



“El 90 por ciento de los 100 principales sitios web se ha clasificado como sitios de redes sociales o de búsqueda y más del 47 por ciento de estos sitios admite contenido generado por los usuarios.”

**Websense Security Labs™,
2009**

Websense®

Soluciones Web Security Gateway

Las tecnologías Web 2.0 interactivas y dinámicas han transformado la web en una plataforma central de aplicaciones comerciales. Ahora, las aplicaciones tradicionales de relaciones con los clientes y de nóminas se realizan forma interactiva a través de la web, mientras que aplicaciones como las redes sociales se utilizan a diario para el reclutamiento, la generación de contactos y otros procesos empresariales. No obstante, Web 2.0 comporta un nuevo riesgo, ya que el contenido dinámico y generado por los usuarios hace que las tecnologías de seguridad tradicionales, como el antivirus y el filtrado de URL, resulten ineficaces. Estas tecnologías tampoco pueden ofrecer control sobre información confidencial saliente publicada en sitios Web 2.0.

Las soluciones Websense® Web Security Gateway lideran el mercado de puertas de enlace web seguras porque ofrecen la mejor protección contra amenazas Web 2.0 modernas con el coste total de propiedad más bajo. Son las únicas soluciones que ofrecen prevención de fuga de información de uso comercial y una administración unificada de implementaciones híbridas de nube / en los sistemas de la empresa. Las soluciones Web Security Gateway permiten a las organizaciones aprovechar la potencia de Web 2.0 sin tener que preocuparse por el malware, el contenido inapropiado o la divulgación de información confidencial.

Cómo funciona

Las soluciones Web Security Gateway inspeccionan el contenido entrante y saliente cuando atraviesa los límites corporativos para proteger a las empresas contra el malware web dinámico, prevenir la fuga de información confidencial saliente y mejorar la productividad de los empleados. La implantación de Websense TruHybrid™ es compatible con un appliance de implantación en los sistemas de la empresa, así como con plataformas de seguridad como servicio (SaaS), al tiempo que administra todo el entorno a partir de una única política e infraestructura de generación de informes. A diferencia de otros enfoques, los clientes de Websense tienen flexibilidad para elegir la plataforma o combinación de plataformas que mejor satisfaga sus requisitos operativos específicos sin incurrir en el gasto que supone gestionar múltiples sistemas.

Las soluciones Web Security Gateway ofrecen:

- **Prevención de fuga de información saliente y controles de cumplimiento de normativas:** La prevención de fuga de información de uso comercial integrada establece los controles necesarios para hacer posibles las comunicaciones salientes con destinos como el correo web y las redes sociales al tiempo que satisface las exigencias de cumplimiento de normativas para controlar la divulgación de información confidencial.
- **Protección contra malware:** el motor de clasificación avanzada (ACE por sus siglas en inglés) Websense TRITON™ protege contra ataques heredados basados en archivos, así como contra ataques dinámicos de secuencia de comandos que sortean las soluciones antivirus tradicionales.
- **Productividad de los empleados que utilizan Web 2.0:** el motor de clasificación avanzada TRITON elimina el contenido inapropiado proveniente de sitios Web 2.0 complejos, dinámicos y protegidos mediante contraseña que no se pueden clasificar con exactitud utilizando soluciones de filtrado de URL tradicionales.
- **El coste total de propiedad más bajo:** la consola TRITON y la implantación de TruHybrid de Websense reducen el número de appliances, de sistemas de administración y de proveedores a los que se debe respaldar en una empresa.
- **Cobertura de seguridad sistemática en toda la empresa:** la implantación de TruHybrid unifica políticas en todas las implementaciones en los sistemas de la empresa y de SaaS. Su política exclusiva se aplica de forma sistemática mientras los usuarios se mueven entre emplazamientos o trabajan desde casa.

“En el primer semestre de 2009, más del 80 por ciento de los 100 principales sitios albergaba contenido malicioso o contenía un redireccionamiento enmascarado a un sitio web no legítimo.”

