



Un libro blanco de Websense®

# Protección de la información esencial

Garantizar la seguridad de los cimientos de su plataforma comercial en Internet

Internet puede ser, a día de hoy, la herramienta de productividad empresarial más importante. Sin embargo, el uso sin límites de esta plataforma comercial puede poner en peligro un activo aún más crítico para las empresas: su información esencial. La información en riesgo puede ir desde propiedad intelectual sensible hasta balances financieros, pasando por información de los clientes y los empleados.

Los directores de seguridad deben dejar de centrarse en proteger las infraestructuras contra ataques del exterior –un modelo adecuado para las fronteras perimetrales e Internet entendido únicamente como fuente de contenido– para hacer hincapié en proteger la información esencial de amenazas combinadas y fugas accidentales o malintencionadas, en línea con la Web 2.0 e Internet como plataforma comercial.

Los requisitos de la seguridad web, la seguridad del correo electrónico y la prevención de fugas de información han cambiado. Le invitamos a seguir leyendo para descubrir cómo.

- [Dónde y por qué fracasan los enfoques tradicionales](#)
- [En qué sentido la precisión y el contexto son la clave de una solución de seguridad efectiva y centrada en la información](#)
- [Qué hacer para proteger la información esencial y decir Sí a –y no bloquear– los procesos empresariales que aprovechan las innovaciones de la Web 2.0 y la poderosa plataforma comercial que es Internet](#)

## Introducción

Hoy en día, Internet afecta a todas las facetas y activos de las empresas. Las organizaciones eficaces dan mucha importancia a Internet como plataforma comercial, mediante el software como servicio y las aplicaciones basadas en web, el teletrabajo y los ecosistemas empresariales ampliados. La plataforma Web 2.0 ofrece ventajas competitivas y nos conduce al concepto de empleado 2.0, el trabajador siempre conectado, en cualquier lugar y en cualquier momento.

Las empresas del pasado ocultaban el código fuente, la investigación en productos y servicios patentados, los balances financieros y la información personal en servidores seguros o detrás de segmentos aislados de la red. Por el contrario, las empresas que miran hacia adelante permiten que esta información esencial circule libremente dentro y fuera de sus límites.

Para los directores de seguridad, la plataforma de Internet es a la vez una amiga y una enemiga. La Web 2.0 permite alcanzar unos niveles sin precedentes de colaboración e intercambio de información, y las empresas que cierran la puerta a las oportunidades que ofrece la Web 2.0 se arriesgan a perder su ventaja competitiva. No obstante, la Web 2.0 también trae consigo un nuevo tipo de riesgo: las amenazas vinculadas a Internet que aprovechan al máximo las nuevas tecnologías y vulnerabilidades. Las amenazas ya no se centran solo en el centro o en los extremos de la red, sino que ahora utilizan la Web 2.0 y la convergencia de las comunicaciones para integrarse de manera invisible en las operaciones cotidianas.

Y tampoco todos los riesgos vienen de fuera: la facilidad de acceso y la transparencia de Internet como plataforma han aumentado los riesgos que provienen del interior de la organización. Da igual que se trate de causar problemas de responsabilidades para la empresa por medio de contenido inadecuado, de reducir la productividad o de permitir fugas accidentales o malintencionadas de información empresarial esencial: los riesgos asociados a Internet hacen que los directores de seguridad tengan que hacer frente a problemas de seguridad cada vez más complejos.

Para adaptarse a estos cambios, también es necesario que evolucionen las protecciones de la información y de la red. Las defensas con un enfoque de tipo “bueno o malo”, basadas en comportamientos o en firmas y que diferencian el tratamiento de la red y de los puestos de usuario no protegen contra estas nuevas amenazas. Y lo que es aún peor: estos enfoques se basan en un modelo simplista de “activar o desactivar” el acceso o el bloqueo, lo que puede limitar seriamente el uso de Internet como plataforma empresarial. Ninguna empresa debería “desconectar” Internet. Internet es una herramienta comercial que debe administrarse y protegerse adecuadamente, como cualquier otro activo significativo de la organización. Los directores de seguridad deben encontrar un modo de decir Sí a estos avances con la confianza de que la información esencial de la empresa está a buen recaudo.

