

Boletín Asesoría Gerencial*

Agosto 2007

Estándar de seguridad para PCI (Payment Card Industry):
una respuesta de seguridad para las transacciones con tarjetas

Introducción

Componentes del
estándar PCI

Tecnologías y
técnicas

¿Qué organizaciones
deben cumplir con el
estándar PCI?

¿Cuándo cumplir con
el estándar PCI?

Conclusiones

Créditos

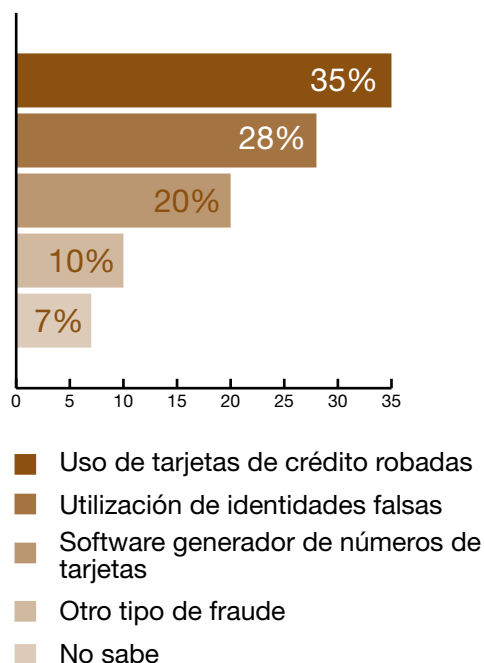




Introducción

El entorno de negocios cambia de forma acelerada y las nuevas tecnologías influyen cada vez más la gestión de las organizaciones y en la manera de hacer negocios, por lo cual, el concepto de “Seguridad de la Información” ha incrementado su importancia en el ámbito de las organizaciones, debido a la constante aparición de vulnerabilidades.

En la búsqueda del equilibrio, es necesario entonces procurar el uso de la tecnología, pero con controles que permitan minimizar el riesgo de fraude y robo de información. En este sentido, una de las mayores preocupaciones de los comercios en línea, es el fraude con tarjetas de crédito, y muchas fuentes señalan que, sólo en Estados Unidos las Instituciones Financieras han perdido alrededor 3.000 millones de dólares por fraudes electrónicos con tarjetas de crédito y débito. Así, si revisamos los fraudes más comunes asociados a este rubro, encontramos la siguiente gráfica:



Fuente: “8th Annual Online Fraud Report”

Figura N° 1. Fraudes más comunes con tarjetas

Adicionalmente, al consultar la fuente www.gfi.com encontramos los siguientes casos:

- Un proveedor de servicios por Internet, informó que un trabajador de su compañía pudo obtener la información de 79.000 clientes que realizaron pagos con tarjetas de débito y crédito (Enero de 2007).
- Una importante empresa de ventas por catálogos en Internet, denunció una intrusión no autorizada en el sistema electrónico de procesamiento de tarjetas, en la que al menos 45,6 millones de números de tarjetas de crédito y débito fueron posiblemente por hackers (Febrero de 2007).

Estas referencias nos conducen a resumir la situación actual como sigue:

- La banca en línea y las ventas por medio del comercio electrónico han incrementado los ataques de hackers.
- Los datos de la banda magnética de las tarjetas frecuentemente son copiados, lo que incluye un riesgo adicional.



Introducción

Componentes del estándar PCI

Tecnologías y técnicas

¿Qué organizaciones deben cumplir con el estándar PCI?

¿Cuándo cumplir con el estándar PCI?

Conclusiones

Créditos

Introducción (cont.)

- La información comprometida de los tarjetahabientes, perjudica la reputación y prestigio de las compañías, en especial, a las marcas.
- Existe un impacto en la confidencialidad de los consumidores, y en consecuencia una baja en el consumo.

PCI (Payment Card Industry) como respuesta a eventos con tarjetahabientes

Desde hace algunos años, las “Marcas”, como se acostumbra a referir a las principales empresas responsables de la concesión y gestión de servicio de pagos con tarjetas y operaciones electrónica, han tenido normativas de seguridad a ser cumplidas por sus asociados.

