

# Boletín de Asesoría Gerencial\*

La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP

No. 8 - 2009

Contenido Cerrar Imprimir Página anterior Página siguiente



*ESPIÑEIRA, SHELDON y ASOCIADOS*

Firma miembro de

*PRICEWATERHOUSECOOPERS* 

# Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

▶ [Introducción](#)

---

▶ [La respuesta de los proveedores de Software](#)

---

▶ [Caso 1: Integrando el proceso de aprobación de privilegios de acceso con los sistemas de información](#)

---

▶ [Caso 2: Automatizando los controles sobre privilegios de acceso sobre conflictos de segregación de funciones](#)

---

▶ [Caso 3: Revisión periódica de privilegios de acceso asignados y segregación de funciones](#)

---

▶ [Caso 4: Soluciones “Apaga Fuegos” \(Firefighting\) en la asignación de privilegios de acceso](#)

---

▶ [Obtener el máximo provecho de las herramientas por medio de la implementación de un marco de control interno](#)

---

▶ [Créditos / Suscribirse](#)

---

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP

### Introducción

Considerando la crisis financiera a nivel mundial que se vive en la actualidad, los inversionistas, entes reguladores y otros “stakeholders” han incrementado sus niveles de exigencia frente a las Compañías, evaluándolas no solo por sus resultados financieros, sino también por la capacidad que tengan de demostrar que son operadas bajo altos estándares de eficiencia y seguridad.

En este sentido, los aspectos relacionados con la Gobernabilidad y el cumplimiento de los controles internos relacionados con la gestión de privilegios de acceso y seguridad han cobrado mayor importancia, considerando que los riesgos relacionados con las brechas de seguridad se han incrementando de forma importante en la medida en que en los últimos años las Compañías han venido automatizando sus operaciones e implantando sistemas integrados ERP.

Es importante destacar que es mucho lo que la comunidad de gobernabilidad, seguridad informática y control interno ha trabajado en definir estándares y mejores prácticas sobre los procedimientos de gestión de privilegios de acceso. En la figura número 1, se muestra un diagrama con los procesos relacionados con la gestión de privilegios de acceso de acuerdo a las mejores prácticas.



Para visualizar la Figura No. 1 haga click en el icono.

Figura N°1 Procesos y controles para la gestión de privilegios de acceso en aplicaciones.

Adicionalmente, entre los principales controles clave la gestión de privilegios de acceso destacan los siguientes aspectos:

- Solicitud formal por parte de un supervisor sobre la asignación y modificación de los privilegios de acceso asignados a usuarios.
- Revisión de la solicitud por parte de personal funcional de nivel aprobatorio suficiente, dentro del área o proceso de negocio involucrado.
- Evitar la asignación de privilegios de súper usuarios. En caso que sea necesario, la asignación debe ser sujeta de aprobación por un nivel superior al normal y debe otorgarse de forma temporal.
- Cuando se otorguen privilegios de acceso especiales, deben definirse y documentarse los controles de monitoreo y actividades mitigantes.

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP



### Introducción (continuación)

- La Compañía debe realizar y documentar un estudio de cuales privilegios de acceso son incompatibles en cuanto a segregación de funciones se refiere.
- Verificación de todas las asignaciones de privilegios contra la lista de privilegios incompatibles. En caso de presentar incompatibilidad, el otorgamiento de acceso debe negarse o ser sujeto de un nivel de aprobación superior.
- En caso de aprobar accesos a funciones incompatibles, deben definirse formalmente controles de monitoreo y actividades mitigantes del riesgo.
- Revisión periódica de los privilegios de acceso con los dueños de proceso y confirmación de su adecuación.

- Revisión periódica para identificar conflictos de segregación de funciones, los cuales una vez identificados deben ser sujeto de mitigación.
- Revisiones periódicas para identificar y bloquear el acceso a usuarios no utilizados.

Los aspectos mencionados anteriormente han sido analizados por parte de la comunidad de especialistas y auditores, sin embargo, la implementación de los mismos ha estado limitada por la ausencia de herramientas integradas a los sistemas (ERP) que permitan su automatización, por lo cual a menudo la función de seguridad se ve forzada a implementar mecanismos manuales a un mayor costo y con menor garantía que los controles no serán omitidos.

