: none"> <li>▪ Documentos de nivel 1             <ul style="list-style-type: none"> <li>• Manual de seguridad</li> </ul> </li> <li>▪ Documentos de nivel 2             <ul style="list-style-type: none"> <li>• Procedimientos</li> </ul> </li> <li>▪ Documentos de nivel 3             <ul style="list-style-type: none"> <li>• Instrucciones, checklists y formularios</li> </ul> </li> <li>▪ Documentos de nivel 4             <ul style="list-style-type: none"> <li>• Registros</li> </ul> </li> </ul>
-------------	--------------------------------------	--

E.59	Plan de Tratamiento de Riesgos	<p>Metodología de evaluación y tratamiento de riesgos</p> <p>Evaluación de riesgo</p> <p>Criterios para la aceptación de riesgos</p> <p>Tratamiento del riesgo</p> <p>Revisiones periódicas de la evaluación y el tratamiento de riesgos</p> <p>Declaración de aplicabilidad y Plan de tratamiento del riesgo</p> <p>Informes</p> <p>Gestión de registros guardados en base a este documento</p> <p>Anexos:</p> <ul style="list-style-type: none"><li>• Plantilla de Plan de Tratamiento de Riesgos</li><li>• Cuadro de evaluación de riesgos</li><li>• Cuadro de tratamiento de riesgos</li><li>• Informe sobre evaluación y tratamiento de riesgos</li><li>• Declaración de Aplicabilidad</li></ul> <p>Debe estar acorde a la norma.</p>
E.32	Constancia de implantación de la sede electrónica del Registro	<p>Arquitectura tecnológica</p> <p>Checklist de funcionalidad que cubre sede electrónica</p> <p>Pruebas de funcionamiento</p> <ul style="list-style-type: none"><li>• Anexos: Documento de instalación de la solución en los servidores</li><li>• Pantallas de funcionalidad de Sede Electrónica</li><li>• Manual de administrador de sede electrónica</li></ul>

*[Handwritten signatures and initials]*





ACTA REUNIÓN DE TRABAJO PROYECTO

E.55	Documento de alcance del SGSI	Definición del alcance del SGSI  Procesos y servicios registrales  Unidades organizativas  Ubicaciones  Redes e infraestructura de TI que apoyan los procesos registrales.  ANEXO: Activos de información del alcance  Debe estar acorde a la norma.
E.56	Documento de Políticas de Seguridad de la Información	Documentos de referencia  Terminología básica sobre seguridad de la información  Gestión de la seguridad de la información  Apoyo para la implementación del SGSI  Propuesta de Política Detallada y Normativa de Seguridad de la Información  Debe estar acorde a la norma y al alcance definido (E.55)

*[Handwritten signatures]*



ACTA REUNIÓN DE TRABAJO PROYECTO

E.65	Documentación del material de capacitación "Seguridad de la información" y evidencia de participación en la capacitación	<p>Resumen ejecutivo</p> <p>Objetivo del curso</p> <p>Detalle de asistentes</p> <p>Información del instructor</p> <p>Metodología de capacitación</p> <p>Programa del proceso de capacitación</p> <p>Evidencia de la capacitación dada</p> <p>Material utilizado</p>
E.66	Informe de auditoría interna del SGSI	<p>Objetivo de la auditoría</p> <p>Metodología</p> <p>Elementos de la auditoría</p> <p>Ejecución del plan de auditoría</p> <p>Novedades</p> <p>Conclusiones</p> <p>Anexos</p> <p>Capacitación</p> <p>Plan de auditoría</p> <p>Informe de auditoría</p>

6. GESTION DE SEGUIMIENTO

DIFUSION:	RPDMQ: AE
MONITOREO:	RPDMQ: AE / PE

9

CONTRATO COMPLEMENTARIO No. 003-2016

CÓDIGO DEL PROCESO LICBS-002-RDMQ-2014

**"MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO"**

**COMPARECIENTES:**

Comparecen a la celebración del presente contrato, por una parte el Registro de la Propiedad del Distrito Metropolitano de Quito, representado por el Doctor Pablo Falconí Castillo, en calidad de Registrador de la Propiedad (E), al que en adelante se le denominará CONTRATANTE; y, por otra, las empresas integrantes del Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE, conformada por las compañías Archivos Digitales MEB S.A.; y, Seventeenmile S.A., representadas por la señora Eva Larsen Montoya, en calidad de Procuradora Común, en adelante y para efectos de este contrato se denominará, LA CONTRATISTA. Las partes se obligan en virtud del presente contrato complementario, al tenor de las siguientes cláusulas:

**Cláusula Primera.- ANTECEDENTES:**

1.1 El numeral 2 del artículo 48 de la Ley Orgánica del Sistema Nacional de Contratación Pública dispone: "La licitación es un procedimiento de contratación que se utilizará en los siguientes casos: (...) Para contratar la adquisición de bienes o servicios no normalizados, exceptuando los de consultoría, cuyo presupuesto referencial sobrepase el valor que resulte de multiplicar el coeficiente 0,000015 por el monto del Presupuesto inicial del Estado del correspondiente ejercicio económico (...)".

1.2 Los artículos 49 al 55 del Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública, establecen el procedimiento del proceso de licitación.

1.3 Con Resolución No. RPDMQ-2014-065 de 8 de septiembre de 2014, el Doctor René Almeida Luna, Registrador de la Propiedad (E), resolvió disponer el inicio de proceso de licitación No. LICBS-002-RPDMQ-2014 generado para "MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO".

1.4 Mediante resolución No. RPDMQ-2014-082 de 11 de noviembre de 2014, el Doctor René Almeida Luna, Registrador de la Propiedad (E) del Municipio del Distrito Metropolitano de Quito, adjudicó el proceso de Licitación No. LICBS-RPDMQ-002-2014, cuyo objeto es "MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO", al oferente CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE.

1.5 El 22 de diciembre de 2014 se suscribió el contrato 019-2014 entre el Registro de la Propiedad del Distrito Metropolitano de Quito y , las empresas integrantes del Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE, conformada por las compañías Archivos Digitales MEB S.A.; y, Seventeenmile S.A., por el monto de tres millones seiscientos setenta y cinco mil novecientos

Handwritten signatures and initials, including "P.F.", "M", and "A".





diecisiete dólares de los Estados Unidos de América con 52/100 (USD \$3.675.917,52) sin incluir IVA; y, un plazo de ejecución de hasta 24 meses, contados a partir de la suscripción del contrato.

1.6 Mediante Oficio No. CMS-RPQ-2016-185 del 9 de diciembre de 2016, el Consorcio Archivos Digitales MebSeventeenmile recomienda al Administrador del Contrato No. 019-2014, Andrés Eguiguren lo siguiente: "(...) ejecutar un proceso modificatorio del marco contractual con la finalidad de incluir productos y alcances que relacionen de manera técnica los entregables y permitan la consecución de los objetivos del proyecto (...); y además que: "(...) El consorcio Consorcio Archivos Digitales Meb Seventeenmile conoce que para la ejecución de algunos entregables del contrato 19-2014, el sistema registral SIREL debe encontrarse en producción, por lo que, para el efecto el sistema debería cumplir con al menos las siguientes condiciones: a) Que se encuentre en ejecución de pruebas BETA; b) Que se hayan aprobado los módulos del flujo registral (que inicia con la petición y la entrega de los productos registrales al usuario); c) Que todos los actos registrales cumplan con la funcionalidad, conforme a la planificación acordada por las partes; y, d) Que se pueda crear folio real y permita la actualización del mismo (cualquier acto o contrato ingresado por el ciudadano que afecte a dicho folio pueda ser inscrito en el mismo), así como también poder emitir las certificaciones inherentes al mismo. De igual manera permita la gestión de folio personal y folio cronológico. En este sentido es necesario ratificar dichas condiciones a efectos de que, una vez que el Consorcio cumpla con las mismas puedan ser consideradas para la generación de los entregables que requieran de dicho hito (...)"

1.8 Mediante memorando No. RPDMQ-PROYMIRP-2016-1211A-M de 11 de diciembre de 2016, el Ing. Andrés Eguiguren en su calidad de Administrador de Contrato presenta el informe técnico y autoriza la suscripción del Contrato Complementario al Contrato Principal No. 19-2014, con fecha 12 de diciembre de 2016, aprobado mediante sumilla inserta por el Dr. Pablo Falconí Castillo, Registrador de la Propiedad (E), dispuso: "DACJ: "Informe".

1.9 Mediante memorando No. RPDMQ-DACJ-2016-193-M de 12 de diciembre de 2016, el Ab. Agustín Vásconez Granja en su calidad de Director de Asesoría y Control Jurídico del Registro de la Propiedad del Distrito Metropolitano de Quito, remite un Informe Jurídico al Doctor Pablo Falconí Castillo, Registrador de la Propiedad (E) mediante el cual señala que es procedente la elaboración de un contrato complementario con las empresas integrantes del Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE, conformada por las compañías Archivos Digitales Meb S.A.; y, Seventeenmile S.A., conforme las condiciones solicitadas por el Administrador del Contrato.

1.10 Mediante sumilla inserta en memorando No. RPDMQ-DACJ-2016-193-M del 12 de diciembre de 2016, el señor Registrador de la Propiedad (E), dispuso: "Proceder con elaboración del Contrato".

1.11 El artículo 85 de la Ley Orgánica del Sistema Nacional de Contratación Pública establece lo siguiente: "En el caso de que fuere necesario acaso ampliar, modificar, o complementar una obra o servicio determinado por causas imprevistas o técnicas, debidamente motivadas, presentadas con su ejecución, el Estado o la Entidad Contratante podrá celebrar con el mismo contratista, sin licitación o concurso, contratos complementarios que requiera la atención de las modificaciones antedichas, siempre que se mantengan los precios de los rubros del contrato original, reajustado a la fecha de celebración del respectivo contrato complementario".

**CLAÚSULA SEGUNDA.- DOCUMENTOS DEL CONTRATO:**

Forman parte integrante del presente contrato complementario los siguientes documentos:

M  
C

Handwritten signatures and initials in the bottom right corner.