Websense Security Labs, 2009

Motor de clasificación avanzada

Las soluciones Websense Web Security Gateway incluyen el motor de clasificación avanzada Websense TRITON, el motor de análisis de seguridad bidireccional más preciso* que combina el análisis entrante con la prevención en profundidad de fuga de información saliente. El motor de clasificación avanzada combina seguridad tradicional y técnicas de vanguardia de clasificación de contenido, como, por ejemplo, antivirus, filtrado de URL, servicios de reputación y tatuaje numérico para clasificar de forma precisa los riesgos entrantes y salientes. El motor de clasificación avanzada, que utiliza Websense ThreatSeeker® Network, analiza el contenido a medida que atraviesa la puerta de enlace con análisis de seguridad en tiempo real, clasificación de contenido en tiempo real y prevención de fuga de información de uso comercial.

Análisis de seguridad en tiempo real

La tecnología antivirus sola no puede seguir el ritmo de los ataques dinámicos y de secuencia de comandos que dominan el panorama de amenazas web. El análisis de seguridad en tiempo real patentado de Websense se enfrenta a estas amenazas de día cero por medio de la identificación de contenido malicioso sobre la marcha, sin necesidad de consultar bases de datos de ataques ya conocidos.

Clasificación de contenido en tiempo real

Many El filtrado de URL tradicional no puede clasificar de forma precisa buena parte de los sitios que se utilizan más habitualmente. Por ejemplo: una sola página de Google o Facebook puede contener una mezcla de elementos de contenido que abarque múltiples categorías, lo que impide aplicar una única categoría. En consecuencia, muchas organizaciones se ven forzadas a bloquear recursos valiosos indiscriminadamente o a ignorar políticas de uso aceptable y permitir el acceso ilimitado a destinos Web 2.0 dinámicos.

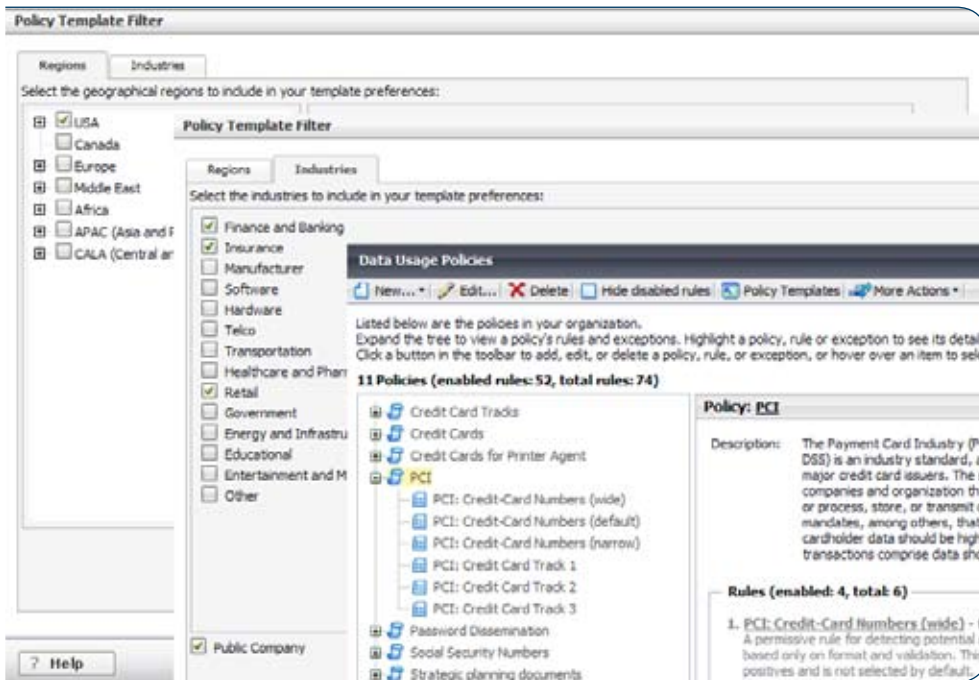
Las soluciones Web Security Gateway ofrecen clasificación de contenido en tiempo real para ampliar de forma precisa las políticas de uso aceptable a sitios Web 2.0 dinámicos por medio de la clasificación sobre la marcha de elementos de contenido dentro de cada página web. Si un elemento de contenido concreto infringe la política, este se puede eliminar de la página mientras que la información que cumpla con las normativas se permite. Esta funcionalidad exclusiva permite tener un amplio acceso a destinos comerciales Web 2.0 al tiempo que se mantiene la productividad y el cumplimiento de políticas de uso aceptable.

