Transferencia Segura de Archivos: Un habilitador clave que promueve eficiencia, productividad y seguridad en la gestión de la información

Sebastian Miranda

Septiembre 2021

Patrocinado por: tranxfer | secure file exchange

Introducción

La digitalización está cambiando la forma en que las organizaciones llevan a cabo sus negocios y las relaciones sociales. Un aumento de productividad y eficiencia probado y un efecto colateral indeseado que es el aumento de las vulnerabilidades, brechas y riesgo digital, adquieren cada vez más importancia.

La forma en que las organizaciones llevan a cabo sus negocios y las relaciones sociales están cambiando. La pandemia de COVID-19 obligó a muchas organizaciones a adoptar nuevas medidas para mantener la productividad y seguridad en entornos remotos. Se han transformado los paisajes empresariales y el mundo del trabajo, y se está redefiniendo el concepto de empresa, los límites de producción, consumo y distribución. Esto está creando enormes oportunidades, ya que han surgido nuevos productos, procesos y técnicas, pero también ha creado amenazas, sobre todo en materia de seguridad, donde los ciberataques han aumentado más de un 400%.

Datos destacados

- Más del 70% de las organizaciones en España han acelerado su proceso de transformación digital y han digitalizado el puesto de trabajo como primera solución a la continuidad de negocio y seguridad física.
- Estudios de IDC indican que la gestión de usuarios, identidades y accesos es una de las principales prioridades para el 34% de las empresas en España.
- En el mundo de la seguridad en España, los gastos más representativos están relacionados con los servicios gestionados, servicios de integración y seguridad del endpoint. Estos representan el 55% de la inversión para 2021.
- El gasto en blockchain seguirá teniendo un fuerte crecimiento para el periodo 2021-2024 con una tasa de crecimiento anual compuesto (CAGR) cercana al 42%.

Debido a este reciente cambio global y a las nuevas tecnologías, la forma de trabajar de las empresas ha cambiado. Ahora tenemos servicios automatizados, humanos que hablan con máquinas y viceversa. En la era de los contenidos de internet, todo se puede copiar. Las empresas cada vez necesitan más de herramientas que garanticen la seguridad y la trazabilidad de todas las transacciones que se producen dentro del perímetro. Sin embargo, este problema se resuelve con la ayuda de una máquina de confianza, diseñada y desarrollada por Satoshi utilizando las tecnologías existentes, por ejemplo, un mecanismo de encriptación avanzado y un algoritmo de consenso.

Las organizaciones se están enfrentando a un creciente número de amenazas, riesgo de acceso a la información y a la sofisticación de los ciberdelincuentes. Es importante destacar que en un entorno de convergencia de redes IT con OT e internet de las cosas, cada vez más las organizaciones presentan la necesidad de gestionar no solamente identidades de personas y accesos, sino que hay una creciente tendencia de interacciones entre usuarios cada vez más conectados de manera remota haciendo uso de múltiples dispositivos. Esto incluye gestionar todos los objetos físicos y lógicos que tengan la capacidad de transferir datos a través de una red, poniendo el foco siempre en la confianza.

Todas las acciones humanas que requieran confianza necesitan de la trazabilidad registrada como prueba, utilizando el historial de transacciones que han ocurrido en el pasado. Las empresas necesitan mantener un registro de la prueba de que se ha firmado un acuerdo o de que ha ocurrido un evento en un momento determinado.

Conclusión

Las compañías que logren interactuar con sus clientes y grupos de interés mediante procesos amigables y sin fricciones mientras mantienen la seguridad y el cumplimiento, van a alcanzar una notable ventaja competitiva.

Alcanzar la ventaja en una economía digitalizada requiere de iniciativas para optimizar la gestión segura de datos y archivos. Esto supone unos retos a las organizaciones como son la gestión de la identidad digital, la soberanía del dato y la orquestación e integración de los entornos de TI.

