Deloitte.

Integridad de Aplicaciones - Oracle
Optimice el control interno y mejore el desempeño del negocio

Integridad de Aplicaciones - Oracle

Con el fin de mejorar y automatizar los procesos del negocio, las organizaciones que actualmente tienen o bien, están implementando sistemas de Planificación de Recursos Empresariales (*Enterprise Resource Planning* o ERP), como Oracle E-Business Suite, PeopleSoft, y JDEdwards, entre otros, esperan lograr beneficios tales como: reducción en costo de las operaciones, mayor eficiencia de los activos y mejor calidad de la información. Sin embargo, existe un área que ha demostrado ser difícil de mantener; la de riesgos y controles.

Este documento analiza ciertos detalles sobre el tema y expone algunas soluciones útiles para su organización.

Desafíos de seguridad y control

Existen seis temas recurrentes que inciden en el equilibrio adecuado entre el control y el riesgo:

1. **Carencia de entendimiento.** La complejidad de los ERPs presenta riesgos inherentes para los que es necesario contar con una infraestructura de control bien diseñada. Para el diseño adecuado de esta infraestructura de control, es vital tener un entendimiento integral de las actividades de control que pueden y deben ser configuradas en los aplicativos o módulos del ERP.
2. **Ineficiencia en los controles del sistema ERP.** Los auditores continúan levantando hallazgos, pero sin recomendaciones prácticas para su implementación.
3. **Segregación de funciones (SOD).** La efectividad de los controles automáticos que soportan los procesos de negocio se ven afectados por la falta de segregación de funciones, tanto a nivel estructura como de los accesos de usuarios dentro de los módulos del ERP.
4. **Subutilización de controles automatizados y del sistema ERP.** Los controles manuales son utilizados en lugar de habilitar los controles automáticos y de sistema disponibles en los ERPs.
5. **Falta de administración de "súper usuarios".** Accesos no controlados a los sistemas ERP para los usuarios de soporte.
6. **Optimización de controles.** El enfoque actual de cumplimiento crea múltiples programas separados o desvinculados con éste, los cuales tienen que sortear las inconsistencias y la ineficiencia del manejo de requerimientos de múltiples fuentes de control.

Adicionalmente, se considera que gran parte del éxito de una organización depende de su habilidad para establecer claramente sus objetivos y las estrategias para su logro; sin embargo, dichas estrategias están o estarían incompletas si no se consideran los obstáculos o riesgos asociados.

En las últimas décadas, los riesgos que pensábamos "improbables", están sucediendo. Los desastres naturales, así como la situación económica actual, han tenido un efecto dominó totalmente inesperado. Esto provoca que la administración de riesgos deje de ser un "buen deseo" y se convierta en un imperativo en los negocios. No obstante, su implementación debe enfrentar y solucionar un aspecto muy común en los negocios: la administración por silos, es decir, con objetivos, enfoques y actividades separadas de las áreas de la organización.

Controles débiles en el ERP

Consecuencias

A continuación se explican los principales efectos de un deficiente control en el sistema ERP.

Datos sensitivos

Los ERPs almacenan datos sensibles sobre transacciones, clientes, proveedores y recursos humanos, puesto que son necesarios para automatizar los procesos clave de las organizaciones. Cuando el ERP es controlado inapropiadamente, los riesgos para su negocio pueden ir desde una fuga de datos de información sensible, hasta fraude en procesos de compra o pago, y errores materiales en las cuentas.

Requerimientos de cumplimiento

Existe una creciente necesidad de cumplimiento por parte de los accionistas para reportar y demostrar la eficacia de los controles clave de negocio soportados por los sistemas ERP. Cuando los controles implementados son manuales o demandan grandes recursos, pueden resultar en una sobrecarga innecesaria y en quejas del negocio sobre "la compleja administración de los controles".

Reputación

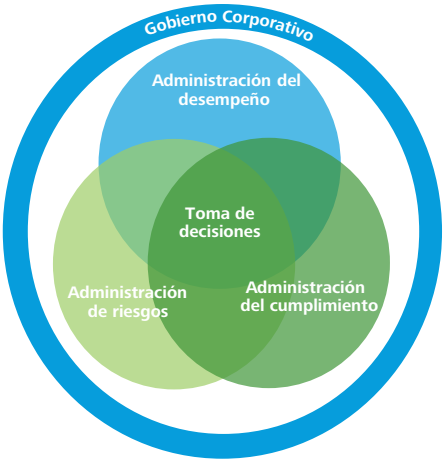
Ciertas instituciones buscan una ventaja competitiva a través de la transformación de sus prácticas empresariales internas, especialmente con el uso de centros de servicios compartidos y funciones subcontratadas que podrían llegar a afectar significativamente el sistema ERP al ocasionar fallas de control. En este sentido, mantener una buena reputación interna y externa en el mercado es la clave.