**400 millones de dólares: el valor de los secretos comerciales robados por un científico de DuPont para venderlos a una empresa china de la competencia<sup>1</sup>**

## Una protección adecuada de la información esencial

La aplicación de una protección adecuada es tan vital como subjetiva. Cada empresa debe proteger su información sensible y sus flujos de trabajo de una manera acorde con su entorno, riesgos y postura con respecto al riesgo. Analicemos los retos actuales y las soluciones disponibles.

### La información sensible y regulada, ¿se puede identificar? ¿Se puede prevenir su fuga?

**La situación:** La información es, hoy en día, la moneda de las organizaciones. Bases de datos, repositorios de documentos, aplicaciones para compartir archivos, sistemas de archivos de usuarios finales y dispositivos de almacenamiento portátiles son los lugares en los que se almacena y desde los que se accede a la información. Se intercambia dentro de la organización y se comparte con distribuidores, socios comerciales, usuarios finales, consumidores, instancias gubernamentales y muchos otros agentes externos.

**El problema:** A menudo, esta información se almacena, utiliza e intercambia de manera inadecuada. Además, cada día es objetivo de más ataques y robos. No proteger la información puede traducirse en el incumplimiento de normativas, multas, pleitos, pérdidas de ventajas competitivas, daños en la imagen de marca e incluso violaciones de la seguridad nacional. La proliferación de aplicaciones basadas en web y del intercambio de información agravan estos riesgos.

**La respuesta actual:** Las herramientas tradicionales de prevención de fugas de información se fundamentan en controles simplistas de “encender y apagar” basadas en tecnologías primitivas de identificación de la información. Por ejemplo, un sistema sencillo que “adivine” el riesgo en función de la aparición de ciertas palabras clave puede generar falsos positivos o detectar muchas coincidencias que, en realidad, no constituyan ningún tipo de infracción. Además, estos resultados suponen barreras para la transmisión y recuperación de archivos e información. Bloquear el movimiento de la información o eliminar información en reposo con este enfoque cargado de falsos positivos puede llegar, literalmente, a detener el flujo de información y, por extensión, las propias operaciones empresariales. Además, estas soluciones de “encender y apagar” generalmente no toman en consideración las políticas o el flujo de trabajo de las organizaciones, de modo que no permiten adaptar los controles a los cambios en las necesidades empresariales.

Unos funcionarios japoneses, que nunca deberían haber tenido esta información en sus sistemas, descargaron información clasificada sobre el sistema de defensa antimisiles AEGIS de los Estados Unidos durante un intercambio de archivos de pornografía.<sup>2</sup>

Un estudio de la American Management Association afirmaba que el 18% de empresas bloquean el acceso de sus empleados a blogs externos.<sup>3</sup>  
¿Por qué se preocupan las empresas de qué blogs visitan sus empleados? Cisco fue demandada por el blog externo de un empleado.<sup>4</sup>

“Las amenazas relacionadas con la web son tan virulentas que incluso las empresas a las que no les preocupa la pérdida de la productividad no las pueden ignorar.” – Burton Group.<sup>5</sup>

<sup>2</sup> <http://www.infosecnews.org/hypermail/0704/13040.html>

<sup>3</sup> <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/>

<sup>4</sup> <http://www.forbes.com/technology/forbes/2008/0407/044a.html>

<sup>5</sup> Informe “Web Filtering: Completing the Evolution from Acceptable-Use to Serious Malware Defense”.  
Burton Group Security and Risk Management Strategies, 1 de enero de 2008

### ¿Pueden los directores de TI decir Sí a los blogs?

**La situación:** Los blogs son un gran ejemplo de intercambio de información y contenido generado por los usuarios de la Web 2.0. Los blogs pueden ayudar, por ejemplo, a una organización financiera a descubrir empresas en las que invertir, a una empresa del sector de los medios de comunicación a juntar ideas para guiones o a una empresa de tecnología a buscar oportunidades en el mercado y aumentar el conocimiento de su marca.

**El problema:** Intercambiar información inocente está bien, pero ninguna entidad quiere que sus usuarios tengan problemas a causa de las vulnerabilidades de un blog, introduzcan contenido inadecuado en la red de la organización, pierdan el tiempo o, lo que es todavía peor, publiquen información sensible de los clientes, nuevos guiones o propiedad intelectual. Recordemos que estos asuntos implican responsabilidad para la organización.

**La respuesta actual:** Las soluciones de seguridad del contenido y la red tradicionales sólo pueden responder prohibiendo totalmente la comunicación con la blogosfera o permitiéndola sin restricciones, con todos los riesgos que ello implica. Esta respuesta tan radical no está en línea con las necesidades empresariales de intercambio de información y uso de herramientas modernas.

