



“La fuga de información a través de la web es cuatro veces más probable que a través del correo electrónico.”

**Data Loss Open  
Security Foundation**

## Websense

# Soluciones para la prevención de fugas de datos e información

El impacto negativo de las filtraciones de información es claro: desde una reputación de marca manchada hasta multas reglamentarias. Un único incidente de fuga de información puede reducir la ventaja competitiva de una empresa, mermar la confianza del consumidor y resultar en multas por parte de los organismos reguladores. El problema se agrava con la rápida proliferación de dispositivos informáticos móviles, el uso extendido de dispositivos periféricos y el fácil acceso a software de intercambio de archivos; todo ello crea más oportunidades para la fuga de información. Websense ofrece soluciones integrales de protección de datos que ayudan a proteger su información esencial porque ofrecen visibilidad con respecto a qué información es confidencial, dónde está almacenada, cómo se transmite y quién la utiliza.

### Cómo funciona

Las soluciones de protección de datos de Websense® protegen a las organizaciones contra una amplia variedad de escenarios de fuga de información con un único sistema de definición de políticas para la prevención de fuga de información en la red y en los puestos de usuario, y el descubrimiento de información confidencial utilizando exploraciones tanto locales como de la red. Estas soluciones están disponibles como módulos individuales o como una suite integrada, lo que permite alcanzar el más alto nivel de flexibilidad de implantación.

Los módulos individuales disponibles en las soluciones de protección de datos de Websense ofrecen funcionalidades de prevención de fuga de información específicas para satisfacer las necesidades propias de cada organización. Websense Data Security Suite incluye todos los módulos y ofrece una solución integral.

Además, hemos integrado nuestra tecnología de prevención de fuga de información de uso comercial en nuestras soluciones de seguridad web y del correo electrónico para que las organizaciones puedan adoptar fácilmente una solución escalable completamente eficaz para prevenir las amenazas entrantes y gestionar los riesgos salientes relacionados con la fuga de información y el cumplimiento de las normativas. Ya sea partiendo de las soluciones de prevención de fuga de información integradas en las soluciones de seguridad web o del correo electrónico de Websense o partiendo de la implantación de módulos individuales de protección de datos, los clientes pueden escalar rápidamente su implantación a Websense Data Security Suite para proteger otros canales y aprovechar todas las funcionalidades de prevención de fuga de información.

### Websense Data Security Suite

Websense Data Security Suite incluye cuatro módulos integrados, gestionados mediante un único sistema de definición de políticas, que juntos ofrecen visibilidad y control sobre la fuga de información en la red y en los puestos de usuario, así como un descubrimiento de información exhaustivo a lo largo de los sistemas de almacenamiento de la empresa.

- **Websense Data Monitor:** controla la fuga de información en la red (web, correo electrónico, FTP y otros)
- **Websense Data Protect: (incluye Websense Data Monitor)** aplica controles automatizados y basados en políticas para bloquear, poner en cuarentena, redirigir a gateway de cifrado, auditar y registrar o notificar las infracciones a los usuarios
- **Websense Data Endpoint:** aplica controles automatizados basados en políticas para identificación de información en uso mediante aplicaciones y dispositivos periféricos en puestos de usuario; descubrimiento y clasificación local de información confidencial
- **Websense Data Discover:** descubre y clasifica información confidencial almacenada en depósitos de la empresa, con medidas correctivas personalizables, incluida la eliminación de archivos

(HTTP), web segura (HTTPS) y tráfico de correo electrónico (SMTP), lo que elimina la necesidad de soluciones de proxy de terceros adicionales y caras. Se integra con cualquier solución Websense Web Security, que direcciona el tráfico web saliente a Websense Data Monitor para el análisis.



“Hasta que recibimos el informe inicial de la solución Websense teníamos un nivel de visibilidad cero de la seguridad de nuestra información.”

