

Por qué las empresas necesitan archivar los correos electrónicos

Las principales razones de por qué la importancia de archivar correo electrónico corporativo

A pesar del crecimiento en el uso de correo electrónico y mensajería instantánea en las empresas, la preservación de dicha correspondencia electrónica esta todavía sujeta a debate. Este documento se enfoca en estas incertidumbres y explica el por qué archivar correo electrónico debe ser parte integral de cada empresa. También examina los diferentes métodos para la implementación y administración de soluciones de archivo de correo electrónico en una empresa también como especifica los requerimientos claves que un sistema completo de archivo de correo debería incluir.

Introducción

En una encuesta reciente, SERVO preguntó a 100 de sus clientes más importantes qué proyectos ellos estarían más próximos a realizar en el 2005. Interesantemente, el archivo de correo electrónico esta dentro de las 5 principales prioridades corporativas para ese año. Esto también se ve reflejado en las tendencias del mercado, las cuales muestran un incremento de seis veces en la demanda de soluciones de archivo de correo electrónico. Este documento explica el por qué el archivo de correo es importante.

Introducción	2
El valor corporativo del correo electrónico	2
¿Cuál es el significado 'verdadero' del archivo de correo electrónico?	3
¿Cuáles son las razones primarias para archivar correo electrónico?	4
Implementando y administrando soluciones de archivo de correo electrónico.....	8
¿Qué características debe tener una solución de archivo de correo electrónico?	9
Acerca de GFI	11
Referencias	12

El valor corporativo del correo electrónico

Dentro de los últimos cuatro años, el correo electrónico se ha convertido en el canal primario de comunicación en negocios. Provee a la empresas con un rápido medio de transporte de correspondencia de negocios tales como ordenes, cotizaciones y transacciones de ventas, en virtualmente cualquier área geográfica con el menor esfuerzo posible. Un estudio hecho por el investigador de mercado Gartner Group reveló que las empresas conducen casi el 97% de sus comunicaciones a través de correos electrónicos. Además en una encuesta reciente, Osterman Research encontró que el correo electrónico es ahora aceptado como confirmación escrita de aprobación de órdenes en 79% de las empresas.

Debido a que el correo electrónico se ha convertido en el sustituto electrónico de documentación legal de negocios, la información que es entregada a través de esta correspondencia electrónica constituye un registro. Consecuentemente, tal correspondencia debe ser retenida por un mínimo de tiempo, normalmente establecido por los estatutos. Debido a la predominancia del correo electrónico en la industria de los negocios, varias piezas de legislación han sido creadas para proteger la privacidad personal, reforzar los estándares de gobernabilidad corporativa y mantener conducta ética. El Acto Sarbanes - Oxley (SOX), el acto Gramm - Leach Bliley (GLBA) y el acto de libertad de información (FOIA), son algunos ejemplos de tales legislaciones.

¿Cuál es el significado 'verdadero' del archivo de correo electrónico?

Un archivo de correo electrónico es un repositorio generalmente mantenido en un ambiente no en producción para proveer preservación segura de correo electrónico para propósitos operacionales y de cumplimiento legal. Un 'verdadero' sistema de archivo de correo electrónico automáticamente extrae el contenido del mensaje y adjuntos de los correo entrantes / salientes y después de indexarlos, los almacena en un formato de solo lectura. Esto asegura que los registros archivados sean mantenidos en su estado original.

El archivo de correo electrónico modera la demanda de espacio de almacenamiento al reducir la cantidad de correos electrónicos en línea en el servidor de correo. Además el archivo de correo electrónico consume menos almacenamiento físico que otros métodos de almacenamiento de correo electrónico.

El acercamiento activo adoptado por las soluciones de archivo de correo electrónico asegura que la empresa tenga una copia accesible y centralizada de todos sus correos electrónicos. Esto provee protección adicional contra borrado intencional o accidental de correos electrónicos por parte de los usuarios finales. El archivo de correo electrónico también elimina la necesidad de buscar por archivos personales en cada una de las máquinas locales cuando soporte para litigación es requerido.