1. Los que acrediten la capacidad de los comparecientes.
2. La Resolución de Inicio No. RPDMQ-2014-065 de 08 de septiembre de 2014.
3. La Resolución de Adjudicación No. RPDMQ-2014-082 de 11 de noviembre de 2014.
4. Contrato 019-2014 suscrito el 22 de diciembre de 2014, entre el Registro de la Propiedad del Distrito Metropolitano de Quito y las empresas integrantes del Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE, conformada por las compañías Archivos Digitales MEB S.A.; y, Seventeenmile S.A.
5. Documentos citados en la cláusula anterior de Antecedentes.

### **CLAÚSULA TERCERA.- OBJETO DEL CONTRATO COMPLEMENTARIO**

El objeto del Contrato complementario es determinar el alcance de ingreso a producción del sistema registral SIREL; complementar el alcance de los entregables: E.67 Informe de auditoría de certificación en ISO9001:2008; E.68 Informe de auditoría de certificación en ISO 27001; E.78 Informes de seguimiento trimestrales de la ejecución del plan de comunicación; y, E.79 Informe de coordinación de seguimiento del proyecto hasta su estabilización definitiva, complementar el alcance con los entregables: E.80 Informe de Soporte tecnológico para la estrategia de salida a usuarios de software registral; y, E.81 Informe de Soporte técnico registral.

### **CLAÚSULA CUARTA.-COMPLEMENTARIO**

#### **4.1. Entrada a producción del sistema registral SIREL**

Para la ejecución de algunos entregables del contrato 19-2014, el sistema registral SIREL debe encontrarse en producción, por lo que, para el efecto el sistema debería cumplir con al menos las siguientes condiciones:

- a) Que se encuentre en ejecución de pruebas BETA.
- b) Que se hayan aprobado los módulos del flujo registral (que inicia con la petición y la entrega de los productos registrales al usuario).
- c) Que todos los actos registrales cumplan con la funcionalidad, conforme a la planificación acordada por las partes.
- d) Que se pueda crear folio real y permita la actualización del mismo (cualquier acto o contrato ingresado por el ciudadano que afecte a dicho folio pueda ser inscrito en el mismo), así como también poder emitir las certificaciones inherentes al mismo. De igual manera permita la gestión de folio personal y folio cronológico.

En este sentido se ratifica éstas condiciones a efectos de que, una vez que el Consorcio cumple con las mismas puedan ser consideradas para la generación de los entregables que requieran de dicho hito.





**4.2 Alcance de salida a la ciudadanía del sistema SIREL**

Para la salida a la ciudadanía del sistema SIREL, deberá cumplirse:

- a) La salida a la ciudadanía del sistema SIREL será de responsabilidad del Registro de la Propiedad del Distrito Metropolitano de Quito, previo a lo cual LA CONTRATISTA entregará el sistema integral (Gestor Documental, Sistema Registral, sede electrónica) totalmente funcional de acuerdo a las necesidades del RPDMQ y recibido a satisfacción, con la firma del acta correspondiente, que permita la gestión de todos los trámites que actualmente está atendiendo el RPDMQ desde su ingreso hasta la entrega del producto final al ciudadano, en el marco de Folio Real, Folio Personal y Folio Cronológico además de los reportes solicitados. LA CONTRATISTA deberá cumplir con todos los requerimientos del sistema registral de conformidad con el contrato principal y, que además incluye: la aprobación de los flujos registrales con todos los actos registrales, observaciones requeridas y mejoras aceptadas<sup>1</sup>.

**4.3. Complementar el alcance del entregable E.67 Informe de auditoría de certificación en ISO9001:2008**

El entregable E.67 Informe de auditoría de certificación en ISO9001:2008 mantendrá el alcance del contrato principal 19-2014 en el subcomponente 7. Gestión de la Calidad y Seguridad de la Información - Implantación de ISO 9001 y 27001, del Componente C.2 Modernización integral del RP e incluirá el acompañamiento técnico para la formulación del plan de solución de las no conformidades que podría entregar la empresa certificadora.

Handwritten mark: a large '1' with a diagonal slash through it.

**4.4 Complementar el alcance del entregable E.68 Informe de auditoría de certificación en ISO 27001**

El entregable E.68 - Informe de auditoría de certificación en ISO 27001 se mantendrá el alcance del contrato principal 19-2014 en el subcomponente 7. Gestión de la Calidad y Seguridad de la Información - Implantación de ISO 9001 y 27001, del Componente C.2 Modernización integral del RP e incluirá el acompañamiento técnico para la formulación del plan de solución de las no conformidades que podría entregar la empresa certificadora.

**4.5 Complementar el alcance del E.78 Informes de seguimiento trimestrales de la ejecución del plan de comunicación**

El entregable E.78 "Informes de seguimiento trimestrales de la ejecución del plan de comunicación" mantendrá el alcance del contrato principal 19-2014 en el Subcomponente 8. Administración del cambio, del Componente C.2 Modernización integral del RP incluyendo recomendaciones que se puedan realizar durante la ejecución del plan de comunicación.

Handwritten mark: a large 'X'.

<sup>1</sup> Se anexa el presente el listado de observaciones y mejoras solicitadas

Handwritten initials and marks in the bottom right corner.



**4.6 Complementar el alcance del entregable E.79 Informe de coordinación de seguimiento del proyecto hasta su estabilización definitiva**

El entregable E.79 "Informe de coordinación de seguimiento del proyecto hasta su estabilización definitiva" mantendrá el alcance del contrato principal 19-2014 en el Subcomponente 8. Administración del cambio, del Componente C.2 Modernización integral del Registro de la Propiedad incluyendo el alcance de los entregables adicionales que se suscriban en este contrato complementario y actualizaciones que fueren necesarias.

**4.7 Complementar el objeto del contrato incluyendo el entregable E.80 Informe de Soporte tecnológico para la estrategia de salida a usuarios de software registral, el cual se integrará al subcomponente 4 Sede Electrónica del componente C.2 Modernización Integral del RPQ.**

El entregable E.80 Informe de Soporte tecnológico para la estrategia de salida a usuarios de software registral mantendrá el siguiente alcance:

- Acompañamiento en la estrategia de salida a usuarios de conformidad con el plan de implantación aprobado entre LA CONTRATISTA y el administrador del contrato:
  - Elaboración en conjunto entre el Registro de la Propiedad del Distrito Metropolitano de Quito y LA CONTRATISTA del plan de salida a la ciudadanía del sistema registral;
  - Revisión de disponibilidad y recomendaciones de afinamiento de servicios tecnológicos del Registro de la Propiedad del Distrito Metropolitano de Quito, relacionados con el sistema registral y gestor documental
  - El Soporte Técnico en Sitio que LA CONTRATISTA deberá poner a disposición del Registro de la Propiedad del Distrito Metropolitano de Quito de segundo nivel (a la funcionalidad del sistema registral y gestor documental) para reaccionar de manera inmediata ante novedades que se pudieran presentar durante la Salida a Producción del Sistema de Folio Real y hasta la finalización del contrato complementario.
  - Solventar en conjunto con el Registro de la Propiedad del Distrito Metropolitano de Quito los problemas tecnológicos que no permitan avanzar en el flujo de trabajo implementado en el Sistema de Folio Real, a fin de evitar suspensión en la atención a la Ciudadanía durante la Salida a Producción del Sistema de Folio Real.
  - Brindar hasta 100 horas de programación adicional a la funcionalidad del sistema registral que ingresó a producción durante la ejecución del contrato complementario, previo a la factibilidad técnica acordada entre las partes.

**4.8 Complementar el objeto del contrato incluyendo el entregable E.81 Informe de Soporte técnico registral, el cual se integrará al subcomponente 2 Procesos Registrales del componente C.2 Modernización Integral del RPQ.**

El entregable E.81 Informe de Soporte técnico registral mantendrá el siguiente alcance:

- Soporte para la creación de folio real durante la ejecución del contrato complementario; y
- De ser necesario brindar soporte de ajuste a procesos registrales durante la ejecución del contrato.



**CLÁUSULA QUINTA.- PRECIO DEL CONTRATO**

Conforme se establece en la cláusula cuarta del contrato principal No. 019-2014 "Precio del Contrato", el valor estipulado para el pago a la contratista por el objeto del contrato "MODERNIZAR DE MANERA INTEGRAL EL REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO" es de tres millones seiscientos setenta y cinco mil novecientos diecisiete dólares de los Estados Unidos de América con 52/100 (USD \$3.675.917,52) más IVA.

Para la suscripción del contrato complementario, de acuerdo al requerimiento aprobado en memorando No. RPDMQ-DACJ-2016-193-M del 12 de diciembre de 2016, no se incrementa el monto del contrato principal.

**CLÁUSULA SEXTA.- PLAZO**

Conforme se establece en la cláusula séptima del contrato principal el "Plazo", para la entrega de la totalidad de los bienes y servicios contratados en su totalidad a entera satisfacción del Registro de la Propiedad del Distrito Metropolitano de Quito.

De acuerdo al requerimiento aprobado en memorando RPDMQ-DACJ-2016-193-M del 12 de diciembre de 2016 se aprobó una prórroga de plazo de hasta 4 meses, contados a partir de la fecha de la terminación del contrato principal.

Los entregables serán presentados de conformidad con lo siguiente:

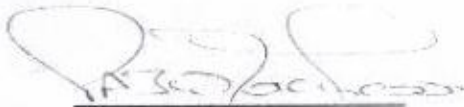
- E.67 "Informe de auditoría de certificación en ISO9001:2008", a los ciento quince días de suscrito el contrato complementario;
- E.68 "Informe de auditoría de certificación en ISO 27001", a los ciento quince días de suscrito el contrato complementario;
- E.78 "Informes de seguimiento trimestrales de la ejecución del plan de comunicación", a los ciento quince días de suscrito el contrato complementario;
- E.79 "Informe de coordinación de seguimiento del proyecto hasta su estabilización definitiva, complementar el alcance con los entregables", a los ciento quince días de suscrito el contrato complementario;
- E.80 "Informe de Soporte tecnológico para la estrategia de salida a usuarios de software registral", a los noventa días de suscrito el contrato complementario; y,
- E.81 "Informe de Soporte técnico registral", a los noventa días de suscrito el contrato complementario;

**CLÁUSULA SÉPTIMA.- RATIFICACIÓN**

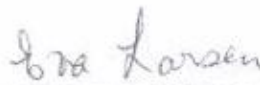
Las partes se ratifican y se afirman en las condiciones y términos estipulados en todas y cada una de las cláusulas del Contrato No. 19-2014 que no hayan sido modificadas por el presente instrumento contractual complementario.