**Roger McIlmoyle**  
director de Servicios de Tecnología de TLC Vision

### Websense Data Monitor

Websense Data Monitor es la solución líder de prevención de fuga de información de red para controlar y generar informes sobre fugas de información. A diferencia de las soluciones de la competencia que únicamente se centran en qué información confidencial se está fugando, Websense Data Monitor proporciona contexto automáticamente para identificar qué información de clientes se está fugando, así como información en tiempo real sobre quién está utilizando la información confidencial y adónde se dirige.

Websense Data Monitor ofrece:

- **Niveles inigualables de visibilidad** con respecto a aplicaciones Web 2.0, como, por ejemplo, conocimiento en tiempo real del destino para saber qué información se envía adónde y quién la envía.
- **Identificación exacta de la información confidencial** con un conjunto exhaustivo de tecnologías, como, por ejemplo, plantillas de políticas para la información regulada y el tatuaje numérico de información confidencial conocida.
- **Arquitectura flexible** para reducir los costes de implantación, como, por ejemplo, integración con Websense Web Security.

### Websense Data Protect

Basándose en las funcionalidades de Websense Data Monitor, Websense Data Protect es la solución líder de prevención de fuga de información de red para controlar y proteger automáticamente contra la fuga de información. Con niveles de control granulares y automatizados, Websense Data Protect ayuda a prevenir la fuga de información confidencial con una necesidad menor de esfuerzo y de intervención manual.

Websense Data Protect ofrece:

- Opciones de **aplicación automatizada basada en políticas**, como, por ejemplo, bloqueo, cuarentena, eliminación de archivos, cifrado, auditoría / registro y notificación de usuario en tiempo real.
- **Potente sistema de definición de políticas escalable** que ofrece visibilidad y control sobre la información confidencial en su red.
- Características y funcionalidades de **Websense Data Monitor**.

### Websense Data Endpoint

Websense Data Endpoint amplía la visibilidad y el control a los puestos de usuario con respecto a qué información confidencial está y debe estar almacenada, quién la utiliza, cómo se utiliza, adónde se transfiere y qué medida en tiempo real se toma para prevenir la fuga de información en el puesto de usuario. Websense Data Endpoint, que ofrece niveles inigualables de visibilidad y control con respecto a copiar / pegar, capturas de pantalla, impresiones y transferencia a medios extraíbles, puede aplicar políticas en el entorno de puesto de usuario con gastos generales mínimos.

Websense Data Endpoint ofrece:

- **Aplicación automatizada**, como, por ejemplo, bloqueo, control / eliminación de aplicaciones, auditoría / registro, confirmación y notificación de usuario.
- **Niveles inigualables de visibilidad y control** con respecto a copiar / pegar, acceso a archivos, capturas de pantalla e impresiones para aplicaciones de software de cliente (p. ej.: aplicaciones con comportamiento de red cifrado y evasivo como Skype), puestos de usuario (independientemente de la ubicación) y dispositivos periféricos.
- **Eficiencia operativa** con un impacto mínimo en el puesto de usuario, como, por ejemplo, opciones para desactivar el descubrimiento cuando se usa la batería.
- **Identificación exacta de la información confidencial** con un conjunto exhaustivo de tecnologías.
- **Descubrimiento y clasificación** de toda la información confidencial en el puesto de usuario.

## Websense Data Discover

Websense Data Discover es una solución sin agentes que explora de forma remota recursos compartidos, bases de datos, servidores de correo electrónico, depósitos de datos y escritorios de redes específicas para descubrir y clasificar información confidencial. Aplica automáticamente políticas de protección de datos en estos sistemas por medio de medidas de aplicación, como, por ejemplo, cifrado, eliminación de archivos, sustitución de archivos, notificación, auditoría y registro de incumplimientos de políticas.