Sin embargo, debido a las pérdidas por fraudes realizados con tarjetas de crédito y el esfuerzo que representaba al sistema financiero cumplir con tal diversidad de normativas, fue necesario el desarrollo de un enfoque unificado, por lo que se fundó en Septiembre de 2006, el Consejo de Normas de Seguridad de la Industria de Medios de Pago PCI Security Standards Council, para coordinar y administrar acciones relativas a la

seguridad de la información relacionada a tarjetas de pago y sus titulares, así como para garantizar que la norma “PCI Data Security Standard” (PCI-DSS) permanezca en el tiempo, y se realicen las adaptaciones producto de los cambios en la tecnología y nuevos escenarios de fraude.

Sus fundadores son: American Express, Discover Financial Services, JCB International Credit Card, MasterCard Worldwide and Visa International; y entre sus principales objetivos están:

- Mantener y actualizar el PCI-DSS.
- Entrenar y certificar los QSAs (Qualified Security Assessors).
- Entrenar y certificar los ASVs (Approved Scannig Vendors).

¿Qué es el estándar de seguridad PCI?

El PCI DSS (Payment Card Industry Data Security Standard) es un estándar de seguridad que incluye: requerimientos para el manejo de la seguridad, políticas, procedimientos, arquitectura confiable de red, diseño de software y otras medidas de protección. Este estándar aplica no sólo a los bancos, sino también a compañías que

acepten pagos con tarjeta, desde tiendas en línea (“on-line”) a operadores móviles y a compañías intermediarias.

Este estándar de seguridad en el sector de tarjetas de pago, se basa en lineamientos que fueron creados de forma independiente por cuatro (4) compañías, a saber:

1. El programa de seguridad de información de cuentas VISA (AIS, Account Information Security Program) y el programa de seguridad de información de titulares afiliados de tarjeta (CISP, Cardholder Information Security Program);
2. El programa de protección de datos de Mastercard (SDP, Site Data Protection);
3. La política operativa de seguridad de American Express (DSOP, Data Security Operative Policies); y
4. El programa de cumplimiento normativo y seguridad de información de Discover (DISC, Data Security Guidelines).



[Introducción](#)[Componentes del estándar PCI](#)[Tecnologías y técnicas](#)[¿Qué organizaciones deben cumplir con el estándar PCI?](#)[¿Cuándo cumplir con el estándar PCI?](#)[Conclusiones](#)[Créditos](#)

Introducción (cont.)

El principio básico de este estándar, es restringir el almacenamiento o acceso de información de autenticación, la cual va desde el código de verificación, la información contenida en la banda magnética, el nombre del tarjetahabiente, las fechas de expiración, entre otros. De igual forma, el alcance del estándar se extiende hacia todos los componentes del ambiente de datos de los emisores y procesadores de transacciones de pago con tarjetas, como por ejemplo: servidores, aplicaciones, dispositivo de red, etc.

Adicionalmente, es importante mencionar que:

- El estándar también incluye como anexo, las consideraciones para la aplicabilidad de las Normas de Seguridad de Datos en la Industria de las Tarjetas de Pago (PCI-DSS) para Proveedores de Servicios de Hospedaje.
- PCI anunció recientemente (11 de Septiembre de 2007), la incorporación de los requerimientos de seguridad para los Dispositivos de Entrada de PINES (PED).

Componentes del estándar PCI

PCI establece un conjunto completo de estándares de seguridad mundiales para todos los comerciantes y proveedores de servicios relacionados con el almacenamiento, la transmisión o el procesamiento de datos de titulares de tarjetas de todos los servicios principales correspondientes.

Para certificar el cumplimiento oficial con el estándar PCI, se debe realizar una auditoría que compruebe que los estándares se cumplen adecuadamente. A ésta le siguen auditorías de cumplimiento con las normativas trimestrales y anuales, cuyos requisitos exactos dependerán de la clasificación del comerciante.

