3 pasos fundamentales para prevenir que su personal utilice herramientas de colaboración no autorizadas

Si su personal utiliza herramientas de intercambio de archivos basadas en la nube que usted prohíbe, es probable que sea consciente de los desafíos que esto crea dentro de su organización y su estrategia de información. En un informe reciente de investigación de AIIM, **What's happening with file sync and share?**, las organizaciones compartieron las tres mayores áreas de preocupación:

- Falta de visibilidad del contenido compartido y dónde está ubicado
- Incapacidad de controlar quién comparte y accede a su información
- Riesgo de otorgar el acceso no intencional

Con estos desafíos en mente, ¿cómo puede empoderar a sus empleados para realizar su trabajo y a su vez prevenir que utilicen herramientas no autorizadas? Más allá del paso obvio de restringir el acceso a las URL para ciertos productos basados en la nube, hay tres pasos esenciales que puede seguir para garantizar un intercambio seguro del contenido.

1 PASO 1: EDUCAR A SUS EMPLEADOS

Cuando se les preguntó cómo sus organizaciones abordan los desafíos actuales de compartir información, un asombroso 65 % de los encuestados en el estudio AIIM citaron la educación como su principal método de defensa.

Curiosamente, como señala esta investigación, las organizaciones confían más en la educación que en otras soluciones tangibles como el uso de la tecnología o la aplicación estricta de políticas.

Con esto en mente, ¿cómo se puede empoderar a alguien para hacer algo a la vez que se le hace consciente de los riesgos de una mala decisión? A través de la educación adecuada, por supuesto.

Es como la lección que todos aprendimos de niños: "detente, mira y escucha". Puede adaptar esta conversación para ayudar a sus empleados **a detenerse y pensar antes de compartir información con otros**.

ShareBase® by Hyland

2 PASO 2: OFRECER UNA HERRAMIENTA ÚTIL Y APROBADA POR LA ORGANIZACIÓN PARA LOS EMPLEADOS (NO SÓLO CORREO ELECTRÓNICO)

En el mundo del intercambio de contenido, el correo electrónico es una herramienta que no se puede ignorar. De hecho, el 85 % de los encuestados por AIIM mencionó el uso de correo electrónico para compartir, y lo ubicaron en el primer lugar en la lista, incluso por encima de las aplicaciones de colaboración basadas en la nube.

Entonces, ¿por qué las herramientas de colaboración basadas en la nube se están volviendo tan populares si el correo electrónico ha estado allí todo el tiempo? Aunque se utiliza con frecuencia, el correo electrónico presenta exactamente las mismas preocupaciones que las herramientas de colaboración basadas en la nube.

Primero, hay una falta de visibilidad sobre lo que se comparte y dónde está. Por supuesto, el correo electrónico puede proporcionar cierta capacidad para rastrear quién compartió qué y con quién; sin embargo, nadie niega que esta es una tarea engorrosa en el mejor de los casos.

¿El correo electrónico le da la capacidad de controlar quién comparte y accede a su información o mitiga el riesgo de otorgar acceso no intencional?
Por supuesto que no. Tan pronto como un correo electrónico sale de su servidor, puede llegar a manos de cualquier persona.

Por el contrario, otras formas de compartir incluyen el envío de una unidad USB cifrada con contraseña o la configuración de un sitio de descarga FTP. Si bien estos métodos abordan algunas de las preocupaciones y pueden ser válidos en algunas situaciones, ambos son métodos más lentos para compartir documentos de forma segura.

Es evidente que se necesita una alternativa viable y segura de intercambio de archivos para enfrentar estos desafíos, que ofrezca la velocidad del correo electrónico pero la misma seguridad y control de los sitios FTP y unidades USB.

3 PASO 3: ASIGNAR UN PROPIETARIO CLARO PARA EL PROBLEMA

En la encuesta de AIIM, cuando se propuso la pregunta: "¿quién es el responsable de asegurar el uso adecuado de las herramientas, políticas y procedimientos para compartir contenidos? No hay un estándar claro entre las organizaciones.

De hecho, el 45 % de las organizaciones dijo que era responsabilidad del personal de TI; el 33 % dijo que era de los ejecutivos de línea de negocio, del jefe de departamento o propietario de proceso; el 21 % dijo que era responsabilidad del gerente/director de gobierno de la información; el 11 % dijo que era del director general de cumplimiento; y el resto dijo que era del director de informática, del director de operaciones u otro.

El 32 % que tiene a alguien dedicado a la gestión de la información o al cumplimiento de normativas merece una felicitación. Este es un excelente papel y departamento para poseer esta área, ya que pueden ver de manera integral la forma en que se gestiona la información a través de todas las herramientas.

En el caso de aquellas organizaciones que no cuentan con personal para un puesto de gobierno o cumplimiento dedicado, deben tomar algunas decisiones. El paso clave es elegir a alguien a quien responsabilizar por el problema de compartir contenido y luego, asegurarse de que todos los miembros de su organización sepan dónde está la responsabilidad.

Si bien existen muchos desafíos, hay un camino claro para combatir el dilema de compartir contenido y evitar que sus empleados utilicen herramientas no autorizadas: Educarles, proporcionarles una alternativa viable y asignarles la titularidad sobre el tema.

Recuerde, no puede impedir que los empleados compartan el contenido, pero usted puede ayudarles a que paren, piensen y luego elijan la herramienta correcta para compartir.

Obtenga más información en **ShareBase.com »**

ShareBase® by Hyland