

Poder Ejecutivo del Estado de Querétaro

***Carta de observaciones y
recomendaciones por el año que
terminó el 31 de diciembre de 2014***

Al Secretario de Planeación y Finanzas del Estado de Querétaro

23 de septiembre de 2015

Germán Giordano Bonilla
Secretario de Planeación y Finanzas
Poder Ejecutivo del Estado de Querétaro

En relación con nuestra auditoría de los estados financieros del Poder Ejecutivo del Estado de Querétaro por el año que terminó el 31 de diciembre de 2014, hemos considerado el control interno relevante para la preparación y presentación de los estados financieros por parte de la Entidad, únicamente con el fin de diseñar la extensión, alcance y oportunidad de los procedimientos de auditoría que sean adecuados en las circunstancias, y no con la finalidad de expresar una opinión sobre la efectividad del control interno de la Entidad.

Nuestra evaluación de la estructura del control interno no comprendió un estudio y evaluación detallada de ninguno de sus elementos, y no fue efectuada con el propósito de desarrollar recomendaciones detalladas o evaluar la eficacia con la cual la estructura del control interno de la Entidad permite prevenir o detectar todos los errores e irregularidades que pudieran ocurrir. Los asuntos tratados aquí fueron considerados durante nuestra auditoría y no modifican nuestra opinión de auditoría fechada el 23 de septiembre de 2015 sobre dichos estados financieros.

El informe adjunto también incluye comentarios y sugerencias con respecto a otros asuntos financieros y administrativos, los cuales notamos durante el curso de nuestra auditoría de los estados financieros. Todos estos comentarios se presentan como sugerencias constructivas para la consideración de la Administración, como parte del proceso continuo de modificaciones y mejoramiento de la estructura del control interno existente y de otras prácticas y procedimientos administrativos y financieros.

Las respuestas de la Administración a los comentarios o sugerencias no formaron parte de nuestra auditoría por lo que no tomamos responsabilidad sobre ellas.

Este informe es únicamente para la información y uso del Poder Ejecutivo del Estado de Querétaro y de otros que consideren deban tener conocimiento, dentro de la organización y no pretende ser y no debe ser utilizado por ninguna otra parte distinta a las especificadas.

Deseamos expresar nuestro agradecimiento por la cortesía y cooperación extendida a nuestros representantes durante el curso de su trabajo. Nos agradecería discutir estas recomendaciones en mayor detalle, de ser necesario y, asimismo, proporcionar la ayuda necesaria para su implantación.

Estamos a sus órdenes para cualquier aclaración o ampliación sobre el contenido de este informe.

Atentamente,

Galaz, Yamazaki, Ruiz Urquiza, S. C.
Miembro de Deloitte Touche Tohmatsu Limited

C.P.C. José Ramón Galván Ramos

ÍNDICE

		Página
✓	OBSERVACIONES	
No.	Título de la observación	
1	Actualización de manuales	4
2	Análisis de antigüedad de cuentas por cobrar	4
3	Participación estatal en sociedades mercantiles	5
4	Bienes muebles	5
a.	Bajas	5
b.	Depreciación	5
✓	RECOMENDACIONES	
5	Conciliaciones bancarias automatizadas	6
6	Bienes otorgados en comodato	6
a.-	Bienes en Comodato OMCP-SEDESU-CCM/063/2013 y OMCP-SESEQ-CC1/001/2015	6
b.-	Bienes en Comodato OMCP-SEDESU-CCM/107/2013	6
7.	Cálculo de Salario Diario Integrado	7
8.	Adjudicaciones Directas: Expediente	7
9.	Seguimiento a observaciones	7
10.	Procedimientos de consolidación	8

OBSERVACIONES

1 ACTUALIZACIÓN DE MANUALES

Observación:

Los manuales de procedimientos de políticas y control interno de las siguientes direcciones tienen fechas de vigencia anteriores al periodo auditado;

- Manual de procedimientos de la dirección de ingresos, vigencia mayo de 2006.
- Manual de procedimientos de la dirección de informática, vigencia 28 febrero de 2007.
- Manual de procedimientos de la dirección de presupuesto y gasto público, vigencia 15 octubre de 2006.