En resumen, respaldado por MasterCard, Visa, American Express, Diners Club y JCB Cards, el estándar PCI cubre seis (6) diferentes aspectos y establece doce (12) requerimientos relacionados con la administración de la seguridad, políticas, procedimientos, arquitectura de redes, diseño de software y otras medidas de protección, que se deben cumplir de manera continua, tal como se menciona a continuación:

Construir y mantener una red segura

1. Instalar y mantener una configuración de firewalls para protección de los datos, considerando aspectos como: segmentación de red, utilización de IP Masquerading (NAT), etc.
2. No utilizar los valores por omisión (configuraciones por defecto) para passwords y parámetros de seguridad.

Proteger la información de los titulares de las tarjetas

3. Proteger la información almacenada (y en particular restringir el almacenamiento de información sensible, como: Track1 / Track2, CVV2, PIN Block, entre otros).
4. Cifrar la información de los tarjetahabientes y otra información crítica cuando sean transmitidas mediante redes públicas.



[Introducción](#)[Componentes del estándar PCI](#)[Tecnologías y técnicas](#)[¿Qué organizaciones deben cumplir con el estándar PCI?](#)[¿Cuándo cumplir con el estándar PCI?](#)[Conclusiones](#)[Créditos](#)

Componentes del estándar PCI (cont.)

Mantener un programa de gestión de vulnerabilidades

5. Utilizar y actualizar regularmente software antivirus.
6. Desarrollar y mantener sistemas y aplicaciones seguras, aplicando las últimas actualizaciones de seguridad e incorporando los estándares de seguridad de la información a lo largo del ciclo de desarrollo de software.

Implementar medidas estrictas de control de acceso

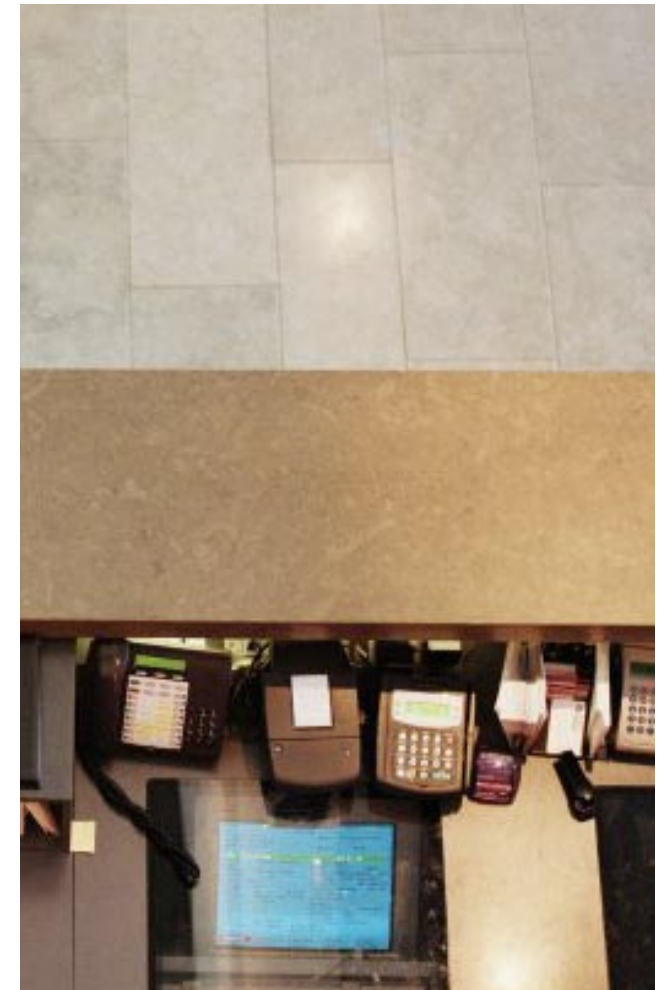
7. Restringir el acceso a los datos en función de requerimientos de negocio (business need-to-know).
8. Asignar un identificador único de usuario a cada persona que tenga acceso a equipo de computación o sistema, evitando el uso de identificadores genéricos.
9. Restringir el acceso físico a la información de los titulares de las tarjetas, asegurando físicamente los medios de información, almacenando los backups de manera segura e implantando una política de destrucción de medios.

