

Tips para mantener la seguridad de tus archivos en teletrabajo

La digitalización de los procesos en los diferentes sectores empresariales es un hecho. Las empresas más tradicionales están considerando invertir en automatización, pues ir a la oficina ya no es un requisito y lo que comenzó como un arreglo temporal por la pandemia, se ha consolidado como el modelo más habitual.

Por supuesto, la tecnología se ha convertido en la herramienta clave para hacerla verdaderamente productiva, según Worky, el software global en línea de recursos humanos.

En este sentido, no asombra la creciente adopción de dispositivos y soluciones tecnológicas que además de permitir trabajar desde cualquier lugar, facilitan y ahorran tiempos en los procesos laborales.

Consciente de esto y reconociendo la información como el insumo clave para toda organización, Adobe garantiza la seguridad en los archivos PDF. Para esto, integra los más altos estándares de privacidad en sus archivos, monitoreando constantemente el panorama de amenazas en evolución para adelantarse a las actividades malintencionadas y ayudar a garantizar seguridad a sus usuarios:

“Sabemos que son cientos las amenazas a las que se exponen los

archivos que podemos recibir y compartir, para evitar cualquier ataque aplicamos cientos de procesos y controles de seguridad que además de ayudarnos a cumplir con los estándares, regulaciones y certificaciones aceptados por la industria, también ayudan a proteger el software en todas nuestras aplicaciones e implementaciones”, afirmó Dario Llorente, Head of Latam Channel Sales en Adobe.

De esta manera, Adobe Document Cloud cumple con los requisitos de la industria al incluir SAFE BioPharma y FedRAMP, los cuales garantizan el cumplimiento normativo y permiten 4 aspectos fundamentales:

1. Proteger los archivos ante una copia o edición

Si necesita que sus documentos no se puedan imprimir, copiar o incluso imprimir, Document Cloud tiene la opción para que lo restrinja. Puede decidir qué acciones se realizan en sus propios documentos.

2. Escoger qué información dar

Hay información sensible que no todos los involucrados necesitan saber, puede censurar textos, imágenes y hasta páginas completas para que los que reciban el documento tenga acceso a los datos que usted elija (como datos personales, cifras, firmas, etc.). Además, al censurar esa información, a diferencia de otros programas, con Document Cloud borra inmediatamente la metadata haciendo que sea imposible hackearlo.

3. Seguridad para compartir archivos

Los documentos que cree con Acrobat – Document Cloud se etiquetan automáticamente como privados por seguridad, es decir, el único que los puede ver es el usuario que lo cargó en la nube. Para compartir puede dar la opción de `_solo ver` `_(solo lectura)` o `_revisar` `_(para poder comentar)` y compartirlo a través de un link.

4. Controlar los accesos

Adobe ofrece dos opciones para mayor ciberseguridad: certificados o contraseñas. Las contraseñas deberán introducirse antes de poder abrirlo y usted escoge cuál poner.

Sin embargo, aunque las empresas son cada vez más conscientes de que las normativas de seguridad ahorran tiempo a la vez que garantizan un flujo de trabajo seguro de forma coherente, no siempre saben cómo aplicarlas.

Según Adobe, Se puede evidenciar el gran abanico de herramientas digitales que existen en el mercado con las cuales las organizaciones pueden asegurar su información y documentación, esto bajo un contexto de constantes cambios en los modelos de trabajo.