Solución

Los especialistas de Deloitte consideran como una solución a la problemática antes mencionada el uso del modelo de gestión soportado por la Suite de Oracle GRC. Este esquema promueve la forma en que una organización:

- Promueve una cultura de gobierno, riesgo y cumplimiento (GRC) de forma automática
- Facilita la comunicación y cooperación entre los diferentes actores en la gestión del negocio (aquellos involucrados con los riesgos y los controles)
- Controla y asigna roles y responsabilidades sobre las funciones involucradas
- Coordina los esfuerzos de gestión de una biblioteca única de riesgos y controles
- Documenta, prueba y reporta en tiempo real el estado que guarda el control interno
- Coordina y mantiene el flujo de las actividades de los diferentes involucrados en el cumplimiento interno y regulatorio.

La integración que ofrece la Suite de Oracle GRC consiste en la aplicación de un vocabulario, un enfoque y un proceso común, pudiendo contar con el apoyo de herramientas tecnológicas. Asimismo, el modelo coordina las actividades que incentivan el flujo constante de información en la empresa.



Deloitte le ayuda a encontrar el equilibrio

Enfoque de seguridad y control

En la actualidad, los reportes tecnológicos y financieros han comenzado a incrementar su complejidad, mientras que la dependencia de la información generada en estos sistemas y procesos es aún mayor. En adición, nuevas regulaciones en algunos países han puesto un gran énfasis en los controles internos y con frecuencia requieren de un aseguramiento independiente de la efectividad de estos controles en las organizaciones.

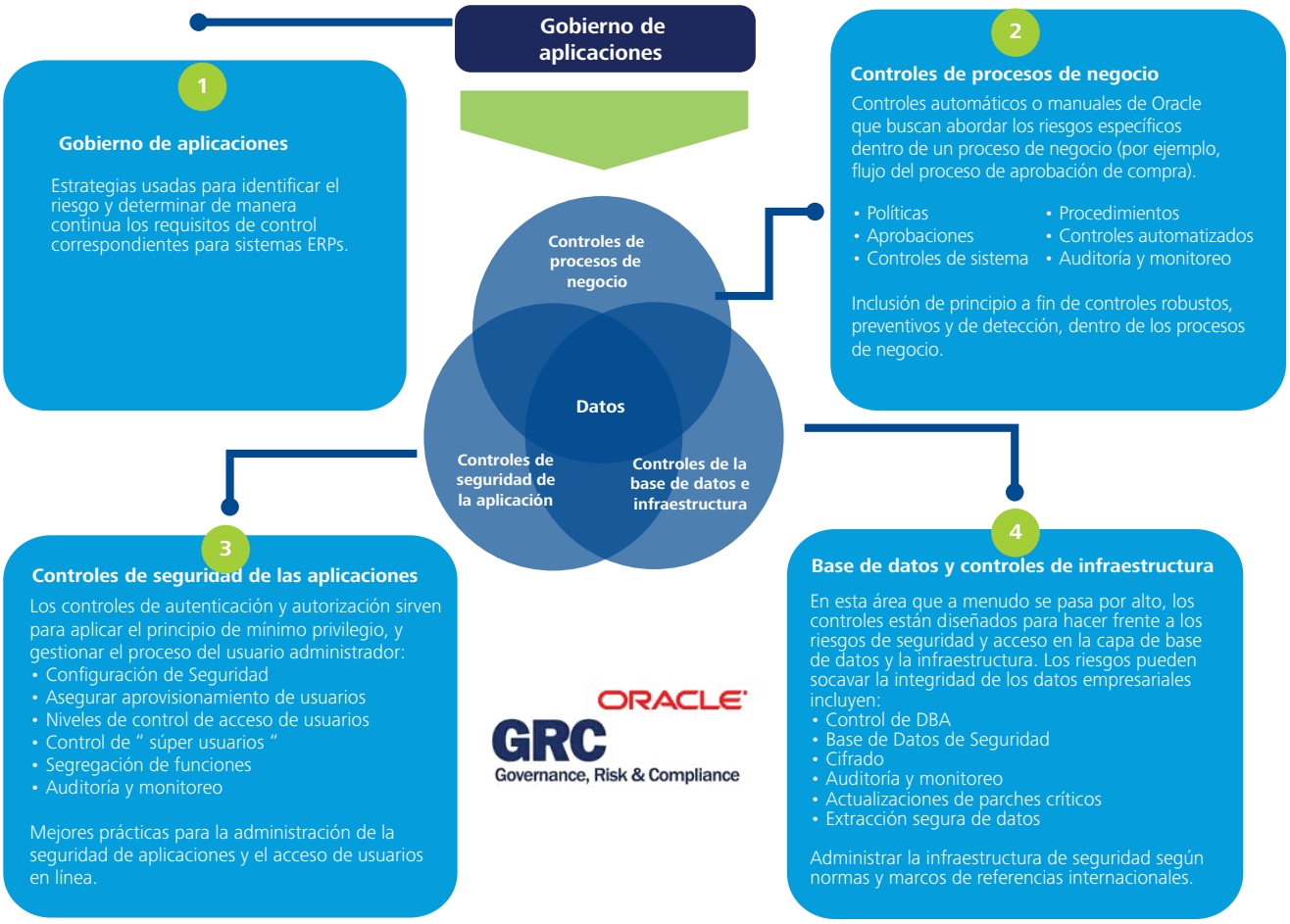
Atender el diseño, la documentación y la operación de los controles es crítico para asegurar tanto la exactitud como la puntualidad de la información usada en el procesamiento y generación de los reportes financieros, y en la administración para la toma de decisiones.