Vigilar y evaluar regularmente las redes

10. Registrar y realizar el monitoreo de todos los accesos a recursos de la red y a la información de los titulares de las tarjetas, para lo cual se hace necesario la activación de logs de auditoría, así como su revisión.
11. Evaluar regularmente los sistemas y procesos de seguridad, considerando la ejecución de periódica de un diagnóstico de vulnerabilidades, evaluación de controles y acceso a la red, pruebas de intrusión anuales, entre otros.

Mantener una Política de Seguridad de la Información

12. Mantener una política que atienda específicamente la seguridad de la información, implementando un programa formal de concientización.





Introducción

Componentes del estándar PCI

Tecnologías y técnicas

¿Qué organizaciones deben cumplir con el estándar PCI?

¿Cuándo cumplir con el estándar PCI?

Conclusiones

Créditos

Tecnologías y técnicas

Las siguientes estrategias son aplicables al cumplimiento del estándar PCI. A continuación un resumen de las recomendaciones que comprende el estándar:

- Confidencialidad y autenticación:

Este es el objetivo central del estándar PCI: proteger la información de las tarjetas de crédito de los consumidores. Desafortunadamente, los desarrolladores no tienen control total y global sobre el proceso de operación de tarjetas de crédito.

En un mundo ideal, los datos de las tarjetas de crédito se podrían intercambiar directamente entre la compañía de la tarjeta de crédito y la persona, pero la realidad es otra: los datos de las tarjetas de crédito a menudo pasan por varios agentes intermediarios, algunos de los cuales los consumidores desconocen, pero se ven obligados a confiar de forma implícita. La mejor solución que se puede implementar desde la perspectiva de una sola organización, es la de asegurar que los datos se hayan cifrado correctamente y que sólo los sistemas o los agentes autorizados puedan tener acceso a la información.

- Registro y auditoría:

Este es el segundo aspecto más importante en cuanto a cumplimiento del estándar PCI. Los desarrolladores deben asegurarse que su código proporcione las facilidades para registrar todas las transacciones y eventos asociados a las cuentas de los tarjetahabientes.

Desafortunadamente, es difícil para los comerciantes determinar proactivamente casos de fraude de tarjetas de crédito, ya que no disponen de un banco con información centralizada de patrones de consumo, que indique qué pautas de uso son irregulares en una cuenta dada. Desde la perspectiva de PCI, es importante garantizar que las transacciones realizadas con las tarjetas, queden registradas, por lo cual, las aplicaciones desarrolladas internamente deberán cumplir con esta premisa a fin de poder suministrar la información cuando sea requerida.

Según Gartner: “la protección de datos de clientes es mucho menos costosa que la reparación de una brecha de seguridad en la que los registros quedan expuestos y son mal utilizados potencialmente. Los requisitos de cumplimiento de Payment Card Industry (PCI) brindan a las empresas una buena justificación para incrementar la protección de los datos”.





Estándar de seguridad para PCI (Payment Card Industry): Una respuesta de seguridad para las transacciones con tarjetas

> Inicio > Imprimir > Salir



Introducción

Componentes del estándar PCI

Tecnologías y técnicas

¿Qué organizaciones deben cumplir con el estándar PCI?

¿Cuándo cumplir con el estándar PCI?

Conclusiones

Créditos

¿Qué organizaciones deben cumplir con el estándar PCI?

El cumplimiento del estándar PCI es una ventaja, ya que mejora el soporte de interoperabilidad, además de proveer al usuario un entorno confiable en cuanto a sus transacciones, bien sea de débito o crédito. Cumplir con esta normativa asegurará que los datos de usuario no queden atrapados en formatos electrónicos.

Ahora bien, el estándar PCI aplica a toda organización que procese información de tarjetas de crédito o débito, incluyendo comercios y proveedores de servicio que almacenen, procesen o transmitan datos de tarjetas de crédito/débito. Es importante mencionar, que si una organización está catalogada en algunas de las actividades descritas anteriormente, PCI es un requisito, tal como lo establece el PCI Security Standards Council: “los requisitos establecidos en los Normas de Seguridad de Datos de Tarjetas de Pago (PCI-DSS) son aplicables sólo si se guarda, procesa o transmite un número de cuenta primario (PAN, Primary Account Number). Si este número de cuenta primario no se guarda, procesa o transmite, no se aplican estos requisitos”.