**CLÁUSULA OCTAVA.- ACEPTACIÓN DE LAS PARTES**

Las partes declaran expresamente su aceptación a todo lo convenido en el presente contrato complementario por lo que, libre y voluntariamente, previo el cumplimiento de todos y cada uno de los requisitos exigidos por las leyes de la materia, a cuyas estipulaciones se someten y suscriben cinco ejemplares de igual contenido y valor en la ciudad de Quito, Distrito Metropolitano a los 13 días del mes de diciembre de 2016.



**Dr. Pablo Falconi Castillo**  
**REGISTRADOR DE LA PROPIEDAD (E)**  
**DISTRITO METROPOLITANO DE QUITO**  
**EL CONTRATANTE**



**Sra. Eva Larsen Montoya**  
**PROCURADOR COMÚN**  
**CONSORCIO ARCHIVOS DIGITALES MEB**  
**SEVENTEENMILE**  
**LA CONTRATISTA**

 Elaborado por: Belén Durán	 Aprobado por: Andrés Eguiguren	 Revisado por: José Luis Aucancela
Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016
 Revisado por: Patricio Espín	 Revisado por: Marcelo Cornejo	 Revisado por: Agustín Vásconez
Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016
 Revisado por: Fátima Rodríguez	 Revisado por: Ricardo Romero	 Revisado por: Freddy Herrera
Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016	Fecha: 13 de diciembre de 2016



Memorando N.- RPDQM-PROYMIRP-2017-0308B-M

Quito, D.M., 08 de marzo de 2017

**PARA:**

Darwin Anibal Garzón Carrión  
**MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.57 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Darwin Anibal Garzón Carrión  
**MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.58 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Johanna Patricia Berrezueta Pineda  
David Alejandro Salazar Estevez  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.60 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

José Eduardo Báez Pérez  
**MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.62 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

José Rodolfo Taipe Guaño  
Luz Verónica Flor Solís  
Oswaldo José Paz y Miño Ramón  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.61 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Darwin Anibal Garzón Carrión  
**MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.63 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Doris Capucine Ochoa Ramírez  
Miguel Angel Palacios Giler  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.55 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Wilson Raúl Vela Gómez  
Daniel Ricardo Sierra Chiriboga  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.56 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Johanna del Rosario Maldonado  
José Rodolfo Taipe Guaño  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.59 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

Daniel Ricardo Sierra Chiriboga  
**MIEMBRO DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.65 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

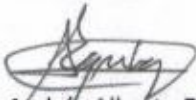
José Rodolfo Tapie Guaño  
César Antonio López Viteri  
**MIEMBROS DE LA COMISIÓN DE ENTREGA-RECEPCIÓN PARCIAL DEL ENTREGABLE E.66 DEL  
CONTRATO NO.019-2014 REGISTRO DE LA PROPIEDAD DEL DMQ**

**ASUNTO:** Informe de Entrega de Oficio DEMPILERPQ-00134-2017 al Consorcio

Estimados por medio del presente pongo en su conocimiento que con fecha 31 de enero del 2017 mediante oficio N°.- RPDMQ- PROYMIRP-2017-0131A-OF se entregó el Oficio DEMPILERPQ-00134-2017 al Consorcio ARCHIVOS DIGITALES MEB SEVENTEENMILE, informando la evaluación del contenido de los productos puestos a consideración de Fiscalización.

Sin otro particular por el momento, aprovecho la oportunidad para reiterarle mis más altos sentimientos de consideración y estima.

Atentamente



Andrés Alberto Eguiguren Eguiguren.

**GERENTE DEL PROYECTO DE MODERNIZACION INTEGRAL DEL RPDMQ  
ADMINISTRADOR DEL CONTRATO N° 019-2014**





Recibido  
31/ene/2017 16:30  
Byron Perances  
R.  
C.C. 4709077702

Oficio No. RPDMQ-PROYMIRP-2017-0131A-OF

Quito, 31 de enero de 2017

**ASUNTO:** Informe de Fiscalización de Entregables relacionados con ISO 27001

Señora  
Eva Larsen Montoya  
PROCURADORA COMÚN  
CONSORCIO ARCHIVOS DIGITALES MEB SEVENTEENMILE

De mi consideración:

La empresa Fiscalizadora ha presentado el informe de los Entregables relacionados con ISO 27001, con las observaciones enfocadas al ajuste de dichos productos;

Estas observaciones deberán realizarse en el plazo máximo de 15 días acorde a lo estipulado en los informes de Fiscalización.

Atentamente


Andrés Eguiguren  
GERENTE DE PROYECTO MODERNIZACIÓN INTEGRAL RPDMQ  
ADMINISTRADOR DE CONTRATO No. 019-2014  
REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO

**ANEXO:** Informe de Fiscalización de Entregables relacionados con ISO 27001

**DEMPILE S.A.**  
Compañía Consultora Técnica

OFICIO: DEMPILE-RPQ-00134-2017  
Quito, 19 de enero de 2017

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

  
24/01/17  
12:00

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 un INFORME 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 inherentes 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, con la finalidad de considerar la información como "validada" fiscalización propone anexas a

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina. Ed. Monasterio Plaza, piso 10  
Telfs. (593-2) 6012447 / 6012443  
www.dempile.com / info@dempile.com  
Quito - Ecuador







## DEMPIL S.A.

Compañía Consultora Técnica

este entregable los documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.

Como introducción al documento debe colocarse:

- o Diagnóstico inicial del RPQ el cual de existir debe incluirse como anexo y colocar una referencia al mismo en el documento.

El documento desde la página 31 hasta la 269 está compuesta principalmente de los anexos que deben especificar y justificar:

- o Validar la información del anexo, esto es, anexar a este entregable documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.
- o 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 versiona las fichas inicialmente recolectadas y no se tenga que ingresar la información nuevamente desde cero.

El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.

Las observaciones emitidas por fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.

Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se haya cumplido lo requerido.

**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**

# DEMPILE S.A.

Compañía Consultora Técnica

## Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, con la finalidad de considerar la información como "validada" fiscalización propone anexar a este entregable los documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.
- Como introducción al documento debe colocarse:
  - o Diagnóstico inicial del RPQ el cual de existir debe incluirse como anexo y colocar una referencia al mismo en el documento.
- El documento desde la página 32 hasta la 204 está compuesta principalmente de los anexos que deben especificar y justificar:
  - o Validar la información del anexo, esto es, anexar a este entregable los documentos como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.
  - o 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 versiona las fichas inicialmente recolectadas y no se tenga que ingresar la información nuevamente desde cero.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se haya cumplido las observaciones requeridas. D

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina, Ed. Monasterio Plaza, piso 10

Teléfono: (593-2) 6012442 / 6012443

[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)

Quito - Ecuador





## DEMPILE S.A.

Compañía Consultora Técnica

- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peñonetas, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se tengan las observaciones.

### 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:
  - o Regulaciones y procedimientos internos aplicables a la entidad, listar las regulaciones a las que hace referencia, debido a que no se puede citar de manera genérica.
  - o Modelo de Valor, Modelo de Salvaguardas, Modelo de Procedimientos.
- En la sección PROCESOS Y SERVICIOS se hace mención a:
  - o La matriz de competencias institucional, adjuntar mediante anexo dicha matriz.
  - o En esta misma sección se habla de los procesos cubiertos para el alcance del SGSI pero se debe adjuntar el documento de procesos en su última versión, 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, adjuntar el documento de propuesta.

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina. Ed. Monasterio Plaza, piso 10  
Tels. (593-2) 6012442 / 6012441  
[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)  
Quito - Ecuador

10



**DEMPILE S.A.**  
Compañía Consultora Técnica

E.60: Manual de procedimientos de control

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, con la finalidad de considerar la información como "válida" fiscalización propone anexar a este entregable los documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis, o su justificación.
- Si bien el documento es un manual se solicita incorporar:
  - Anexos que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ; los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
  - Incorporar en los formatos propuestos particularidades propias de RPQ es decir aterrizar la propuesta de lo genérico al caso puntual RPQ.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ; los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

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

E.63: Cuadro de mando de seguridad de la información

Observaciones encontradas:



# DEMPILE S.A.

Compañía Consultora Técnica

- Se indica que la información del documento presentado no ha sido validada, con la finalidad de considerar la información como "válida" fiscalización propone anexar a este entregable los documentos como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.
- 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. Anexar documento de referencia y fuente.
- Se hace referencia al organograma 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 qué criterio se escogió los indicadores y la aprobación del RPQ de aceptación de los indicadores.
- En el Anexo del documento se encuentra un matrix 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 debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que las observaciones hayan sido acogidas.

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina Ed. Mercaderes Plaza, piso 10  
Tulsa. (593-2) 6012442 / 6012443  
[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)  
Quito - Ecuador



**DEMPIL S.A.**  
Compañía Consultora Técnica

E.61: Declaración de aplicabilidad de controles

Observaciones encontradas:

- Se puede anexar oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos, en caso de existir o justificar.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que las observaciones hayan sido acogidas.

E.62: Manual de procedimientos del SGSI

Observaciones encontradas:

- Se indica que la información del documento presentado no ha sido validada, con la finalidad de considerar la información como "validada" fiscalización propone anexar a este entregable los documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis, o justificar.
- Si bien el documento es un manual se solicita incorporar:
  - o Anexos que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
  - o Incorporar en los formatos propuestos particularidades propias de RPQ es decir aterrizar la propuesta de lo genérico al caso puntual del RPQ.



# DEMPILE S.A.

Compañía Consultora Técnica

- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se tengan las observaciones.

## 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:
  - o Regulaciones y procedimientos internos aplicables a la entidad, listar las regulaciones a las que hace referencia, debido a que no se puede citar de manera genérica.
  - o Modelo de Valor, Modelo de Salvaguardas, Modelo de Procedimientos.
- En la sección PROCESOS Y SERVICIOS se hace mención a:
  - o La matriz de competencias institucional, adjuntar mediante anexo dicha matriz.
  - o En esta misma sección se habla de los procesos cubiertos para el alcance del SGSI pero se debe adjuntar el documento de procesos en su última versión, 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, adjuntar el documento de propuesta.