Prevención de fuga de información de uso comercial

La prevención de fuga de información de uso comercial integrada establece los controles necesarios para hacer posibles las comunicaciones comerciales salientes con destinos como el correo web y las redes sociales al tiempo que satisface las exigencias de cumplimiento de las normativas para controlar la divulgación de información confidencial. A diferencia de otros enfoques cuyas funcionalidades de prevención de fuga de información se limitan a la inspección de palabras clave o que requieren integraciones de terceros complejas, las soluciones Web Security Gateway ofrecen todas las funcionalidades de la solución de prevención de fuga de información líder del mercado de Websense para tráfico de red http, https y FTP. Incluye más de 800 políticas listas para su aplicación, tatuaje numérico para una inspección en profundidad del contenido y una generación de informes de cumplimiento exhaustiva.

La integración de la prevención de fuga de información web con las soluciones Web Security Gateway reduce de forma importante el coste total de propiedad porque elimina la necesidad de hardware de prevención de fuga de información de terceros dedicado en cada emplazamiento corporativo. En el caso de organizaciones con planes a largo plazo de prevención de fuga de información, la prevención de fuga de información web también ofrece una sólida protección de la inversión: una simple actualización de software es todo lo que se necesita para ampliar el control más allá de la web y abarcar otros tipos de tráfico (correo electrónico, mensajería instantánea y P2P), puestos de usuario e información en reposo (p. ej.: bases de datos, recursos compartidos, Exchange y SharePoint). Por consiguiente, para ampliar la cobertura de la prevención de fuga de información web a otros canales no se requiere una modificación. Se mantiene la política y las inversiones en infraestructura existentes.

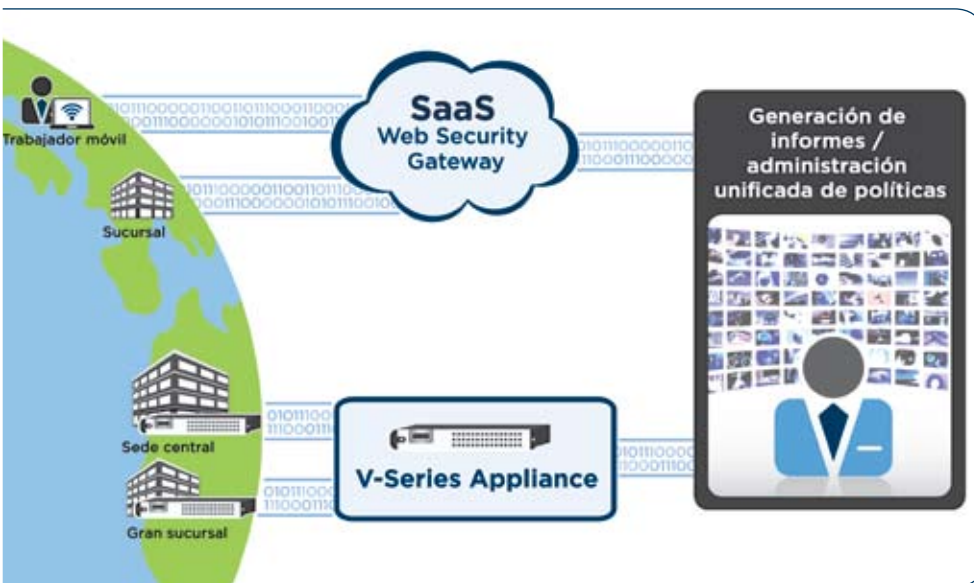
* <http://www.websense.com/content/tolly-report-reg.aspx>



Sencillos asistentes de políticas de prevención de fuga de información ayudan a los administradores a definir rápidamente políticas de mejores prácticas que cumplan los requisitos normativos regionales y específicos del sector.

Implantación de TruHybrid

La implantación de TruHybrid ofrece la flexibilidad para seleccionar una combinación de plataformas de implantación en los sistemas de la empresa y de SaaS al tiempo que administra todo el entorno con un sistema de administración unificada exclusivo. Con la plataforma SaaS, puede ampliar la seguridad a sucursales o usuarios móviles. Al mismo tiempo, puede implantar appliances de alto rendimiento en centros de datos, grandes sucursales y emplazamientos corporativos. Independientemente de la combinación de opciones de SaaS o de appliance elegida, usted define una sola política para toda la empresa en un lugar. Este enfoque unificado no sólo reduce el coste de gestionar implementaciones híbridas en los sistemas de la empresa / de SaaS, sino que también garantiza una cobertura de seguridad sistemática en todos los entornos.