Sin embargo, es importante mencionar que el PCI Security Standards Council no reemplazará los

programas de cumplimientos de las marcas individuales que lo conforman: las marcas participantes de manera individual, determinarán que compañías deben cumplir no tan sólo con lo establecido en PCI, sino también con el programa de seguridad establecido en cada marca. De igual forma, cada marca establecerá las sanciones (suspensión o revocación de privilegios para procesar transacciones) o multas a ser canceladas por una compañía que no esté en cumplimiento.

Por ejemplo, para el 30 de Septiembre de 2007, VISA ha establecido multas de hasta \$25.000 para los comercios que no cumplan con el estándar. Ahora bien, para la aplicabilidad del estándar PCI, los comerciantes se categorizan en niveles diferentes según su volumen promedio anual de transacciones de tarjeta de crédito, y esto se debe al intento de conciliar las dificultades asociadas a la necesidad de equilibrar la seguridad con la carga práctica. Cuantas más transacciones procese una organización, más importante será que cumpla con los estándares PCI para atender riesgos más significativos.

En la siguiente figura se muestra los requerimientos de validación, según la categoría de los comercios.

Para ampliar la imagen, haga click sobre el cuadro ▾

Categoría	Transacciones al año (en US\$)	Revisión en sitio	Auto evaluación	Scanning de la Red
Nivel 1	Más de 6 millones	Si	No	Trimestral
Nivel 2	150K - 6 millones	No	Anual	Trimestral
Nivel 3	20K - 150K	No	Anual	Trimestral
Nivel 4	Menos de 150K	No	Anual	Trimestral

Figura N° 2 Requerimientos de validación vs. categoría de los comercios

Retorno

Como dato curioso, y tomando las estadísticas de VISA, sólo el 18% de los comercios “Nivel 1” estaban para el año 2006 en cumplimiento con el estándar, a diferencia del año 2007, que han obtenido un 35%. Otro 51% de los comercios, reportado que cumplen con el estándar, pero un 93% han certificado que no almacenan PIN, números de verificación de las tarjetas u otra información de la tarjeta de crédito. Ahora bien, es importante mencionar, que no porque una organización esté cumplimiento actualmente con el estándar PCI-DSS, significa que ésta continuará siendo certificada de manera indefinida, debido a los cambios en el entorno, nuevas tecnologías y nuevas vulnerabilidades. En general, el cumplimiento 100% del estándar no es sólo para un momento específico.



Introducción

Componentes del estándar PCI

Tecnologías y técnicas

¿Qué organizaciones deben cumplir con el estándar PCI?

¿Cuándo cumplir con el estándar PCI?

Conclusiones

Créditos

¿Cuándo cumplir con el estándar PCI?

En términos generales, se estima que para finales de 2007, las organizaciones que acepten transacciones de tarjetas de crédito o débito deben estar en cumplimiento con el estándar. Sin embargo, se han establecido las siguientes fechas importantes:

31 de Marzo 2007:

Comerciantes con Nivel 1 y 2 deben demostrar cómo almacenan los datos de los tarjetahabientes.

30 de Septiembre de 2007:

Todos los comerciantes de Nivel 1 deben cumplir completamente con PCI – DSS

31 de Diciembre de 2007:

Todos los comerciantes de Nivel 2 deben cumplir completamente con PCI – DSS

Conclusiones

Para lograr determinar una evaluación adecuada con respecto a los controles en tecnologías de información y en particular lo relacionado a la seguridad, de manera sustancial, los auditores deberán tomar el liderazgo en estos esfuerzos, ya que se enfrentan cotidianamente a la necesidad de validar y sustentar sus opiniones acerca de los controles internos que garantizan razonablemente la confiabilidad de la información que se genera y por ende el cumplimiento de sus metas y objetivos.

En resumen, el estándar PCI brinda las herramientas y medidas necesarias para ayudar en el desarrollo de una cultura internacional de seguridad entre los comerciantes, propiciando así el auge sostenido del comercio electrónico; asimismo, implementando los mecanismos adecuados que minimizan los riesgos, las transacciones electrónicas con tarjetas de crédito/débito pueden convertirse en operaciones cotidianas, que generen confianza en los clientes.