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina, Ed. Monasterio Plaza, piso 10  
Tels. (593-2) 6012447 / 6012448  
[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)  
Quito - Ecuador



**DEMPILÉ S.A.**  
Compañía Consultora Técnica

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

- o 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 y proyección de información.
- o 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.

- o El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- o Se presenta un gráfico de arquitectura de red actualizado. 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:

- o Se hace referencia a servicios del municipio y servicios de terceros debe anexarse documentos que permitan determinar de dónde se sacó ese listado de servicios para validación.

En la sección VALIDEZ Y GESTIÓN DE DOCUMENTOS:

- o Se presenta una fecha de validez que indicaría que el documento revisado por fiscalización ya no es válido. Corregir

En la sección ANEXO:

- o Se evidencia que los activos de información tienen levantados mediante fichas que indica que no han sido aprobadas, es mandatorio adjuntar las fichas de acuerdo a proyección.



# DEMPILE S.A.

Compañía Consultora Técnica

- o Se indica que la fecha de levantamiento es de 2015 con actualización Agosto de 2016 esto debe entregarse proyectado al nuevo sistema informática.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se hayan solventado las observaciones.

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

### Observaciones encontradas:

- Incluir como documentos de referencia a los documentos siguientes:
  - o Fichas de captura.
  - o Alcance del SGSI.
  - o Riesgos inherentes.
  - o 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:
  - o Hacer primero referencia a la última versión de manual de procesos de RPQ para validar que los procesos constan en el manual.

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina Ed. Monasterio Plaza, piso 10  
Telfs. (593-2) 6012442 / 6012443  
[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)  
Quito - Ecuador

2



## DEMPILE S.A.

Compañía Consultora Técnica

- o Los procesos que acá se nombren deben tener coherencia con los procesos objeto del alcance en el Entregable E53.
- o 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 valdar 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.
- 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 la 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 exterior al interior y fuera del RPQ.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por fiscalización en este entregable son en su mayoría referentes a errores de forma y ANEXOS faltantes a los cuales se hace referencia que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.





# DEMPILE S.A.

Compañía Consultora Técnica

- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se corrija lo indicado.

## 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, con la finalidad de considerar la información como "válida" fiscalización propone anexar a este entregable los documentos tales como oficios, correos electrónicos, peticiones, actas de reuniones, etc., de tal manera que la información pueda ser contrastada para su aceptación o análisis.
- Como introducción al documento debe colocarse:
  - o Diagnóstico inicial del RPQ el cual de existir debe incluirse como anexo y colocat una referencia al mismo en el documento.
- 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.
- El entregable debe estar proyectado al estado en el cual los futuros sistemas se encuentren en producción, es decir, el análisis de riesgos debe hacerse en base a la arquitectura final definida para los nuevos sistemas informáticos calculando los riesgos de los activos como se van a encontrar en producción.
- Las observaciones emitidas por Fiscalización son en su mayoría referentes a ANEXOS faltantes que reflejen que la información contenida en el documento fue obtenida mediante el levantamiento de información en RPQ, los documentos correspondientes a ese levantamiento pueden provenir de oficios, correos electrónicos, peticiones, etc. A funcionarios de RPQ para ser considerados válidos.
- Tiempo prudencial para completar la información: Se estima prudencial entregar un plazo máximo de 15 días para la entrega de toda la documentación faltante y corrección de cada ítem solicitado en este documento.

---

Av. Eloy Alfaro y Av. 6 de Diciembre, esquina. Ed. Monasterio Plaza, piso 10  
Tels. (593-2) 6312442 / 6812443  
[www.dempile.com](http://www.dempile.com) / [info@dempile.com](mailto:info@dempile.com)  
Quito - Ecuador

ef

Vertical text on the left margin, likely a scanning artifact or reference code.



**DEMPILE S.A.**  
Compañía Consultora Técnica

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** No se recomienda su aceptación hasta que se corrija lo indicado.

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

Observaciones encontradas:

Indicar 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:** No se recomienda su aceptación hasta cumplir con las observaciones.

E.66. Informe de auditoría interna del SGSI

Observaciones encontradas:

- Este informe de auditoría interna puede ser considerado como un ejercicio inicial de preparación válido a la fecha. Sin embargo, se recomienda realizar auditorías frecuentes y periódicas para medir el avance de implementación del SGSI.

**CONCLUSIÓN CON RESPECTO AL PRODUCTO:** Se recomienda su aceptación.

Atentamente,

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

Abg. Marcelo Dávala Martínez  
**LÍDER DEL EQUIPO DE**  
**FISCALIZACIÓN**





# Declaración de Aplicabilidad de Controles

PRODUCTO E-61

CONSORCIO MEB SEVENTEEN MILE

Quito, Agosto 2016

	<b>PRODUCTO E61</b>	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

**Contenido**

1. Objetivo, alcance y usuarios.....	5
2. Documentos de referencia .....	5
3. Aplicabilidad de los controles .....	5
4. Aceptación de los riesgos residuales .....	47
5. Validez y gestión de documentos .....	48
6. Glosario de Términos .....	49



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

### DECLARACIÓN DE APLICABILIDAD

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

**Historial de modificaciones**

Fecha	Versión	Creado por	Descripción de la modificación
DD-MM- AAAA	0.1	Alberto Pazmiño P	Descripción básica del documento



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

### 1. Objetivo, alcance y usuarios

El objetivo del presente documento es bosquejar en una primera instancia qué controles son adecuados para implementar en el Registro de la Propiedad, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo facilitar la aprobación formal de la implementación de los controles mencionados.

Para la versión definitiva de este documento es necesario que previamente se aprueben de manera formal lo siguiente:

1. FICHAS DE CAPTURA DEL ACTIVOS DE INFORMACIÓN Y SUS VALORACIONES
2. MODELO DE VALOR: Inventario de activos de información y sus valoraciones en las dimensiones de seguridad.
3. MODELO DE RIESGOS INHERENTES
4. MODELO DE RIESGOS RESIDUALES
5. METODOLOGÍA DE TRATAMIENTO DE LOS RIESGOS

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001:2013. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos empleados del Registro de la Propiedad que cumplen una función dentro del SGSI.

### 2. Documentos de referencia

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos

### 3. Aplicabilidad de los controles

Son aplicables todos los controles del Anexo A de la norma ISO 27001:2013:

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.5	Políticas de seguridad de la información					
A.5.1	Dirección de la gerencia para la seguridad de la información					
A.5.1.1	Políticas para seguridad de la información				Todas las políticas indicadas bajo esta columna	
A.5.1.2	Revisión de políticas para seguridad de la información	Si			Cada política tiene un propietario designado que debe revisar el documento según un intervalo planificado	Por implementar
A.6	Organización de la seguridad de la información	Si				
A.6.1	Organización interna					



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si			Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI. Si es necesario, el [cargo] define responsabilidades adicionales.	
A.6.1.2	Segregación de deberes	Si			Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra.	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (S/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.6.1.3	Contacto con autoridades	Si			[Estrategia de continuidad del negocio], [Plan de respuesta a los incidentes]	
A.6.1.4	Contacto con grupos de interés especial	Si			El [cargo] es el responsable de supervisar [detallar los nombres de grupos de interés y foros de seguridad]	
A.6.1.5	Seguridad de la información en gestión de proyectos	Si			El gerente de proyecto debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.6.2	Dispositivos móviles y tele-trabajo	Si				
A.6.2.1	Política sobre dispositivos móviles	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo], [Política Trae tu propio dispositivo (BYOD)]	
A.6.2.2	Tele-trabajo	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo]	
A.7	Seguridad relacionada con el personal					
A.7.1	Antes del empleo					

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.7.1.1	Selección	Si			El [cargo] verifica a cada candidato [describir el método para las verificaciones; por ej., revisando el CV, poniéndose en contacto con empleadores anteriores, verificando antecedentes penal, situación financiera, etc.]; [Política de seguridad para proveedores]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.7.1.2	Términos y condiciones de empleo	Si			Todos los empleados firman la [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]	
A.7.2	Durante el empleo					
A.7.2.1	Gestión de responsabilidades	Si			La dirección exige activamente que todos los empleados, proveedores y socios implementen todas las reglas del SGSI	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.7.2.2	Concienciación, educación y capacitación sobre Seguridad de la información	Si			Política de seguridad de la información, Plan de capacitación y concienciación, [Política de seguridad para proveedores]	
A.7.2.3	Proceso disciplinario	Si			[Procedimiento para gestión de incidentes], [Declaración de aceptación de los documentos del SGSI]	
A.7.3	Terminación o cambio del empleo					



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.7.3.1	Terminación o cambio de responsabilidades del empleo	Si			Todos los acuerdos con proveedores y socios contienen cláusulas que siguen vigentes después de finalizado el empleo, como también las [Declaraciones de confidencialidad] firmadas con los empleados.	
A.8	Gestión de activos					
A.8.1	Responsabilidad sobre los activos					
A.8.1.1	Inventario de activos	Si			[Inventario de activos], [Política de clasificación de la información]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.8.1.2	Propiedad de los activos	Si			[Inventario de activos], [Política de uso aceptable]	
A.8.1.3	Uso aceptable de los activos	Si			[Política de Uso aceptable]	
A.8.1.4	Devolución de activos	Si			[Política de Uso aceptable], [Política de seguridad para proveedores]	
A.8.2	Clasificación de la información	Si				
A.8.2.1	Clasificación de la información	Si			[Política de Clasificación de la Información]	
A.8.2.2	Etiquetado de la información	Si			[Política de Clasificación de la Información]	
A.8.2.3	Manejo de activos	Si			[Política de Clasificación de la Información]	
A.8.3	Gestión de medios	Si				



