NEWSLETTER

grupobeit.com

BLOG DEL CEO

La ciberseguridad ya no es un tema técnico ni exclusivo del área de TI. Hoy es una decisión estratégica de negocio que impacta directamente la continuidad operativa, la confianza de clientes y socios, y el valor de la organización...

EDICIÓN 56

Filtrado Web, DLP y CASB en 2026 — Controles críticos para proteger datos, identidad y nube

En 2026, las organizaciones ya no pierden información únicamente por malware avanzado.

EVENTOS

Estuvimos presentes en **RSA Conference 2026** en compañía de algunos de nuestros principales clientes, el evento más importante a nivel mundial en ciberseguridad, innovación y gestión de riesgos

NOTICIA BEIT

Fugas de datos en México evidencian la falta de control en nube y navegación

Durante los últimos meses, México ha enfrentado una ola sin precedentes de filtraciones de datos que han expuesto información sensible de decenas de millones de ciudadanos

Edición 56

Filtrado Web y Data Loss Prevention: dos decisiones estratégicas que definen la ciberseguridad moderna

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

La ciberseguridad ya no es un tema técnico ni exclusivo del área de TI. Hoy es una **decisión estratégica de negocio** que impacta directamente la continuidad operativa, la confianza de clientes y socios, y el valor de la organización.

En nuestra experiencia acompañando a empresas de distintos sectores, hay dos controles que consistentemente marcan la diferencia entre una postura reactiva y una postura madura de seguridad: el **filtrado web y Data Loss Prevention (DLP)**. No son herramientas aisladas, son **cimientos** sobre los que se construye una estrategia sólida de protección de la información.

El riesgo ya no entra por la puerta trasera

Durante años, el enfoque tradicional de ciberseguridad se centró en proteger el perímetro. Hoy ese perímetro prácticamente desapareció. Trabajo híbrido, aplicaciones SaaS, navegación web constante y uso de herramientas de IA han creado un entorno donde el riesgo entra con un clic.

Las cifras son claras. De acuerdo con datos consolidados por la Anti-Phishing Working Group (APWG), en 2025 se registraron más de **3.8 millones de sitios de phishing**, muchos de ellos activos solo por horas antes de desaparecer, lo que dificulta su detección tradicional. Además, estudios con base en el Verizon Data Breach Investigations Report confirman que el phishing está presente en más del 36 % de los incidentes de seguridad y sigue siendo uno de los principales vectores iniciales de ataque.

Filtrado web: control, prevención y resiliencia

El filtrado web es una de las formas más efectivas de reducir superficie de ataque desde el origen. No se trata únicamente de bloquear sitios “prohibidos”, sino de prevenir que usuarios accedan de forma involuntaria a contenidos maliciosos, dominios de phishing, descargas infecciosas o plataformas no confiables.

Un análisis del Ponemon Institute señala que las organizaciones que utilizan filtrado web avanzado reducen pérdidas asociadas a incidentes originados por navegación maliciosa en un promedio de 1.4 millones de dólares anuales, al evitar infecciones de malware y exposición a sitios de riesgo.

Desde una perspectiva ejecutiva, el filtrado web cumple tres funciones clave: reduce el riesgo operativo, protege al usuario sin frenar la productividad, y aporta visibilidad sobre comportamientos de navegación que pueden convertirse en incumplimientos o incidentes.

La otra cara del riesgo: cuando los datos se escapan desde adentro

Si el filtrado web protege el punto de entrada, Data Loss Prevention (DLP) protege lo que más valor tiene: la información.

Hoy, el mayor riesgo para los datos no proviene solo de actores externos. El riesgo interno es una de las principales causas de pérdida de información. Según el Fortinet 2025 Insider Risk Report, el 77 % de las organizaciones experimentó incidentes de pérdida de datos provocados por usuarios internos en los últimos 18 meses, y en más del 60 % de los casos el origen fue negligencia o desconocimiento.

Este dato es clave: la mayoría de las fugas ocurren durante actividades legítimas del trabajo diario, como compartir archivos, subir información a nubes personales, reenviar correos o utilizar herramientas de inteligencia artificial sin controles adecuados.

El costo real de perder datos

La pérdida de información no solo es un riesgo legal o reputacional; es un impacto financiero directo. El IBM Cost of a Data Breach Report 2024 revela que el costo promedio global de una brecha de datos alcanzó los 4.88 millones de dólares, el mayor incremento interanual desde la pandemia. En industrias reguladas, este impacto es aún mayor debido a multas, litigios y pérdida de confianza.

Adicionalmente, el mismo reporte confirma que las brechas relacionadas con errores humanos y manejo inadecuado de datos representan cerca de una cuarta parte de los incidentes, reforzando la necesidad de controles específicos para prevenir la fuga de información desde dentro.

Aquí es donde DLP deja de ser una herramienta técnica y se convierte en un habilitador del negocio.

Data Loss Prevention: visibilidad antes que castigo

Un error frecuente es pensar que DLP existe solo para bloquear. En realidad, las estrategias más efectivas de prevención de pérdida de datos se basan en visibilidad, contexto y supervisión inteligente.