Un estudio realizado por Osterman Research indica que el 46% de las empresas hacen uso de copias de seguridad en cinta para "archivar" sus correos electrónicos. Se debe notar que el almacenamiento de "copia de seguridad" y "el archivo" sirve 2 propósitos diferentes. Copias de seguridad están dirigida a guardar datos actuales contra el evento de falla o desastre, mientras que el archivo protege los datos de tal manera que pueden ser accedidos cuando sea necesario. El costo de encontrar registros electrónicos para un proceso de descubrimiento, puede ser bastante alto, requiriendo meses de mano de obra de IT para escarbar en las cintas de copia de seguridad. Los sistemas de archivo de correo electrónico proveen funciones de búsqueda y obtención avanzadas. Estas permiten a los usuarios el rastrear mensajes de correo electrónico de una manera efectiva en costo y tiempo. Sin un efectivo sistema de archivo de correo electrónico, el encontrar un registro de correo electrónico es peor que tratar de encontrar una aguja en un pajar. En el caso Murphy Oil USA versus Flour Daniel, al defendido le fue ordenado restaurar e imprimir todos los correos electrónicos contenido en las 93 cintas de copia de seguridad y solventar los costos totales envueltos en la realización de esta operación cuyo valor total fue \$6.2 millones de dólares.

Las soluciones de archivo de correo electrónico permiten a los administradores configurar restricciones de acceso. Estas restricciones aseguran y protegen los derechos de propiedad intelectual así como también asegurar la integridad de datos y confidencialidad en

cumplimiento con los estatutos.

¿Cuáles son las razones primarias para archivar correo electrónico?

Hay cuatro razones predominantes para una empresa para archivar su correo electrónico. Estas son: cumplimiento legal, soporte para litigación, administración de almacenamiento y administración de conocimiento.

Cumplimiento legal

El nuevo ambiente regulatorio, es una de los principales razones detrás del incremento en la demanda de soluciones de archivo de correo electrónico. Es estimado que más de 10,000 regulaciones de cumplimiento han sido creadas alrededor del mundo. Controles más estrictos y penalidades más severas están forzando a las empresas a asumir el cumplimiento regulatorio más seriamente. En Marzo de 2004, Banco de América fue multado por \$10 millones de dólares por la Comisión de Seguridades y Cambio (SEC), por fallar en retener registros de correo electrónico por el tiempo estipulado por la regulación y por fallar en enviar la información solicitada por el SEC a tiempo.

Aunque en materia de datos, los estatutos regulatorios varían de acuerdo a la industria, todos los registros pertinentes a la actividad económica de las empresas están sujetos a cumplir con las regulaciones. Estos incluyen registros de empleados y clientes, correspondencia entre empresas y documentación financiera. Por ejemplo, el Acto Sarbanes - Oxley (SOX), afecta a todas las industrias e impone penalidades severas a cualquiera que deliberadamente altere o borre documentos con el intento de defraudar a terceros. Este acto necesita que los auditores retengan los papeles de auditoria por un mínimo de cinco años contados desde el final del año fiscal. Aunque esta es una ley de Estados Unidos, el Acto SOX es también aplicable a empresas Europeas listadas en Estados Unidos también como a empresas que hacen negocios con Estados Unidos. Para mayor información acerca de Sarbanes - Oxley, por favor visite <http://www.s-ox.com/>

Otras legislaciones definen requisitos para industrias reguladas específicas. Por ejemplo, la Comisión de Seguridades y Cambio (SEC) y la Asociación Nacional de Negociadores de Seguridades (NASD), son dos de los reguladores que gobiernan la comunidad financiera. Las reglas 17a-3/a-4 del SEC Rules y las reglas 3010/3110 del NASD, obligan a las empresas corredores de bolsa / negociadoras, a mantener y almacenar todos los correos electrónicos pertinentes a su actividad de mercado por un periodo mínimo de 6 años. Estas reglas también imponen que por los primeros dos años, esta documentación debe ser mantenida en un almacenamiento fácilmente accesible e indexado. Firmas de Inversión como Deutsche Bank Securities Inc., Goldman Sachs & Co., Morgan Stanley, Solomon Smith Barney Inc. y U.S. Bancorp Piper Jaffray Inc. fueron todas ellas multadas con \$1.65 millones de dólares cada una por no cumplir con la regla del SEC 17a-4 y por fallar en producir correos electrónicos

solicitados durante el curso de una investigación. Para mayor información acerca del SEC y del NASD por favor visite <http://www.sec.gov/> y <http://www.nasd.com/>.

