docusign

Las mejores prácticas para la seguridad y gestión de documentos electrónicos

eBook

Introducción

Más tecnología, más atención a la ciberseguridad

En la era digital, la gestión de documentos electrónicos se ha convertido en una práctica fundamental para empresas y organizaciones de todo tipo. La transición de los documentos físicos a su contraparte digital trae consigo una serie de ventajas significativas, como la accesibilidad instantánea, la eficiencia operativa y la reducción del uso de papel.

Sin embargo, la digitalización también conlleva nuevos desafíos en términos de ciberseguridad. Implementar buenas prácticas de gestión documental es esencial para garantizar la autenticidad, integridad y seguridad de todos los documentos corporativos.

Entonces, ¿cómo llevar a la práctica una gestión de documentos electrónicos que tenga a la seguridad como eje?

Este eBook tiene como objetivo explorar la importancia de la seguridad en la gestión documental. Además, examinaremos el papel de la firma electrónica como una herramienta clave para asegurar la validez y seguridad de los documentos en el entorno digital.

La gestión de documentos electrónicos frente a la gestión en papel

En la actualidad, presenciamos una transición hacia la gestión de documentos electrónicos, dejando atrás los métodos tradicionales basados en papel, que son menos amigables con el medio ambiente, más costosos y complicados.

Priorizar los documentos electrónicos frente al papel supone que cada vez más organizaciones adoptan soluciones en la nube como las firmas electrónicas y distintos software de gestión documental.

En efecto, según un informe reciente de la firma KMPG, **9 de cada 10 negocios ya han avanzado en la adopción de sistemas en la nube**.

En cuanto a las herramientas específicas de gestión de documentos digitales, la implementación es más lenta, pero no por eso menos significativa. De acuerdo a datos de Statista, los departamentos que más utilizan herramientas de gestión documental son:

62% Ventas	57% Marketing	53% Finanzas	41% TI
39% Legal	35% Operaciones	28% Recursos Humanos	

Como anticipamos, la transición del papel hacia lo digital requiere la puesta en marcha de herramientas y procesos que puedan **garantizar la seguridad de la información**, tanto de la empresa como de sus clientes y proveedores.

Y allí está el mayor desafío: de acuerdo al informe mencionado de KMPG, el **58% de los equipos de ciberseguridad admiten estar atrasados en sus procesos**.

A partir de estos datos, se abren dos preguntas relevantes: ¿cuáles son las ventajas de la gestión electrónica de documentos que hacen que las empresas decidan llevarla a cabo?, y ¿qué medidas tomar para afrontar con éxito el desafío de la seguridad?

Las ventajas de gestionar documentos de manera electrónica

La gestión de documentos electrónicos ofrece una amplia gama de ventajas que explican su adopción por parte de empresas de todos los tamaños e industrias. A continuación, exploraremos algunas de las más destacadas, centrándonos en la seguridad de los documentos electrónicos y otros aspectos relevantes.

Seguridad

Los documentos electrónicos proporcionan niveles superiores de seguridad en comparación con los documentos en papel. Al implementar buenas prácticas y medidas como la encriptación de datos, el control de acceso basado en roles y la autenticación de usuarios, es posible proteger la integridad y confidencialidad de los documentos electrónicos.

Disponibilidad instantánea y colaboración

Al estar almacenados en formato digital, los documentos pueden ser consultados, compartidos y modificados de manera simultánea por múltiples usuarios, lo que facilita la colaboración en tiempo real, acelera los procesos de toma de decisiones y mejora la eficiencia operativa en general.

Eficiencia operativa y ahorro de costos

Eliminando la necesidad de manejar y almacenar documentos físicos, se reduce el tiempo y los recursos dedicados a tareas manuales y repetitivas.

Las soluciones de gestión documental automatizan flujos de trabajo, como la aprobación y firma de documentos, **lo que acelera los procesos y minimiza los errores humanos**. A largo plazo, este proceso permite un ahorro significativo de costos asociados con la compra de papel, impresión, almacenamiento físico y transporte.