Los organizaciones están en la búsqueda de formas de trabajo inteligentes, y un framework unificado que integre soluciones de seguridad de manera simple, facilite la gestión y brinde mejor experiencia al usuario alcanzando la confianza digital, parece ser el camino ideal por parte de los proveedores de servicios.

Una parte esencial del trabajo inteligente es la transferencia de archivos y datos de manera eficiente y segura. Esto puede ayudar a una empresa a lograr múltiples objetivos relacionados con los datos, como los requisitos de cumplimiento, la trazabilidad y autenticación de documentos, la gestión segura de datos sensibles y la mejora de la eficiencia operacional.

La gestión de identidades ha sido y seguirá siendo una prioridad para las organizaciones, pues es un habilitador fundamental para el negocio que permite la implantación de estrategias alineadas con las necesidades de la organización es una parte fundamental en la coyuntura actual de modelos de trabajo híbrido.

En este contexto, los profesionales de la ciberseguridad se centran en los siguientes objetivos de control al diseñar los esquemas de protección de sus datos:

- Confiabilidad: Asegurar que los datos permanezcan secretos y no sean vistos o usados por personas inapropiadas.
- Integridad: Garantizar que los datos son legítimos y no son modificados por partes inapropiadas.
- Disponibilidad: Garantizar que los datos estén disponibles para su uso por las partes apropiadas.
- Propiedad: Garantizar que los sistemas en uso nos obstaculicen las necesidades existentes y no se utilicen de forma que puedan perjudicar a la organización o hacerla responsable de alguna acción.
- Transferencia: Garantizar que el envío y recepción de información y archivos se realiza en un entorno seguro infranqueable.

Hacia la búsqueda de la identidad digital y de la seguridad en el intercambio de información

Es necesario que las organizaciones aborden la digitalización de sus negocios de forma integral, lo que supone afrontar múltiples desafíos relacionados con la ciberseguridad, la adaptación a nuevas normativas, la capacidad de procesar una ingente cantidad de datos o la forma de trabajar y de comunicarse con clientes o empleados. Todo ello, sin perder de vista el control presupuestario.

La implantación de nuevas soluciones tecnológicas es la única vía para poder adaptarse con agilidad a las actuales y cambiantes condiciones del mercado, automatizar procesos, garantizar la seguridad de la información, cumplir con la legalidad vigente y proporcionar un experiencia de usuario excelente.

El crecimiento de amenazas cada vez más sofisticadas y enfocadas a verticales supone un mayor riesgo para las organizaciones. Los usuarios son cada vez más el objetivo de los ciberdelincuentes y, por esa misma razón, el enfoque de la ciberseguridad debe pasar por una cobertura integral, desde una infraestructura tecnológica adecuada, hasta la formación y concienciación en seguridad para los empleados.

Proteger las comunicaciones mediante encriptación y protección del mensaje es vital hoy en día, así como también asegurar que el mensaje llega al destinatario correcto y que sólo este sea capaz de recibir la documentación mediante una clave o un doble factor. La misma relevancia tiene asegurar que el contenido de la información expire en tiempo y forma para garantizar la protección de usuarios y empresa. La información que no existe no puede ser vulnerada.

La digitalización está cambiando la forma en que las organizaciones llevan a cabo sus negocios y las relaciones sociales. Además, la pandemia de COVID-19 ha obligado a muchas organizaciones a adoptar nuevas medidas para mantener la productividad y seguridad en entornos remotos. Un aumento de productividad y eficiencia probado y un efecto colateral indeseado que es el aumento de las vulnerabilidades, brechas y riesgo digital, adquieren cada vez más importancia. Todo esto, ha sido posible gracias a las soluciones de identidad digital.

El cambio a la interacciones y transacciones digitales se basa en soluciones de autenticación, autorización y acceso, que sean transparentes, de fácil uso, escalables y seguras. En un entorno donde el perímetro tradicional de seguridad está difuminado y aparecen cada vez más dispositivos y datos, las soluciones de gestión de identidades y activos digitales se han convertido en un imperativo estratégico de la noche a la mañana.