Recomendación:

Realizar a la mayor brevedad posible, las actualizaciones correspondientes a los manuales antes mencionados, en los cuales se describan los sistemas de control interno y las políticas a seguir, y así se mantenga monitoreado el cumplimiento de dichos procedimientos.

Comentarios de la entidad:

2 ANÁLISIS DE ANTIGÜEDAD DE CUENTAS POR COBRAR

Observación:

Al 31 de diciembre de 2014 y 2013 no se han tenido movimientos de la siguiente cuenta, ya que se tiene plenamente identificado dicho importe por contabilidad de egresos, por lo que se procedió a reclasificarla a largo plazo.

OTROS DERECHOS A RECIBIR EFECTIVO O EQUIVALENTES	
12291 A LARGO PLAZO	<u>\$32,397,074</u>

Recomendación:

Establecer los mecanismos por los cuales se llevará a su recuperación, aplicación o cancelación.

3 PARTICIPACIÓN ESTATAL EN SOCIEDADES MERCANTILES

Observación:

Toda vez que esta información se encuentra en proceso de integración por parte del Poder Ejecutivo del Estado de Querétaro. En lo que respecta al el Aeropuerto Intercontinental de Querétaro, S.A. de C.V. ("AIQ"), por un importe de \$126,096,746, cotejando la información de los estados financieros al 31 de diciembre de 2014 del AIQ, presenta un deterioro como se muestra a continuación:

Importe de la inversión s/ GEQ al 31/12/2014	\$126,096,746
Patrimonio AIQ \$64,013,643 al 75% de participación	<u>48,010,230</u>
Posible pérdida o deterioro de la inversión	<u>\$ 78,086,516</u>

Recomendación:

Integrar la información financiera necesaria y suficiente de las entidades antes mencionadas, así como obtener de parte del secretario de actas de las empresas anteriormente mencionadas, la confirmación del número de acciones que se tienen en la Compañía Centro Sur, S.A. de C.V.

Adicionalmente crear las subcuentas al plan de cuentas "12141 PARTICIPACIONES Y APORTACIONES DE CAPITAL A LARGO PLAZO EN EL SECTOR PÚBLICO" en las que se identifiquen las inversiones que se tienen en cada sociedad.

En el caso del AIQ, si bien el impacto del deterioro no es material, nuestra recomendación es que recabe y que se evalúe si estas inversiones presentan deterioro.

Comentarios de la entidad:

4 BIENES MUEBLES E INMUEBLES

Observación:

a. Derivado de cambios en el sistema, al 31 de diciembre de 2014, existen bajas de Bienes Muebles (principalmente equipo de cómputo) pendientes de aplicar por el área de Contabilidad de Egresos por un importe de \$49,143,295, debido a la entrega tardía de los oficios de control patrimonial hacia contabilidad, estos se encuentran fechados en 2015, fecha posterior al cierre del ejercicio, en donde se entregaban las bajas a aplicar en el sistema Oracle.

Recomendación:

Entregar de manera oportuna la información por el departamento de Control Patrimonial al departamento de Contabilidad de Egresos.

Comentarios de la entidad:

Observación:

b. Adicionalmente también derivado de la entrega tardía de la información correspondiente a depreciación de bienes muebles por el departamento de Control Patrimonial, se generó un desfase en la información mostrada por el Departamento de Contabilidad de Egresos, el cual muestra un importe en libros de depreciación acumulada de \$54,166,966 mientras el Departamento de Control Patrimonial tenía una depreciación por un importe de \$72,662,317 al 31 de diciembre de 2014.

Recomendación

Entregar de manera oportuna la información por el departamento de Control Patrimonial al departamento de Contabilidad de Egresos.

Comentarios de la entidad:

RECOMENDACIONES

5 CONCILIACIONES BANCARIAS AUTOMATIZADAS

Antecedentes:

Al tener un sistema como el Oracle, se pueden realizar varios reportes de forma automática, tal es el caso de las conciliaciones bancarias, las cuales a la fecha de revisión de nuestra auditoría se realizan de forma manual por la Dirección de contabilidad con la colaboración de Tesorería. A la fecha de la revisión se continúa trabajando en la emisión de estos reportes.