Para atender esta situación, en Deloitte contamos con la práctica de Enterprise Risk Services/Technology Risk (ERS/TR), que provee servicios multidisciplinarios relacionados con la seguridad, los controles en procesos financieros y la gestión de tecnología de información (TI). Además, proporciona:

- Gobierno de aplicaciones
- Controles de procesos de negocio (optimización de procesos de control interno del negocio y de la tecnología)
- Controles de seguridad de las aplicaciones (aseguramiento de controles en la implementación de sistemas ERP)
- Base de datos y controles de infraestructura
- Servicios de GRC soportados con herramientas tecnológicas
- Gobierno de TI y evaluaciones de infraestructura de TI
- Servicios de evaluación y limpieza de datos en implementación y migraciones de sistemas ERP

Con el objetivo de potenciar estos servicios, Deloitte trabaja en coordinación con Oracle para proporcionar una práctica común con un fuerte enfoque técnico y de negocios en la gestión de activos de información críticos. Combinando a fondo el cumplimiento normativo y el conocimiento de industrias con la suite completa de soluciones tecnológicas de Oracle, nuestros clientes en común obtienen un enfoque constante para abordar sus problemas de negocio, reducir costos, optimizar el rendimiento del negocio y permitir un cambio sostenible. Por otra parte, con un amplio conocimiento basado en la experiencia de Deloitte, las organizaciones pueden reducir significativamente el tiempo y esfuerzo que normalmente requerirían en la implementación y mejoras en el desarrollo de estas soluciones.

Así pues, estos socios globales trabajan en la implementación de GRC y las soluciones de cumplimiento que se pueden entregar a través de la Suite de Oracle GRC y otros productos.


Gobierno de aplicaciones
1
Gobierno de aplicaciones
Estrategias usadas para identificar el riesgo y determinar de manera continua los requisitos de control correspondientes para sistemas ERPs.
2
Controles de procesos de negocio
Controles automáticos o manuales de Oracle que buscan abordar los riesgos específicos dentro de un proceso de negocio (por ejemplo, flujo del proceso de aprobación de compra).
• Políticas
• Aprobaciones
• Controles de sistema
• Procedimientos
• Controles automatizados
• Auditoría y monitoreo
Inclusión de principio a fin de controles robustos, preventivos y de detección, dentro de los procesos de negocio.
Controles de procesos de negocio
Datos
Controles de seguridad de la aplicación
Controles de la base de datos e infraestructura
3
Controles de seguridad de las aplicaciones
Los controles de autenticación y autorización sirven para aplicar el principio de mínimo privilegio, y gestionar el proceso del usuario administrador:
• Configuración de Seguridad
• Asegurar aprovisionamiento de usuarios
• Niveles de control de acceso de usuarios
• Control de " súper usuarios "
• Segregación de funciones
• Auditoría y monitoreo
Mejores prácticas para la administración de la seguridad de aplicaciones y el acceso de usuarios en línea.
ORACLE
GRC
Governance, Risk & Compliance
4
Base de datos y controles de infraestructura
En esta área que a menudo se pasa por alto, los controles están diseñados para hacer frente a los riesgos de seguridad y acceso en la capa de base de datos y la infraestructura. Los riesgos pueden socavar la integridad de los datos empresariales incluyen:
• Control de DBA
• Base de Datos de Seguridad
• Cifrado
• Auditoría y monitoreo
• Actualizaciones de parches críticos
• Extracción segura de datos
Administrar la infraestructura de seguridad según normas y marcos de referencias internacionales.

Nuestra metodología

La firma apoya a las empresas en el establecimiento de procesos y controles eficaces y eficientes que reflejan tanto los riesgos como los objetivos del negocio. De esta manera se busca obtener un equilibrio en la gestión del riesgo y transformar a la institución en una empresa inteligente al riesgo. Para lograrlo se deben supervisar la gestión y la estructura de monitoreo de efectividad del sistema de controles, su infraestructura y la realización de mejoras en los procesos.