Por lo tanto, resulta muy importante que una empresa utilice herramientas que añaden un nivel de confianza a la autenticidad de sus datos personales y empresariales. Para las empresas empieza a ser fundamental asegurarse de la autenticidad de los archivos. Es aquí donde la identidad digital, la integridad y la autenticidad se ponen en valor.

Ante esto, los proveedores de soluciones tienen un papel clave a desempeñar, permitiendo a las organizaciones entrar a la curva de recuperación y la nueva normalidad, como empresas confiables y preparadas para el futuro.

Ciberseguridad y Ciberataques

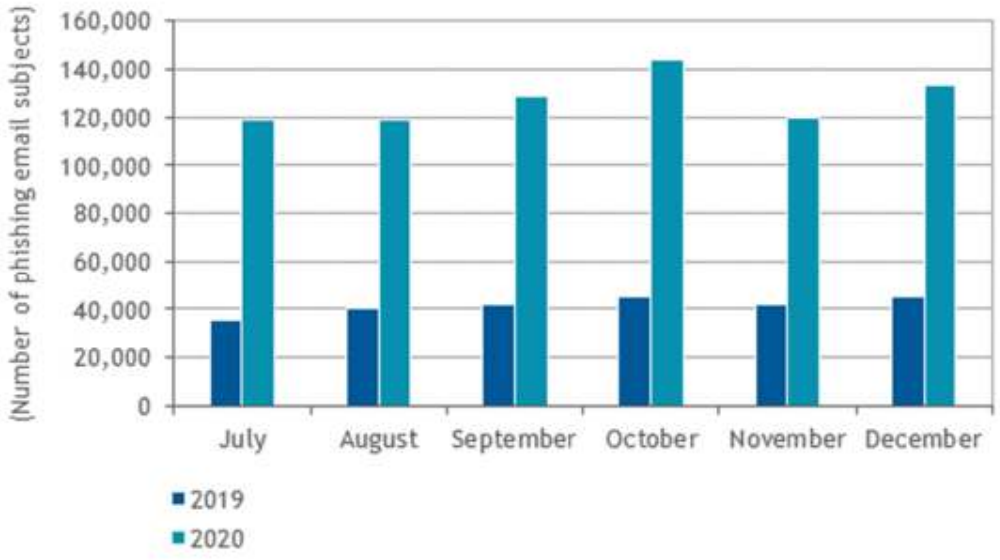
La ciberseguridad es hoy una de las industrias en crecimiento y una de las herramientas más necesarias para los negocios. Los ataques al correo electrónico son uno de los principales dolores de cabeza. En un mundo globalizado, con constante flujo de datos e interacción, es fácil que se presenten en algún momento virus, troyanos, ransomware y cualquier tipo de malware si no se está preparado. Ante esto, no debemos subestimar el hecho de que estos ataques maliciosos tienen la capacidad de hundir una empresa.

Un ciberataque es un conjunto de acciones ofensivas contra sistemas de información. Pueden tener objetivos diferentes, como atacar equipos y sistemas para anular los servicios que presta una empresa, sustraer información almacenada en las bases de datos o robar la identidad de los trabajadores para cometer fraudes.

El correo electrónico es uno de los medios de comunicación más utilizados en los últimos tiempos a través de Internet. Pero, es cierto que aunque se haya mejorado la seguridad de este medio, sigue habiendo debilidades que permite a los ciberdelincuentes poder robar información personal de los usuarios. De hecho, el canal de entrada de los ciberataques más comunes es el email, y entre ellos se encuentra: El ransomware, phishing, fraude al CEO y *Man in the Middle*. Además, el correo electrónico incrementa la vulnerabilidad empresarial, la extensión generalizada del uso del email como herramienta de comunicación principal entre empresas y usuarios los pone en cierto riesgo sin que ellos sean del todo conscientes.