Adicionalmente, en situaciones en las cuales sea necesario asignar privilegios por situaciones de emergencia, modificaciones constantes a los privilegios asignados debido a rotación de

funciones o ante limitaciones en la plantilla de personal, la gestión de privilegios de acceso puede adquirir niveles de complejidad difíciles de manejar.

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP



### La respuesta de los proveedores de Software

Esta situación comenzó a cambiar desde algún tiempo, debido a que los proveedores de sistemas integrados (ERP) y Compañías de Software comenzaron a desarrollar soluciones para automatizar la gestión de seguridad, de manera integrada con los sistemas de información. En tal sentido, han surgido muchas propuestas interesantes orientadas a los siguientes aspectos: Integración de los controles de aprobación de privilegios al sistema, automatización de controles de aprobación de accesos a funciones incompatibles, revisión periódica de privilegios de acceso y soluciones para otorgar privilegios de emergencia (Firefighting).

### Caso 1: Integrando el proceso de aprobación de privilegios de acceso con los sistemas de información

Bajo un entorno no automatizado, las solicitudes de asignación de privilegios de acceso se realizan por medio de planillas manuales firmadas, por medio de formas electrónicas, correos electrónicos e inclusive herramientas de "Workflow". Sin embargo, estas soluciones no están integradas a los sistemas de información en los cuales se otorgan los privilegios, por lo cual no esta garantizada la ejecución de estos controles.

Para responder a esta situación los proveedores de software han desarrollado herramientas que integran la aprobación de privilegios con el sistema de información, bajo este esquema, el usuario ingresa la solicitud directamente al sistema de información, una vez el administrador asigna los privilegios el sistema esta configurado para solicitar

aprobación a los supervisores y dueños de proceso adecuados, luego de la cual estos privilegios se hacen efectivos.

### Caso 2: Automatizando los controles sobre privilegios de acceso sobre conflictos de segregación de funciones

La asignación de privilegios de acceso incompatibles desde el punto de vista de segregación de funciones es siempre una posibilidad abierta en todo sistema integrado ERP, bien sea por requerimientos específicos del negocio e inclusive debido a errores en el diseño de roles de acceso. El identificar dichas asignaciones incompatibles representa un esfuerzo complejo y costoso, considerando que implica revisiones manuales al momento de la asignación, e inclusive búsquedas periódicas sobre las bases de datos.

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP



### La respuesta de los proveedores de Software (continuación)

Como respuesta a esta situación, se han desarrollado herramientas integradas a los sistemas de información comerciales que le permiten al usuario definir cuales privilegios de acceso se consideran incompatibles, para luego al momento de otorgar el acceso, estos sean identificados automatizadamente y no se permita la asignación, o en su defecto solicita una aprobación electrónica a un nivel superior, integrada al sistema de información, asegurando de esta forma el cumplimiento de los controles. Dicho procedimiento puede ser configurado también al momento de asignar privilegios de súper usuario.

### Caso 3: Revisión periódica de privilegios de acceso asignados y segregación de funciones

Independientemente de que tan robustos sean los controles, el movimiento de personal y la necesidad de realizar modificaciones constantes tarde o temprano podría ocasionar asignaciones inadecuadas de privilegios de acceso, bien sea por cambios en el departamento o función e inclusive retiro de la Compañía. Para mitigar esta situación, tradicionalmente las Compañías han dependido de revisiones periódicas sobre los usuarios y sus privilegios, e inclusive por medio de auditorías a los accesos.

En los últimos tiempos han aparecido en el mercado, soluciones que permiten automatizar las revisiones periódicas, e inclusive integrar las herramientas al sistema de información utilizado.

En este sentido, han surgido herramientas de reporte para identificar usuarios no utilizados, usuarios con acceso a funciones sensitivas y usuarios con acceso a conflictos de segregación de funciones:

### Identificación de cuentas de usuarios no utilizadas:

Los datos de usuarios en la mayoría de los sistemas de información pueden ser utilizados para identificar cuanto tiempo ha transcurrido desde el último acceso de una cuenta, para luego dependiendo de la configuración, los privilegios de acceso sean bloqueados automatizadamente.