Cumplimiento normativo y auditoría

Contando con herramientas de control de versiones, trazabilidad y registro de actividades, se simplifica la auditoría y se garantiza el cumplimiento normativo. Del mismo modo, la capacidad de aplicar permisos y restricciones de acceso a los documentos electrónicos ayuda a asegurar que solo las personas autorizadas puedan acceder y manipular la información confidencial, evitando incumplimientos legales y potenciales fugas de información.

Sostenibilidad

Independizar los procesos del papel disminuye la deforestación y evita la generación de residuos asociados a la eliminación de documentos físicos. En ese sentido, la transición hacia documentos electrónicos **fomenta prácticas empresariales responsables desde el punto de vista ambiental,** al reducir la huella de carbono relacionada con la producción, transporte y eliminación de papel.

Mejores prácticas para la seguridad y gestión de documentos electrónicos

En términos simples, la ciberseguridad se refiere a las medidas y prácticas diseñadas para proteger los sistemas informáticos, las redes y la información digital contra amenazas cibernéticas.

Como vimos, la seguridad en la gestión de documentos electrónicos es esencial para proteger la confidencialidad, integridad y disponibilidad de la información. Aquí nuestros consejos más importantes para que este sistema pueda tener cabida dentro de las organizaciones.

Almacenar de forma segura los archivos

El almacenamiento seguro de archivos es crucial para proteger la información sensible. Algunas prácticas recomendadas incluyen:

- Utilizar sistemas de almacenamiento en la nube con altos estándares de seguridad, como cifrado de datos, autenticación de usuarios y copias de seguridad regulares.
- Aplicar políticas de control de acceso para que solo los usuarios autorizados puedan acceder a los archivos.
- Implementar medidas de encriptación — transformación de datos en un formato codificado para proteger su confidencialidad y seguridad — para proteger la confidencialidad de los archivos, tanto en tránsito como en reposo.
- Establecer permisos y niveles de acceso adecuados a los diferentes roles dentro de la organización.
- Realizar auditorías periódicas para detectar posibles vulnerabilidades y asegurar el cumplimiento de las políticas de seguridad establecidas

Mantener la seguridad de los dispositivos informáticos

La seguridad de los dispositivos informáticos empleados para acceder y gestionar documentos electrónicos es crucial, y puede lograrse a través de diversas prácticas como:

- Mantener los dispositivos actualizados con los últimos parches de seguridad y actualizaciones del sistema operativo.
- Usar software antivirus y antimalware actualizado en todos los dispositivos. Establecer contraseñas fuertes y únicas para acceder a los dispositivos e incluir la autenticación multifactor (MFA) cuando sea posible.
- Evitar el uso de redes wifi públicas o inseguras al acceder a documentos electrónicos confidenciales.
- Utilizar herramientas de cifrado de datos en los dispositivos - proceso de transformación de la información en un formato ilegible y seguro - para proteger la información en caso de pérdida o robo.

Elegir socios comerciales con certificaciones de seguridad

Cuando las organizaciones trabajan con socios comerciales o proveedores de servicios de gestión documental, es importante asegurarse de que cumplan con altos estándares de seguridad, además de:

- Verificar que los socios tengan certificaciones reconocidas en materia de seguridad, como ISO 27001, que garantiza que siguen las mejores prácticas en torno a la seguridad de la información.
- Revisar las políticas de seguridad y privacidad del proveedor para asegurarse de que se alineen con los estándares y regulaciones vigentes.
- Establecer acuerdos de confidencialidad y seguridad con los socios comerciales, que incluyan cláusulas que protejan la confidencialidad y el manejo seguro de los documentos electrónicos.

Capacitar a empleados y colaboradores

Es fundamental capacitar y concienciar a los empleados sobre la importancia de la seguridad en la gestión de documentos electrónicos.

Esto incluye educar sobre la manipulación segura de archivos, el uso adecuado de contraseñas, la identificación de correos electrónicos o enlaces sospechosos y la adopción de buenas prácticas en el manejo de la información.

Adoptar la firma electrónica

La firma electrónica proporciona una capa adicional de autenticación y verificación en los procesos de firma y envío de documentos digitales, brindando una mayor confianza y seguridad tanto para las empresas como para los usuarios.