Recomendación:

Evaluar la posibilidad implementar conciliaciones bancarias automáticas con la finalidad de ahorrar tiempos y evitar errores involuntarios.

Comentarios de la entidad:

6 BIENES OTORGADOS EN COMODATO

Antecedentes:

a.- Durante nuestra revisión de los contratos de comodato al 31 de diciembre de 2014, no se nos proporcionaron los contratos siguientes: OMCP-SEDESU-CCM/063/2013 y OMCP-SEC DE SALUD-CC1/01/2015, ya que nos informó el departamento de Control Patrimonial que dichos contratos se encontraban en proceso de firma por algunos de los funcionarios responsables, a la fecha de nuestra revisión.

Recomendación:

Realizar revisiones periódicas anticipándose a la fecha de vencimiento y obtener las firmas a tiempo de los contratos de comodato. Así como evitar demoras en constituir la renovación y/o en su caso obtener todas las firmas del contrato de comodato, ya que al 11 de junio de 2015, aún no se habían podido recabar las firmas de los funcionarios que intervienen en los instrumentos referidos.

Comentario de la Entidad:

Antecedentes:

b.- Durante nuestra revisión de los contratos de comodato al 31 de diciembre de 2014, no se identificó el número OMCP-SEDESU-CCM/107/2013, argumentado el departamento de Control Patrimonial que se encuentra extraviado.

Recomendación:

Llevar un mejor control de los contratos de comodato, del estatus, la fecha de vigencia, dependencia responsable, así como funcionario a cargo. Realizar revisiones con el fin de tener perfectamente identificado en que estatus del proceso se encuentra cada contrato.

Comentario de la Entidad:

7 CÁLCULO DE SALARIO DIARIO INTEGRADO

Antecedentes:

En la revisión del cálculo realizado del salario diario integrado, observamos que existen algunas diferencias en dichas retenciones efectuadas a los servidores públicos.

El Poder Ejecutivo del Estado de Querétaro utiliza para el cálculo del SDI el factor 1.2493, sin embargo dicho factor debe ser calculado en base a las prestaciones específicas de cada trabajador. Las diferencias se muestran a continuación:

NOMBRE DEL TRABAJADOR:

NO. DE TRABAJADOR:

S.D.I. SEGÚN AUDITORÍA

S.D.I. SEGÚN ENTIDAD

DIFERENCIA

% DE DIFERENCIA

Jimenez Ontiveros Thania Maria	Arredondo Gomez Leonardo
158563	117587
1,640	444
1,666	421
26	(22)
2%	5%

Recomendación: Verificar diferencias con la finalidad de evitar implicaciones fiscales futuras.

Comentarios de la entidad:

8 ADJUDICACIONES DIRECTAS: EXPEDIENTE

Antecedentes:

No se entregó la siguiente Licitación, ya que según comentarios de la persona encargada del departamento de adquisiciones, se encontraba en proceso de revisión por la ESFE:

Licitación Pública

No de Contrato: OMDAF/240914/02-C01

Proveedor: Detroit Diesel Allison de México, S.A. de R.L. de C.V.

Recomendación:

Se recomienda que se tenga una copia o digitalizada la información.

Comentarios de la entidad:

9 SEGUIMIENTO A OBSERVACIONES

Recomendación:

Es importante que el Poder Ejecutivo del Estado de Querétaro, de cumplimiento y seguimiento oportuno a las observaciones que emitan en breve los órganos fiscalizadores.

10 PROCEDIMIENTOS DE CONSOLIDACIÓN

Antecedentes:

Revisamos el procedimiento de consolidación seguido por la Dirección de Contabilidad, notando que el mismo está apegado a los lineamientos señalados por el CONAC.

* * * * *

Deloitte.

Presentación de Observaciones Auditoría 2014.