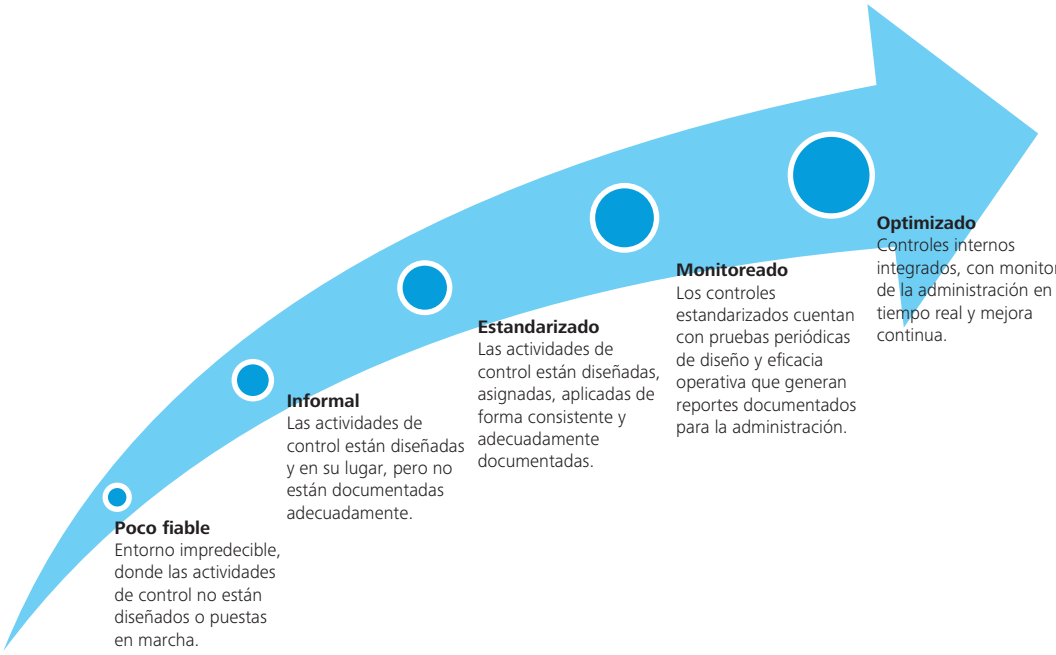
Nuestra metodología consiste en una práctica especializada por industria que soporta nuestras herramientas y la Suite de Oracle GRC, mismas que son diseñadas a la medida de su organización para alcanzar sus retos y la optimización de los controles. Este proceso considera las siguientes fases:

Fortalecimiento de controles internos

La presencia de sistemas ERP es cada vez más frecuente en todos los aspectos de los entornos de negocio de las organizaciones, con la expectativa de obtener beneficios sustanciales. Por su propia naturaleza, como el sistema nervioso central de las organizaciones, esta herramienta conlleva ciertos riesgos inherentes y sin una infraestructura de control bien diseñada, estos riesgos pueden presentar tanto problemas financieros como operativos para la organización. En Deloitte podemos ayudarle en la implementación, configuración y mantenimiento de una combinación óptima de los controles internos para administrar estos sistemas.

¿Dónde está ahora y dónde quiere estar?

Una vez analizado el estatus actual de los controles internos que tiene actualmente su organización, nuestros expertos pueden ayudarle a pasar de un nivel de poca confiabilidad hacia un nivel optimizado. Incluso si su empresa se encuentra en alguno de los otros niveles (informal, estandarizado o de monitoreo), contamos con la experiencia para apoyarle en el desarrollo de estrategias que podrían elevar sus estándares de calidad en materia de control interno.