La implantación de TruHybrid unifica la administración de implementaciones híbridas en los sistemas de la empresa / de SaaS.

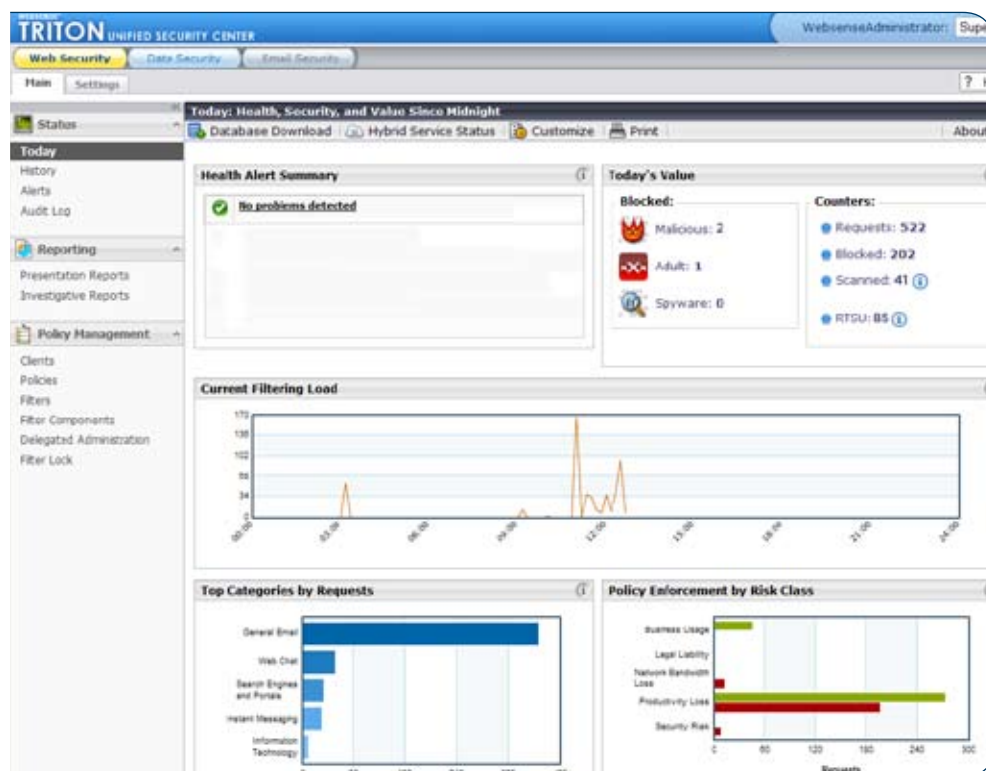
“Confiamos en el appliance de puerta de enlace web segura V10000™ de Websense para que nuestras enfermeras puedan obtener de forma rápida y segura la información que necesitan. Con el análisis en tiempo real y la capacidad para crear políticas flexibles en torno al uso de Internet, no me preocupa que nuestras enfermeras visitantes se topen con un sitio web infectado con código malicioso para el robo de información o que envíen accidentalmente datos confidenciales de los pacientes al lugar equivocado.”

Larry Whiteside

Director de Seguridad
Visiting Nurse Service
of New York

“Hasta un 57 por ciento de los ataques web maliciosos incluye código para el robo de información.”

Websense Security Labs, 2009



Los paneles de control interactivos de la consola TRITON ofrecen acceso instantáneo a la actividad de amenazas y de incumplimiento de políticas en cuanto esta se produce.

Control y visibilidad del tráfico SSL

El aumento del uso de tráfico SSL ha creado puntos flacos para los filtros de URL heredados y abre la puerta trasera a las amenazas y a la fuga de información. Las soluciones Web Security Gateway ofrecen visibilidad y control del tráfico SSL, lo que permite a las organizaciones aplicar una política a todas las comunicaciones web.