Gobierno del Estado de Querétaro
Enterprise Risk Services, Soporte a Auditoría Financiera

Enero-Diciembre 2014



Contenido

Objetivo

Alcance de nuestra revisión

Glosario de Valores

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Contenido

Objetivo

Alcance del Trabajo

Glosario de Valores

Observaciones

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Objetivos de la revisión

Como parte integral de la auditoría de estados financieros para saber si el ambiente de control de la empresa conduce generalmente a un procesamiento de información financiera confiable y a un control interno efectivo, es necesario realizar una evaluación del ambiente de procesamiento de la información. **Nuestro trabajo debe verse dentro del contexto de la auditoría financiera y no como una auditoría de sistemas como tal.**

De acuerdo con lo anterior, los principales objetivos de nuestra revisión son:

- Realizar una evaluación del control interno del área de sistemas y concluir si el ambiente de procesamiento soporta la generación de información financiera confiable.
- Proporcionar recomendaciones de valor agregado a **Gobierno del Estado de Querétaro.**, de tal forma que le permita fortalecer el control interno de la organización.

- Final comentada

Contenido

Objetivos de la Revisión

Alcance del Trabajo

Glosario de Valores

Observaciones

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Alcance del Trabajo 2014

Como parte del plan general de auditoria, obtuvimos un conocimiento suficiente de los Controles Generales del Computador de acuerdo con nuestra metodología conforme al siguiente esquema:



Centro de Datos y Operaciones de Red

Seguridad de Acceso

Cambio en los Programas.

ORACLE, AD, ORACLE BD

Contenido

Objetivos de la Revisión

Alcance del Trabajo

Glosario de Valores

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Glosario de Valores

Cada comentario se encuentra clasificado con base en el riesgo y la importancia en que deberá ser atendido. Dicha trascendencia se describe a continuación:

RIESGO

Alto

Representa alta probabilidad de una pérdida inmediata de la integridad y/o confidencialidad de la información. Deberá ser atendido lo antes posible.

Medio

Representa probabilidad de un riesgo potencial en la pérdida de la integridad, validez o confidencialidad de la información. Deberá ser atendido en un rango razonable.

Bajo

Representa probabilidad de un riesgo mínimo en la pérdida de la integridad de la información. Deberá ser atendido cuando sea posible.

ESFUERZO

Alto

Se necesita un esfuerzo inmediato para la solución de este posible riesgo y se necesita más de un mes para poder solucionarlo.

Medio

Requiere un esfuerzo no inmediato, sin embargo deberá atenderse mediante prioridades.

Bajo

Podrá ser arreglado inmediatamente.

Contenido

Objetivos de la Revisión

Alcance del Trabajo

Glosario de Valores

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

1 Planeación de la Continuidad del Negocio

Recurrente

Observación

No se cuenta con un Plan de Recuperación en caso de Desastre (DRP), en el cual queden documentados los pasos necesarios para restituir la operación de servicios y aplicaciones.

Impacto

Indisponibilidad de los recursos que sean necesarios para operar los procesos clave a un nivel aceptable para el negocio.

Si una entidad no cuenta con un plan de continuidad del negocio viable y completo, la restauración de los procesos y de los sistemas de información se verá probablemente retrasada y es probable que la entidad incurra en pérdidas financieras innecesarias en caso de alguna emergencia u otra interrupción no planeada.

Dichas pérdidas podrían incluir pérdida de ingresos, debido a la incapacidad de prestar servicio a los clientes y/o gastos innecesarios, debido a la necesidad de agilizar la restauración de los servicios.

Recomendación

Elaborar un análisis inicial que sirva para el desarrollo del plan que contenga los siguiente:

- Ubicaciones clave del procesamiento de cómputo
- Sistemas de aplicación y requerimientos del usuario para los procesos clave
- Actividades de usuario final para los procesos clave
- Telecomunicaciones y redes
- Bases de datos clave, almacenes de información, etc.
- Recursos humanos
- Seguridad personal de los empleados y de otras personas

Comentado

Nombre: Horacio Flores



Puesto: Director TI

Comentarios del Cliente

Comentario: ya se tiene el equipamiento, pero aun es necesario el armado y establecer un presupuesto.