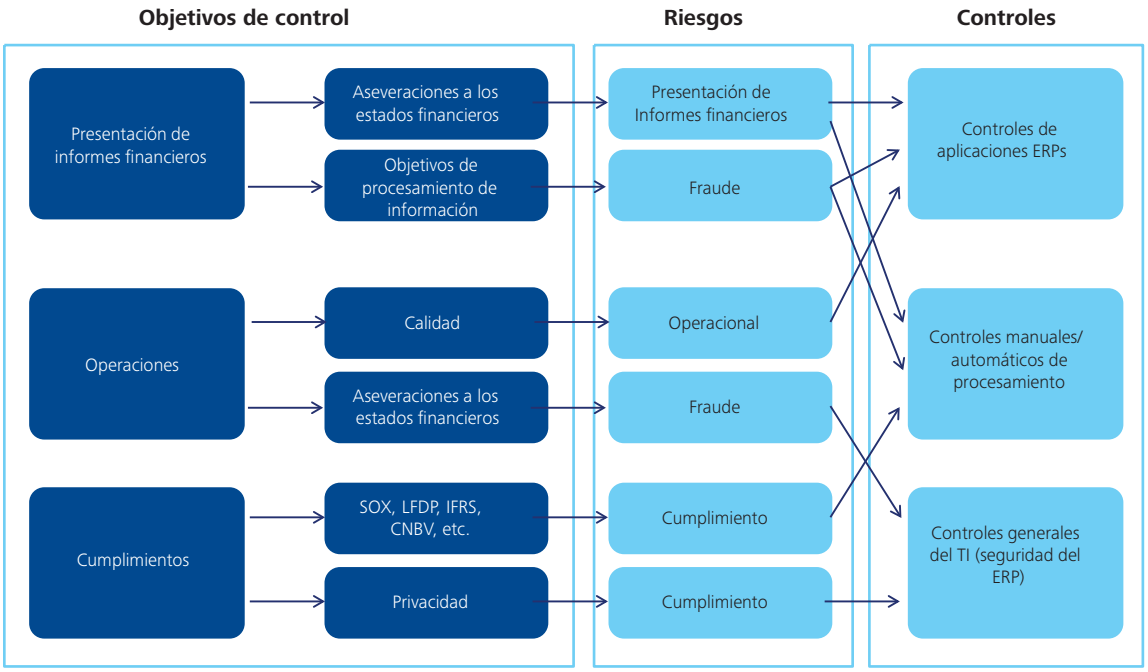


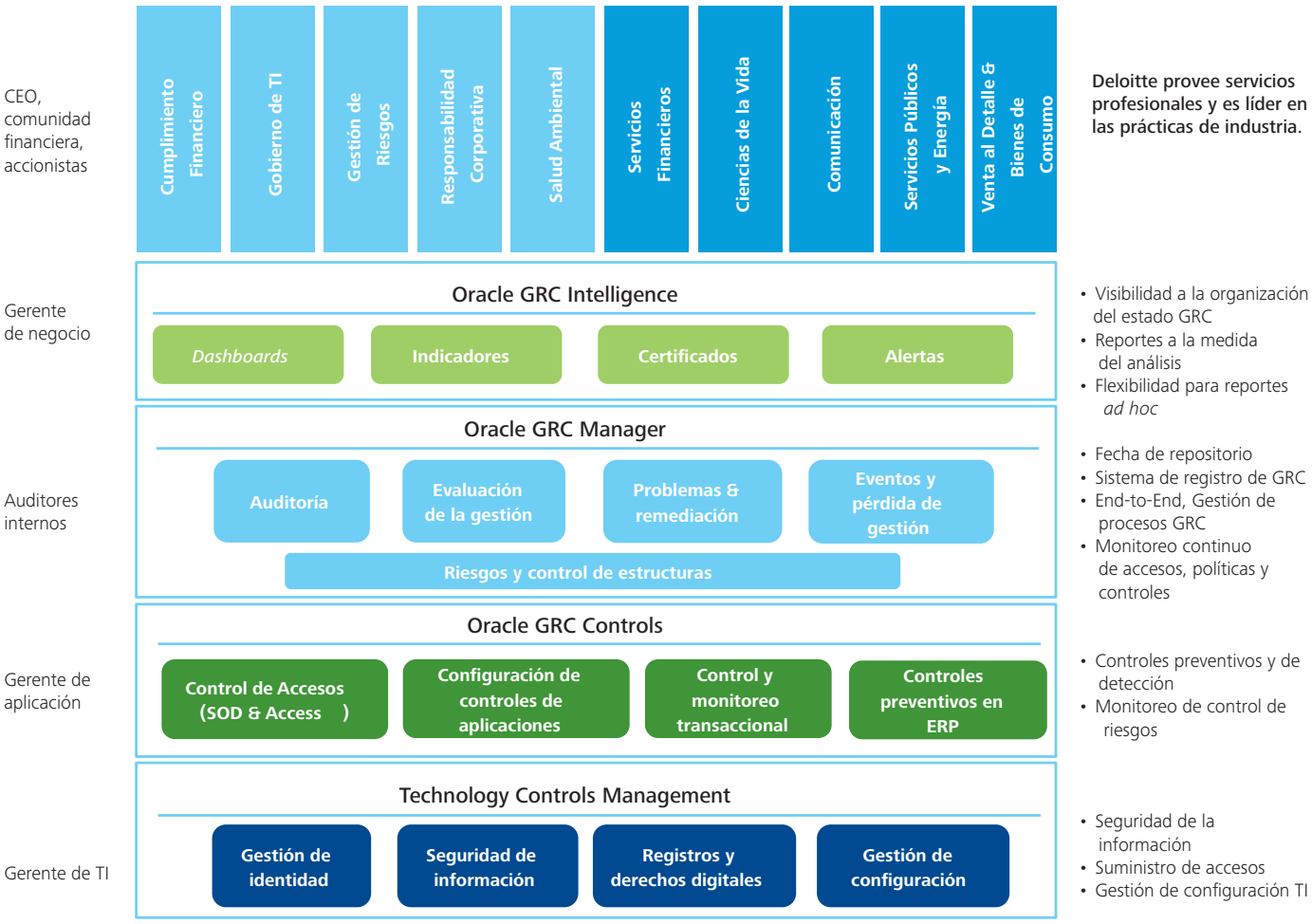
Mejoras en la estructura de control

Las empresas están evolucionando, diversificándose, adquiriendo otros negocios, fusionándose, dejando de invertir, externalizando sus procesos (*outsoucing*) y reestructurándose para tomar ventaja de un mercado dinámico y continuamente cambiante. No obstante, la proliferación de los requisitos de cumplimiento de las normativas está impidiendo este crecimiento.

Muchas organizaciones han respondido mediante la creación de funciones, la formalización de procedimientos o la estratificación de los procesos de control en la parte superior de las funciones existentes. Este mayor nivel de complejidad, con su costo inherente, es en gran parte resultado de la respuesta de la administración a cada falta de cumplimiento, obligación o expectativa regulatoria.

En Deloitte podemos contribuir a que las organizaciones construyan un marco fuerte y robusto de control interno, proporcionando soluciones tecnológicas para simplificar y automatizar los procesos manuales. No obstante, es importante destacar que la tecnología por sí sola no puede resolver las deficiencias inherentes y las ineficiencias entre los procesos de negocio y las prácticas actuales de trabajo; más bien se requiere de una estrategia integral.





Suite de Oracle GRC

Después de incrementar su enfoque en el gobierno corporativo y el control interno, las organizaciones necesitan mecanismos exitosos para lograr el cumplimiento de las normativas y satisfacer una gran variedad de las demandas de los clientes, incluyendo mejoras en el desempeño.