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.8.3.1	Gestión de medios removibles	Si			[Política de Clasificación de la Información]	
A.8.3.2	Eliminación de medios	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de eliminación y destrucción]	
A.8.3.3	Transferencia de medios físicos	Si			[Política de Clasificación de la Información]	
A.9	Control de acceso	Si				
A.9.1	Requisitos comerciales para el control de acceso	Si				
A.9.1.1	Política de control de acceso	Si			[Política de control de acceso]	
A.9.1.2	Acceso a redes y a servicios de red	Si			[Política de control de acceso]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.9.2	Gestión de acceso del usuario	Si				
A.9.2.1	Registro de usuarios y baja	Si			[Política de control de acceso] / [Política de claves]	
A.9.2.2	Concesión de acceso de usuarios	Si			[Política de control de acceso] / [Política de claves]	
A.9.2.3	Gestión de derechos de acceso privilegiado	Si			[Política de control de acceso]	
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Si			[Política de control de acceso] / [Política de claves]	
A.9.2.5	Revisión derechos de acceso del usuario	Si			[Política de control de acceso]	
A.9.2.6	Eliminación o ajuste de derechos de acceso	Si			[Política de control de acceso]	
A.9.3	Responsabilidades del usuario	Si				



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.9.3.1	Uso de información secreta de autenticación	Si			[Política de uso aceptable], [Política de control de acceso] / [Política de claves]	
A.9.4	Control de acceso a aplicaciones y sistemas	Si				
A.9.4.1	Restricción al acceso a la información	Si			[Política de control de acceso] / [Política de clasificación de la información]	
A.9.4.2	Procedimientos de registro en el terminal	Si			Existe un proceso de registro seguro para todos los ordenadores de la red	
A.9.4.3	Sistema de gestión de claves	Si			[Política de control de acceso] / [Política de claves]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.9.4.4	Uso de programas de utilidad privilegiada	Si			Solamente el [cargo] tiene derecho para usar programas de utilidad privilegiada	
A.9.4.5	Control de acceso al código fuente del programa	Si			El código fuente del programa se archiva [describir la implementación técnica] y solamente el [cargo] tiene derechos de acceso	
A.10	Criptografía	Si				
A.10.1	Controles criptográficos	Si				
A.10.1.1	Política del uso de controles criptográficos	Si			[Política del uso de controles criptográficos]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.10.1.2	Gestión clave	Si			[Política del uso de controles criptográficos]	
A.11	Seguridad física y del entorno	Si				
A.11.1	Áreas seguras	Si				
A.11.1.1	Perímetro de seguridad física	Si			Las áreas con información sensible están protegidas [describir cómo, con paredes, etc.]	
A.11.1.2	Controles de entrada físicos	Si			El acceso a las áreas seguras del RDP deben estar controladas [describir cómo: tarjetas de acceso, entrada principal con guardia, etc.]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.1.3	Seguridad de oficinas habitaciones e instalaciones	Si			No se puede acceder a las instalaciones desde áreas públicas y las áreas seguras no son visibles para personas ajenas a la empresa	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.1.4	Protección ante amenazas externas y ambientales	Si			Hay un sistema de alarma instalado y conectado al centro de monitoreo de [nombre del proveedor del servicio de seguridad]; hay cámaras de vigilancia instaladas; está implementada la protección contra incendios [describir cómo] y contra inundaciones [describir cómo]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.1.5	Trabajo en áreas seguras	Si			[Procedimientos para trabajo en áreas seguras]	
A.11.1.6	Áreas de entrega y carga	Si			Las áreas de acceso público son controladas [describir cómo] y las áreas de carga y descarga [indicar cuáles] están controladas [describir cómo]	
A.11.2	Equipos	Si				



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.1	Ubicación y protección del equipo	Si			Todo el equipamiento o está ubicado en un área físicamente protegida, y el equipamiento o altamente sensible [indicar cuál] está ubicado en [nombre del área segura; por ej., sala de servidores]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.2	Servicios públicos	Si			Los aparatos de alimentación continua [indicar cuáles; por ej., dispositivos de UPS, generadores de electricidad, etc.] están instalados para [indicar para qué equipos de TI y de otra clase]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.3	Seguridad en el cableado	Si			Los cables de energía y de datos están instalados dentro de áreas seguras del RDP y, donde no fue posible, están protegidos [indicar cómo]	
A.11.2.4	Mantenimiento de equipo	Si			El [carga] debe llevar un registro de mantenimiento de todos los equipos, según las instrucciones del fabricante; y debe garantizar el mantenimiento en tiempo y forma	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.5	Eliminación de activos	Si			[Política de Uso aceptable]	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo]	
A.11.2.7	Eliminación segura o re-uso del equipo	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de eliminación y destrucción]	
A.11.2.8	Equipo de usuario desatendido	Si			[Política de uso aceptable] / [Política de pantalla y escritorio limpio]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.9	Política de pantalla y escritorio limpio	Si			[Política de uso aceptable] / [Política de pantalla y escritorio limpio]	
A.12	Seguridad operativa	Si				
A.12.1	Procedimientos y responsabilidades operativos	Si				
A.12.1.1	Procedimientos operativos documentados	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.1.2	Gestión de cambios	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de gestión de cambio]	
A.12.1.3	Gestión de capacidad	Si			El [cargo] es el responsable de supervisar el uso de los activos de tecnologías de la información y las comunicaciones y de planificar la capacidad necesaria	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.1.4	Separación de ambientes de desarrollo, prueba y operativo	Si			Los sistemas de desarrollo, de pruebas y operacional es están separados	
A.12.2	Protección contra software malicioso	Si				
A.12.2.1	Controles contra software malicioso	Si			La herramienta utilizada es [indicar la herramienta que se utiliza], [Política de uso aceptable]	
A.12.3	Copias de seguridad	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.3.1	Copia de seguridad de la información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de creación de copias de seguridad], [Política de uso aceptable]	
A.12.4	Registros y supervisión	Si				
A.12.4.1	Registro de eventos	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.4.2	Protección de la información del registro	Si			Los registros no pueden ser eliminados sin el permiso otorgado por la persona autorizada	
A.12.4.3	Registros del administrador y operador	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.4.4	Sincronización de relojes	Si			Los relojes de los sistemas en todos los ordenadores están sincronizados [indicar cómo están sincronizados y con qué fuente horaria correcta]	
A.12.5	Control del software operacional	Si				
A.12.5.1	Instalación de software en sistemas operativos	Si			[Política de Uso aceptable]	
A.12.6	Gestión de vulnerabilidad técnica	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.6.1	Gestión de vulnerabilidades técnicas	Si			El [cargo] es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el [cargo] debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades	
A.12.6.2	Restricciones sobre instalación de software	Si			[Política de Uso aceptable]	
A.12.7	Consideraciones de auditoría de los sistemas de información	Si				



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.7.1	Controles de auditoría sobre sistemas de información	Si			Cada auditoría se planifica y coordina con la dirección; las auditorías se realizan solamente con derechos de acceso de sólo lectura	
A.13	Seguridad de las comunicaciones	Si				
A.13.1	Gestión de seguridad de red	Si				
A.13.1.1	Controles de red	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.13.1.2	Seguridad de los servicios de red	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	
A.13.1.3	Segregación en redes	Si			La red se separa de la siguiente manera: [indicar qué segmentos de la red están separados, indicar si la separación es física o lógica]	
A.13.2	Políticas y procedimientos para	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.13.2.1	Políticas y procedimientos para transferencia de la información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de transferencia de la Información] , [Política Trae tu propio dispositivo (BYOD)]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.13.2.2	Acuerdos sobre transferencia de información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de transferencia de la información]	
A.13.2.3	Mensajes electrónicos	Si			[Política de clasificación de la información] , [Política de uso aceptable]	
A.13.2.4	Acuerdos de confidencialidad y no divulgación	Si			El formulario [Declaración de confidencialidad] es predefinido	
A.14	Adquisición, desarrollo y mantenimiento de sistemas	Si				

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.1	Requisitos de seguridad de los sistemas de la información	Si				
A.14.1.1	Análisis de requerimientos y especificaciones para seguridad de la información	Si			Al adquirir nuevos sistemas de información o al cambiar los vigentes, el [cargo] debe documentar los requisitos de seguridad en la [Especificación de requerimientos de seguridad]	
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	Si			[Política de desarrollo seguro]	
A.14.1.3	Protección de transacciones de servicios de aplicaciones	Si			[Política de desarrollo seguro]	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.2	Seguridad en procesos de desarrollo y soporte	Si				
A.14.2 .1	Política de desarrollo seguro	Si			[Política de desarrollo seguro]	
A.14.2 .2	Procedimientos para control de cambios	Si			[Política de desarrollo seguro]	
A.14.2 .3	Revisión técnica de aplicaciones luego de cambios en la plataforma operativa	Si			El [cargo] es el responsable de supervisar y probar todas las aplicaciones luego de aplicar cambios en los sistemas operativos pero antes de que sean puestos en producción	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Sí/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.2.4	Restricciones sobre cambios a paquetes de software	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de gestión de cambio]	
A.14.2.5	Principios de ingeniería para sistema seguro	Si			[Política de desarrollo seguro]	
A.14.2.6	Ambiente de desarrollo seguro	Si			[Política de desarrollo seguro]	
A.14.2.7	Desarrollo externalizado	Si			[Política de seguridad para proveedores], [Política de desarrollo seguro]	
A.14.2.8	Prueba de seguridad del sistema	Si			[Política de desarrollo seguro]	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.2.9	Prueba de aceptación del sistema	Si			[Política de desarrollo seguro]	
A.14.3	Datos de prueba	Si				
A.14.3.1	Protección de datos de prueba	Si			[Política de desarrollo seguro]	
A.15	Relaciones con proveedores	Si				
A.15.1	Seguridad de la información en las relaciones con proveedores	Si				
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	Si			[Política de seguridad para proveedores ]	
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	Si			[Política de seguridad para proveedores ]	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Si			[Política de seguridad para proveedores ]	
A.15.2	Gestión de servicio de entrega de proveedores	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.15.2.1	Supervisión y revisión de servicios de proveedores	Si			[Política de seguridad para proveedores]	
A.15.2.2	Gestión de cambios en los servicios de proveedores	Si			[Política de seguridad para proveedores]	
A.16	Gestión de los incidentes de seguridad de la información	Si				
A.16.1	Gestión de los incidentes y mejoras en la seguridad de la información	Si				
A.16.1.1	Responsabilidades y procedimientos	Si			[Procedimiento para gestión de incidentes]	
A.16.1.2	Reporte de eventos de seguridad	Si			[Procedimiento para gestión de incidentes]	
A.16.1.3	Reporte de debilidades de seguridad de la información	Si			[Procedimiento para gestión de incidentes]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Si			[Procedimiento para gestión de incidentes]	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Si			[Procedimiento para gestión de incidentes], [Plan de respuesta a los incidentes]	
A.16.1.6	Aprendizaje a partir de los incidentes en seguridad de la información	Si			[Procedimiento para gestión de incidentes], [Procedimiento para medidas correctivas]	
A.16.1.7	Recolección de evidencia	Si			[Procedimiento para gestión de incidentes]	
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.17.1	Continuidad de seguridad de la información	Si				
A.17.1.1	Planificación de continuidad seguridad de la información	Si			[Procedimiento para identificación de requisitos], [Política de continuidad del negocio], [Metodología para el análisis del impacto en el negocio], [Estrategia de continuidad del negocio]	
A.17.1.2	Implementación de continuidad de seguridad de la información	Si			[Plan de continuidad del negocio]	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Si			[Plan de mantenimiento y revisión del SGCN], [Plan de prueba y verificación], [Formulario de revisiones posteriores a incidente]	
A.17.2	Redundancias	Si				
A.17.2.1	Disponibilidad de instalaciones para proceso de información	Si			[Estrategia de recuperación para infraestructura de TI]	
A.18	Cumplimiento	Si				
A.18.1	Cumplimiento de requerimientos legales y contractuales	Si				
A.18.1.1	Identificación de la legislación aplicable y de requerimientos contractuales	Si			[Lista de requisitos legales, normativos, contractuales y de otra índole]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.18.1.2	Derechos de propiedad intelectual	Si			[Política de Uso aceptable]	
A.18.1.3	Protección de registros	Si			[Procedimiento para control de documentos y registros], [Política de desarrollo seguro]	
A.18.1.4	Privacidad y protección de información personal identificable	Si			El [cargo] es el responsable de implementar los requerimientos legales relacionados con la protección de datos personales	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.18.1.5	Regulación de controles criptográficos	Si			[Lista de requisitos legales, normativos, contractuales y de otra índole] / [Política del uso de controles criptográficos]	
A.18.2	Revisiones de seguridad de la información	Si				
A.18.2.1	Revisión independiente de seguridad de la información	Si			[Procedimiento para auditoría interna], auditoría de certificación realizada por [nombre de la entidad de certificación]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	Fecha: 15/08/2016