Se tiene planeado comenzar el próximo año (Enero) con una primera fase básica para continuar con la detección de necesidades del proyecto.

- Final comentada

Riesgo	
Esfuerzo	

2 Parámetros de contraseñas

Observación

Se encontraron debilidades en las políticas de contraseñas actuales:

Dominio

- Longitud mínima de contraseña: No configurado
- Vigencia de contraseña: No configurado
- Historial de contraseñas: No configurado
- Complejidad de contraseña: Deshabilitada
- Número máximo de intentos fallidos: No configurado

Oracle financiero

- Vigencia de contraseña: 60 días

Base de datos

- Vigencia de contraseña: 60 días

Sistemas legados

- Longitud mínima de contraseña: No configurado
- Complejidad de contraseña: Deshabilitada
- Número máximo de intentos fallidos: 3
- Bloqueo de la cuenta: Habilitada

Linux:

- Use Shadow Passwords: Habilitado
- User Fingerprint Reader: Habilitado
- Local Authorization is Sufficient: Habilitado

2 Parámetros de contraseñas

Impacto

Las contraseñas fijas incrementan el riesgo de que puedan ser adivinadas u obtenidas por un individuo no autorizado utilizando diversos métodos de ataque.

Incrementa la probabilidad de que personal interno adivine los passwords de otros usuarios. Esta debilidad en la seguridad facilita a los intrusos acceder a los sistemas.

La combinación de intentos junto con las otras anteriores presentan un escenario perfecto para que cualquier usuario se le facilite accesos no autorizados a los sistemas de aplicación.

Recomendación

Implementar las políticas de control de acceso recomendadas, tanto para Dominio, Linux, Base de Datos y Aplicaciones.

En cuanto a la longitud de password , el numero mínimo de caracteres recomendable que debe contener es de 8 o mayor.

El número de intentos fallidos considerados recomendable es de 3

El intervalo mínimo recomendable de cambio de password es de 0

El intervalo máximo de recomendable de cambio de password son 30 días

El número de segundos después de que el sistema forzará la desconexión del usuario cuando su tiempo de acceso (log on) expira, esta opción deberá ser usada a consideración de la gerencia en base a la operación del negocio

El historial de password recomendado es de 6 o mayor

Comentario: se va a revisar este tema por aplicativo la factibilidad de hacer las adecuaciones y robustecimiento de los parámetros.



- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

12

Riesgo	
Esfuerzo	

3 Procedimiento Altas y Bajas

Observación

No existe un procedimiento formal para realizar altas, bajas y cambios de usuarios de los sistemas.

Impacto

Manipulación de la cuenta de usuario dado de baja por otro empleado activo en la entidad, pudiendo ejecutar transacciones no autorizadas que pueden llegar a ocasionar pérdida de información.

Que los usuarios tengan más accesos que los necesarios para realizar sus funciones.

Recomendación

Establecer un procedimiento formal para la solicitud de altas, bajas de usuarios de los sistemas.

Comentarios del Cliente

Comentario: se establecerá el procedimiento y se utilizara un sistema de service desk para ayudar al proceso.

- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

Riesgo



Esfuerzo



4 Control de cambios

Observación

No cuentan con un procedimiento para el control de cambios a la aplicación Oracle Financial y Base de Datos.

Impacto

Cambios inapropiados al sistema de Aplicación y Base de Datos.

Recomendación

Establecer un procedimiento formal para llevar el control de cambios de las aplicaciones, base de datos y sistema operativo.

Comentarios del Cliente

Comentario: se implementara la misma herramienta de service desk para la parte usuaria.

- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

Riesgo



Esfuerzo



5 Cambios Active Directory

Oportunidad de mejora

Los cambios o HotFixes aplicados a Windows que fueron seleccionados, no cuentan con información suficiente que documente las pruebas realizadas a cada uno antes de ser implementados en el servidor productivo de Windows.