Estándar de seguridad para PCI (Payment Card Industry): Una respuesta de seguridad para las transacciones con tarjetas

> Inicio > Imprimir > Salir



Introducción

Componentes del estándar PCI

Tecnologías y técnicas

¿Qué organizaciones deben cumplir con el estándar PCI?

¿Cuándo cumplir con el estándar PCI?

Conclusiones

Créditos

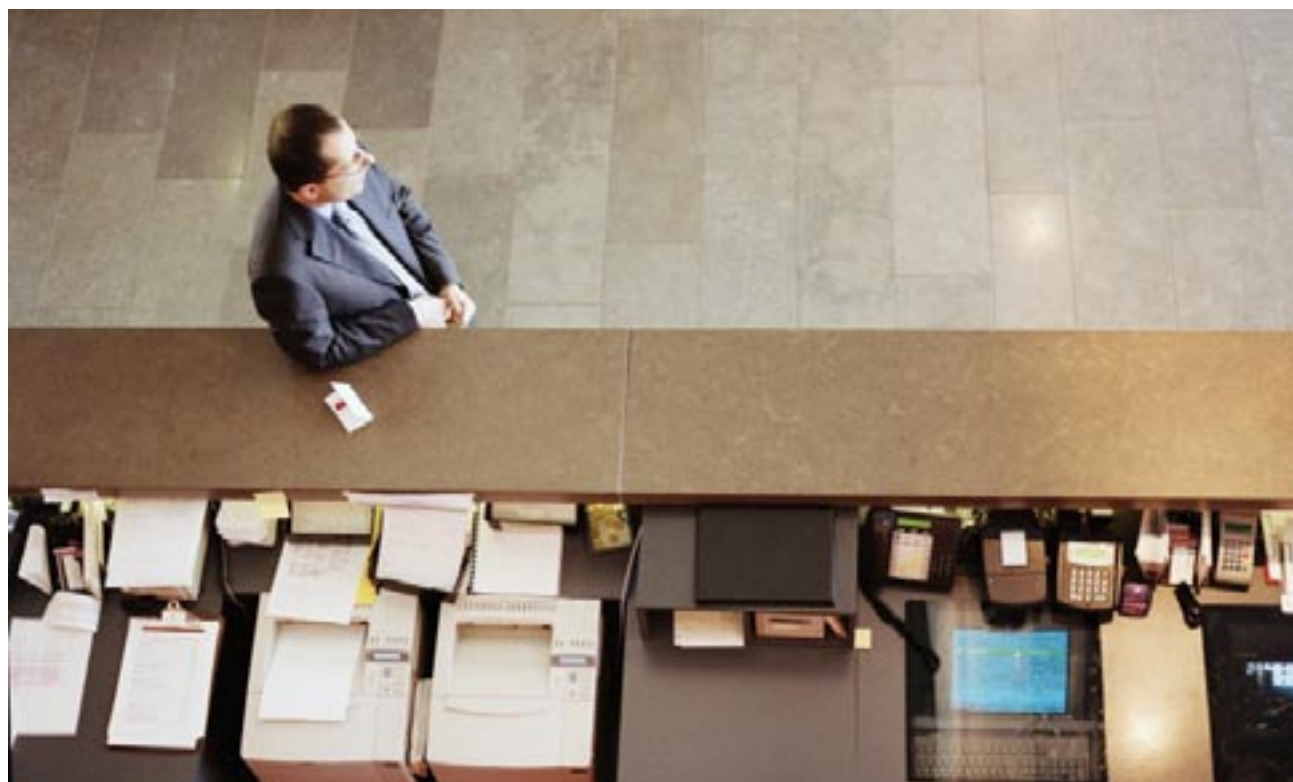
Boletín Asesoría Gerencial

El Boletín Asesoría Gerencial es publicado mensualmente 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 master: (58-212) 700 6666

Si está interesado en recibir en su correo electrónico este Boletín, por favor envíenos su dirección de e-mail a:
advisory.venezuela@ve.pwc.com



© 2007. 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