Uno de sus principales beneficios es la capacidad para garantizar la integridad y autenticidad de los documentos. Al utilizar técnicas criptográficas, la firma electrónica asegura que el contenido del documento no haya sido alterado desde su firma, y que la identidad del firmante sea verificable. Esto evita la manipulación y el fraude de documentos, ya que cualquier alteración o intento de falsificación sería detectado de inmediato.

¿Cuáles son los riesgos y amenazas que sufren las empresas?

Entonces, ¿por qué es tan importante invertir en la seguridad de los documentos electrónicos?

Al implementar medidas adecuadas y buenas prácticas en materia de seguridad, las organizaciones pueden evitar una serie de problemas y riesgos que **podrían afectar su reputación, operaciones y cumplimiento normativo**, como por ejemplo:

- Fugas y pérdida de información confidencial.
- Acceso no autorizado y uso indebido de la información.
- Incumplimiento normativo y legales.
- Interrupción de operaciones y pérdida de productividad.
- Daño a la imagen de marca y pérdida de confianza.

Las formas más comunes de ciberataque

Algunas de las formas más comunes de ciberataques incluyen:

Malware

El software malicioso es una forma de ataque cibernético que involucra la infiltración de programas o código malicioso en un sistema o red y puede causar daños significativos, como robo de información, interrupción de servicios, destrucción de datos o toma de control de sistemas.

Phishing

Un método en el que los atacantes intentan engañar a los usuarios haciéndose pasar por entidades legítimas, como bancos, empresas o servicios en línea, solicitando información confidencial, como contraseñas, números de tarjetas de crédito o datos personales.

Ingeniería social

Los ciberdelincuentes pueden hacerse pasar por empleados, representantes de servicio al cliente o incluso amigos en las redes sociales para obtener acceso no autorizado a sistemas o información sensible.

Ataques de fuerza bruta

Utilizando programas informáticos para intentar miles o millones de combinaciones hasta que encuentran la correcta. Los ataques de fuerza bruta son riesgosos porque pueden tener éxito si las contraseñas son débiles o fáciles de adivinar.

Ataques de denegación de servicio (DDoS)

Que buscan abrumar un sistema o red con un gran volumen de tráfico falso o solicitudes, lo que provoca la saturación y la interrupción del servicio legítimo.

Ataques de inyección SQL

Aprovechando las vulnerabilidades en las aplicaciones web que no validan correctamente las entradas del usuario. Los atacantes pueden enviar comandos SQL maliciosos a la base de datos subyacente, lo que les permite extraer, modificar o eliminar datos almacenados en la base de datos.

Qué motivan los ciberataques

Independientemente de su tamaño, toda empresa puede ser objeto de un ciberataque. Esto se debe a que las compañías poseen activos de interés para los ciberdelincuentes, como información financiera, personal y confidencial.

Algunas de las razones por las cuales existe este tipo de riesgo son:

Valor de la información

Dado que puede incluir datos confidenciales, secretos comerciales, información financiera, datos personales, entre otros.

Beneficios económicos

La información obtenida puede tener un alto valor en el mercado clandestino y, por lo tanto, los ciberdelincuentes tienen como objetivo obtener beneficios económicos a partir de ella.

Motivaciones personales

Algunos ciberdelincuentes pueden tener motivaciones personales para acceder a la información de una organización, como perjudicar a una empresa o a individuos específicos, obtener ventajas competitivas o simplemente causar daño por diversión.