La información que se proporcionó fueron pantallas de Windows en la ventana de actualizaciones en donde se pueden ver las actualizaciones de Windows, sin embargo, la información solicitada sería utilizada para obtener la evidencia de las pruebas realizadas a cada uno de estos cambios de seguridad en el sistema operativo.

Recomendación

Llevar a cabo un procedimiento de control de cambios adecuado que ayude a mitigar cualquier tipo de error de los parches instalados en los sistemas.

Impacto

Si los cambios que son implementados en producción no se realizan de acuerdo a un correcto proceso de administración de cambios pueden tener impacto negativo en la operación y provocar cortes de tiempo indeterminado en los sistemas lo que implica esfuerzos desproporcionados para su solución o recuperación.

Comentarios del Cliente

Comentario: se realizara un procedimiento para documentar adecuadamente estos casos.



- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

15

Riesgo	
Esfuerzo	

©2014 Galaz, Yamazaki, Ruiz Urquiza, S.C.

6 Seguridad Active Directory

Oportunidad de mejora

En el control de dominio, Active Directory, se tiene activa la cuenta Guest.

Impacto

La cuenta activa contribuirá a aumentar el riesgo de que usuarios no autorizados obtengan acceso administrativo a Active Directory con el que puedan dañar de forma intencionada o accidental su organización al copiar o eliminar datos confidenciales o al deshabilitar la red.

Recomendación

Deshabilitar la cuenta de invitado. Para eliminar la posibilidad de accesos no autorizados

Asegurar la cuenta de invitado. Para administrar los accesos al sistema por medio de esta cuenta.

Comentarios del Cliente

Comentario: Se analizara el tema y se llevaran a cabo los cambios pertinentes.

- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

16

Riesgo



Esfuerzo



©2014 Galaz, Yamazaki, Ruiz Urquiza, S.C.

7 Seguridad de activos

Oportunidad de mejora

Al entrar a las instalaciones de Dirección Informática, no se controla el acceso de computadoras personales u otro equipo.

Impacto

Este tipo de debilidad en el control de equipos externos facilita:

- Robo de equipos, material, documentos en mochilas de los visitantes
- Intercambio de Laptops dentro de la entidad.

Recomendación

Todas las personas que entren a la entidad sean registradas en las bitácoras.

Implementar una bitácora para el registro de equipo externo con autorización de salida.

Comentarios del Cliente

Comentario: Se esta analizando el plan para la seguridad de la información y activos.



- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

17

Riesgo	
Esfuerzo	

©2014 Galaz, Yamazaki, Ruiz Urquiza, S.C.

8 Normativa desactualizada

Oportunidad de mejora

No se tienen actualizada la Normatividad Informática de la Administración Pública Estatal.

Impacto

Contar con normas desactualizadas que no permitan tener un control sobre los procesos.

Recomendación

Llevar un control de versiones de todas las políticas y procedimientos aplicables para el Gobierno del Estado en materia de TI.

Comentarios del Cliente

Comentario: ya esta la nueva versión y esta por aprobarse.



- Final comentada

Comentado

Nombre: Horacio Flores

Puesto: Director TI

18

Riesgo	
Esfuerzo	

©2014 Galaz, Yamazaki, Ruiz Urquiza, S.C.