### ¿Hay herramientas que puedan diferenciar con precisión entre contenido Web 2.0 bueno y malo?

**La situación:** La Web 2.0 es algo muy diferente del mundo de sitios web informativos con sencillas categorías de contenido. La Web 2.0 utiliza la programación dinámica para construir páginas web que presentan contenido cambiante para adaptarse a las circunstancias, el historial y los atributos del usuario. Y no hablamos solamente de la visita para relajarse a MySpace, sino de webs comerciales –como Wikipedia, LinkedIn, YouTube y Google– que permiten la investigación legítima y las operaciones comerciales.

**El problema:** Los cambios en las tecnologías de Internet permiten que muchos criminales pongan la información confidencial en su punto de mira y busquen su revelación accidental. Además del contenido aceptable y seguro, los sitios Web 2.0 también pueden albergar, de manera transitoria, malware y contenido nocivo sin supervisión ni regulación alguna. Ya no hay botones de tipo “haga clic para aceptar” para alertar a los usuarios. Los enlaces corruptos, widgets maliciosos y secuencias de comandos incrustadas introducen el malware en el contenido y en las páginas web. Los usuarios que visiten sitios benignos pueden ser redirigidos a sitios que exploran el ordenador del usuario en busca de información sensible, contraseñas y vulnerabilidades.

**La respuesta actual:** Las respuestas actuales giran alrededor de conceptos tradicionales de bloqueo basados en la calificación, buena o mala, de cada sitio web. Estas soluciones han quedado atrás con respecto a los cambios en lo referente a la vulnerabilidad del contenido. Añadir la variable de la reputación no es suficiente para hacer frente a estas amenazas basadas en el contenido. Por ejemplo, la reputación de MySpace varía en función del contenido que se sirva en cada página, o cuando sitios fiables como MSNBC pierden su fiabilidad a nivel de contenido, la reputación es totalmente irrelevante. Sin que este contenido se considere parte integral del estudio detallado de cada sitio y de su clasificación, las soluciones tradicionales seguirán bloqueando páginas seguras y permitiendo el acceso a sitios peligrosos, lo que no permite realizar un uso empresarial seguro de la web.

Uno de los 26.000 sitios afectados por una vulnerabilidad en un motor de búsqueda, MSNBC fue pirateado justo antes de la retransmisión del torneo de baloncesto universitario de la NCAA, en marzo de 2008.<sup>6</sup>

La presencia cada vez más común de amenazas multicanal está haciendo cambiar el mercado de la seguridad de los contenidos. Actualmente, un enfoque de silos para el filtrado web y del correo electrónico ya no es una respuesta adecuada a estas amenazas. – Forrester Research<sup>7</sup>

#### ¿Las soluciones de seguridad pueden proteger a los usuarios y la información de ataques que combinen el correo electrónico y la Web 2.0?

**La situación:** Las aplicaciones web y el correo electrónico están intrínsecamente relacionadas en aplicaciones de correo web y los mensajes con contenido HTTP. Estos canales de comunicación también se utilizan en otras aplicaciones empresariales, como las soluciones de ERP y CRM, especialmente en el caso de los servicios gestionados. La convergencia de canales de comunicación optimiza los flujos de trabajo, reduce los errores y permite operar de manera ininterrumpida.

**El problema:** Las círculos del crimen comercial de hoy en día combinan spam, correo electrónico y aplicaciones en sus ataques multicanal. Por ejemplo, una amenaza combinada entrante típica puede utilizar el correo electrónico para que los destinatarios vayan a URL falsas, o incluso a URL muy conocidas en las que se ha incrustado código malicioso para capturar contraseñas de cuentas de correo electrónico e instalar keyloggers o troyanos en sus sistemas. Lo que resulta más peligroso es que este malware puede adaptarse para que robe información específica de gran valor para el usuario y la empresa. Estas amenazas focalizadas a veces no se detectan, especialmente en sitios de nicho específicos de cada industria.