Cuidado de la salud es otra industria altamente regulada. El Acto de responsabilidad de portabilidad de seguro de salud (Health Insurance Portability Accountability Act - HIPAA), cubre cualquier tipo de registros en forma de papel o electrónicos que contienen información personal y detalles relevantes a la historia medica de un individuo. Esta información es conocida como Información de salud protegida (PHI). Aunque presente probablemente en pocos mensajes de correo electrónico, todas las empresas están obligadas a administrar esta información de acuerdo a las regulaciones del HIPAA. Firmas que están sujetas a las regulaciones HIPAA incluyen proveedores de cuidados de salud, firmas aseguradoras de salud, manejadoras de reclamos de cuidados de salud y empleados que proveen servicios de salud. El periodo de preservación para registros médicos varía entre 5 a 6 años. Sin embargo, ciertos estatutos obligan la retención de tal documentación durante la vida completa del paciente e incluso dos años después de la muerte del paciente. Para mayor información acerca de HIPAA, por favor visite <http://www.hipaa.com/>.

La administración de comidas y medicinas (FDA), es la junta regulatoria que control alas firmas que producen las medicinas, dispositivos médicos, cosméticos y bienes comestibles. El conjunto de regulaciones que gobierna la administración de registro en estas industrias es conocido como GxP. Para mayor información acerca de FDA y sus regulaciones, por favor visite <http://www.fda.gov/>.

Agencias del gobierno también deben mantener archivados los mensajes de correo electrónico. Estas deben cumplir con las regulaciones dadas por el Acto de libertad de información (FOIA), el Acto Patriota, Administración del archivo nacional de registros (NARA), y otras entidades legislativas. Para mayor información, por favor visite <http://www.usgs.gov/foia/>, <http://www.archives.gov/>.

Aunque existen muchas regulaciones y cada una parece tener sus propios requisitos, el cumplimiento esta basado en tres conceptos principales:

1. **Permanencia de datos** – La noción de que los datos deben ser retenidos en su estado original sin ser alterados o borrados.
2. **Seguridad de datos** – La información retenida desde ser protegida contra todas las amenazas de seguridad las cuales incluyen acceso por personal no autorizado también como cualquier cosa que pudiera dañar físicamente o peligrar la disponibilidad de la información.
3. **Auditibilidad** – El concepto de tener información apropiadamente protegida pero fácilmente accesible a tiempo por personal autorizado a cualquier momento que se requiera.

No todos los correos electrónicos están cubiertos bajo las regulaciones a cumplir. Algunas excepciones incluyen spam que claramente no necesita ser guardado, y correos electrónicos personales, aunque este último puede ser solicitado como soporte para litigación durante una investigación.

Soporte para litigación

Casi todas las empresas en el curso de actividades de negocios se ven implicadas en demandas. El “descubrimiento” en litigación, es el proceso en el que las partes involucradas en una demanda se les es solicitado por una corte judicial, el enviar información que es relevante al caso. La empresa que recibe la solicitud de “descubrimiento”, esta obligada a buscar entre sus registros y luego enviar toda la información relevante / solicitada de una manera rápida. El costo de producir la información para litigación puede ser bastante grande y puede en algunos casos sobrepasar los daños causantes de la demanda. Esto es más común en empresas donde no tienen implementada una solución adecuada de archivo de correo electrónico. Por ejemplo, el costo para restaurar 77 cintas de copias de seguridad en el caso Zubulake versus Warburg (USB Bank), fue de \$165,954 dólares, y los costos relativos a la revisión fueron en total \$107,694 dólares.

