tranxfer | secure file exchange

Cómo evitar el Shadow IT

Shadow IT describe a cualquier tipo de estructura utilizada sin la aprobación del área de Tecnología de la Información (IT). Esta práctica puede tomar muchas formas.

¿Qué está pasando en las empresas?

Sólo el 7%
de las aplicaciones SaaS gratuitas de internet cumplen con los estándares mínimos de seguridad

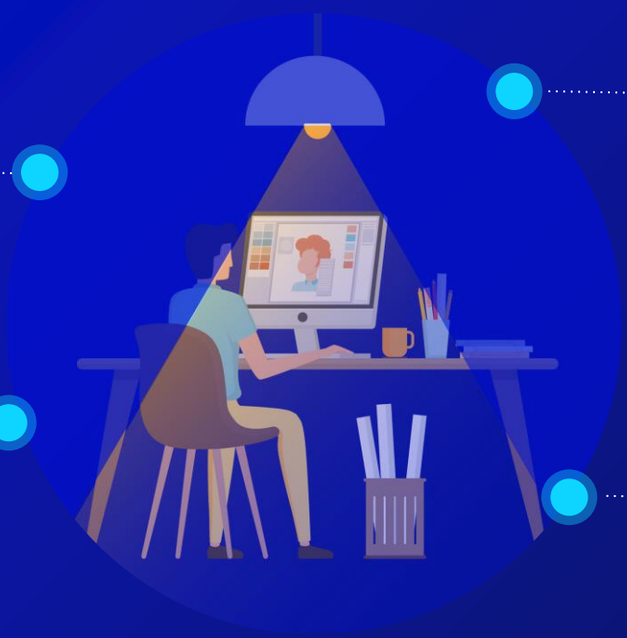
Los bancos y seguros
son las organizaciones que mayor riesgo corren debido al Shadow IT

Una tercera parte
de los trabajadores comparten y suben datos corporativos a herramientas externas a la organización, según IBM Security

Los 5 riesgos más habituales

Uso de un canal no-seguro y no reconocido por el departamento IT.

Desconocimiento de la ubicación de los servidores y del almacenamiento de la información.



Peligro de fuga de información por parte de la organización.

Exposición de la organización por incumplimiento de la normativa GDPR.

¿Cómo combatir el Shadow IT con Tranxfer?

- Permite tener **trazabilidad** de la información, todo lo que entra y sale del perímetro corporativo.
- Es una herramienta que cumple con la **regulación GDPR**
- Permite despliegue de la herramienta **adaptándose e integrándose y manteniendo todas sus características** al entorno y sistema de tu empresa.
- **Garantizar la securización de los canales de envío y recepción de información, que convivirán con el correo electrónico habitual, las plataformas de compartición y repositorios tradicionales de documentos.**

Integrable con:

Office 365 Google Workspace

PIDE TU DEMO GRATUITA
tranxfer.com | 622 867 206

tranxfer | secure file exchange

Cómo evitar el Shadow IT

Shadow IT describe a cualquier tipo de estructura utilizada sin la aprobación del área de Tecnología de la Información (IT). Esta práctica puede tomar muchas formas.

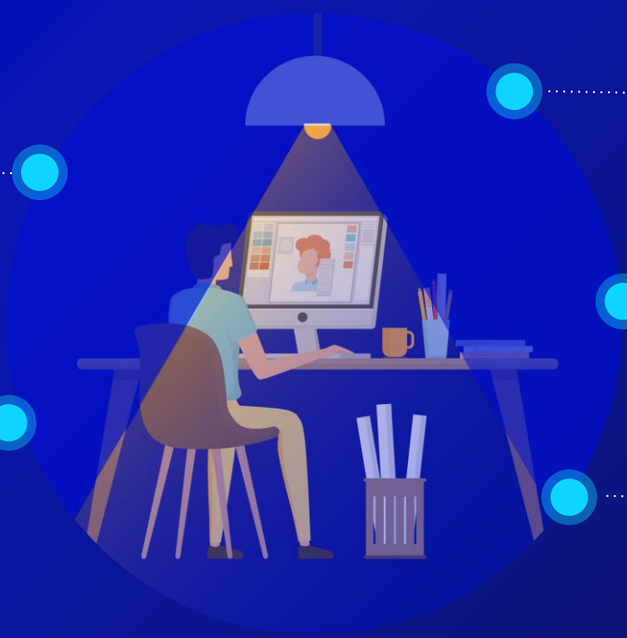
¿Qué está pasando en las empresas?

Sólo el 7%
de las aplicaciones SaaS gratuitas de internet cumplen con los estándares mínimos de seguridad

Los bancos y seguros
son las organizaciones que mayor riesgo corren debido al Shadow IT

Una tercera parte
de los trabajadores comparten y suben datos corporativos a herramientas externas a la organización, según IBM Security

Los 5 riesgos más habituales



- Enviar información comprometedora de la compañía a través de un canal no-seguro y no reconocido por el departamento IT.
- Desconocimiento de la ubicación de los servidores y del almacenamiento de la información.
- Facilidad de acceso a las herramientas sin necesidad de instalar ningún tipo de software.
- Peligro de fuga de información por parte de la organización sin saber motivo.
- Exposición de la organización por incumplimiento de la normativa GDPR.

Como combatir el Shadow IT

Concienciación

Brindar entrenamientos y capacitaciones sobre temas relacionados con la seguridad de la información, instruir a los usuarios sobre los riesgos inherentes a sus actividades.

Identificación y monitoreo

Identificar aplicaciones, software y procesos que se ejecutan en las sombras dentro de una red puede ser una tarea difícil.

Análisis de riesgo y adecuación

Después de la identificación, es necesario ver qué impacto tiene este software o hardware en la red e iniciar el proceso de análisis para determinar la mejor manera de eliminarlo del entorno.

Gestión de procesos y análisis de necesidades

En general, la gestión de los procesos es más responsabilidad de las áreas responsables que del departamento de tecnología de una empresa. Una de las formas en que se mitigan estos riesgos es hacer que el ciclo de análisis del proceso sea continuo.

Integrable con:

Office 365 Google Workspace