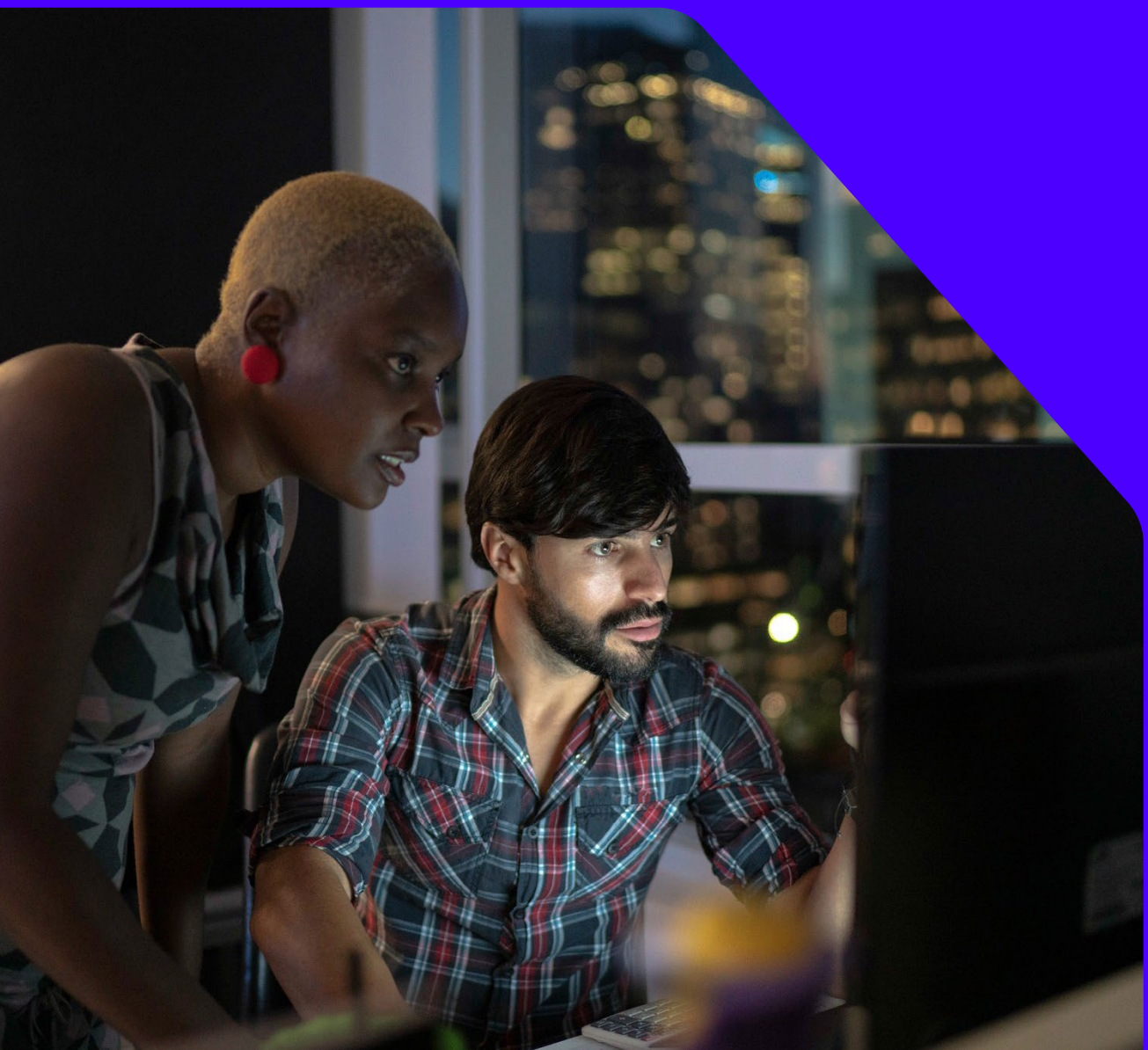
Vulnerabilidades tecnológicas

Que pueden estar relacionadas con sistemas operativos desactualizados, configuraciones incorrectas, fallos de seguridad en software o aplicaciones, entre otros. Los ciberdelincuentes buscan aprovechar estas vulnerabilidades para acceder de manera no autorizada a la información.

Para evitar estas amenazas, resulta necesario adoptar herramientas y soluciones digitales que proporcionen mecanismos de seguridad de datos, que son los aliados ideales para mitigar y prevenir diversos tipos de daño potencial a las empresas.

Ciberseguridad y la firma electrónica

Con el desarrollo tecnológico actual, no hay empresa que trabaje 100% de forma manual en el manejo de datos. Tanto las de reciente creación como las más conservadoras utilizan algún tipo de tecnología para recopilar, almacenar, procesar y analizar información.



Como hemos visto, existen varios recursos tecnológicos que actúan, de forma conjunta o separada, en la protección de datos de una empresa como: conexiones seguras, cifrado de datos, firma electrónica, almacenamiento en la nube, antivirus y antimalware. Aprende por qué la firma electrónica es una solución que promueve más seguridad a la empresa.