Websense Data Discover ofrece:

- **Descubrimiento y clasificación de información confidencial** almacenada en la red en ubicaciones conocidas por medio de la exploración de variedades de direcciones IP específicas donde se sabe que reside información confidencial.
- **Reparación automatizada** de información confidencial no protegida en depósitos de datos.
- **Eficiencia operativa con un impacto mínimo en el rendimiento del servidor** porque las exploraciones se programan fuera de las horas punta.
- **Identificación exacta de la información confidencial** con un conjunto exhaustivo de tecnologías y mediante el empleo de plantillas de políticas para información regulada y el tatuaje numérico de información confidencial conocida.
- **Potente sistema de definición de políticas escalable** que ofrece visibilidad y control sobre toda la información confidencial.

## Reducción del coste y de la complejidad

Una cobertura integral de seguridad de prevención de fuga de información puede incluir múltiples implementaciones de software y hardware que pueden incrementar el coste total de la solución y aumentar la complejidad. El aumento en el coste y la complejidad es el mayor reto al que se enfrenta la mayoría de implementaciones de prevención de fuga de información. Con las soluciones de protección de datos de Websense, las organizaciones pueden empezar con una solución de prevención de fuga de información pequeña pero efectiva, como, por ejemplo, Websense Web Security Gateway, y escalar a Data Security Suite a medida que dichas organizaciones crecen y sus requisitos aumentan. Además, Data Security Suite es fácil de implantar y gestionar, y puede estar operativa en menos de una hora. Las funcionalidades de alta integración de las soluciones de protección de datos de Websense también minimizan la cantidad de hardware necesario para implantar una solución integral.

## Generación de informes y administración de seguridad de contenidos unificada

Management Las funcionalidades de generación de informes y administración son críticas en cualquier implantación de soluciones de seguridad. No sólo deben ofrecer interfaces intuitivas simples, sino que también tienen que unificar muchas tareas que a veces abarcan múltiples soluciones de seguridad. La consola Websense TRITON™ administra las soluciones de prevención de fuga de información de Websense. Esta consola combina las funcionalidades de administración y generación de informes para tecnologías web, del correo electrónico y de prevención de fuga de información en una sola interfaz basada en web, lo que resulta en un mayor grado de visibilidad y control. Incluye más de 55 informes incorporados, amplias funcionalidades de personalización, asistentes de políticas, plantillas de configuración y otras funcionalidades innovadoras para reducir el coste y simplificar enormemente las tareas de administración.

Ya sea que se implemente Websense Data Security Suite, uno de los módulos de protección de datos, o soluciones de seguridad web o de seguridad del correo electrónico, la consola Websense TRITON ofrece una única solución de administración para todas sus necesidades de seguridad, actuales o futuras.



“[En el caso de las filtraciones internas,] dos tercios fueron el resultado de acciones deliberadas y el resto fueron accidentales.”

### Verizon Business

2009 Data Breach [Filtración de información 2009]




## Visibilidad y control con conocimiento del destino

“El 31 por ciento de los incidentes de fuga de información sobre los que se ha informado se atribuye al robo de un ordenador portátil, al robo de un escritorio o a la pérdida de soportes..”

**DatalossDB**

Open Security Foundation



**Alerta de la competencia**

---

**Datos:** PCI e información de identificación personal  
**Fuente:** 10.14.222.21  
**Canal:** Web  
**Destino:** 10.14.222.21

VS



**Alerta de Websense**

---

**Base de datos:** PCI e información de identificación personal, y de datos de clientes  
**Fuente:** Joe User x1234,  
 juser@company.com  
 Cargo: asociado  
 Departamento: Finanzas  
 Manager: Jane Manager x1234  
 jmanager@company.com  
**Canal:** Web  
**Destino:** mail.google.com  
**Tipo:** sitio de correo web personal  
**Ubicación:** Mountain View, CA

- Contexto limitado
- Más trabajo para el administrador de TI

Considere una alerta típica de fuga de información en la que sólo consten la dirección IP y el canal de aplicación, lo que hace que sea el director de TI el responsable de determinar a quién se debe notificar y qué destinos específicos pueden estar recibiendo información confidencial.

