

# Asegure su Negocio con Protección de Data



*Sus clientes exigen privacidad de datos y esperan que usted haga negocios con su información de una manera segura. Debido a la alarmante frecuencia con la que filtraciones de datos ocurren a nivel mundial, es evidente que las defensas de perímetro y sistemas de detección de intrusos no son suficientes para prevenir que la información llegue a ser expuesta.*

*Ya sea que usted implemente una metodología de seguridad estratificada, o que su enfoque sea data-céntrico, asegurar su información confidencial es un componente de máxima importancia para su negocio. Y es aquí donde SecurDPS Enterprise se adapta perfectamente a sus intereses empresariales.*

Filtraciones o violaciones de datos pueden causar daños severos a empresas que procesan información confidencial o sensible. El cumplimiento de las leyes y regulaciones requieren que las organizaciones desarrollen estrategias de seguridad efectivas para proteger la información valiosa que poseen. Por ejemplo, PCI-DSS exige que el Número Primario de cada Cuenta (PAN) en las tarjetas de pago sea hecho ilegible cada vez que se archive, y HIPAA provee privacidad de datos y provisiones de seguridad para proteger la información médica. Adicionalmente, GDPR, que entró en efecto en mayo del 2018, provee reglas y requerimientos internacionales en torno a las leyes y derechos de protección de data que son cruciales tanto para negocios como para individuos.

Poder reducir la complejidad que implica acatar las reglas de cumplimiento, es un factor – minimizar el riesgo, o por lo menos minimizar el impacto de riesgo es el otro factor. Es un hecho comprobado que los delincuentes cibernéticos constantemente están tratando de burlar los sistemas de seguridad de data para obtener acceso al interior de las organizaciones. Sin embargo, como muchos informes de la industria han mostrado, cuando ocurren filtraciones o violaciones de datos, los costos pueden ser astronómicos debido a los efectos en el precio de las acciones, la retención de clientes y la reputación del nombre de la empresa.

Otro factor importante que motiva a las compañías a proteger su datos confidenciales es la necesidad de permanecer competitivas y obtener nuevas oportunidades de negocio. Algunas organizaciones solamente trabajan con compañías que tienen la habilidad de compartir información ya protegida, en lugar de tener que asumir ellos mismos la responsabilidad de protegerla. En este aspecto, las compañías que tienen la habilidad de proteger información van a estar en una posición más ventajosa para atraer nuevos clientes.

Sin embargo, poner en marcha aplicaciones existentes con mecanismos compatibles y apropiados de protección de datos en reposo, puede llegar a ser una tarea de enormes proporciones. SecurDPS Enterprise ofrece la tecnología necesaria para proteger exitosamente datos confidenciales en reposo, con un esfuerzo mínimo y sin necesidad de cambiar las aplicaciones existentes. SecurDPS Enterprise permite que las organizaciones tengan un control completo de su información confidencial, minimizando los costos de cumplimiento y reduciendo significativamente el riesgo de filtraciones de datos.

## Al usar SecurDPS Enterprise su negocio puede

- > Reducir el impacto comercial ya que SecurDPS reemplaza la información confidencial vulnerable con tokens que en caso de ser expuestos, no pueden ser utilizados pues carecen del significado original del dato.
- > Asegurar un verdadero cumplimiento de todas las leyes y regulaciones (PCI, HIPAA, GDPR), ya que SecurDPS reduce significativamente las faltas de cumplimiento al satisfacer el requisito de que no exista información confidencial en los componentes empresariales principales.
- > Evitar ser expuesto accidentalmente por miembros del interior de su organización o por proveedores ajenos a la misma, gracias a que de ahora en adelante la información confidencial no va a estar disponible, porque requerirá una autorización apropiada para exponer el dato original.
- > Continuar creciendo y expandiéndose a nuevas áreas de negocio, debido a que puede intercambiar datos con otras compañías sin riesgo de exponer información confidencial.
- > Reducir la dependencia de controles de compensación llevados a cabo como medida temporal para obtener aprobación de las auditorías de seguridad.