Por qué la firma electrónica es más segura

La firma electrónica es una de las tecnologías centrales de la gestión de documentos electrónicos y puede ser más segura que sus contrapartes de papel.

Esto se debe a que, entre otras razones, la firma electrónica tiene muchas capas de seguridad y autenticación integradas, además de que es prueba de transacción admisible ante las cortes:

Registro electrónico

A diferencia de las firmas con tinta, las firmas electrónicas tienen un registro electrónico que sirve como registro de auditoría y prueba de transacción. El registro de auditoría incluye el historial de acciones tomadas en el documento, como cuándo se abrió, leyó y firmó. Si uno de los signatarios disputa su firma, o si hay dudas sobre la transacción, este registro de auditoría está disponible para todos los participantes en la transacción y pueden resolver dichas objeciones.

Certificados de finalización

Los certificados de finalización detallados pueden incluir información específica sobre cada signatario del documento, incluyendo la divulgación del consumidor que indica que el signatario acordó usar firma electrónica, la imagen de la firma, sellos de hora de eventos clave y la dirección IP del signatario y otra información relevante.

Sello contra manipulación

Una vez que se ha completado el proceso de firma, todos los documentos se sellan electrónicamente mediante el uso de Public Key Infrastructure (PKI), una tecnología estándar de la industria. Este sello indica que la firma electrónica es válida y que el documento no ha sido manipulado ni alterado desde la fecha de la firma.

Una solución de firma electrónica adecuada debería poder proveer todo lo anterior. Asimismo, debe contar con certificaciones de terceros neutros que confirmen sus declaraciones. La certificación ISO 27001 es el más alto nivel de garantía de seguridad disponible en el mundo.

En suma, la firma electrónica ofrece una mayor seguridad en comparación con la firma manuscrita. Esta utiliza procesos de autenticación que permiten verificar de manera fehaciente la identidad de las personas y la autenticidad de los actos.

Cada paso del proceso tiene un alto nivel de seguridad, garantizando:

Autenticidad y no repudio

A través de técnicas criptográficas para garantizar la autenticidad del firmante y prevenir el repudio posteriors.

Integridad del documento

Cualquier modificación realizada en el documento después de haber sido firmado electrónicamente se detecta de inmediato, ya que alteraría la firma digital.

Seguridad en la transmisión y almacenamiento

Esto garantiza que las firmas electrónicas no sean interceptadas o modificadas durante la transmisión y que los documentos firmados estén protegidos contra accesos no autorizados.

Registro y trazabilidad

La firma electrónica deja un rastro digital y un registro detallado de las transacciones, incluyendo información sobre quién firmó el documento, cuándo se realizó la firma y cualquier otro dato relevante. Esto contribuye a la reducción de fraudes.

¡Hablemos!

La gestión de documentos electrónicos en reemplazo del papel presenta numerosas ventajas para las organizaciones. No obstante, contar con tecnologías de punta y medidas de seguridad acordes es primordial para proteger datos sensibles y garantizar la integridad y autenticidad de los documentos.