Un gobierno eficaz, una administración del riesgo y el cumplimiento de programas de conformidad –apoyados por la tecnología– son los elementos que le permitirán cumplir ambos objetivos.

Ya que lograr el cumplimiento, como componente clave de los programas GRC, es una propuesta costosa para la mayoría de las organizaciones, los ejecutivos y los administradores tienden a verlo como un costo al realizar negocios.

Pocas instituciones aplican un acercamiento integrado a su administración de riesgos y actividades de cumplimiento. En lugar de esto, la administración de riesgos y los procesos de cumplimiento son a menudo segregados en silos funcionales, ligados a una regulación específica o entre capas a través de los procesos de negocio existentes.

Muchas organizaciones confían en procesos manuales, los cuales contienen errores e inconsistencias y son difíciles de repetir y sostener. Las aproximaciones manuales a la administración de riesgos y el cumplimiento dificultan para las instituciones tanto la obtención de la visibilidad de su exposición a riesgos, como la colocación de controles que permitan administrar dichos riesgos.

Beneficios GRC

Colocar al GRC en el corazón de la estrategia de negocio puede convertir la administración de riesgos en una fuente de ventajas competitivas.

Una aproximación integrada a GRC, donde la administración de riesgos y el cumplimiento están soportados por una sólida estructura de gobierno y de tecnología, puede entregar valor a largo plazo. Esto puede apoyar en la mejora de los procesos de negocio y las medidas de desempeño, así como proveer a la administración con información que le permita tomar decisiones estratégicas bien informadas.

Deloitte-Oracle

Al trabajar muy de cerca con proveedores tecnológicos como Oracle, Deloitte ayuda a las organizaciones a crear programas de GRC integrados y sostenibles; ya que nuestra aproximación cumple con los cuatro componentes que deben ser integrados para obtener beneficios de este tipo de estrategias: personas, procesos, información y tecnología.

Junto con Oracle GRC, ayudamos a nuestros clientes a:

- Definir una visión estratégica para desarrollar un programa integral de GRC
- Realizar una evaluación del estado actual de las capacidades de GRC e identificar los *gaps* y requerimientos para los controles clave de riesgo, utilizando Oracle GRC o las herramientas propias de Deloitte
- Implementar e integrar la solución en alienación con la visión estratégica de los clientes
- Personalizar la Suite de Oracle GRC para los requerimientos y necesidades específicas de los clientes
- Implementar las soluciones elegidas, pues contamos con el conocimiento y la experiencia en las áreas claves de GRC, tales como la seguridad de la información y la administración de datos y recursos
- Diseñar y configurar reportes para cumplir con las regulaciones de los clientes y las necesidades de administración de riesgos
- Conducir planes y pruebas, remediaciones y actividades de entrenamiento para mantener la efectividad del programa GRC, del personal y de las políticas

Controles generales de TI y revisiones de seguridad

Los ambientes de TI han incrementado su complejidad a medida que crece la confianza/dependencia de la información proporcionada por las áreas de sistemas y procesos de TI. Las recientes y emergentes regulaciones que apuntan a restaurar la confianza de los inversionistas han colocado un mayor énfasis en el control interno, por lo que hoy en día es más común ver el requerimiento para contar con evaluaciones independientes sobre la efectividad del control interno.

Cada vez más jugadores en el mercado requieren de una perspectiva de análisis de riesgo enfocado en la aplicación de controles claves y efectivos como parte de su acercamiento hacia la evaluación, diseño e implementación del control interno. Adicionalmente, la administración de riesgos por sí misma se encuentra en la cima de la agenda del Consejo debido a fallas en procesos de alto perfil o presiones regulatorias agresivas, lo que incrementa los requerimientos de cumplimiento que necesitan integrarse al marco de control interno de la compañía.

Cuando se otorga confianza en los "controles de sistema" se utilizan herramientas en conjunto con "Practicas de Ayuda" propietarias que ayudan al aseguramiento de una configuración en los parámetros más importantes para proveer controles de sistema claves. Los reportes predefinidos también facilitan la revisión de parámetros de aplicación y configuraciones de usuario. Asimismo, una opción avanzada de consultas (*query*) permite a los expertos en controles soportados por los diferentes ERPs, analizar la configuración de cualquier parámetro dentro del ambiente productivo de estos sistemas.

En apoyo a estos requerimientos, nuestra práctica esta soportada por un "equipo" de recursos globales, herramientas enfocadas y conocimientos sobre "practicas estándar de la industria" (ITIL, COBIT). Además, proveemos el entrenamiento, la capacitación y la tecnología que su organización podría necesitar.