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Si			Todos los propietarios de activos de información, como también la dirección, revisan periódicamente la implementación de los controles de seguridad	
A.18.2.3	Revisión del cumplimiento técnico	Si			El [cargo] es el responsable de verificar que los sistemas de información cumplan técnicamente con los requerimientos de seguridad	

#### 4. Aceptación de los riesgos residuales

Debido a que no se han formalizado los procesos necesarios para alcanzar un plan de reducción de riesgos, por medio de la presente se aceptan todos los



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

siguientes riesgos residuales (lista a ajustarse luego de la formalización de los procedimientos previs):

1. Todos los riesgos con valor 0, 1 o 2.
2. Los riesgos que no pudieron ser reducidos a los niveles mencionados en el punto anterior luego de la aplicación de los controles, de acuerdo con el siguiente cuadro:

[Completar el cuadro con datos de todos los riesgos específicos que no son aceptables; utilizar el Cuadro de tratamiento de riesgos para tomar los datos].

Nr o.	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Nuevo impacto	Nueva probabilidad	Riesgo residual

## 5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario del presente documento es el [cargo], que debe verificar y, si es necesario, actualizar el documento por lo menos una vez al año e inmediatamente después de las revisiones de evaluación de riesgos y de las actualizaciones del Cuadro de evaluación de riesgos y del Cuadro de tratamiento de riesgos.

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

- Cantidad de no conformidades debido métodos de implementación de controles específicos no definidos claramente.
- Cantidad de no conformidades debido a objetivos del control no definidos claramente.
- Cantidad de controles para los cuales no es posible medir el logro de objetivos.

[cargo]  
[nombre]

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

## 6. GLOSARIO DE TÉRMINOS

### **Activo o activo de información**

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

### **Amenaza**

Causa potencial de un incidente que puede infringir daños a un sistema de información o a una organización.

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad.

### **Análisis de impacto**

Estudio de las consecuencias que tendría una parada de X tiempo sobre la organización.

### **Análisis de riesgos**

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

### **Ataque**

Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006].

Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

### **Auditoría de seguridad**

Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

### **Autenticidad**

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Aseguramiento de la identidad u origen. [Magerit:2006]

Autenticación: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones. Magerit:1997].

### **Certificación**

Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.

### **Confidencialidad**

Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [UNE 71504:2008]

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. [Magerit:2006]

Característica que previene contra la divulgación no autorizada de activos del dominio

### **Declaración de aplicabilidad**

Documento formal en el que, para un conjunto de salvaguardas, se indica si son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

### **Dimensión de seguridad**

Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.

### **Disponibilidad**



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [UNE 71504:2008]  
Característica que previene contra la denegación no autorizada de acceso a activos del dominio.

#### **Estado de riesgo**

Informe: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.

#### **Evaluación de salvaguardas**

Informe: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

#### **Gestión de riesgos**

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. [UNE-ISO Guía 73:2010]

Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [Magerit:2006]

Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

#### **Impacto**

Consecuencia que sobre un activo tiene la materialización de una amenaza.

Resultado de un suceso que afecta a los objetivos.

#### **Impacto residual**

Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información

#### **Integridad**

Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008]

Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio.

#### **Modelo de valor**

Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

### **Plan de seguridad**

Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

### **Riesgo**

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Efecto de la incertidumbre sobre la consecución de los objetivos. [UNEISO Guía 73:2010]

Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997].

Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo.

### **Riesgo acumulado**

Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

### **Riesgo potencial o Riesgo Inherente**

Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes.

### **Riesgo repercutido**

Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.

### **Riesgo residual**

Riesgo remanente en el sistema después del tratamiento del riesgo. [UNEISO Guía 73:2010].

Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006]

Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

### **Salvaguarda o Control**

Procedimiento o mecanismo tecnológico que reduce el riesgo.

Control: Medida que modifica un riesgo.



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/08/2016

### **Seguridad**

La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

### **Seguridad de la información**

Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.

### **Sistema de información**

Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008]

Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997]

Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. [CESID:1997]

### **Tratamiento de riesgos**

Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010]

El proceso de selección e implantación de las medidas o salvaguardas para prevenir, impedir, reducir o controlar los riesgos identificados. [UNE 71504:2008]

### **Trazabilidad**

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008]

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [ISO/IEC 7498-2:1989]

Responsabilidad: Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997]

### **Valor**

De un activo. Es una estimación del coste inducido por la materialización de una amenaza.

Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE]



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/08/2016</b>

**Valor acumulado**

Considera tanto el valor propio de un activo como el valor de los activos que dependen de él.

Bienes de abolengo: Los heredados de los abuelos. [DRAE]

**Vulnerabilidad**

Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.

Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia. [UNE-ISO Guía 73:2010]



# Declaración de Aplicabilidad de Controles

PRODUCTO E-61

CONSORCIO MEB SEVENTEEN MILE

Quito, Agosto 2016

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

**Contenido**

1. Objetivo, alcance y usuarios.....	4
2. Documentos de referencia .....	5
3. Aplicabilidad de los controles .....	6
4. Aceptación de los riesgos residuales .....	24
5. Validez y gestión de documentos.....	25
6. Glosario de Términos .....	26



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

### DECLARACIÓN DE APLICABILIDAD

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

**Historial de modificaciones**

Fecha	Versión	Creado por	Descripción de la modificación
DD-MM- AAAA	0.1	Alberto Pazmiño P	Descripción básica del documento

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

## 1. Objetivo, alcance y usuarios

El objetivo del presente documento es bosquejar en una primera instancia qué controles son adecuados para implementar en el Registro de la Propiedad, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo facilitar la aprobación formal de la implementación de los controles mencionados.

Para la versión definitiva de este documento es necesario que previamente se aprueben de manera formal lo siguiente:

1. FICHAS DE CAPTURA DEL ACTIVOS DE INFORMACIÓN Y SUS VALORACIONES
2. MODELO DE VALOR: Inventario de activos de información y sus valoraciones en las dimensiones de seguridad.
3. MODELO DE RIESGOS INHERENTES
4. MODELO DE RIESGOS RESIDUALES
5. METODOLOGÍA DE TRATAMIENTO DE LOS RIESGOS

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001:2013. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos empleados del Registro de la Propiedad que cumplen una función dentro del SGSI.



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

## 2. Documentos de referencia

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

### 3. Aplicabilidad de los controles

Son aplicables todos los controles del Anexo A de la norma ISO 27001:2013:

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección? no elección	Objetivos del control	Método de implementación	Estado
A.5	Políticas de seguridad de la información					
A.5.1	Dirección de la gerencia para la seguridad de la información					
A.5.1.1	Políticas para seguridad de la información				Todas las políticas indicadas bajo esta columna	
A.5.1.2	Revisión de políticas para seguridad de la información	Si			Cada política tiene un propietario designado que debe revisar el documento según un intervalo planificado	Por implementar
A.6	Organización de la seguridad de la información	Si				
A.6.1	Organización interna					
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si			Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI Si es necesario, el [cargo] define responsabilidades adicionales	
A.6.1.2	Segregación de deberes	Si			Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.6.1.3	Contacto con autoridades	Si			[Estrategia de continuidad del negocio], [Plan de respuesta a los incidentes]	
A.6.1.4	Contacto con grupos de interés especial	Si			El [cargo] es el responsable de supervisar [detallar los nombres de grupos de interés y foros de seguridad]	
A.6.1.5	Seguridad de la información en gestión de proyectos	Si			El gerente de proyecto debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto	
A.6.2	Dispositivos móviles y tele-trabajo	Si				
A.6.2.1	Política sobre dispositivos móviles	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo], [Política Trae tu propio dispositivo (BYOD)]	
A.6.2.2	Tele-trabajo	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo]	
A.7	Seguridad relacionada con el personal					
A.7.1	Antes del empleo					