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP



### La respuesta de los proveedores de Software (continuación)

#### Revisión periódica de accesos a transacciones sensitivas:

Existen herramientas de reportes integradas a los sistemas ERP que permiten definir cuales funciones o transacciones son consideradas sensitivas, por ejemplo aprobar un pago, crear un cliente, modificar el número de cuenta bancaria de un proveedor, entre otras; Una vez definida, se pueden emitir listados con los usuarios con acceso a dichas funciones, para luego proceder a revisarlos con los dueños de proceso o supervisores, permitiendo depurar los privilegios de acceso de forma periódica.

#### Revisión periódica de accesos a conflictos de segregación de funciones:

Al igual que en el caso de acceso a transacciones sensitivas, se han desarrollado herramientas que permiten definir las funciones consideradas incompatibles por la Compañía, para luego emitir reportes de acceso.

La Compañía puede considerar emitir dichos reportes de forma periódica, por ejemplo mensualmente y definir las medidas a tomar sobre los conflictos identificados.

#### Caso 4: Soluciones “Apaga Fuegos” (Firefighting) en la asignación de privilegios de acceso

Independientemente de que tan robusta sea la gestión de privilegios de acceso, tarde o temprano se presentarán situaciones en las cuales los usuarios requerirán de privilegios de acceso extraordinarios y la Gerencia de seguridad

deberá responder de forma rápida, bien por situaciones como un proceso contable de cierre mensual con una fecha de reporte cercana o la necesidad de hacer cargas masivas de datos en los sistemas de información.

Bajo dicha situación la Gerencia pudiera cometer el error de asumir dichas situaciones de emergencia como permanentes, otorgando privilegios de acceso permanentes a funciones críticas que solo se requieren en situaciones excepcionales.

Por fortuna, los proveedores de los principales sistemas informáticos de planificación empresarial han reconocido la necesidad de automatizar dichos mecanismos de control y han comenzado comercializar soluciones de “Apaga Fuego” (Firefighting), las cuales permiten automatizar la asignación de privilegios de acceso en casos de emergencia.

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP

### La respuesta de los proveedores de Software (continuación)

De esta forma, la Compañía puede asignar de forma rápida e integrada en la aplicación los privilegios de acceso de emergencia, los cuales poseen un flujo de aprobaciones e inclusive período de vigencia. Luego de cumplida la vigencia, el sistema automatizadamente elimina la asignación de privilegios extraordinarios.

Para ampliar: haga click sobre la imagen

 Retorno

### Obtener el máximo provecho de las herramientas por medio de la implementación de un marco de control interno

Las herramientas anteriormente presentadas pudieran no ser aprovechadas al máximo sino se definen formalmente y con claridad los controles sobre los privilegios de acceso, los riesgos que estos mitigan y los responsables de su ejecución.

Adicionalmente, deben estar definidos los mecanismos de monitoreo de la efectividad operativa y las pistas de auditoría relacionadas con cada uno.

En primer lugar es necesario documentar cada control de acceso y luego establecer la funcionalidad específica de las herramientas que apoyarán su ejecución, alineando de esta forma los objetivos de control con la funcionalidad de las herramientas.

Para lograr dicha implementación, es recomendable un enfoque como el que se muestra en la figura número 2.

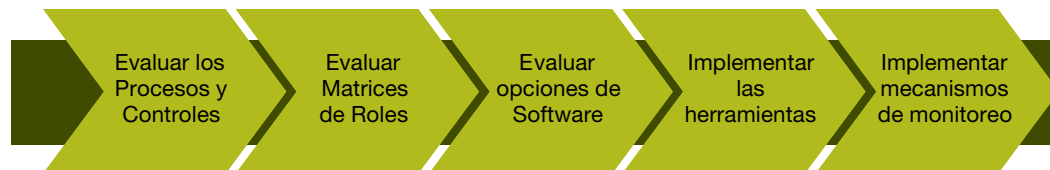


Figura N° 2. Enfoque para la automatización de controles de acceso a aplicaciones