Un problema con las solicitudes de descubrimiento es que no hay un tiempo específico de qué tan atrás en tiempo la empresa debe buscar. Es requerido para empresas que provean todas las copias del correo electrónico relevante a lo solicitado, sin importar que tan antiguas estas sean. La totalidad y disponibilidad de todos los registros solicitados y el tiempo requerido para extraer esta información, depende mucho de la administración de almacenamiento de correos electrónicos y del comportamiento del empleado. Documentación electrónica puede ser localizada en cada sitio y medio razonable. Esto incluye servidores de correo electrónico, archivos PST en los escritorios, portátiles, PDAs, cintas de copiad de seguridad y otros medios removibles. Correos electrónicos almacenados en almacenes locales de mensajes tales como discos duros individuales o normalmente otros medios removibles, es raramente beneficioso para el empleador. Aparte de los altos costos involucrados en la búsqueda en cada una de las máquinas en una empresa en una solicitud de descubrimiento, esto representa un riesgo de seguridad y de propiedad intelectual para la empresa. Además, la existencia de este almacenamiento de información de usuario final, es generalmente desconocido para los miembros del equipo de IT y puede ir sin notarse en una búsqueda de descubrimiento. Cuando correo electrónico no es almacenado en un archivo verdadero y centralizado, el restaurarlo consume una gran cantidad de tiempo y dinero normalmente mayor a \$25,000 dólares. Reglas recientes han reconocido que la empresa que provee la información debe correr con los costos de descubrimiento sin derecho a reembolso.

Información de soporte para litigación debe ser exacta, completa y posiblemente en su estado original. Debido a que sistemas de copias de seguridad son propensos a errores, entonces puede ocurrir pérdida o destrucción de datos. Una empresa que falle en enviar la información solicitada en un descubrimiento legal puede ser encontrada culpable de “Obstrucción”. Este es

un término legal utilizado para describir la destrucción impropia de evidencia (por ejemplo, borrado de correo electrónico de la empresa). Tales circunstancias pueden llevar a un veredicto ordenado por la corte a favor de la otra parte o puede llevar a la corte a asumir que la pérdida de información fue peligrosa para la parte que falló en producirla. Esto ocurrió en el caso Zubulake versus USB AG bank fue debido a la falla del banco al no entregar la evidencia de correo electrónico solicitada, juez del distrito Shira Scheindlin indicó al jurado para inferir que la evidencia no entregada era peligrosa para el banco. Otras consecuencias por “obstrucción” son grandes multas. Philip Morris International, una de las más grandes empresas de tabaco del mundo fue multada con \$2.75 millones de dólares por destruir correos electrónicos en violación a la orden 1999.

Administración de almacenamiento

Los almacenes de mensajes continúan creciendo significativamente. Es estimado que una de cuatro empresas esta experimentando un crecimiento en exceso de un 25% por año. Este dramático incremento en los requisitos de almacenamiento es principalmente atribuido al incremento en el uso del correo electrónico en general, agregando el aumento de adjuntos los cuales incrementaron el tamaño del correo electrónico promedio de 22 KB a 350 KB. De hecho, se estima que cerca del 50% de las empresas están brindando más de 150 MB de almacenamiento por usuario. Empresas usualmente hacen uso de cuotas de almacenamiento de correo electrónico para prevenir el crecimiento y degradación del rendimiento del servidor. La desventaja de las cuotas es el efecto que ellas tienen en la productividad del usuario final. Aparte de detener a los usuarios de usar su correo cuando la cuota es excedida, cuotas tiene más implicaciones serias. Por ejemplo, cuotas y los consecuentes bloqueos podrían hacer que los usuarios borren mensajes importantes de su buzón para poder abrir espacio para nuevo correo.

El incremento en el uso del correo electrónico también como el crecimiento relativo en el tamaño del correo electrónico también ha afectado la eficiencia, confiabilidad y velocidad de los servidores de mensajes. Un estudio realizado por Osterman Research afirma que los almacenes de correo electrónico están creciendo a un 37% anualmente. Consecuentemente, mantener correo electrónico en un formato de almacenamiento “en línea” necesitará más espacio físico de almacenamiento también como un incremento en la potencia del hardware para manejar estas cargas.

El cumplimiento de las regulaciones ha contribuido aún más al incremento en la demanda de almacenamiento al obligar a las empresas a preservar correo electrónico antiguo por tiempos predefinidos de tiempo.

Mientras que soluciones de almacenamiento pueden ser usadas para manejar el problema del crecimiento del almacenamiento de mensajes, una solución de archivo de correo electrónico provee una manera más versátil de manejar el problema. Aparte de centralizar sus registros de correo electrónico, una solución eficiente de correo electrónico almacenará los correos electrónicos en un formato comprimido, resultando en considerables ahorros en espacio de

disco al compararse con un almacén tradicional de correo. Además, los correos electrónicos serán automáticamente archivados tan pronto como ellos pasan a través del almacén de mensajes, y así los usuarios pueden limpiar sus buzones de correo sin preocuparse de perder correos electrónicos importantes. Adicionalmente, una solución de archivo de correo electrónico que permita a usuarios autorizados ver correos electrónicos desde un repositorio central, alentarán a los usuarios a hacerlo sin tener grandes archivos PST almacenados localmente. Considerando el hecho de que archivos PST usualmente toman entre 2 a 5 veces más de espacio físico que un archivo de correo electrónico, esto sumaría un considerable ahorro en espacio de disco.