Contenido

Objetivos de la Revisión

Alcance del Trabajo

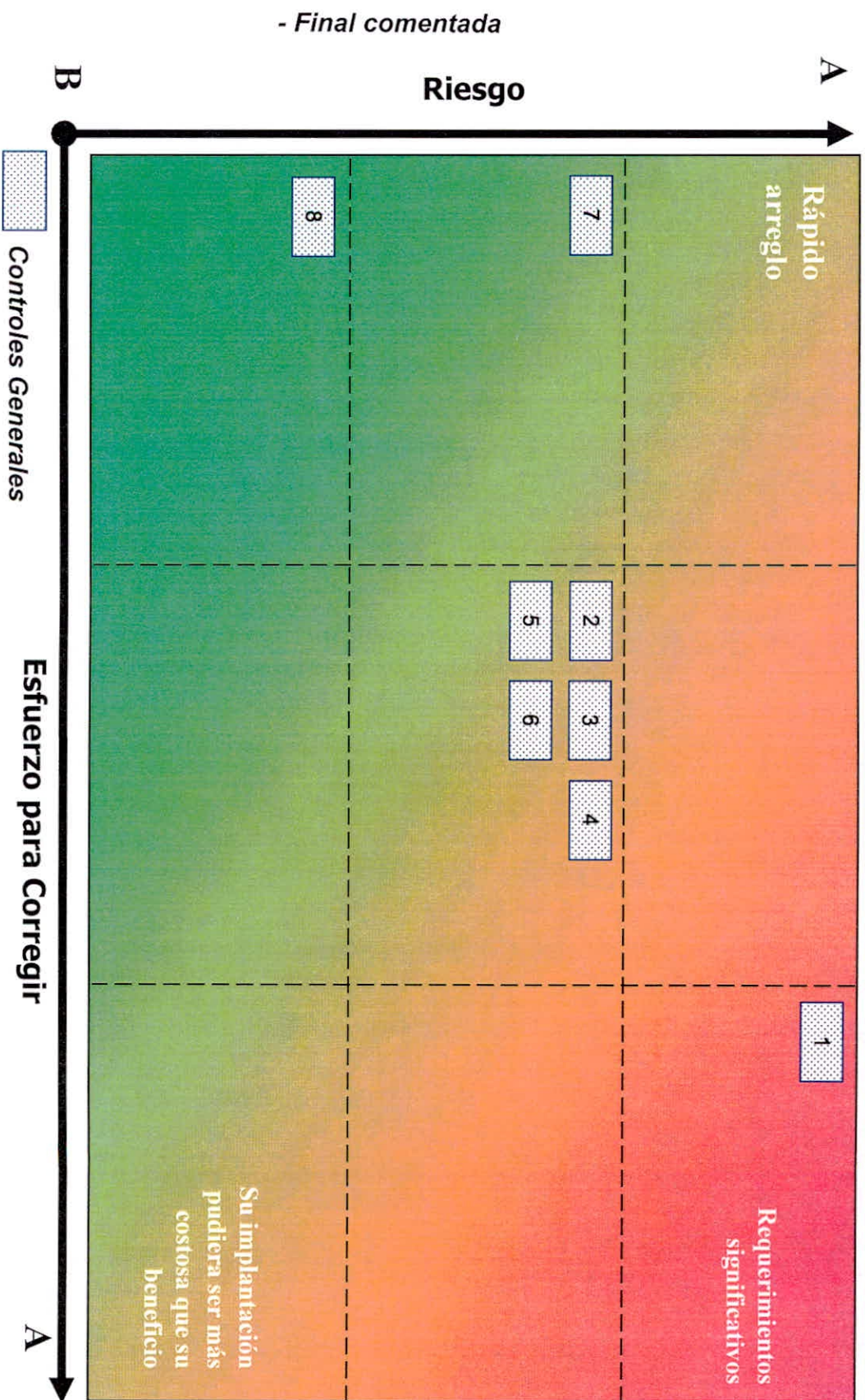
Glosario de Valores

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Mapa de riesgos



Contenido

Objetivos de la Revisión

Alcance del Trabajo

Glosario de Valores

Observaciones de Controles Generales del Computador 2014

Mapa de Riesgos

Uso de la información

Uso de la Información

Limitación:

- De acuerdo a la planeación y ejecución de la auditoría de estados financieros para **Gobierno del Estado de Querétaro** para los años que terminaron el 31 de Diciembre de 2014 levantamos y registramos nuestro entendimiento del ambiente de procesamiento de la información y realizamos pruebas de los controles generales del computador, esto con el objeto de definir nuestros procedimientos de auditoría a fin de emitir una opinión sobre dichos estados financieros y no así para proporcionar un aseguramiento en el control interno de la compañía.

Uso de la Información:

- La información aquí contenida es exclusiva para el uso de **Gobierno del Estado de Querétaro**. El contenido de este documento no debe ser utilizado por entidades distintas a la descrita anteriormente.

- Final comentada

Deloitte.