En la misma línea, las vulnerabilidades que tiene el email, a nivel de seguridad, hace que correos electrónicos maliciosos pasen las barreras de seguridad sin ningún problema ,los ciberdelincuentes mejoran sus técnicas para poder enviar este tipo de contenido y que parezca fiable.

Figura 1. Unique Phishing Email Subjects (2019-2020).



Fuente: IDC, Worldwide Corporate Endpoint Security Forecast, 2021–2025.

Nunca conformes, los cibercriminales se abalanzaron sobre una superficie de ataque ampliada por el rápido cambio al teletrabajo. La oportunidad para estos actores es innegable por el cambio en los

mecanismos de seguridad perimetral corporativos y usuarios finales que se conectan a sistemas y aplicaciones a través de redes domésticas no administradas con una combinación de propiedad personal y dispositivos de propiedad corporativa que probablemente no se monitorizan con el mismo grado de diligencia que en tiempos previos a la pandemia. Además, arrojados a condiciones de trabajo inusuales y enfrentando múltiples incertidumbres, los usuarios finales fueron vistos, con razón, de una manera susceptible a las tácticas de los cibercriminales que se aprovechan de las emociones humanas, como el phishing perpetrado a través del correo electrónico (ver figura 1).

Proteger los activos de la empresa y su información.

El mundo se encuentra en un momento marcado por cambios extraordinarios e incertidumbre, donde se hace visible una creciente demanda por servicios con un nuevo nivel de análisis de datos, automatización, y capacidades de inteligencia artificial para lograr la continuidad de negocio, la resiliencia digital y la eficiencia operativa.

IDC espera que el gasto europeo en *Robotic Process Automation* (RPA) crecerá a una tasa de crecimiento anual compuesto (CAGR) del 12%, hasta llegar a los €24.778 millones en 2024, donde las organizaciones del sector manufactura y consumo representarán el gasto en un 68% y 11% respectivamente. Las empresas más grandes están incrementando el gasto especialmente en tecnologías como cloud (principal impulsor de innovación), inteligencia artificial y automatización para minimizar el impacto de la crisis, y están identificando oportunidades para abordar los retos en el camino hacia la nueva normalidad. A medida que las agendas de los directores para respaldar estas iniciativas digitales evolucionan, la automatización se consolida rápidamente como la piedra angular de la futura organización.

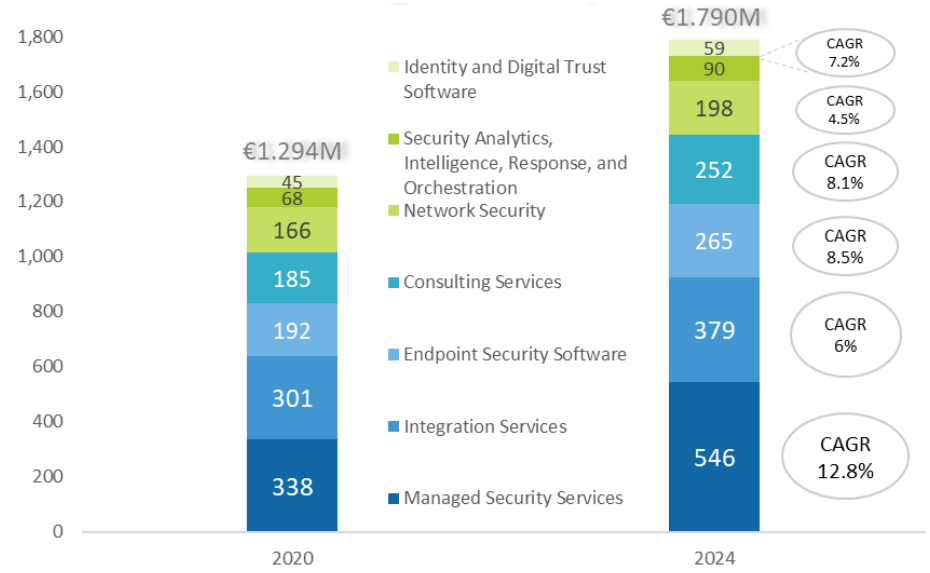
Esta futura organización se caracteriza porque tiene una visión a futuro con un enfoque hacia la optimización de la automatización de procesos para impulsar la creación de valor y la experiencia del cliente, que además demanda idoneidad en el diseño y desarrollo de productos y servicios. En la misma línea, es bastante obvio que la pandemia de COVID-19 ha cambiado las expectativas y prioridades tanto de clientes, como de proveedores, empleados y partners, pero las organizaciones ahora están buscando la manera de aprovechar la hiperautomatización (que incluye RPA junto con otras tecnologías y soluciones) para resolver incidencias de negocio y lograr los objetivos de negocio.