Reportes recientes de Proofpoint señalan que solo el 38 % de las organizaciones cuenta con un programa maduro de DLP, a pesar de que el 85 % sufrió al menos un evento de pérdida de datos en el último año. Esto evidencia una brecha entre conciencia del problema y ejecución real.

Implementar DLP permite entender dónde viajan los datos, quién accede a ellos, cómo se usan y cuándo existe un comportamiento anómalo. Cuando se integra adecuadamente, reduce el riesgo sin afectar la productividad, al tiempo que fortalece el cumplimiento normativo.

La combinación que marca la diferencia

Filtrado web y DLP no deben verse como controles aislados. Juntos crean una barrera inteligente de protección que aborda tanto la entrada de amenazas como la salida no autorizada de información.

El primero reduce drásticamente la exposición a malware y phishing; el segundo protege los activos más críticos ante errores humanos, uso indebido o exfiltración no intencional. De acuerdo con análisis comparativos de IBM y Ponemon Institute, las organizaciones que combinan controles preventivos y visibilidad de datos reducen significativamente el tiempo de detección y contención de incidentes, disminuyendo hasta en millones el impacto de una brecha.

Conclusión

Desde la perspectiva de liderazgo, la pregunta ya no es si debemos invertir en ciberseguridad, sino dónde hacerlo para maximizar impacto y resiliencia. El filtrado web y Data Loss Prevention no son gastos; son decisiones estratégicas que protegen ingresos, operaciones y reputación.

En un entorno donde los ataques evolucionan más rápido que nunca y los datos se mueven sin fricción, la prevención es la mejor estrategia. Implementar estos controles es dar un paso firme hacia una ciberseguridad que acompaña al negocio, en lugar de reaccionar cuando el daño ya está hecho.

Fuentes:

- Pishing Activity Trends Reports. Consultado en: APWG
- Report: 90% of Cyberattacks Start with Pishing. Consultado en: Report: 90% of Cyberattacks Start With Phishing - Programs.com
- Inisder Risk Report 2025: Fortinet. Consultado en: 2025-insider-risk-report-ftnt.pdf
- Cost of a Data Breach Report 2024. Consultado en: Cost of a Data Breach Report 2024

Filtrado Web, DLP y CASB en 2026 — Controles críticos para proteger datos, identidad y nube

En 2026, las organizaciones ya no pierden información únicamente por malware avanzado. La realidad es más compleja: el uso de aplicaciones cloud no gobernadas, errores humanos y accesos indebidos son hoy las principales fuentes de fuga de información y riesgos regulatorios.

Los controles tradicionales perimetrales son insuficientes. Las plataformas de **Web Filtering, Data Loss Prevention (DLP) y Cloud Access Security Broker (CASB)** se han convertido en componentes esenciales de una postura de seguridad moderna y alineada al negocio.

Los datos respaldan esta evolución.Según el **IBM Cost of a Data Breach Report 2025,** el **82 % de las brechas involucran datos almacenados o procesados en entornos cloud,** y el costo promedio global de una brecha ya supera los USD 4.5 millones. Organizaciones con controles maduros de protección de datos reducen el impacto financiero hasta en USD 1.76 millones.

Por su parte, el Verizon Data Breach Investigations Report 2025 (DBIR) confirma que el uso indebido de credenciales y el acceso a aplicaciones web continúan siendo uno de los vectores de ataque más frecuentes, especialmente en entornos híbridos y de trabajo remoto.

Para 2026, una estrategia sólida de protección de información debe construirse sobre tres pilares fundamentales:

1. Filtrado Web avanzado y control de navegación

Hoy, más del 70 % del tráfico corporativo se dirige a aplicaciones y servicios web, muchos de ellos fuera del radar de TI.

Gartner estima que para 2026, más del 65 % de las brechas estarán relacionadas con el uso no autorizado de servicios SaaS y navegación hacia contenidos maliciosos o de alto riesgo.

Un esquema moderno de Web Filtering debe permitir:

- Clasificación dinámica de URLs y aplicaciones
- Bloqueo de contenido malicioso y phishing
- Identificación de Shadow IT
- Aplicación de políticas por usuario, rol e identidad

El filtrado web ya no es solo prevención de malware: es control del riesgo digital en tiempo real.

2. DLP como eje de protección de datos sensibles

El principal desafío ya no es dónde están los datos, sino cómo se mueven.
De acuerdo con IBM, el 68 % de las brechas involucran errores humanos, como envío accidental de información, cargas a nubes personales o uso indebido de dispositivos.

Un DLP maduro debe ofrecer:

- Descubrimiento y clasificación automática de datos (PII, financieros, regulatorios)
- Protección de datos en movimiento, en reposo y en uso
- Prevención de fuga vía correo, web, endpoints y nube
- Integración con flujos de respuesta automatizada (SOC)

Las organizaciones que implementan DLP de forma integral reducen de manera significativa la probabilidad y el impacto de exfiltración de información.

3. CASB: visibilidad y control total sobre la nube

Microsoft reporta en su Digital Defense Report 2025 que el abuso de aplicaciones cloud legítimas es hoy una de las técnicas favoritas de los atacantes por su baja tasa de detección.