Accesos sensibles y SOD

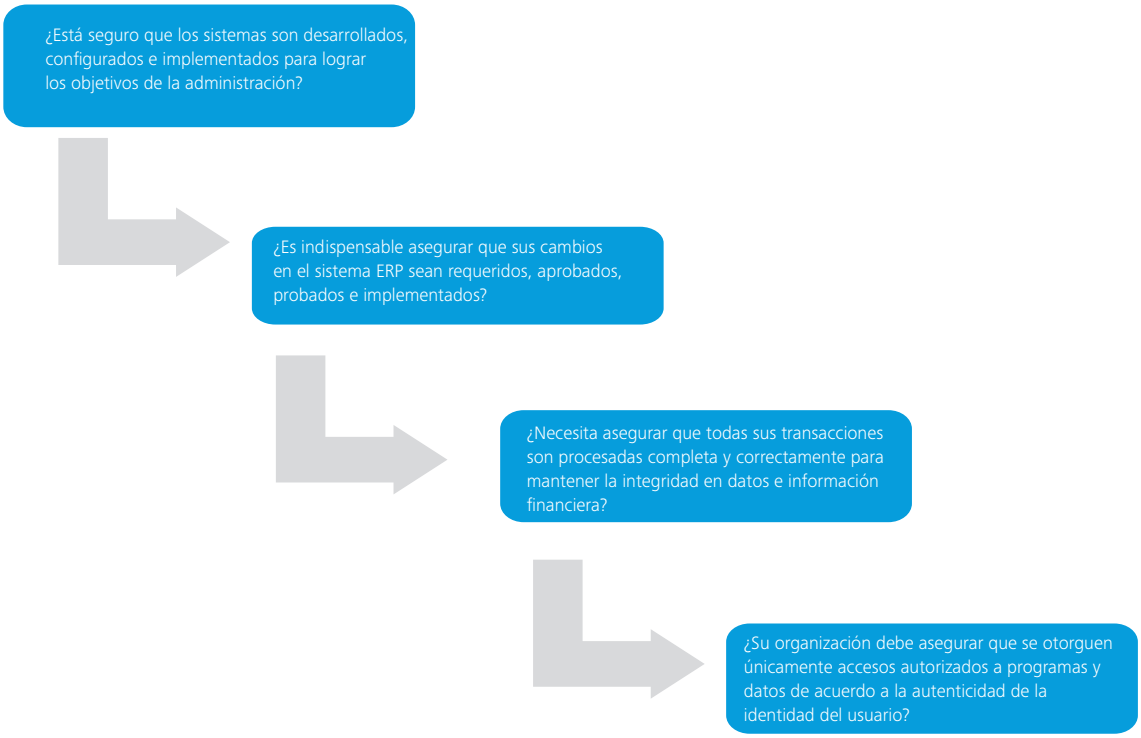
Tanto los gerentes de negocio como los de tecnología han notado que el manejo de riesgos SOD dentro de un sistema ERP puede ser una tarea complicada, pero muchos de ellos no están conscientes de los riesgos verdaderos asociados a esto. Por ejemplo, las auditorías comúnmente revelan usuarios que cuentan con la habilidad de crear proveedores y pagarles, a pesar de varios reportes y controles que nunca han identificado/marcado esto como un problema. Monitorear riesgos de SOD no sólo asegura el cumplimiento, sino que también reduce potenciales pérdidas financieras. Ambos, dinero y tiempo, pueden ser ahorrados utilizando herramientas automatizadas para SOD, en comparación con la ejecución manual de pruebas de verificación.

La adquisición, instalación y configuración de la Suite de Oracle GRC y otras herramientas para controlar SOD puede ser de gran ayuda para reducir la inversión de tiempos de manera significativa.

Soluciones adicionales

De igual manera, en Deloitte le ayudamos a:

- Analizar y validar el estado actual de su ambiente de acceso al sistema
- Evaluar riesgos de acceso y SOD en su organización, considerando su negocio, industria y necesidades particulares de cumplimiento
- Renovar procesos y re-ubicar tareas para atender eficientemente posibles conflictos
- Diseñar e implementar nuevas reglas de acceso y de SOD en su sistema ERP, tomando en cuenta su actual estructura organizacional de controles automáticos y manuales
- Seleccionar e implementar la Suite de Oracle GRC
- Rediseñar e implementar procedimientos fundamentales para la administración de acceso a usuarios, soportando la efectividad continua de los accesos restringidos y de los objetivos de SOD



Beneficios del proceso de Oracle para la aplicación de controles

Entre los beneficios de este proceso encontrará:

- Mayor visibilidad de las interdependencias de riesgo
- Continuidad en el costo-beneficio de los controles y las pruebas
- Disminución de costos al reducir los recursos necesarios para controlar y gestionar el riesgo
- Aumento de la confianza en el diseño y efectividad operativa de los controles
- Sostenibilidad, flexibilidad y desarrollo de estructuras visibles y controles automatizados
- Sistematización del proceso para anticipar y controlar los riesgos

¿Cómo puede ayudar Deloitte?

Deloitte cuenta con un plan de cuatro etapas para la aplicación de control interno a través de la Suite de Oracle GRC que se integra en el plan de trabajo:

1. **Análisis.** Evaluación basada en el riesgo de determinar nuevamente el alcance. Incluye:
   - Identificación de la responsabilidad funcional de toda la organización y el esquema de presentación de informes y puntos de vista
   - Establecimiento de la SOD
   - Realización del análisis de las deficiencias de los procesos y los controles contra la buena práctica de Deloitte (basada en el conocimiento de la industria)
   - Reconocimiento de los dueños de la información
   - Determinación de las políticas y procedimientos que soportan los controles clave y de configuración
   - Registro de los controles y ajustes