- Conocimiento del usuario y del destino
- Corrección más rápida

Con Websense Data Monitor resulta fácil ver que un usuario en Finanzas (**quién**) ha perdido la información de la Industria de Tarjetas de Pago (PCI) y de identificación personal por un canal web (**cómo**), a través de una URL de correo web específica (**dónde**): esto ofrece visibilidad *de manera eficiente*. Esta alerta también es relevante y fácilmente comprensible, dado que se genera en tiempo real, por lo que proporciona datos de contacto, cargo y cualquier otra cosa que ofrezca la integración con Websense Web Security.

## Conocimiento de aplicaciones y control de dispositivos en los puestos de usuario

Los empleados pueden generar riesgo al copiar datos en dispositivos de almacenamiento periféricos desde aplicaciones locales. Si un empleado copia datos de una aplicación de la empresa en software de correo electrónico local, Websense informa de este suceso con datos sobre el usuario, el puesto de usuario, la información confidencial, la aplicación y el destino de esa información. Otras soluciones DLP de puesto de usuario no ofrecen suficiente visibilidad con respecto a aplicaciones y datos, por lo que bloquean acciones que, en realidad, pueden ser actividades comerciales legítimas.

## Descubrimiento exhaustivo para una corrección eficaz

Una vez que se ha producido la filtración de información, un inventario actual de esos datos ayuda a determinar las posibles fuentes de la fuga. Websense Data Discover utiliza la exploración en red de los repositorios de datos para encontrar información confidencial en ubicaciones conocidas, clasificar esa información e iniciar la medida correctiva; por ejemplo: el cifrado o la eliminación de archivos. La visualización de la gestión de incidentes incluye un enlace al archivo específico, la categoría en la que se incluyen esos datos (datos con huella digital o información regulada), el propietario del archivo (para asignar el incidente para su corrección), y cualquier medida correctiva que ya se haya aplicado para tratar la infracción. Si se utiliza con Websense Data Endpoint, que descubre datos en uso mediante un agente de software localmente, la solución ofrece un descubrimiento exhaustivo escalable para sistemas en línea y fuera de línea.

Características	Ventajas
Opciones de aplicación en tiempo real automatizadas en toda la red, puesto de usuario y depósitos de datos descubiertos	<ul style="list-style-type: none"> <li>• <b>Opciones de aplicación flexibles;</b> por ejemplo: notificación de usuario, auditoría / registro, etc.</li> <li>• <b>Tráfico de red:</b> poner en cuarentena, bloquear, direccionar a puerta de enlace de cifrado de terceros y eliminar contenido</li> <li>• <b>Actividad de puesto de usuario:</b> bloquear mover / copiar / imprimir información confidencial de aplicaciones a dispositivos externos, bloquear imprimir pantalla, notificación de usuario y confirmación / auditoría / registro de usuario</li> <li>• <b>Descubrimiento:</b> eliminación o sustitución (utilizando credenciales y secuencias de comandos automatizadas), y cifrado (integración de terceros con cifrado de archivos Voltage) de datos almacenados</li> </ul>