El gasto europeo en RPA está estimado para 2021 en €17.644 millones y tiene una tasa de crecimiento anual compuesto CAGR a 2024 del 12%

El gasto de TI en seguridad en España para 2020 es de € 1.460 millones y se espera un crecimiento CAGR a 2024 del 8.3%.

Figura 2. Inversión en seguridad en España (2021-2024).

Transferencia Segura de Archivos: Un habilitador clave que promueve eficiencia, productividad y seguridad en la gestión de la información



Fuente: IDC's Worldwide Security Spending Guide

En el mundo de la seguridad en España, los gastos más representativos están relacionados con los servicios gestionados, servicios de integración y seguridad del endpoint. Estas tres categorías representan el 55% de la inversión para 2021, que asciende según nuestras estimaciones, a €1.586 millones.

Sin embargo, la gestión de identidades ha sido y seguirá siendo una prioridad para las organizaciones, pues es un habilitador fundamental para el negocio ya que además de proporcionar la primera línea de defensa frente a accesos no autorizados, las áreas internas de la organización necesitan disponer de formas rápidas y simples de poder entender quién – o en cada vez más casos "qué" – conforman sus usuarios digitales, con el objeto de poder construir experiencias más atractivas y personalizadas conforme demandan clientes y empleados. Estamos en una coyuntura que hace esencial replantear algunas de las estrategias para dar respuesta a una problemática creciente en cuanto a amenazas, la migración al cloud, y que estas estrategias estén alineadas con las necesidades de la organización es una parte fundamental para sacarle valor a las funcionalidades de las soluciones que se encuentran en el mercado.

Conjuntamente, la gestión de riesgos es sin duda una de las áreas más críticas en la agenda de cualquier responsable de seguridad de la información, y más aun considerando el rápido cambio en el panorama de amenazas junto con la necesidad de abordar todos los componentes fundamentales de las arquitecturas de TI y procesos (endpoint, red, mensajería, web, dispositivos móviles, cloud y tecnología operativa).

En este sentido, la encuesta europea sobre seguridad de TI muestra que en el 34% de los casos para España, una de las principales prioridades para 2020 ha sido gestionar usuarios, identidades y accesos.

Algunas de las fuerzas que más están impactando el mercado de la gestión de identidades actualmente son:

- La identidad es el core de la seguridad, y esta debe ser intuitiva, fácil de usar y generar confianza.
- La autenticación remota sin fricciones.
- Transformación digital teniendo lugar en trimestres, no años.
- Gestión de privilegios disponible "*Just-in-time*" para más usuarios.

IDC espera que la seguridad como servicio es el modelo en el que las organizaciones gestionarán los retos más relevantes en los próximos años, dado que la seguridad en el contexto de cloud permite a los usuarios nuevas formas de implementar su estrategia de protección de datos, mayor resiliencia y acceso en tiempo real a la información. Según datos de IDC, el 38% de las empresas españolas tendrá seguridad en cloud en dos años.

