

Cumplimiento de la HIPAA

Automatice y simplifique el cumplimiento de la HIPAA con DataSecurity Plus



Automatice y simplifique el cumplimiento de la HIPAA con DataSecurity Plus

La Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA) y la Ley de Tecnología de la Información de Salud para la Salud Económica y Clínica (HITECH) imponen las normas que deben seguir las empresas para proteger y mantener la confidencialidad de la información de salud personalmente identificable. Una ventaja añadida del cumplimiento de la HIPAA y la HITECH, que es obligatorio para todas las entidades que transmiten información de salud, es que le permite esquivar de forma proactiva tanto las amenazas externas como el abuso de privilegios internos.

Cumpla con la HIPAA/HITECH utilizando DataSecurity Plus

DataSecurity Plus dispone de amplios informes para ayudarle a cumplir las normas de seguridad de datos de HIPAA y HITECH. Con estos informes, puede obtener información significativa sobre los accesos, las modificaciones y los permisos de los archivos críticos para ayudar a mitigar las amenazas internas.

A continuación encontrará una lista de informes que puede utilizar para demostrar que su organización cumple con la HIPAAA.

Normas HIPAA/HITECH	Informe o alerta de DataSecurity Plus
Monitorear todas las modificaciones de la información de salud protegida (PHI) en los servidores de archivos para detectar y resolver las violaciones, si las hubiera	Informe de todos los cambios de archivos/carpetas
	Informe de archivos eliminados/sobrescritos
	Informe de cambios en los permisos de seguridad
	Informe sobre los archivos más modificados
	Crear informe de eventos
	Informes de eventos de cambio de nombre/traslado
	Informe de archivo modificado después de N días
Auditar e informar de todos los accesos de datos a la PHI para garantizar que no se produzcan cambios no autorizados.	Informe de todos los intentos fallidos
	Informe de eventos leídos
	Informe sobre los archivos más visitados
	Informe de la mayoría de los accesos por procesos/usuario
	Informe de archivo accedido después de N días
Supervisa y monitorea todos los cambios en los derechos de acceso y los permisos del servidor de archivos para identificar anomalías.	Informe de permisos NTFS
	Informe de permisos de uso compartido

Utilice las funciones personalizadas e integradas de las alertas para auditar regularmente las actividades relacionadas con los archivos/carpetas.	Alerta de archivo/carpetas movida o renombrada
	Alerta de cambios en la seguridad de los
	archivos/carpetas
	Alerta de archivo/carpetas eliminada
Detecte y responda a los accesos masivos con respuestas personalizadas y automatizadas.	Alerta de archivos multimedia
	Alerta de archivo ransomware
	Alerta basada en umbrales

* Con esta herramienta de cumplimiento de la HIPAA también puede generar informes personalizados basados en la ruta de los archivos, los usuarios, el horario de trabajo, etc.

DataSecurity Plus

ManageEngine DataSecurity Plus es una solución de visibilidad y seguridad de datos. Supervisa y alerta sobre las modificaciones y el movimiento de archivos críticos en servidores de archivos, failover clusters, estaciones de trabajo y USB. Los usuarios pueden localizar y analizar los archivos que contengan PII/ePHI almacenados en servidores de archivos de Windows, failover clusters y entornos de OneDrive mediante reglas de detección de datos integradas. Su función de prevención de pérdida de datos (DLP) ayuda a detectar y responder al robo de datos sensibles a través de USB, correo electrónico, impresoras y más. También proporciona informes de auditoría detallados que ayudan a las organizaciones a agilizar el cumplimiento de múltiples normativas de TI.

Para explorar estas funciones y ver [DataSecurity Plus en acción](#), .

Para saber más sobre DataSecurity Plus, visite www.datasecurityplus.com.

↓ Download free trial

\$ Get a quote

Explore las soluciones de DataSecurity Plus



Auditoría del servidor de archivos

Audite e informe sobre los accesos y modificaciones de los archivos, con alertas en tiempo real y respuestas automatizadas para las actividades críticas de los archivos.

[Learn more](#)

Análisis de archivos

Analice la seguridad y el almacenamiento de los archivos, gestione los archivos basura, optimice el uso del espacio en disco e identifique las vulnerabilidades de los permisos.

[Learn more](#)

Evaluación del riesgo de los datos

Descubra y clasifique los archivos que contienen datos confidenciales, como PII, PCI y ePHI, combinando la inspección de contenidos y el análisis contextual.

[Learn more](#)

Prevención de la pérdida de datos

Detecte e interrumpa las pérdidas de datos a través de los USB, el correo electrónico, las aplicaciones web y las impresoras; monitoree la actividad de los archivos en los endpoints; y mucho más.

[Learn more](#)

Protección en la nube

Supervise el tráfico web de la empresa y aplique políticas para bloquear el uso de aplicaciones web inapropiadas, de riesgo o maliciosas.

[Learn more](#)