Administración de conocimiento

Un sistema de correo electrónico de una empresa es un repositorio completo de conocimiento corporativo. Puede contener grandes cantidades de información de correo electrónico útil la cual es usualmente vital para un negocio y el permitir acceso a este activo corporativo puede hacer a los usuarios más productivos.

Un sistema de archivo de correo electrónico puede proveer apropiadas herramientas de administración de conocimiento (por ejemplo, organización de registros de correos electrónicos, funciones de búsqueda y recuperación avanzadas), que permita a IT y a usuarios finales un mejor manejo de la base de conocimiento contenida en el archivo de correo electrónico de la empresa.

Implementando y administrando soluciones de archivo de correo electrónico

Hay dos métodos principales para la implementación y administración de soluciones de archivo de correo electrónico:

- Una solución completamente dentro de la empresa
- Una solución alojada en la cual el archivo es mantenido en un centro de datos de un tercero.

Una solución de archivo de correo electrónico dentro de la empresa, involucra tener su repositorio de correo electrónico en un servidor dentro del edificio de la empresa. Probablemente la principal ventaja de un archivo propio es que la información sensible de la empresa es almacenada detrás de un cortafuegos de la empresa y es manejado por sus propios empleados. Esto asegura un mejor control sobre la integridad de los datos y confidencialidad. En este caso, la empresa confía enteramente e independientemente se sus propios recursos y puede entonces acceder al estado de cumplimiento a cualquier momento. La principal desventaja son los costos involucrados y el impacto inmediato que el sistema puede tener sobre el departamento de IT de la empresa. Para implementar un archivo de correo electrónico interno, la empresa debe comprar un programa adecuado de archivo de

correo electrónico también como el hardware (servidor) que alojará el archivo.

Soluciones alojadas en terceros, requieren bajos costos comparado con el costo de soluciones dentro de la empresa. Clientes pueden arrancar y ejecutar rápidamente sin invertir en hardware y empleados de IT. Costos de ejecución también son bajos debido a las nuevas capacidades y las actualizaciones de software/hardware son generalmente implementados por el proveedor. En soluciones alojadas, una aplicación de software localizada en el servidor de correo electrónico corporativo, captura correo electrónico y lo migra fuera de línea vía Internet a una bodega de datos del tercero para archivar. Usuarios autorizados pueden acceder los datos almacenados fuera de línea usando un navegador web o un cliente de correo electrónico compatible.

Sin embargo un estudio realizado por Osterman Research afirma que casi el 70% de las empresas prefieren una solución de archivo de mensajes que es operado completamente dentro de la empresa. Esta percepción es primariamente atribuida al hecho de las empresas se sienten más seguras cuando almacenan datos corporativos sensitivos dentro de la empresa, en vez de hacerlo en servidores de terceros afuera de la empresa (tal como archivo alojado fuera de la empresa). Además, las empresas que manejan sus propios sistemas de correo electrónico tienen la última palabra cuando las cosas se tiene que hacer, mientras que en un sistema alojado en un tercero, las prioridades de de la empresa compiten con la de aquellos que proveen el servicio. Tal limitación puede realmente poner a la empresa en un alto riesgo porque los registros archivados podrían estar incompletos y / o no se podrían recuperar en el tiempo requerido para una solicitud. Empresas deben también considerar la posibilidad de un proveedor que se salga del Mercado o que falle en proveer un servicio que cumpla con los estatutos. En tal evento, la empresa se verá forzada a cambiar el proveedor de servicio o cambiarse a una solución dentro de la empresa. En cualquier caso, el servicio de archivo sería interrumpido y dinero extra sería gastado.