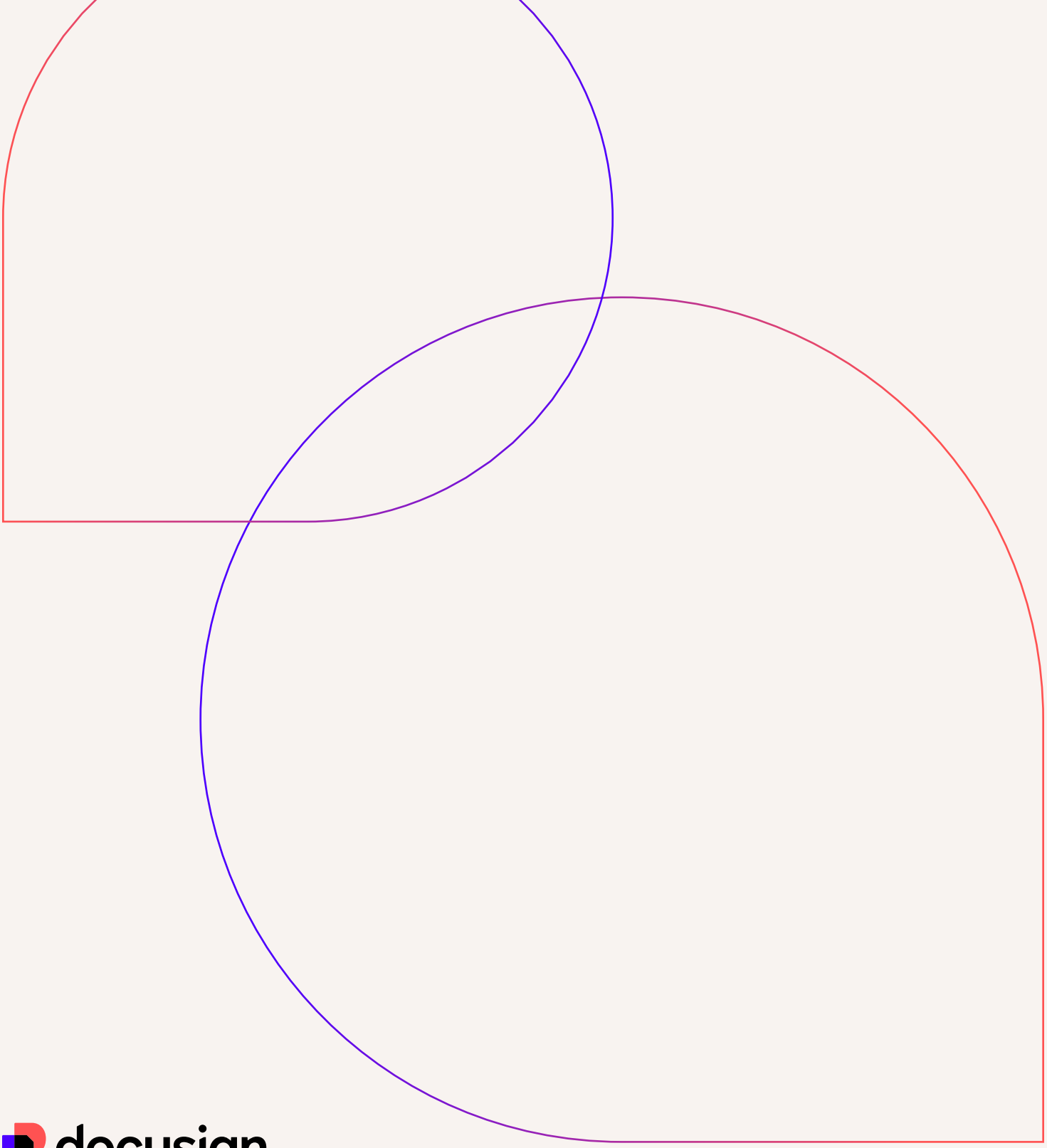
En ese sentido, la firma electrónica es una tecnología segura y capaz de añadir valor a los procesos internos.

Para obtener más información y explorar cómo satisfacer las necesidades de tu empresa en relación con la firma electrónica y la gestión de documentos, te invitamos a entrar en contacto con nosotros.

Habla con uno de nuestros especialistas

Prueba la firma electrónica gratis por 30 días

¡No pierdas la oportunidad de simplificar tus procesos, aumentar la eficiencia y mejorar tus operaciones!



Acerca de Docusign

Docusign ayuda a las organizaciones a conectarse y automatizar la forma en que preparan, firman, ejecutan y gestionan los acuerdos. Como parte de Docusign Agreement Cloud, Docusign ofrece eSignature, la forma número 1 del mundo de firmar electrónicamente en prácticamente cualquier dispositivo, desde casi cualquier lugar y en cualquier momento. Hoy en día, más de un millón de clientes y más de mil millones de usuarios en más de 180 países utilizan Docusign Agreement Cloud para acelerar el proceso de hacer negocios y simplificar la vida de las personas.

Docusign, Inc.
Av Jarrier Barros Sierra 495 Santa Fe,
Zedec Sta Fé, Álvaro Obregón 1219
Ciudad de México
docusign.mx

Para obtener más información
contactomx@docusign.com
01-800-9531-662