**La respuesta actual:** La mayoría de empresas todavía protegen cada dirección y canal de comunicación con soluciones independientes: de filtrado de información y los correos electrónicos salientes, de filtrado de spam y virus entrantes y de bloqueo de URL maliciosas o no deseables. Estos silos independientes examinan las URL o las cabeceras de los mensajes de correo, pero no ambas cosas a la vez, y raramente prestan atención al contenido propiamente dicho o bloquean, de manera proactiva, su transmisión al exterior de la red corporativa. Reaccionan basándose en una visión histórica de las amenazas fundamentada, a su vez, en inspecciones, firmas y análisis de reputación y comportamiento anticuados. Las amenazas combinadas superan con facilidad estas inspecciones mutando y moviéndose por la web mientras roban información.

Marzo de 2008: la importante cadena de supermercados Hannaford Brothers fue demandada después que varias intrusiones en su red hayan comprometido la seguridad de 4,2 millones de registros de tarjetas de crédito.<sup>8</sup>

Estos ejemplos ilustran la complejidad y dificultad que entraña proteger una plataforma como Internet. A juzgar por una encuesta sobre las principales amenazas a la seguridad de las redes elaborada en 2008 por IDC, todo parece indicar que las soluciones tradicionales ya no son adecuadas. La pérdida involuntaria de información encabeza, por primera vez, la lista de preocupaciones de los directores de seguridad:

1. Que los empleados pongan al descubierto, de manera involuntaria, información sensible
2. Troyanos, virus, gusanos y otros tipos de código malicioso
3. Spam
4. Información robada por empleados o socios comerciales
5. Hackers<sup>9</sup>

<sup>7</sup> "Content Security Is Becoming A Competition Among Suites: Websense Rounds Out Its Security Portfolio With Its Acquisition Of SurfControl" by Chenxi Wang, Ph.D., December 2007, Forrester Research, Inc.

<sup>8</sup> [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9070281&taxonomyId=14&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9070281&taxonomyId=14&intsrc=kc_top)

<sup>9</sup> IDC Special Study, "Information Protection and Control Survey: Data Loss Prevention and Encryption Trends," Doc # 211109, March 2008

## Nuevas exigencias

Las soluciones de seguridad deben trasladar el objetivo básico de la protección de evitar que las infraestructuras sufran ataques del exterior –un modelo adecuado para las fronteras perimetrales e Internet entendido como fuente de contenido– a proteger la información esencial de posibles filtraciones de información al exterior, en línea con la Web 2.0 e Internet como plataforma comercial. En vez de trabajar como silos aislados, las protecciones deben colaborar materia de canales de aplicación, técnicas de inspección y perspectivas de uso. A través de la colaboración, estas herramientas podrán examinar, en tiempo real, tanto contenido como contexto, para así identificar y bloquear, con la máxima precisión, todo tipo de amenazas sofisticadas.

Para asegurarse el éxito a largo plazo, estas soluciones deben servir tanto a los directores de seguridad como a los usuarios finales. Los directores de seguridad necesitan visibilidad y un control fiable de las fugas de información. Por su parte, los usuarios finales deben ser productivos y eficaces en su trabajo. Las necesidades de los usuarios finales no se deben trivializar: los usuarios frustrados (o con malas intenciones) encontrarán maneras de sortear las herramientas de seguridad o de insistir en la limitación de las reglas de bloqueo hasta volverlas irrelevantes. Ante tales exigencias, las soluciones deben adaptarse, de manera eficiente, tanto a las amenazas como a las necesidades empresariales.

## Una nueva fórmula para la protección de la información = precisión + contexto

La precisión y el contexto son dos de las claves del éxito. Una identificación precisa requiere un profundo análisis del contenido y la información, tanto en lo externo –en Internet– como en lo interno –atravesando la red y en los servidores y sistemas corporativos–. La precisión debe mantenerse incluso en el momento en que la información y el contenido se utilicen y editen, ya sea en sitios web o en aplicaciones empresariales. Teniendo en cuenta el ritmo de los cambios en el contenido (constantes e instantáneos), identificarlos con precisión requiere unos niveles significativos de recursos informáticos y de investigación, así como compartir toda la información necesaria para detectar amenazas que abarcan varios canales de comunicación: “hay malware en su spam”, “hay un spammer en esta página web” o “esta información no puede publicarse en este blog ni enviarse por correo electrónico a esta dirección”.

Para reconocer el contexto, las soluciones deben tomar en consideración varios aspectos del uso antes de actuar. En vez de pensar en canales tecnológicos –¿Es un correo electrónico? ¿Es una página web?–, las herramientas deben intentar valorar el contenido y la información, así como el contexto en el que se utilizan: ¿Quién es el usuario? ¿De qué tipo de información estamos hablando? ¿Cuáles son los canales de comunicación y aplicaciones que el usuario utiliza para trabajar con la información? Esta perspectiva más amplia crea un sistema de protección rico en matices y de mayor precisión que el enfoque radical, de todo o nada, del pasado. La incorporación del contexto da sentido a los controles y relevancia a las evaluaciones.