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.7.1.1	Selección	Si			El [cargo] verifica a cada candidato [describir el método para las verificaciones; por ej., revisando el CV, poniéndose en contacto con empleadores anteriores, verificando antecedentes penal, situación financiera, etc.]; [Política de seguridad para proveedores]	
A.7.1.2	Términos y condiciones de empleo	Si			Todos los empleados firman la [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]	
A.7.2	Durante el empleo					
A.7.2.1	Gestión de responsabilidades	Si			La dirección exige activamente que todos los empleados, proveedores y socios implementen todas las reglas del SGSI	
A.7.2.2	Concienciación, educación y capacitación sobre Seguridad de la información	Si			Política de seguridad de la información, Plan de capacitación y concienciación, [Política de seguridad para proveedores]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.7.2.3	Proceso disciplinario	Si			[Procedimiento para gestión de incidentes], [Declaración de aceptación de los documentos del SGSI]	
A.7.3	Terminación o cambio del empleo					
A.7.3.1	Terminación o cambio de responsabilidades del empleo	Si			Todos los acuerdos con proveedores y socios contienen cláusulas que siguen vigentes después de finalizado el empleo, como también las [Declaraciones de confidencialidad] firmadas con los empleados.	
A.8	Gestión de activos					
A.8.1	Responsabilidad sobre los activos					
A.8.1.1	Inventario de activos	Si			[Inventario de activos], [Política de clasificación de la información]	
A.8.1.2	Propiedad de los activos	Si			[Inventario de activos], [Política de uso aceptable]	
A.8.1.3	Uso aceptable de los activos	Si			[Política de Uso aceptable]	
A.8.1.4	Devolución de activos	Si			[Política de Uso aceptable], [Política de seguridad para proveedores]	
A.8.2	Clasificación de la información	Si				
A.8.2.1	Clasificación de la información	Si			[Política de Clasificación de la Información]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.8.2.2	Etiquetado de la información	Si			[Política de Clasificación de la Información]	
A.8.2.3	Manejo de activos	Si			[Política de Clasificación de la Información]	
A.8.3	Gestión de medios	Si				
A.8.3.1	Gestión de medios removibles	Si			[Política de Clasificación de la Información]	
A.8.3.2	Eliminación de medios	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de eliminación y destrucción]	
A.8.3.3	Transferencia de medios físicos	Si			[Política de Clasificación de la Información]	
A.9	Control de acceso	Si				
A.9.1	Requisitos comerciales para el control de acceso	Si				
A.9.1.1	Política de control de acceso	Si			[Política de control de acceso]	
A.9.1.2	Acceso a redes y a servicios de red	Si			[Política de control de acceso]	
A.9.2	Gestión de acceso del usuario	Si				
A.9.2.1	Registro de usuarios y baja	Si			[Política de control de acceso] / [Política de claves]	
A.9.2.2	Concesión de acceso de usuarios	Si			[Política de control de acceso] / [Política de claves]	
A.9.2.3	Gestión de derechos de acceso privilegiado	Si			[Política de control de acceso]	
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Si			[Política de control de acceso] / [Política de claves]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.9.2.5	Revisión derechos de acceso del usuario	Si			[Política de control de acceso]	
A.9.2.6	Eliminación o ajuste de derechos de acceso	Si			[Política de control de acceso]	
A.9.3	Responsabilidades del usuario	Si				
A.9.3.1	Uso de información secreta de autenticación	Si			[Política de uso aceptable], [Política de control de acceso] / [Política de claves]	
A.9.4	Control de acceso a aplicaciones y sistemas	Si				
A.9.4.1	Restricción al acceso a la información	Si			[Política de control de acceso] / [Política de clasificación de la información]	
A.9.4.2	Procedimientos de registro en el terminal	Si			Existe un proceso de registro seguro para todos los ordenadores de la red	
A.9.4.3	Sistema de gestión de claves	Si			[Política de control de acceso] / [Política de claves]	
A.9.4.4	Uso de programas de utilidad privilegiada	Si			Solamente el [cargo] tiene derecho para usar programas de utilidad privilegiada	
A.9.4.5	Control de acceso al código fuente del programa	Si			El código fuente del programa se archiva [describir la implementación técnica] y solamente el [cargo] tiene derechos de acceso	
A.10	Criptografía	Si				
A.10.1	Controles criptográficos	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.10.1.1	Política del uso de controles criptográficos	Si			[Política del uso de controles criptográficos]	
A.10.1.2	Gestión clave	Si			[Política del uso de controles criptográficos]	
A.11	Seguridad física y del entorno	Si				
A.11.1	Áreas seguras	Si				
A.11.1.1	Perímetro de seguridad física	Si			Las áreas con información sensible están protegidas [describir cómo, con paredes, etc.]	
A.11.1.2	Controles de entrada físicos	Si			El acceso a las áreas seguras del RDP deben estar controladas [describir cómo: tarjetas de acceso, entrada principal con guardia, etc.]	
A.11.1.3	Seguridad de oficinas habitaciones e instalaciones	Si			No se puede acceder a las instalaciones desde áreas públicas y las áreas seguras no son visibles para personas ajenas a la empresa	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.1.4	Protección ante amenazas externas y ambientales	Si			Hay un sistema de alarma instalado y conectado al centro de monitoreo de [nombre del proveedor del servicio de seguridad]; hay cámaras de vigilancia instaladas; está implementada la protección contra incendios [describir cómo] y contra inundaciones [describir cómo]	
A.11.1.5	Trabajo en áreas seguras	Si			[Procedimientos para trabajo en áreas seguras]	
A.11.1.6	Áreas de entrega y carga	Si			Las áreas de acceso público son controladas [describir cómo] y las áreas de carga y descarga [indicar cuáles] están controladas [describir cómo]	
A.11.2	Equipos	Si				
A.11.2.1	Ubicación y protección del equipo	Si			Todo el equipamiento está ubicado en un área físicamente protegida, y el equipamiento altamente sensible [indicar cuál] está ubicado en [nombre del área segura; por ej., sala de servidores]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.11.2.2	Servicios públicos	Si			Los aparatos de alimentación continua [indicar cuáles; por ej., dispositivos de UPS, generadores de electricidad, etc.] están instalados para [indicar para qué equipos de TI y de otra clase]	
A.11.2.3	Seguridad en el cableado	Si			Los cables de energía y de datos están instalados dentro de áreas seguras del RDP y, donde no fue posible, están protegidos [indicar cómo]	
A.11.2.4	Mantenimiento de equipo	Si			El [cargos] debe llevar un registro de mantenimiento de todos los equipos, según las instrucciones del fabricante; y debe garantizar el mantenimiento en tiempo y forma	
A.11.2.5	Eliminación de activos	Si			[Política de Uso aceptable]	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Si			[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo]	
A.11.2.7	Eliminación segura o re-uso del equipo	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de eliminación y destrucción]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.11.2.8	Equipo de usuario desatendido	Si			[Política de uso aceptable] / [Política de pantalla y escritorio limpio]	
A.11.2.9	Política de pantalla y escritorio limpio	Si			[Política de uso aceptable] / [Política de pantalla y escritorio limpio]	
A.12	Seguridad operativa	Si				
A.12.1	Procedimientos y responsabilidades operativos	Si				
A.12.1.1	Procedimientos operativos documentados	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	
A.12.1.2	Gestión de cambios	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de gestión de cambio]	
A.12.1.3	Gestión de capacidad	Si			El [cargo] es el responsable de supervisar el uso de los activos de tecnologías de la información y las comunicaciones y de planificar la capacidad necesaria	
A.12.1.4	Separación de ambientes de desarrollo, prueba y operativo	Si			Los sistemas de desarrollo, de pruebas y operacionales están separados	
A.12.2	Protección contra software malicioso	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.12.2.1	Controles contra software malicioso	Si			La herramienta utilizada es [indicar la herramienta que se utiliza], [Política de uso aceptable]	
A.12.3	Copias de seguridad	Si				
A.12.3.1	Copia de seguridad de la información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de creación de copias de seguridad], [Política de uso aceptable]	
A.12.4	Registros y supervisión	Si				
A.12.4.1	Registro de eventos	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	
A.12.4.2	Protección de la información del registro	Si			Los registros no pueden ser eliminados sin el permiso otorgado por la persona autorizada	
A.12.4.3	Registros del administrador y operador	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	
A.12.4.4	Sincronización de relojes	Si			Los relojes de los sistemas en todos los ordenadores están sincronizados [indicar cómo están sincronizados y con qué fuente horaria correcta]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.12.5	Control del software operacional	Si				
A.12.5.1	Instalación de software en sistemas operativos	Si			[Política de Uso aceptable]	
A.12.6	Gestión de vulnerabilidad técnica	Si				
A.12.6.1	Gestión de vulnerabilidades técnicas	Si			El [cargo] es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el [cargo] debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades	
A.12.6.2	Restricciones sobre instalación de software	Si			[Política de Uso aceptable]	
A.12.7	Consideraciones de auditoría de los sistemas de información	Si				
A.12.7.1	Controles de auditoría sobre sistemas de información	Si			Cada auditoría se planifica y coordina con la dirección; las auditorías se realizan solamente con derechos de acceso de sólo lectura	
A.13	Seguridad de las comunicaciones	Si				
A.13.1	Gestión de seguridad de red	Si				
A.13.1.1	Controles de red	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.13.1.2	Seguridad de los servicios de red	Si			[Procedimientos operativos para tecnología de la información y de la comunicación]	
A.13.1.3	Segregación en redes	Si			La red se separa de la siguiente manera: [indicar qué segmentos de la red están separados, indicar si la separación es física o lógica]	
A.13.2	Políticas y procedimientos para	Si				
A.13.2.1	Políticas y procedimientos para transferencia de la información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de transferencia de la Información], [Política Trae tu propio dispositivo (BYOD)]	
A.13.2.2	Acuerdos sobre transferencia de información	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de transferencia de la información]	
A.13.2.3	Mensajes electrónicos	Si			[Política de clasificación de la información], [Política de uso aceptable]	
A.13.2.4	Acuerdos de confidencialidad y no divulgación	Si			El formulario [Declaración de confidencialidad] es predefinido	
A.14	Adquisición, desarrollo y mantenimiento de sistemas	Si				