Sin duda, la automatización es clave en esta coyuntura, como parte del esfuerzo de las organizaciones de darle eficiencia a los sistemas y dar respuesta a algunos de los retos más importantes en materia de seguridad. Por un lado, un creciente número de amenazas cibernéticas, y por otro una notable escasez de capacidades en ciberseguridad hace que las empresas estén buscando cada vez más formas de trabajo más inteligentes, así como también un framework unificado que integre las soluciones de seguridad de manera simple, facilite la gestión, brinde mejores experiencias a los usuarios y se logre la confianza digital.

La importancia de la gestión segura en la transferencia de archivos en la empresa del futuro.

Más que nunca el espacio de trabajo actual requiere de canales seguros para permitir la comunicación entre todas las partes de forma veraz y segura. La vulnerabilidad del correo electrónico y de los entornos de compartición con externos a la organización abren brechas y nuevas vulnerabilidades a la información de las empresas. Todo ello pone de manifiesto la necesidad de incluir herramientas seguras y fácilmente adoptables por parte del empleado para su gestión diaria en el intercambio de ficheros.

Aunque la adopción de políticas de *Smart Work* o el desarrollo de estas puede haber sido ampliamente abordado por las empresas, los datos de IDC indican que la infraestructura para la gestión de los trabajadores remotos no está a la par con la de aquellos que se encuentran físicamente en la oficina, por lo que la colaboración tanto interna como externa se presenta como un reto clave, al igual que el acceso móvil y remoto efectivo.

Esta rápida e imprevista movilización del espacio de trabajo ha llevado a las organizaciones a afrontar el desarrollo y puesta en marcha de soluciones seguras para el intercambio de información que facilitan la ciber resiliencia, lo que lleva a una mayor exposición a las amenazas cibernéticas y, en un giro del destino, a un paso atrás en la continuidad del negocio. En concreto, las operaciones de seguridad han sufrido tensiones en este periodo para garantizar:

- Control lógico y físico y de los dispositivos administrados y no administrados, así como redes de acceso (ejemplo: Wi-Fi en el hogar), que resulta en una imposibilidad de aplicar de forma remota las políticas de seguridad definidas por la empresa en esos puntos de control.
- Monitorización y visibilidad de los equipos y dispositivos, que dificultan la detección y bloqueo de amenazas de seguridad.
- Soluciones corporativas para el intercambio de ficheros de forma segura.

Además de lo anterior, también hay dificultad en la aplicación de las políticas de seguridad que definen el uso correcto y seguro de las herramientas de comunicación corporativas, especialmente el envío y recepción de archivos e información, de forma que se asegure que, a pesar de cualquier situación, los empleados puedan enviar y recibir correos con información confidencial, así como las acciones a llevar a cabo para protegerse contra spam, phishing de credenciales o incluso la suplantación de la identidad de personas o entidades.

Un gran desafío para los trabajadores remotos o móviles es el riesgo que sufren a la hora de enviar o recibir archivos e información debido a las rígidas o anticuadas arquitecturas fijas de VPN o a las políticas de protección de datos. La colaboración efectiva con empleados, clientes y socios significa que, en algún momento, los archivos y documentos tendrán que salir de la seguridad y los límites de la organización. Con el tiempo, esto puede ser tan perjudicial para un negocio como cualquier otra violación de datos. La seguridad debería ayudar a la productividad del trabajador en lugar de impedirla.

Figura 3. Mayores riesgos en la implementación del Smart Work para las organizaciones españolas.

Fuente: IDC, Impacto de COVID-19 en la inversión TIC en España, 2020.

La ciberseguridad y los riesgos de privacidad son el reto más importante al que se enfrentan las organizaciones españolas al implantar políticas de Smart Work

Expectativas de inversiones en tecnología segura y remota debido al cambio de modelo de trabajo.