Un aspecto clave del contexto es Internet como tal: ¿Internet puede considerarse un destino válido para la empresa, o pone en riesgo el cumplimiento de las normativas, la seguridad o información confidencial de la empresa? Este conocimiento contextual combina el conocimiento de la web con el conocimiento de las amenazas para detectar destinos arriesgados, clarificar qué direcciones de correo son de spam y detectar transmisiones inadecuadas. Con él, las organizaciones pueden tomar decisiones más informadas sobre el riesgo de acceder a ciertos recursos en línea o el riesgo de intercambiar información.

Aplicando estos requisitos para precisar la identificación y ofrecer respuestas con conocimiento del contexto, en la tabla siguiente se resumen las características que marcan el paso de un entorno de seguridad basado en la infraestructura a otro basado en la información.

Requisitos para que las soluciones protejan y permitan el uso de la plataforma comercial de Internet

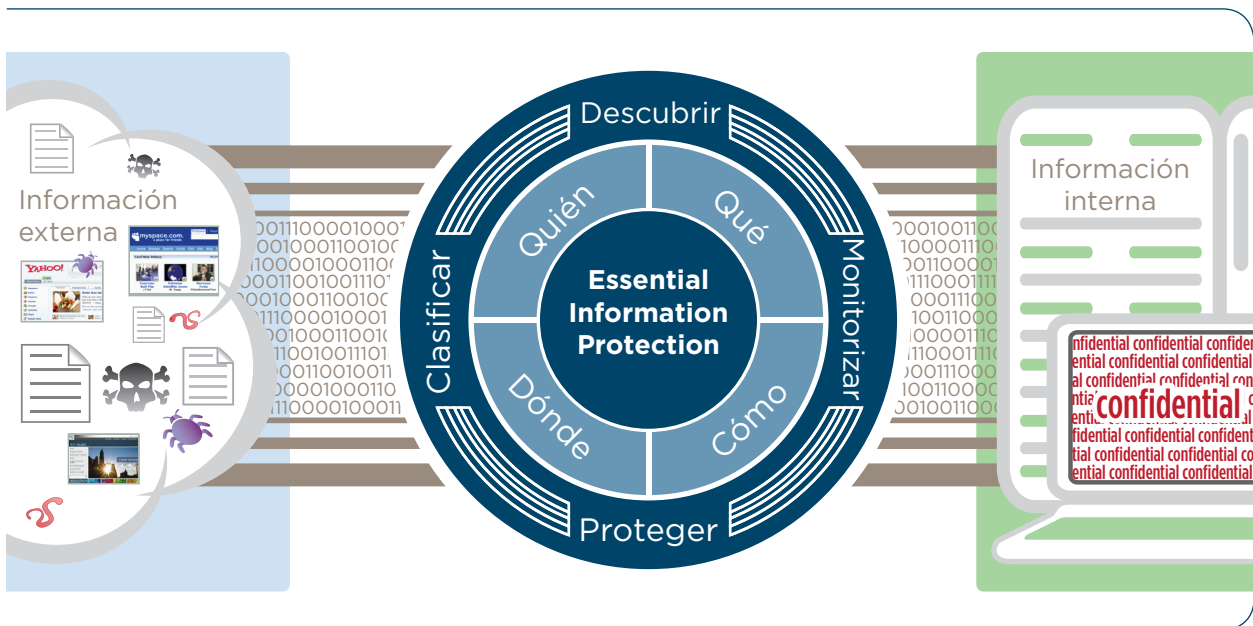
- Características
- Incorpora controles de la web, el correo electrónico y las fugas de información para ofrecer una cobertura integral.
  - Inspecciona los flujos de información entrante y saliente por todos los canales.
  - Combina varias técnicas de detección, identificación y clasificación.
  - Incorpora el conocimiento bidireccional de los usuarios, la información, los canales y los destinos en Internet.
  - Proporciona mecanismos sencillos para implementar políticas precisas y conseguir visibilidad al instante, con la flexibilidad para ajustarlas y crear controles y procesos adicionales a medida que se comprenden mejor los riesgos.
  - A pesar de la naturaleza dinámica del contenido y la información, establece asociaciones duraderas entre las políticas y los usuarios, la información, los destinos y los canales de comunicación.