# ¿Cómo funciona?



*SecurDPS Enterprise protege cientos de millones de transacciones de pago, registros clínicos, archivos de seguros y más, que se ejecutan de manera confiable en el ambiente empresarial de hoy en día.*

*Con más de 20 años de experiencia en protección de información en sistemas en los que esta es su misión fundamental, comforte es el socio perfecto para organizaciones que quieren proteger su posesión más valiosa: los datos.*

*SecurDPS fue diseñado desde el comienzo para garantizar seguridad de datos, en un mundo impulsado por innovaciones en negocios digitales, clientes empoderados e interrupciones tecnológicas continuas.*

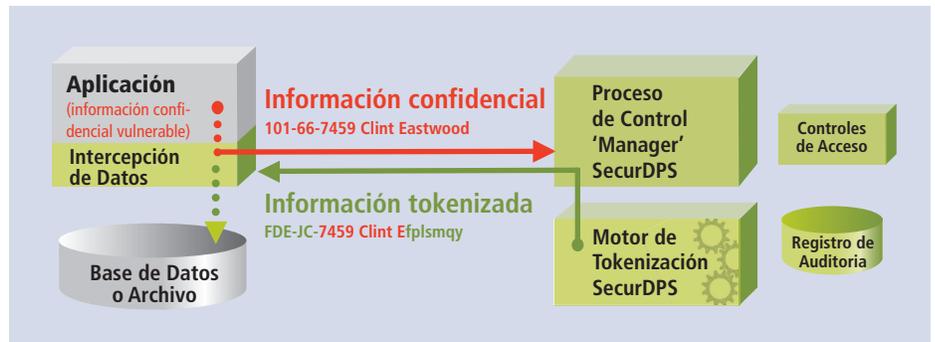
*Estamos aquí para ayudarle a tener éxito proporcionándole experiencia, una innovadora plataforma tecnológica y soporte local.*

*Para mas información, comuníquese con su representante de comforte hoy y visite [www.comforte.com](http://www.comforte.com).*

SecurDPS Enterprise funciona directamente en el hardware existente de su computador o en el entorno de virtualización y se responsabiliza de proteger información confidencial, cumpliendo al mismo tiempo con requisitos y regulaciones claves de las leyes.

SecurDPS Enterprise usa el reconocido método de interceptación de datos para insertar un nivel más de protección en sus aplicaciones empresariales. Combinando esto con mecanismos avanzados para localizar información confidencial, SecurDPS Enterprise opera transparentemente desde sus aplicaciones – lo que significa que su equipo de Desarrollo no tiene necesidad de hacer cambios en los códigos de sus aplicaciones comerciales para proteger la información.

Sin cambiar el formato de registro de la información original, la capacidad de tokenización patentizada de SecurDPS Enterprise reemplaza elementos de información confidencial con tokens (valores sustitutos), garantizando al mismo tiempo un alto rendimiento y un impacto mínimo en el volumen de transacciones o en el intercambio de información. Solo cuando es necesario, se permite acceso a procesos de aplicación autorizados.



Además de proveer protección para información en reposo, SecurDPS Enterprise está habilitado para proteger información en movimiento diseñada para el intercambio de archivos confidenciales entre diferentes sistemas. Estos archivos pueden ser protegidos mediante cifrado o su aplicación puede ser instrumentada para funcionar directamente en los archivos de los sistemas de sus afiliados, por medio de la transferencia segura de archivos SFTP/SSH, eliminando así cualquier almacenamiento intermedio en el servidor.

Capacidades	Valor
<b>Potente sistema de seguridad de tokenización patentizado</b>	Remueve completamente información confidencial de sus sistemas internos reemplazándola con datos generados al azar que no tienen ningún valor comercial para los delincuentes cibernéticos.
<b>Integraciones fuera de lo común</b>	Gaste menos tiempo y dinero en tiempo de desarrollo para llegar a un "estado de protección" ideal, ya que no tendrá que hacer ningún cambio en los códigos de sus aplicaciones.
<b>Control de acceso granular y auditoría</b>	Cumpla los requisitos de cumplimiento de todas las leyes y regulaciones permitiendo acceso para tokenización solamente a usuarios y programas autorizados, y auditando intentos de acceso a su información confidencial.
<b>Implementación elástica y tolerante a fallas</b>	Establezca otro nivel de protección de datos que continuará funcionando en el futuro gracias a su exclusiva capacidad de adaptación. Las diferentes opciones de implementación, ya sea local, en la nube o híbrida, se asegura que usted se mantenga al día con sus estrategias de TI (tecnología de la información). Fallos imprevistos pueden ser resueltos automáticamente sin interrupción de servicio ni impacto a los clientes.