Un CASB moderno permite:

- Descubrir aplicaciones SaaS no autorizadas
- Aplicar políticas de acceso condicional
- Detectar comportamientos anómalos
- Controlar descargas, cargas y compartición de datos
- Cumplir marcos regulatorios como ISO 27001 y NIST
-

En 2026, no existe gobierno de datos sin visibilidad cloud.

Filtrado Web, DLP y CASB ya no son soluciones aisladas; son controles críticos de continuidad operativa, protección reputacional y cumplimiento regulatorio

Fuentes

- IBM — Cost of a Data Breach Report 2025
- Verizon — Data Breach Investigations Report 2025 (DBIR)
- Microsoft — Digital Defense Report 2025
- Gartner — Cloud Security & SSE Forecast 2025

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fugas de datos en México evidencian la falta de control en nube y navegación

NOTICIA BeIT

Durante los últimos meses, México ha enfrentado una ola sin precedentes de filtraciones de datos que han expuesto información sensible de decenas de millones de ciudadanos, tanto en el sector público como privado. Los incidentes no responden únicamente a ataques sofisticados, sino a fallas estructurales en la gobernanza de datos, uso de aplicaciones cloud no controladas y errores humanos recurrentes.

A inicios de 2026, reportes técnicos y periodísticos confirmaron que el grupo de amenazas Chronus logró comprometer sistemas de al menos 20 dependencias públicas, incluyendo SAT, IMSS, SEP y entidades estatales, exponiendo información personal de más de 36 millones de personas, como CURP, RFC, datos médicos y fiscales. Expertos coinciden en que el vector principal del ataque estuvo relacionado con credenciales válidas obtenidas mediante malware tipo infostealer, enlaces maliciosos y accesos cloud sin controles adecuados.

Este patrón no es exclusivo del sector público. De acuerdo con IBM, más del 56% de las brechas a nivel global involucran entornos en la nube, y la falta de visibilidad sobre aplicaciones SaaS es uno de los principales detonantes de fuga de información.

Hallazgos clave en organizaciones mexicanas

Análisis independientes revelan una tendencia preocupante en empresas e instituciones del país:

- **Ausencia de visibilidad sobre aplicaciones SaaS** en uso, lo que permite la proliferación de Shadow IT o Shadow SaaS sin evaluación de riesgos.
- **Falta de políticas efectivas de Data Loss Prevention (DLP)** para proteger datos personales, financieros y regulatorios en correo, web y nube.
- **Controles de navegación obsoletos,** sin aplicación de políticas por identidad ni protección contra phishing avanzado, principal vector de robo de credenciales.

Implicaciones para la protección de datos

Este tipo de filtraciones evidencian riesgos críticos y sistémicos para las organizaciones en México:

- Shadow IT descontrolado, que fragmenta la gestión de datos y dificulta el cumplimiento normativo.
- Fuga silenciosa de información, especialmente a través de nubes personales, correos y descargas no supervisadas.
- Incumplimiento regulatorio, con impacto directo en marcos como la Ley Federal de Protección de Datos Personales, ISO 27001 y regulaciones sectoriales.
- Respuesta tardía a incidentes, derivada de monitoreo fragmentado y ausencia de integración con SOC y NOC.

IBM estima que el ciclo de vida promedio de una brecha supera los 277 días, y cada día sin detección incrementa el impacto financiero, reputacional y legal para la organización.

El rol estratégico de Web Filtering, DLP y CASB

Ante este contexto, la integración de Web Filtering, DLP y CASB, se convierte en un habilitador clave de resiliencia digital:

- Web Filtering por identidad permite bloquear phishing, malware y accesos a aplicaciones no autorizadas.
- DLP unificado previene la fuga de datos en correo, web, endpoints y nube, incluso por error humano.
- CASB ofrece visibilidad completa de aplicaciones SaaS, control granular de datos y detección de comportamientos anómalos.

Las organizaciones que adoptan estos controles reducen significativamente el impacto financiero de una brecha y aceleran los tiempos de contención.

Agenda una asesoría estratégica:

+52 56 5100 8613 admmarketing@buromc.com

RSA Conference

Estuvimos presentes en RSA Conference 2026 en compañía de algunos de nuestros principales clientes, el evento más importante a nivel mundial en ciberseguridad, innovación y gestión de riesgos, que reúne a líderes y tomadores de decisión de la industria a nivel global.

RSAC 2026 fue un espacio clave para analizar las principales amenazas a infraestructuras críticas y servicios públicos, conocer mejores prácticas y marcos regulatorios, así como explorar modelos de gobernanza digital y soluciones tecnológicas que fortalecen la continuidad operativa y la confianza ciudadana.

Como parte de esta experiencia, también invitamos a nuestros clientes a momentos de networking en algunos de los mejores viñedos de San Francisco, USA, así como acceso a eventos exclusivos organizados en conjunto con nuestras marcas aliadas Netskope, Vicarious y Proofpoint.

Seguimos impulsando una visión estratégica de la ciberseguridad, conectando conocimiento, innovación y colaboración internacional.