- Ejemplos
- **Prevención de fuga de información:** La solución debería poder identificar información con precisión en la información en reposo, almacenada en sistemas de archivos y repositorios, la información en movimiento, dentro y fuera de la organización, y la información en uso en aplicaciones en los puestos de usuario. La solución también debería poder entender qué significa esta información con relación a normativas, información confidencial y políticas internas, y permitir la adaptación de dichas políticas a los procesos empresariales. Al mismo tiempo, debería poder aplicar políticas sistemáticas y habilitar flujos de trabajo que vayan desde la gestión de incidencias hasta la respuesta automática a las incidencias y los pertinentes resúmenes, notificaciones e informes detallados.
  - **Control del contenido, la información y los usuarios de los blogs:** La solución debería entender la categoría del blog, poder identificar al usuario e identificar la información en tiempo real con un nivel de precisión que permita bloquear la publicación de cualquier información demasiado privada. Si clasifica correctamente el host web, la reputación y el contenido real del blog, la solución debería evitar riesgos para los usuarios y los sistemas, además del acceso inadecuado al blog.
  - **Amenazas de la Web 2.0:** La solución debería poder entender los sitios web, el contenido web, las aplicaciones y el malware yendo más allá de su reputación, teniendo en cuenta su uso y el contexto de Internet para poder hacer una valoración del riesgo en tiempo real. Las amenazas sólo se podrán bloquear con precisión y en tiempo real con este nivel de comprensión: incluso si fuese una página web muy conocida, de confianza y con buena reputación la que ocultase una amenaza, este riesgo se evitaría.
  - **Amenazas que combinan la web y el correo electrónico:** Una solución debería poder identificar enlaces en los mensajes de correo electrónico y descubrir si conducen a contenido o sitios web malintencionados. A partir de esta precisa identificación, las soluciones deberían poder actuar en tiempo real para bloquear el mensaje de correo y cualquier otro intento de acceder al sitio web peligroso, visualizar contenido inadecuado o transmitir información al destino.

## Diga Sí con Essential Information Protection™

Websense® integra seguridad web, de mensajería y de datos para proteger su toda información esencial y permitir un uso productivo y seguro de una plataforma como Internet. Websense Essential Information Protection defiende las comunicaciones multicanal, garantiza la seguridad al utilizar las tecnologías Web 2.0 y previene las fugas de información. Essential Information Protection utiliza la ThreatSeeker™ Network, una infraestructura avanzada que permite detectar desde el primer momento las amenazas en los canales web y del correo electrónico e identificar y bloquear en tiempo real el acceso a sitios web de alto riesgo mediante técnicas y tecnologías de identificación de la información. Las soluciones de seguridad web, de mensajería y de la información de Websense utilizan la inteligencia en materia de seguridad de la ThreatSeeker Network para proporcionar la protección más actualizada contra fugas de información, contenido no deseado y amenazas malintencionadas.

La ThreatSeeker Network combina análisis binario, heurística, reputación, análisis de imágenes, análisis léxico, detección de patrones, análisis estadístico, procesamiento de lenguaje natural y reconocimiento de huellas digitales en los datos con los conocimientos de expertos investigadores en múltiples disciplinas. Estas técnicas y funcionalidades intrínsecamente coordinadas identifican y clasifican la información y el contenido dentro de la empresa y en Internet con el objetivo de comprender las nuevas amenazas desde el momento de su aparición.



Websense Essential Information Protection clasifica las amenazas externas y monitoriza el uso interno de la información para evitar la fuga de información regulada y/o confidencial.

Las soluciones de Websense utilizan esta precisa clasificación y el contexto de Internet para permitir un uso seguro y adecuado de Internet, garantizar la seguridad de las comunicaciones por correo electrónico y el cumplimiento de políticas y normativas, y prevenir las fugas de información. Estas soluciones se combinan para ir más allá que los sistemas de seguridad tradicionales y proteger contra las amenazas combinadas, que cruzan los vectores de riesgo entrante y saliente y ponen en peligro la información esencial de las organizaciones. Gracias a la integración directa de los productos y con la ayuda de la investigación de la ThreatSeeker Network, este conjunto de productos toma en consideración todos los componentes importantes: el usuario, la información, los canales de comunicación y el destino en Internet.