2. **Diseño.** Racionalización de los controles existentes, así como definición de las funciones y responsabilidades, y diseño de planes de prueba. Involucra:
   - Desarrollo de los flujos de procesos, funciones y responsabilidades de los propietarios y evaluadores de los control
   - Priorización de los riesgos de los procesos y controles
   - Optimización de los controles mediante la eliminación de los controles secundarios o redundantes, y remplazo de costosos controles manuales por automáticos
   - Integración de los requisitos regulatorios en la identificación de riesgos y control de las definiciones
   - Definición y documentación de los planes de prueba, tanto para los controles manuales como para los automáticos
   - Determinación de reportes y alertas

3. **Implementación.** Configuración de la Suite de Oracle GRC y sus componentes. Introduce:
   - Configuración de los controles y planes de prueba
   - Administración de la configuración de flujo de trabajo para alinear las funciones y las responsabilidades de los propietarios de los controles y evaluadores de control
   - Configuración de reportes y alertas
   - Confirmación del cumplimiento de los requerimientos regulatorios

4. ***Go-live* y soporte**. Corrección de los riesgos de deficiencias de control. Incorpora:
   - Identificación de las deficiencias de control desde el control automático o manual de las pruebas
   - Corrección y actualización de la documentación de los controles
   - Supervisión de las actividades y la SOD
   - Incorporación del proceso continuo de gestión de cambio y mejora continua

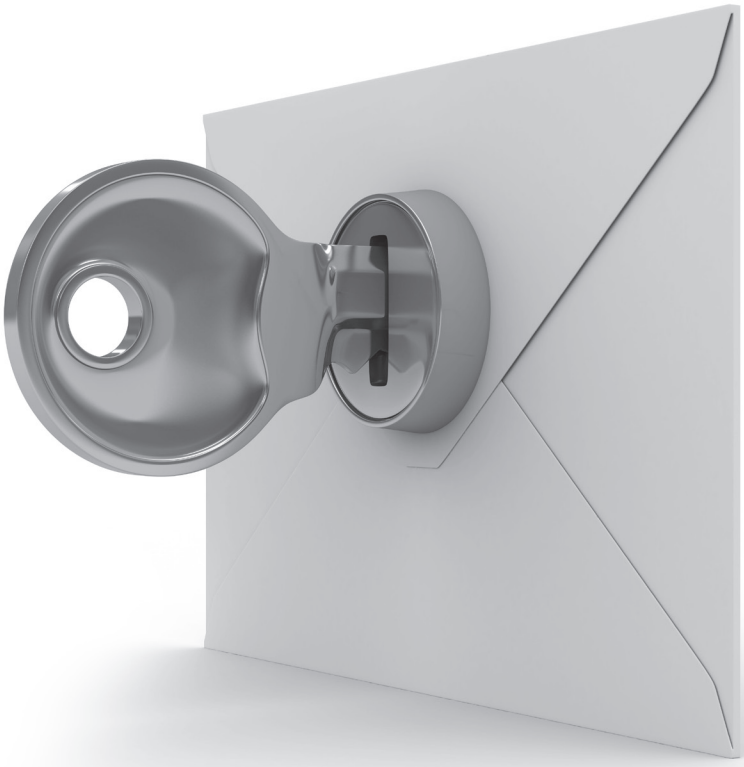
Sobre los servicios de GRC de Deloitte

Deloitte puede ayudar a crear una visión de GRC que sea sostenible a través de:

- Una hoja de ruta para GRC a largo plazo. Aunque los controles del proceso son de vital importancia, reconocemos que son sólo un componente del programa de GRC, por lo que nuestros ojos están enfocados en el objetivo final.
- Una metodología sólida. Existe una diferencia real entre la instalación y puesta en práctica, por lo que Deloitte cuenta con una metodología detallada para la aplicación del proceso y el cumplimiento de los marcos dentro de un entorno Oracle.
- Profundos conocimientos técnicos. Contamos con un largo historial de aplicación de Oracle, controles de seguridad y consultoría de riesgos.
- El trabajo en conjunto con Oracle para ofrecer soluciones de mercado a través de la Suite de Oracle GRC.

Deloitte fusiona profesionales con experiencia en consultoría de negocios, procesos, riesgos y tecnología, seguridad y auditoría interna y operativa. Esto constituye un factor distintivo en el mercado para proyectos de GRC, donde se requiere tener una amplia visión del entorno.

Nuestro principal valor radica en la experiencia para potenciar y maximizar el uso de las herramientas de GRC, evitando que las mismas se conviertan en simples repositorios de procedimientos o datos.



Contactos:

Región Centro
José González Saravia
+52 (52) 5080 6722
jgonzalezsaravia@deloittemx.com

David Rodríguez Fraiz
+52 (52) 5080 6128
drodriguezfraiz@deloittemx.com

Yadira Morales
+52 (52) 5080 6136
yamorales@deloittemx.com

Región Norte
Salomón Rico
Tel. +52 (81) 8133 7351
srico@deloittemx.com

Región Bajío
Víctor Salcedo
Tel. +52 (33) 3819 0555
vsalcedo@deloittemx.com

Región Frontera
Mario García
Tel. +52 (664) 622 7810
magarcia@deloittemx.com

www.deloitte.com/mx