

## Superar el reto del cumplimiento de PCI DSS

Cómo puede ayudar el software Luminet de gestión de fraude empresarial

Uno de los retos más difíciles a que se enfrentan las organizaciones que intentan cumplir el Estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) procede de la sección 10.2.1. Esta sección les exige que “implementen pistas de auditoría automatizadas de todos los componentes del sistema para reconstruir todos los accesos de usuarios individuales a datos de los titulares de las tarjetas”. Además, la sección 10.2.2 exige que deben incluirse en la pista de auditoría “todas las acciones emprendidas por cualquier persona con privilegios administrativos o de administrador”.

### Por qué es difícil crear pistas de auditoría

Cumplir los requisitos de pistas de auditoría de PCI DSS es difícil por cuatro motivos:

1. La mayoría de las aplicaciones, tanto heredadas como modernas, no incluyen un mecanismo de registro que ofrezca una historia completa del acceso de usuarios a los datos del titular de una tarjeta. En muchos casos, los registros sólo incluyen acciones de actualización, y no consultas del usuario ni otras acciones de sólo lectura. Para que sea completa, una auditoría de los accesos de todos los usuarios individuales deben incluir actividades de sólo lectura.
2. Una simple agregación de registros puede cumplir algunos de los requisitos de PCI-DSS, pero no proporciona la pista de auditoría completa que exige la sección 10.2. Si sus registros no contienen suficientes datos o capturan sólo tipos específicos de actividad, entonces la agregación de registros no le ayudará a cumplir la sección 10.2.
3. Desarrollar su propia solución interna implica un trabajo de desarrollo largo y caro. Puede ser necesario cambiar, volver a probar y volver a desplegar miles de programas de aplicaciones de la organización. Después de todo ese trabajo, aún se quedaría sin una visión centralizada y fácil de gestionar de quién hizo exactamente qué y cuándo en todos los sistemas y aplicaciones.
4. Capturar sólo la actividad en bases de datos también puede mantener el incumplimiento, pues la mayoría de las aplicaciones usan identificaciones genéricas de usuario para acceso a bases de datos. Como resultado, no tendrá forma de cumplir el requisito de auditar “todos los accesos individuales”.

Afortunadamente, existe una tecnología que puede ayudarle a superar estos retos.

### Véalo. Grábelo. Analícelo

El software Attachmate Luminet™ se ha diseñado específicamente para que capture una imagen completa de todos los accesos de usuarios a información de tarjetas de pago, de modo que finalmente pueda dejar de peinar crípticos archivos de registro con el fin de crear una historia creíble con fines de auditoría. He aquí cómo funciona Luminet:

- **Ve la actividad de los usuarios**

Luminet le ofrece las herramientas necesarias para definir reglas empresariales adaptables que señalan comportamiento sospechoso basándose en su estrategia de gestión de riesgos. A continuación, Luminet genera alertas en tiempo real relacionadas con patrones cuestionables de actividad, lo que le permite dirigir inmediatamente su atención hacia anomalías.

- **Graba la actividad de los usuarios**

Luminet graba la actividad de los usuarios en tiempo real, pantalla a pantalla, pulsación a pulsación de teclas, creando una pista de auditoría directamente desde la red. Esta pista de auditoría incluye acciones de actualización y de sólo lectura para usuarios normales y con privilegios. Luminet almacena esta información en un repositorio seguro, desde el que puede llevar a cabo potentes búsquedas de texto completo a través de actividad actual o grabada. Estas búsquedas le permiten reproducir visualmente toda pantalla o secuencia de pulsaciones relevante para su auditoría. Paneles de control, gráficos e informes personalizables permiten que sus auditores vean la imagen completa de un vistazo y dirijan su atención hacia actividades que pongan en riesgo el cumplimiento de PCI DSS.