Características	Ventajas
Prevención de fuga de información para aplicaciones de seguridad como servicio (SaaS)	<ul style="list-style-type: none"> <li>• <b>Garantizar que la información confidencial sólo se cuelgue en una aplicación de SaaS identificada y aprobada</b></li> <li>• <b>Determinar el tipo de información que se puede descargar localmente desde una aplicación de SaaS</b></li> </ul>
Funcionalidad Smart Detection para detectar fugas de información a lo largo de múltiples canales de comunicación	<ul style="list-style-type: none"> <li>• <b>Detectar</b> pequeños volúmenes de información confidencial enviados a través de múltiples canales de comunicación</li> <li>• <b>Detectar</b> grandes volúmenes de fuga de información a partir del total de información confidencial enviada durante un periodo de tiempo específico</li> </ul>
Visibilidad con respecto a numerosos canales de red por medio de la monitorización pasiva del tráfico	<ul style="list-style-type: none"> <li>• <b>Monitorización de la Web</b> en red (HTTP), web segura (HTTPS), correo electrónico (SMTP), mensajería instantánea (AOL, Yahoo y MSN), FTP, impresión (agente de OCR opcional) y contenido Web 2.0 dinámico</li> <li>• <b>Reducir las infracciones</b> en un 50 por ciento con notificación de las infracciones al usuario</li> </ul>
Visibilidad con respecto al dispositivo, aplicación y almacenamiento de contenido de información confidencial en sistemas de usuario final	<ul style="list-style-type: none"> <li>• <b>Gestionar el riesgo de fuga de información</b> debido a la movilidad de usuario y al uso indebido de la información</li> <li>• <b>Conocimiento de la ubicación:</b> aplicar políticas dentro y fuera de la red, fuera de línea</li> <li>• <b>Portabilidad:</b> almacenamiento local de huellas digitales con ocupación de almacenamiento mínima</li> <li>• <b>Monitorización de dispositivos y control de unidades de almacenamiento extraíbles</b>, discos duros externos, imprimir, grabar en CD/DVD, copiar / pegar / imprimir pantalla en el portapapeles y acceso a archivos</li> <li>• <b>Monitorización de aplicaciones</b> activadas por el usuario, grupos de usuarios, aplicación predefinida o grupos de aplicaciones</li> <li>• <b>Clasificación</b> por tipo de información regulada, como, por ejemplo, números de tarjetas de crédito</li> </ul>
Descubrimiento de información confidencial en depósitos de datos locales y de red	<ul style="list-style-type: none"> <li>• <b>Descubrimiento exhaustivo:</b> exploraciones de red y exploraciones locales (por medio del agente de software del puesto de usuario); exploraciones ad hoc o programadas</li> <li>• <b>Cobertura:</b> exploración de bases de datos basada en red, recursos compartidos, Exchange y SharePoint; exploración local basada en tipo de archivo, tamaño y antigüedad</li> <li>• <b>Identificación:</b> más de 400 tipos de archivo, incluidos PST de Microsoft Exchange; huellas digitales de archivos y plantillas de cumplimiento</li> </ul>
Identificación de datos incorporada utilizando tecnologías Precise ID™ patentadas	<ul style="list-style-type: none"> <li>• <b>Identificación automatizada exacta de la información confidencial:</b> palabras clave, diccionarios, huella digital, expresiones habituales, umbrales, contexto, proximidad y correlación para información no estructurada y estructurada (p. ej.: base de datos)</li> <li>• <b>Detección eficaz:</b> reducir los falsos positivos y la perturbación del negocio al ignorar datos si no corresponden a información del cliente (utilizando huellas digitales) o si están por debajo del umbral especificado</li> </ul>
Opciones de implantación flexible; por ejemplo: proxy web incorporado e integración con proxies web de terceros	<ul style="list-style-type: none"> <li>• <b>Integración con Websense Web Security:</b> direccionar tráfico HTTP, HTTPS y FTP para el análisis con Websense Data Security mediante protocolo ICAP</li> <li>• <b>No se necesitan soluciones adicionales:</b> HTTP, SMTP, mensajería instantánea, FTP y HTTPS (con Websense Web Security, para proxy web)</li> <li>• <b>Flexible y rentable:</b> (1) modo de monitorización o de protección, (2) puerto de tránsito / SPAN o en línea / derivador, (3) con Websense Web Security o un proxy web estándar, (4) con Websense Email Security o un MTA de conformidad con SMTP</li> <li>• <b>Eficacia:</b> exploraciones de descubrimiento programadas si el sistema no funciona con batería (puesto de usuario); fuera de las horas punta; (cobertura) basada en la red frente a (rendimiento) basado en agente; listas de excepciones en clasificación IP para el descubrimiento de la red</li> <li>• <b>Implantación del agente de puesto de usuario:</b> Microsoft SMS u otros métodos; evitar un conflicto con el antivirus y cortafuegos personales; implantación escalonada con perfiles de usuario; activar / desactivar agente</li> <li>• <b>Protección de la inversión:</b> <i>implantar los módulos escalonadamente, según se requieran</i></li> </ul>



“[Las soluciones Websense] ofrecen un nivel de precisión líder en el sector y buscan automáticamente el contenido presente en toda nuestra organización e identifican dónde reside nuestra información confidencial.”