Controles de aplicaciones avanzados

El aumento de las aplicaciones de red, como, por ejemplo, la mensajería instantánea y el P2P, proporciona a los hackers un medio para perjudicar al negocio y robar información confidencial. Las soluciones Web Security Gateway controlan más de 125 protocolos de red y miles de aplicaciones para reducir el riesgo y prevenir la fuga de información desde aplicaciones no autorizadas. Las medidas relacionadas con las políticas van desde el simple bloqueo de aplicaciones hasta controles de ancho de banda altamente granulares.

Generación de informes y administración de seguridad de contenidos unificada

A Una característica importante también disponible con las soluciones Web Security Gateway, y solamente disponible a través de Websense, es la consola TRITON. Esta fusiona la administración de todas las soluciones de seguridad web, de la información y del correo electrónico de Websense en una única interfaz basada en web. Un panel de control intuitivo incluye más de 55 informes integrados y amplias funcionalidades de personalización para ayudar a clarificar la actividad de usuario, facilitar la resolución de problemas y continuar reduciendo el riesgo. El esfuerzo y el coste administrativo se reducen enormemente en comparación con soluciones de la competencia gracias a numerosas características fáciles de usar, como, por ejemplo, amplias funcionalidades específicas, asistentes de políticas, plantillas de configuración, un subsistema de programación y actualizaciones de contenido automáticas. Dado que con el tiempo la seguridad de contenidos necesita expandirse más allá de la seguridad web, las funcionalidades de administración unificada de la consola TRITON se pueden ampliar fácilmente para gestionar centralmente el correo electrónico y la prevención total de fuga de información.

Características	Ventajas
Implantación de TruHybrid	Reduce el coste total de propiedad y garantiza una política sistemática en toda la empresa por medio de la administración unificada de implementaciones en los sistemas de la empresa y de SaaS.
Prevención de fuga de información de uso comercial	Previene la fuga de información saliente y establece los controles de cumplimiento de las normativas necesarios. Reduce el coste total de propiedad porque evita una implantación compleja de la prevención de fuga de información.
Clasificación de contenido en tiempo real	Asegura el uso de propiedades web de contenido combinado dinámico y protegido mediante contraseña a través del filtrado de contenido sobre la marcha.
Análisis de seguridad en tiempo real	Protege a las organizaciones de malware porque identifica amenazas dinámicas, de secuencia de comandos y desconocidas sobre la marcha.
Consola TRITON	Reduce el coste total de propiedad y los costes de administración del proveedor por medio de la administración unificada de soluciones de seguridad web, de la información y del correo electrónico.
Antivirus integrado	Protege contra ataques de virus basados en archivos utilizando antivirus de terceros y antivirus web avanzados de Websense.
Filtrado web puntero con análisis de reputación avanzado	Habilita la política de uso aceptable de referencia y bloquea sitios maliciosos conocidos. El análisis de reputación multipunto incluye tipo de propiedad, reputación léxica, publicaciones Web 2.0, categoría de URL, vecino más próximo, reputación de búsqueda, historial, edad y geografía.
Actualizaciones en tiempo real de ThreatSeeker Network	Reduce la exposición a amenazas emergentes porque proporciona actualizaciones de seguridad cada cinco minutos.
Visibilidad del tráfico SSL	Permite la inspección de tráfico web cifrado con proxy SSL completo y administración de certificados integrada.
Control de aplicaciones	Minimiza el riesgo, mejora la productividad y reduce el coste del ancho de banda porque administra el uso de aplicaciones y protocolos de red.
Proxy web / memoria caché de uso comercial	Mejora el rendimiento y reduce el coste del ancho de banda al optimizar el tráfico. Admite configuraciones de proxy transparentes y explícitas.
Autenticación de usuarios flexible	Habilita la política basada en usuarios y grupos con autenticación flexible a través de Active Directory, LDAP, RADIUS, Novell y NTLM v2.
Alta disponibilidad y equilibrado de carga	Habilita la redundancia del sistema y la escalabilidad de gran empresa aprovechando el WCCP o balanceadores de carga externos.

Gartner ha colocado a Websense en el cuadrante de los líderes de su Cuadrante Mágico más reciente para enlace de puerta web segura.

Gartner, Inc.