### Acerca de PCI DSS

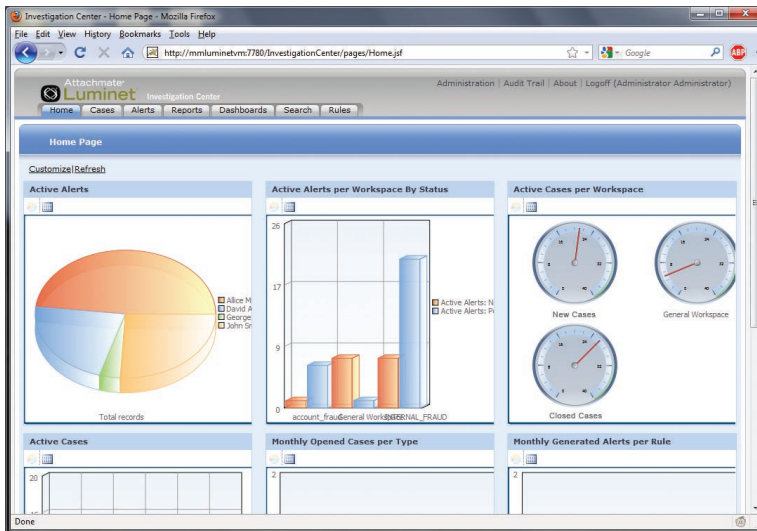
El Estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) lo desarrolló y lo mantiene el Consejo de Estándares de Seguridad de PCI ([pcisecuritystandards.org](http://pcisecuritystandards.org)), un foro abierto global fundado por las principales empresas de tarjetas de crédito para definir los requisitos de procesamiento de información de tarjetas de crédito de las organizaciones.

El objetivo de este estándar es evitar el fraude en tarjetas de crédito y crear medidas coherentes de seguridad en todos los usos de información de tarjetas de crédito. El estándar define 12 requisitos específicos que deben poner en práctica las organizaciones que almacenan, procesan o transmiten datos de titulares de tarjetas.

• **Analiza la actividad de los usuarios**

Luminet le ayuda a distinguir claramente entre actividad dudosa y trabajo legítimo. Una herramienta interactiva detecta patrones en todos los canales en múltiples empleados y departamentos, así como en diversas aplicaciones. Como resultado, usted puede emprender acciones inmediatas y decisivas sobre comportamiento sospechoso.

En otras palabras, Luminet ve, graba y analiza la actividad de usuarios en aplicaciones empresariales, ofreciendo una pista completa de auditoría de todos los accesos individuales a información sensible, como datos de tarjetas de crédito. Luminet le ofrece, sin tener que añadir nuevos controles ni cambiar una sola línea de código de sus aplicaciones existentes, una pista completa de auditoría que le permite cumplir los requisitos 10.2.1 y 10.2.2 de PCI DSS.



Supervise métricas de actividades clave con paneles de control personalizables.

**Luminet:  
Véalo. Grábalo. Analícelo**

El software Luminet de gestión del fraude ve, graba y analiza actividad de usuarios en aplicaciones empresariales. Elimina las conjeturas de la supervisión de aplicaciones, ofreciéndole la inteligencia que necesita para emprender acciones informadas.

Entre sus características clave se incluyen:

- Arquitectura sin agentes
- Supervisión en todos los canales
- Alertas en tiempo real
- Reproducción visual de pantallas de aplicaciones
- Búsqueda al estilo de Google
- Análisis de vínculos gráficos
- Soporte de aplicaciones heredadas
- Suite de gestión de casos
- Paneles de control e informes personalizados

**Acerca de Attachmate**

Attachmate ofrece software avanzado para emulación de terminal, modernización de activos heredados, transferencia gestionada de archivos y gestión de fraude empresarial. Con nuestras tecnologías, más de 65.000 empresas de todo el mundo utilizan sus recursos de TI de formas nuevas y valiosas. [www.attachmate.es](http://www.attachmate.es)



**Sede Central**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL +1 206 217 7500  
FAX +1 206 217 7515

**Oficina Central Para América Latina**  
México  
TEL +52 55 9178 4970  
FAX +52 55 5540 4886

**Oficina Central Para EMEA**  
Países Bajos  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Oficina Central Para España**  
Madrid  
TEL +34 911517111  
TEL +34 911517120

WEB [www.attachmate.es](http://www.attachmate.es)  
EMAIL [info-es@attachmate.com](mailto:info-es@attachmate.com)

Para obtener información sobre las oficinas regionales, visite [www.attachmate.es](http://www.attachmate.es)