**Addison Avenue  
Federal Credit Union**  
Cliente de Websense  
Data Discover

**Especificaciones técnicas:**

**Especificaciones técnicas de Websense Data Security Suite**

*Véase la Guía del usuario para más detalles*

**Protector DSS** (componente de monitorización)

**Recursos del sistema**

*Véase el documento de hardware aprobado para más detalles*

Proveedores aprobados: IBM, HP, Dell, Network Engines

Procesadores Intel Xeon Dual o Quad Core  
RAM de 1, 2 y 4 GB (DIM totalmente introducido en memoria intermedia)

Mínimo 74 GB, unidades de disco duro de conexión "en caliente"

NIC 1000/100/10 Mbps

**Recursos de software (incluidos)**

Sistema operativo Linux reforzado con software de Websense Data Monitor o Data Protect

**Servidor DSS** (componente de gestión)

**Recursos del sistema**

Dos procesadores Intel o AMD de 2,4 GHz o mejor  
RAM de 4 GB

Cuatro discos duros SCSI U320 de 74 GB y 15K RPM

(mínimo) en RAID 1+0

NIC 1000/100/10

**Recursos de software**

Windows Server 2003 edición R2 estándar, último Service Pack

**Puesto de usuario DSS** (agente de software del puesto de usuario)

**Recursos del sistema**

Pentium 4 de 1,8 GHz o superior

• Mínimo RAM de 512 MB en Windows XP, RAM de 1 GB en Windows Vista o Windows Server 2003

• Mínimo 100 MB de espacio libre en el disco duro

**Recursos de software**

Sistemas operativos compatibles

• Windows XP (32 bit)

• Windows Vista (32 bit)

• Windows Server 2003 (32 bit)

**Números de pieza y descripción**

SKU: WDSS-X-XXXX-X

Descripciones: Opciones de

Websense Data Security Suite: nº de usuarios, soporte, agente de impresión, puerta de enlace de contenido, duración de la suscripción y usuarios nuevos / renovados / adicionales.