Algunas empresas perciben las soluciones de archivo alojadas en terceros como una forma de transferir la responsabilidad a un proveedor de outsourcing, pero esto es una concepción errónea, ya que la responsabilidad continua recayendo en el dueño de los datos (tal como la empresa que emplea los recursos de la empresa de outsourcing).

¿Qué características debe tener una solución de archivo de correo electrónico?

- **Mínima intervención del usuario / automatización** – Los correos electrónicos de la empresa tienen que ser archivados automáticamente y con el mínimo de intervención humana posible.
- **Indexación de registros y capacidades de búsqueda** – Los correos electrónicos archivados deben estar indexados, especialmente el contenido de texto, para que las facilidades de búsqueda habiliten la extracción rápida de los registros para soportar

solicitudes regulatorias de auditoria o descubrimiento legal.

- **Política de control de retención de datos** – El sistema debe incluir opciones de configuración a través de las cuales la empresa puede definir su criterio de archivación. Estas opciones deben al menos permitir el archivo de buzones específicos y mensajes desde dominios específicos o desde direcciones de correo electrónico específicas. De esta manera, contenidos que no son necesarios tales como spam y otra correspondencia informal, es automáticamente excluida del archivo.
- **Seguridad / a prueba de alteración** – Un sistema de correo electrónico debe ser capaz de proteger los registros de cualquier pérdida, daño o mal uso. La autenticidad del registro (tal como preservación de un registro en su estado original), es uno de los requisitos claves en muchos de los contenidos de las regulaciones impuestas por las leyes. Además, programas de archivo deben incluir opciones de restricción de acceso.
- **Administración de acceso y usuarios finales a archivos** – Esta opción permite a la empresa utilizar su archivo de correo electrónico como un repositorio central de conocimiento desde el cual usuarios autorizados pueden extraer información requerida durante productividad. Un beneficio adicional es que habilita a usuarios autorizados tales como oficiales de cumplimiento a acceder ellos mismos a la información contenida en el archivo sin necesidad de soporte del equipo de IT.
- **Soporte para múltiples plataformas de mensajería** – El sistema de archivo debe soportar todas las principales plataformas de mensajería para asegurar estándares de compatibilidad.

Acerca de GFI

GFI es un destacado desarrollador de software que proporciona una única fuente para que los administradores de red dirijan sus necesidades en seguridad de red, seguridad de contenido y mensajería. Con una galardonada tecnología, una agresiva estrategia de precios y un fuerte enfoque en las pequeñas y medianas empresas, GFI es capaz de satisfacer la necesidad de continuidad y productividad de los negocios que tienen las organizaciones en una escala global. Fundada en 1992, GFI tiene oficinas en Malta, Londres, Raleigh, Hong Kong, Adelaide y Hamburgo que soportan más de 200.000 instalaciones en todo el mundo. GFI es una empresa enfocada a canal con más de 10.000 partners en todo el mundo. GFI es también Microsoft Gold Certified Partner. Se puede encontrar más información sobre GFI en <http://www.gfihispana.com>.

Referencias

Osterman Research - <http://www.ostermanresearch.com/>.

Tendencias del mercado de archivo de mensajes, 2005-2008.

Cómo evaluar y escoger una solución de archive de mensajes.

Diario de cumplimiento a Sarbanes-Oxley - <http://www.s-ox.com/>.

Lista de elementos a cumplir - <http://www.compliancepipeline.com/>.

Magazín Transformar - <http://www.transformmag.com/compliance/>.

Comisión de Seguridades y Cambios de EE.UU. - <http://www.sec.gov/>.

Asociación nacional de negociadores de seguridades (National Association of Securities Dealers - NASD) - <http://www.nasd.com>.

© 2007 GFI Software. Todos los derechos reservados. La información contenida en este documento representa la visión del momento de GFI sobre lo discutido a la fecha de la publicación. Como GFI debe responder a las condiciones de los cambios del mercado, no debe ser interpretado como obligación por parte de GFI, y GFI no puede garantizar la exactitud de la información presentada después de la fecha de publicación. Este Documento Blanco solo tiene propósito informativo. GFI NO DA GARANTIA, EXPRESA O IMPLICITAMENTE, EN ESTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor y sus logotipos son marcas registradas o marcas de GFI Software en los Estados Unidos y/o otros países. Todos los nombres de producto o empresas mencionados pueden ser marcas registradas de sus respectivos propietarios.