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.1	Requisitos de seguridad de los sistemas de la información	Si				
A.14.1.1	Análisis de requerimientos y especificaciones para seguridad de la información	Si			Al adquirir nuevos sistemas de información o al cambiar los vigentes, el [cargo] debe documentar los requisitos de seguridad en la [Especificación de requerimientos de seguridad]	
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	Si			[Política de desarrollo seguro]	
A.14.1.3	Protección de transacciones de servicios de aplicaciones	Si			[Política de desarrollo seguro]	
A.14.2	Seguridad en procesos de desarrollo y soporte	Si				
A.14.2.1	Política de desarrollo seguro	Si			[Política de desarrollo seguro]	
A.14.2.2	Procedimientos para control de cambios	Si			[Política de desarrollo seguro]	
A.14.2.3	Revisión técnica de aplicaciones luego de cambios en la plataforma operativa	Si			El [cargo] es el responsable de supervisar y probar todas las aplicaciones luego de aplicar cambios en los sistemas operativos pero antes de que sean puestos en producción	
A.14.2.4	Restricciones sobre cambios a paquetes de software	Si			[Procedimientos operativos para tecnología de la información y de la comunicación] / [Política de gestión de cambio]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.14.2.5	Principios de ingeniería para sistema seguro	Si			[Política de desarrollo seguro]	
A.14.2.6	Ambiente de desarrollo seguro	Si			[Política de desarrollo seguro]	
A.14.2.7	Desarrollo externalizado	Si			[Política de seguridad para proveedores], [Política de desarrollo seguro]	
A.14.2.8	Prueba de seguridad del sistema	Si			[Política de desarrollo seguro]	
A.14.2.9	Prueba de aceptación del sistema	Si			[Política de desarrollo seguro]	
A.14.3	Datos de prueba	Si				
A.14.3.1	Protección de datos de prueba	Si			[Política de desarrollo seguro]	
A.15	Relaciones con proveedores	Si				
A.15.1	Seguridad de la información en las relaciones con proveedores	Si				
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	Si			[Política de seguridad para proveedores]	
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	Si			[Política de seguridad para proveedores]	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Si			[Política de seguridad para proveedores]	
A.15.2	Gestión de servicio de entrega de proveedores	Si				
A.15.2.1	Supervisión y revisión de servicios de proveedores	Si			[Política de seguridad para proveedores]	
A.15.2.2	Gestión de cambios en los servicios de proveedores	Si			[Política de seguridad para proveedores]	
A.16	Gestión de los incidentes de seguridad de la información	Si				
A.16.1	Gestión de los incidentes y mejoras en la seguridad de la información	Si				
A.16.1.1	Responsabilidades y procedimientos	Si			[Procedimiento para gestión de incidentes]	

	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.16.1.2	Reporte de eventos de seguridad	Si			[Procedimiento para gestión de incidentes]	
A.16.1.3	Reporte de debilidades de seguridad de la información	Si			[Procedimiento para gestión de incidentes]	
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Si			[Procedimiento para gestión de incidentes]	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Si			[Procedimiento para gestión de incidentes], [Plan de respuesta a los incidentes]	
A.16.1.6	Aprendizaje a partir de los incidentes en seguridad de la información	Si			[Procedimiento para gestión de incidentes], [Procedimiento para medidas correctivas]	
A.16.1.7	Recolección de evidencia	Si			[Procedimiento para gestión de incidentes]	
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	Si				
A.17.1	Continuidad de seguridad de la información	Si				
A.17.1.1	Planificación de continuidad seguridad de la información	Si			[Procedimiento para identificación de requisitos], [Política de continuidad del negocio], [Metodología para el análisis del impacto en el negocio], [Estrategia de continuidad del negocio]	
A.17.1.2	Implementación de continuidad de seguridad de la información	Si			[Plan de continuidad del negocio]	



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SI/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Si			[Plan de mantenimiento y revisión del SGCN], [Plan de prueba y verificación], [Formulario de revisión pos incidente]	
A.17.2	Redundancias	Si				
A.17.2.1	Disponibilidad de instalaciones para proceso de información	Si			[Estrategia de recuperación para infraestructura de TI]	
A.18	Cumplimiento	Si				
A.18.1	Cumplimiento de requerimientos legales y contractuales	Si				
A.18.1.1	Identificación de la legislación aplicable y de requerimientos contractuales	Si			[Lista de requisitos legales, normativos, contractuales y de otra índole]	
A.18.1.2	Derechos de propiedad intelectual	Si			[Política de Uso aceptable]	
A.18.1.3	Protección de registros	Si			[Procedimiento para control de documentos y registros], [Política de desarrollo seguro]	
A.18.1.4	Privacidad y protección de información personal identificable	Si			El [cargo] es el responsable de implementar los requerimientos legales relacionados con la protección de datos personales	
A.18.1.5	Regulación de controles criptográficos	Si			[Lista de requisitos legales, normativos, contractuales y de otra índole] / [Política del uso de controles criptográficos]	



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (Si/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.18.2	Revisiones de seguridad de la información	Si				
A.18.2.1	Revisión independiente de seguridad de la información	Si			[Procedimiento para auditoría interna], auditoría de certificación realizada por [nombre de la entidad de certificación]	
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Si			Todos los propietarios de activos de información, como también la dirección, revisan periódicamente la implementación de los controles de seguridad	
A.18.2.3	Revisión del cumplimiento técnico	Si			El [cargo] es el responsable de verificar que los sistemas de información cumplan técnicamente con los requerimientos de seguridad	

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

#### 4. Aceptación de los riesgos residuales

Debido a que no se han formalizado los procesos necesarios para alcanzar un plan de reducción de riesgos, por medio de la presente se aceptan todos los siguientes riesgos residuales (lista a ajustarse luego de la formalización de los procedimientos previs):

1. Todos los riesgos con valor 0, 1 o 2.
2. Los riesgos que no pudieron ser reducidos a los niveles mencionados en el punto anterior luego de la aplicación de los controles, de acuerdo con el siguiente cuadro:

[Completar el cuadro con datos de todos los riesgos específicos que no son aceptables; utilizar el Cuadro de tratamiento de riesgos para tomar los datos].

Nr o.	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Nuevo impacto	Nueva probabilidad	Riesgo residual

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

## 5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario del presente documento es el [cargo], que debe verificar y, si es necesario, actualizar el documento por lo menos una vez al año e inmediatamente después de las revisiones de evaluación de riesgos y de las actualizaciones del Cuadro de evaluación de riesgos y del Cuadro de tratamiento de riesgos.

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

- Cantidad de no conformidades debido métodos de implementación de controles específicos no definidos claramente.
- Cantidad de no conformidades debido a objetivos del control no definidos claramente.
- Cantidad de controles para los cuales no es posible medir el logro de objetivos.

[cargo]

[nombre]

\_\_\_\_\_  
[firma]



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

## 6. GLOSARIO DE TÉRMINOS

### **Activo o activo de información**

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

### **Amenaza**

Causa potencial de un incidente que puede infringir daños a un sistema de información o a una organización.

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad.

### **Análisis de impacto**

Estudio de las consecuencias que tendría una parada de X tiempo sobre la organización.

### **Análisis de riesgos**

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

### **Ataque**

Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006].

Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.

	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

### **Auditoría de seguridad**

Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

### **Autenticidad**

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Aseguramiento de la identidad u origen. [Magerit:2006]

Autenticación: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones. Magerit:1997].

### **Certificación**

Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.

### **Confidencialidad**

Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [UNE 71504:2008]

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. [Magerit:2006]

Característica que previene contra la divulgación no autorizada de activos del dominio

### **Declaración de aplicabilidad**

Documento formal en el que, para un conjunto de salvaguardas, se indica si son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

### **Dimensión de seguridad**

Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.

### **Disponibilidad**



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [UNE 71504:2008]  
Característica que previene contra la denegación no autorizada de acceso a activos del dominio.

#### **Estado de riesgo**

Informe: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.

#### **Evaluación de salvaguardas**

Informe: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

#### **Gestión de riesgos**

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. [UNE-ISO Guía 73:2010]

Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [Magerit:2006]

Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

#### **Impacto**

Consecuencia que sobre un activo tiene la materialización de una amenaza.

Resultado de un suceso que afecta a los objetivos.

#### **Impacto residual**

Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información

#### **Integridad**

Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008]

Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio.

#### **Modelo de valor**

Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.



	PRODUCTO E61	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

### **Plan de seguridad**

Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

### **Riesgo**

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Efecto de la incertidumbre sobre la consecución de los objetivos. [UNEISO Guía 73:2010]

Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997].

Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo.

### **Riesgo acumulado**

Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

### **Riesgo potencial o Riesgo Inherente**

Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes.

### **Riesgo repercutido**

Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.

### **Riesgo residual**

Riesgo remanente en el sistema después del tratamiento del riesgo. [UNEISO Guía 73:2010].

Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006]

Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

### **Salvaguarda o Control**

Procedimiento o mecanismo tecnológico que reduce el riesgo.

Control: Medida que modifica un riesgo.

	<b>PRODUCTO E61</b>	
CONSORCIO MEB SEVENTEENMILE	Declaración de Aplicabilidad de Controles	Fecha: 15/02/2017

### **Seguridad**

La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

### **Seguridad de la información**

Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.

### **Sistema de información**

Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008]

Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997]

Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. [CESID:1997]

### **Tratamiento de riesgos**

Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010]

El proceso de selección e implantación de las medidas o salvaguardas para prevenir, impedir, reducir o controlar los riesgos identificados. [UNE 71504:2008]

### **Trazabilidad**

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008]

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [ISO/IEC 7498-2:1989]

Responsabilidad: Calidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997]

### **Valor**

De un activo. Es una estimación del coste inducido por la materialización de una amenaza.

Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE]



	<b>PRODUCTO E61</b>	
<b>CONSORCIO MEB SEVENTEENMILE</b>	<b>Declaración de Aplicabilidad de Controles</b>	<b>Fecha: 15/02/2017</b>

**Valor acumulado**

Considera tanto el valor propio de un activo como el valor de los activos que dependen de él.

Bienes de abolengo: Los heredados de los abuelos. [DRAE]

**Vulnerabilidad**

Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza.

Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia. [UNE-ISO Guía 73:2010]