**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

**Italia**  
websense.it

**Brasil**  
websense.com/brasil

**Japón**  
websense.jp

**Colombia**  
websense.com/latam

**Malasia**  
websense.com

**Francia**  
websense.fr

**México**  
websense.com/latam

**Alemania**  
websense.de

**PRC**  
prc.websense.com

**Hong Kong**  
websense.cn

**Singapur**  
websense.com

**India**  
websense.com

**España**  
websense.com.es

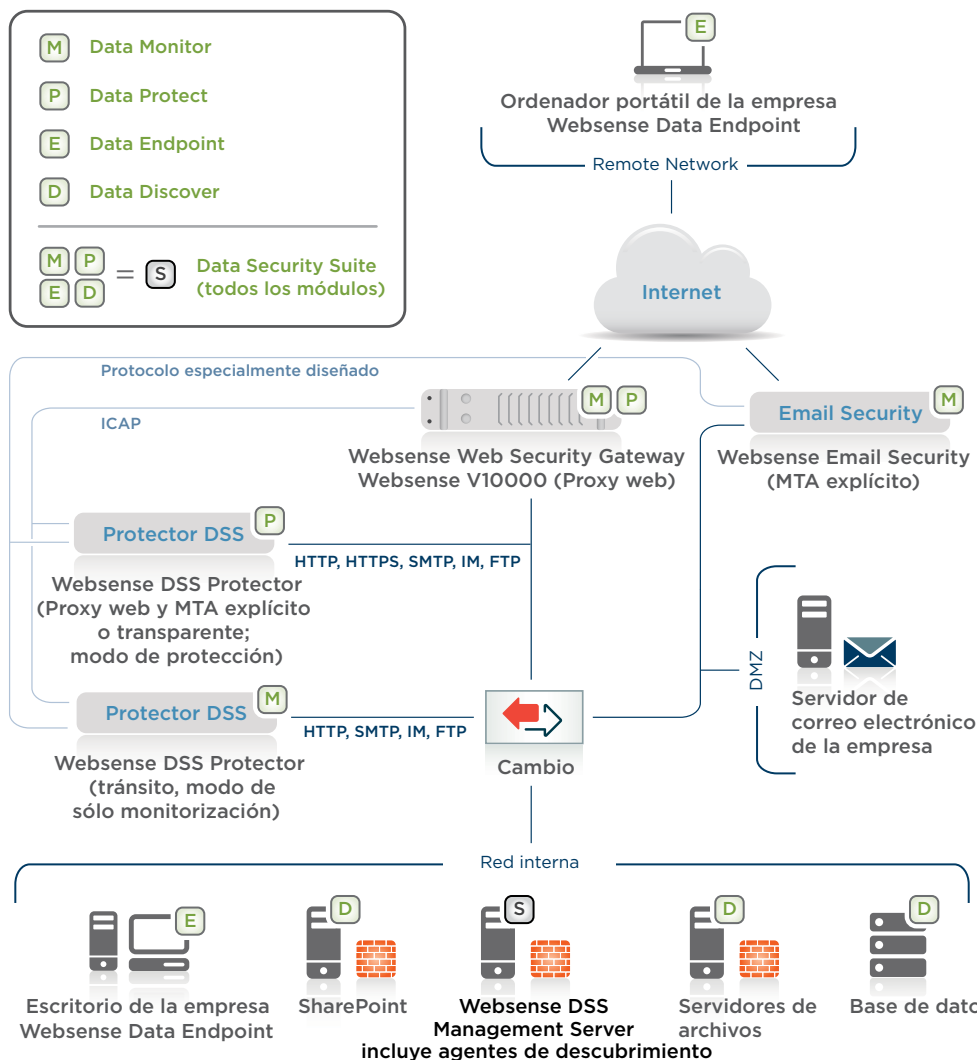
**Irlanda**  
websense.co.uk

**Taiwán**  
websense.cn

**Israel**  
websense.co.uk

**UAE**  
websense.com

Características	Ventajas
Plantillas de políticas integrales y actuales, política centralizada y generación de informes y gestión de incidentes	<ul style="list-style-type: none"> <li>• <b>Asistentes incorporados para mayor facilidad:</b> normativas regionales y del sector (p. ej.: PCI, LOPD española, Graham-Leach-Bliley, HIPAA y SOX); comprobaciones predefinidas: PII (información de identificación personal), PHI (información sanitaria personal), PCI (datos de la tarjeta de crédito) y PFI (información financiera personal).</li> <li>• <b>Aplicar políticas coherentes:</b> red, puesto de usuario y depósitos de datos</li> <li>• <b>Estamos al tanto de las normativas, de manera que no tendrá que:</b> investigar equipos dedicados ni actualizar las plantillas regularmente</li> <li>• <b>Informes incorporados para los auditores y ejecutivos:</b> distribuir informes de cumplimiento protegidos contra modificaciones (PDF) con información sobre el número total de incidentes por...</li> <li>• <b>Red:</b> grupo de usuarios, política, normativa, medida de aplicación, etc.</li> <li>• <b>Puesto de usuario:</b> canal de aplicación / dispositivo, grupo de usuarios, política, normativa, medida de aplicación tomada, etc.</li> <li>• <b>Descubrimiento:</b> dirección IP, tipo de / nombre del depósito, información confidencial (tipo, archivo / registro específico), propietario de la información y medida correctiva</li> </ul>



Para más información, para obtener una versión de evaluación gratuita de las soluciones de protección de datos de Websense o para ver una demostración en línea, vaya a [www.websense.com/evaluations](http://www.websense.com/evaluations).