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP



### Obtener el máximo provecho de las herramientas por medio de la implementación de un marco de control interno (continuación)

A continuación se muestran los pasos del enfoque:

- Realizar un diagnóstico sobre los procesos y controles actuales.
- Documentar el deber ser de los controles sobre privilegios de acceso.
- Para los sistemas de información utilizados por la Compañía, evaluar las opciones existentes de herramientas para la gestión de privilegios de acceso.
- Es buena práctica considerar herramientas integradas a los sistemas ERP que utiliza la Compañía, muchas de las cuales ya están disponibles.
- Realizar una evaluación de las opciones existentes, incluyendo la evaluación del producto y proveedor. Vincular la funcionalidad de la herramienta con los controles documentados.
- Implementar la herramienta, abarcando el proceso de implantación, pruebas y puesta en producción.
- Implementar los mecanismos de seguimiento y monitoreo sobre los controles.

El seguir una base metodológica para implementar los controles de seguridad, permitirá maximizar los beneficios de las herramientas utilizadas, establecer mecanismos que aseguren que los controles tendrán responsables asignados y que por ende obteniendo alta seguridad que serán ejecutados y los riesgos mitigados.

El resultado final será la posibilidad de implementar controles de seguridad efectivos y poder demostrar dicha capacidad a los "Stakeholders".

# Boletín de Asesoría Gerencial

## La próxima generación de herramientas para la gestión de privilegios de acceso en sistemas integrados - ERP

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. \*connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados  
Depósito Legal pp 1999-03CS141  
Teléfono máster: (58-212) 700 6666

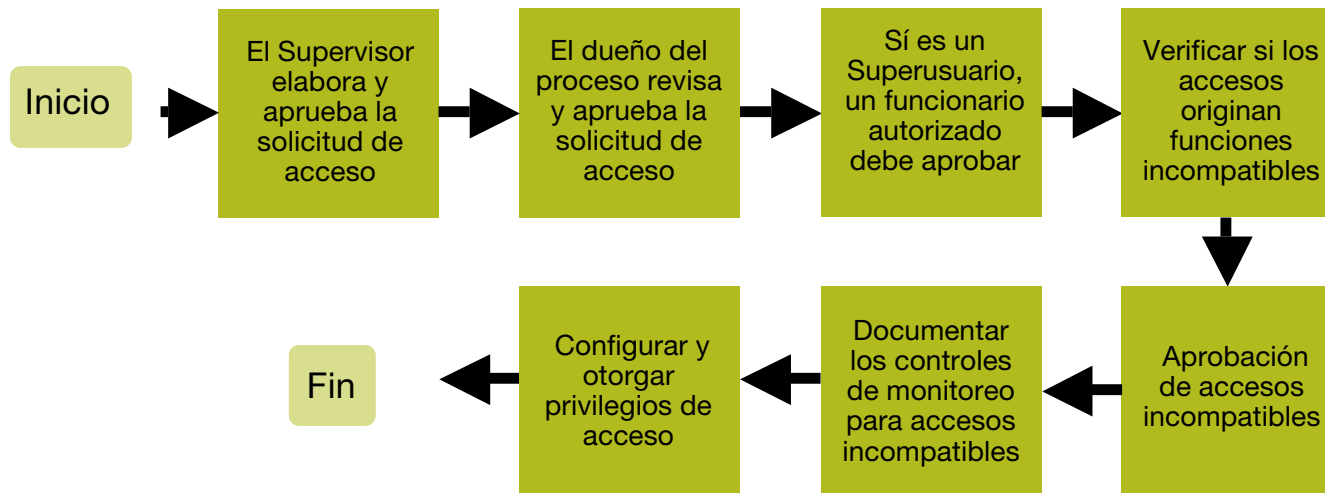


© 2009. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3

# Figura N°1 Procesos y controles para la gestión de privilegios de acceso en aplicaciones.



## Asignación de privilegios de acceso



## Evaluación permanente de privilegios de acceso