“Magic Quadrant for Secure Web Gateway”* [Cuadrante Mágico para puerta de enlace web segura] por Peter Firstbrook y Lawrence Orans, 8 de enero de 2010

Disponibilidad de la plataforma de implantación

Las implementaciones en los sistemas de la empresa se pueden hacer con appliances Websense V-Series™ o con software que se ejecute en servidores de uso general. Las implementaciones de SaaS son compatibles con la solución Websense Hosted Web Security Gateway.

Websense, Inc.
San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

Websense Spain
Madrid, Spain
tel +34 91 28 44 750
fax +34 91 28 44 751
www.websense.es

Australia
websense.com.au

Brasil
websense.com/brasil

Colombia
websense.com/latam

Francia
websense.fr

Alemania
websense.de

Hong Kong
websense.cn

India
websense.com

Irlanda
websense.co.uk

Israel
websense.co.uk

Italia
websense.it

Japón
websense.jp

Malasia
websense.com

México
websense.com/latam

PRC
prc.websense.com

Singapur
websense.com

España
websense.com.es

Taiwán
websense.cn

UAE
websense.com

- **Appliances V-Series:** los appliances V-Series ofrecen rendimiento comercial, fiabilidad y una fácil implantación en los sistemas de la empresa. De eficacia probada en entornos Fortune 100, los appliances V-Series integran redundancia al nivel de los componentes al tiempo que son compatibles con una serie de características de implantación empresariales, como, por ejemplo, el equilibrado de carga y la alta disponibilidad. Los appliances V-Series también se han diseñado para que sean compatibles con futuras soluciones de Websense sin necesidad de utilizar hardware de actualización. De ese modo, aumenta la vida útil y el valor de la plataforma.
- **Hosted Web Security Gateway** las soluciones Websense Hosted Web Security Gateway trasladan los procesos de inspección de seguridad a 10 centros de datos redundantes y disponibles a escala global ubicados en la nube. Este modelo de suministro de SaaS no sólo acelera la implantación, sino que puede reducir de forma significativa los costes operativos al eliminar la necesidad de admitir hardware implementado en los sistemas de la empresa en cada emplazamiento corporativo. Los centros de datos de Websense cuentan con la certificación ISO 27001 para satisfacer los estrictos estándares de seguridad y disponibilidad que resultarían sumamente costosos de cumplir in situ en el caso de organizaciones individuales, especialmente en emplazamientos de oficinas remotas. Si Websense Hosted Web Security Gateway se implementa como una solución sólo de SaaS autónoma, ofrece la ventaja añadida opcional de la integración de seguridad del correo electrónico SaaS.



The Websense V10000™ Appliance

Websense Web Security Gateway Solution Options

Websense Web Security Gateway en cualquier lugar — para implementaciones que requieran TruHybrid implementado en los sistemas de la empresa* / administración de SaaS, prevención de fuga de información de uso comercial o el cliente de Websense Remote Filtering.

Websense Web Security Gateway — para implementaciones en los sistemas de la empresa*.

Websense Hosted Web Security Gateway — para implementaciones de SaaS.

Requisitos mínimos del servidor para las implementaciones de software:

Sistema operativo
Red Hat Linux v4,
actualización 5* o Windows Server 2003/
Server 2008*
 CPU: 2 procesadores dual-core de 2,8 GHz
 Memoria
4GB de RAM

Unidad de disco duro
Dos discos físicos:
* 100 GB para el sistema operativo y los datos provisionales y de aplicaciones, y 100 GB para la memoria caché*
* 100 GB (RAID 1 recomendado)*
 Interfaces de red
Dos interfaces Ethernet 10/100/1000

* Las implementaciones en los sistemas de la empresa se pueden hacer con appliances Websense V-Series o como software que se ejecute en servidores de uso general.

El Cuadrante Mágico es una representación gráfica de un mercado en y por un periodo de tiempo específico. Representa el análisis de Gartner de cómo determinados proveedores se enfrentan a los criterios para ese mercado, tal como los define Gartner. Gartner no promociona a ningún proveedor, producto o servicio representado en el Cuadrante Mágico y no recomienda a los usuarios de tecnología que elijan únicamente a aquellos proveedores situados en el cuadrante de los líderes. El objetivo del Cuadrante Mágico es servir solamente de herramienta de investigación y no pretende ser una guía específica de actuación. Gartner rehúsa todas las garantías, explícitas o implícitas, con respecto a esta investigación, incluidas todas las garantías de comerciabilidad y adecuación a un uso particular.