Con este enfoque, Websense puede identificar y gestionar con precisión, al instante y a la perfección:

- **Quién** tiene permiso para acceder a sitios web, información o aplicaciones específicas.
- **Qué** información es de vital importancia para la organización y debe protegerse a toda costa de filtraciones accidentales o intencionadas.
- **Cómo** pueden comunicar esta información sensible los usuarios, y cómo se pueden utilizar los recursos en línea de modo que resulten más seguros y productivos para la organización.
- **Dónde** pueden ir los usuarios cuando naveguen por la red y adónde se puede enviar con seguridad la información sensible.

Las soluciones integradas de seguridad web, de mensajería y de la información de Websense aumentan la seguridad y la eficiencia de las organizaciones. Websense proporciona la protección necesaria para que los empleados sean productivos en cualquier red, en cualquier momento y en cualquier lugar. Con ellas, los directores de seguridad podrán reducir las responsabilidades legales, hacer cumplir normativas y políticas empresariales, evitar la fuga de información y tener visibilidad de lo que ocurre en su empresa, en vista de estos riesgos en constante evolución. Gracias a la unión de técnicas de investigación avanzadas con controles eficaces e integrados, Websense Essential Information Protection ofrece una combinación única de inteligencia y conocimiento de la web, el contenido y los usuarios para detener las amenazas en origen, ayudando así a las empresas a sacar el máximo provecho de Internet como plataforma de negocios y permitiendo que los directores de seguridad digan Sí a las nuevas tecnologías y funcionalidades.

## Resumen

Aunque hoy en día Internet es un elemento clave para cualquier empresa, su uso pone en riesgo mucha información esencial, desde fórmulas y código fuente confidencial hasta planes de negocios y listas de clientes. Alimentadas por la irrupción de la Web 2.0, las amenazas que combinan Internet y el correo electrónico emplean ahora maniobras furtivas para esquivar las protecciones tradicionales.

Para garantizar que la atenuación de los riesgos esté en sintonía con el clima de amenazas, las empresas deben reevaluar sus enfoques con respecto a la seguridad web, de mensajería y de la información. En vez de pensar en tecnologías, las organizaciones deben pensar en la información. La información es la clave de todo. ¿Cómo se utiliza? ¿Quién la utiliza? ¿Dónde y cuándo es seguro utilizarla? ¿Quién puede recibirla? ¿Mediante qué canales se puede transmitir de manera segura?

Este enfoque centrado en la información significa que, en vez de invertir en silos protectores aislados y con una cobertura limitada, las empresas fusionarán las defensas a través de las tecnologías, los canales de comunicación y las aplicaciones a través de las que se transporta y utiliza la información. Esta integración aumenta la precisión de detección y la calidad de la respuesta. Además de garantizar el cumplimiento proactivo de normativas y políticas, esta integración ofrece un nivel de protección adecuado, ya que permite el uso del contexto para entender usos empresariales y comerciales legítimos y adaptar las respuestas. Al proteger los datos más sensibles, la información esencial de cualquier negocio, las organizaciones pueden utilizar y defender a Internet como plataforma de negocio.

## Acerca de Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), líder mundial en tecnologías integradas de protección web, de mensajería y de información, proporciona su servicio Essential Information Protection a más de 42 millones de empleados de más de 50.000 organizaciones de todo el mundo. El software y las soluciones de seguridad hospedadas de Websense, que se distribuyen a través de su red global de distribuidores, ayuda a las organizaciones a bloquear códigos maliciosos, impedir la pérdida de información confidencial y hacer cumplir las políticas de seguridad y uso de Internet. Para más información, visite [www.websense.com](http://www.websense.com) y:

- **Si desea recibir alertas de seguridad e informes de amenazas, regístrese en**  
<http://www.websense.com/securitylabs/>
- **Para ver más información sobre nuestras soluciones y ver material educativo de apoyo, vaya a**  
<http://www.websense.com/global/en/ProductsServices/>
- **Para descargar libros blancos o casos prácticos y apuntarse a nuestros webcasts, vaya a**  
<http://www.websense.com/global/en/ResourceCenter/>
- **Para descargar versiones de evaluación de nuestras soluciones, vaya a**  
<http://www.websense.com/global/en/Downloads/>
- **Para encontrar y ponerse en contacto con uno de nuestros distribuidores, vaya a**  
<http://www.websense.com/global/en/Partners/Channel/FindPartner/>