Aparentemente los mecanismos de seguridad actuales no son suficientes para protegernos contra ataques más sofisticados, dirigidos y avanzados. Más que nunca, la seguridad del intercambio de información requiere de la incorporación de herramientas que nos permitan certificar la identidad digital de los ficheros y de la información, facilitando así el proceso de detección de amenazas y habilitando el concepto de "confianza digital", lo que permite securizar el dato que generan todos los actores con los que se interacciona (empleados, proveedores y clientes) con independencia del origen de este y del canal por el que se distribuya.

Además, IDC espera que las implementaciones en cloud crezcan a un ritmo significativo. De hecho, en temas de seguridad se espera que la seguridad como servicio sea una realidad para el 38% de las empresas en España en los próximos dos años. En este escenario, la orquestación e integración será fundamental para brindar a las organizaciones la capacidad de elegir modelos de implementación y

lograr coherencia en la forma en que se administran las soluciones tanto de seguridad como de automatización e inteligencia artificial.

Transcurrido un año y medio desde el inicio de la pandemia de COVID-19, las organizaciones están adoptando en su mayoría modelos de trabajo híbridos. En este contexto la flexibilidad por parte de las empresas es un factor crucial que permite no solo continuidad de negocio sino satisfacción del empleado (vital para la retención del talento). Para asegurar la productividad y adecuada conectividad en estos entornos también es fundamental contar con la infraestructura y herramientas necesarias, pues las metodologías de trabajo han cambiado.

A medida que incrementan las transferencias de datos entre organizaciones a causa de la implantación de estos modelos de trabajo híbridos, se ha puesto en relieve una notable necesidad de una gestión más transparente que refleje una adecuada gobernanza de la información, especialmente en las administraciones públicas.

Fundamentalmente, para asegurar el intercambio de información con todas las garantías, es importante desde las organizaciones generar conciencia, mejorar procesos e implementar nuevas tecnologías que doten al empelado de un ecosistema seguro por el cual transferir archivos. Más aún, se espera que las organizaciones capitalicen en su experiencia para promover una gestión transparente de los datos, al mismo tiempo que facilitan el flujo automatizado de información.

Propuesta de Valor de Tranxfer

En el contexto descrito anteriormente y sin importar la industria a la que pertenezca una organización, facilitar la colaboración y el intercambio de archivos y documentos mediante canales seguros entre empleados, clientes y socios es un requisito clave para aumentar la generación de ingresos. Tranxfer otorga, entre otras, estas capacidades de transferencia de archivos que pueden ayudar a una empresa a garantizar la autenticidad, confidencialidad y trazabilidad de los archivos. Desde su plataforma, se puede garantizar la gestión segura de datos sensibles y la mejora de la eficiencia operacional.

Por ello, los profesionales de la ciberseguridad se centran en los siguientes objetivos de control al diseñar los esquemas de protección de sus datos:

- Confiabilidad: Asegurar que los datos permanezcan secretos y no sean vistos o usados por personas inapropiadas.
- Integridad: Garantizar que los datos son legítimos y no son modificados por partes inapropiadas.
- Disponibilidad: Garantizar que los datos estén disponibles para su uso por las partes apropiadas.

- Propiedad: Garantizar que los sistemas en uso nos obstaculicen las necesidades existentes y no se utilicen de forma que puedan perjudicar a la organización o hacerla responsable de alguna acción.
- Transferencia: Garantizar que el envío y recepción de información y archivos se realiza en un entorno seguro infranqueable.

Ahora que se han identificado los objetivos, la organización debe evaluar el riesgo e invertir en soluciones y sistemas que garanticen dicha seguridad.

Tranxfer está encontrando en sus clientes una serie de aspectos relevantes, entre los cuales vale la pena mencionar:

- Protección de datos confidenciales.
- Enviar y gestionar de forma segura los envíos en una plataforma centralizada.
- Simplificación de las auditorías internas y externas.
- Riesgos en la seguridad de la empresa.
- Problemas con los procesos basados en papel.
- Falta de lugar para archivar documentos de manera segura.
- Evitar cambios fraudulentos en los documentos corporativos.
- Expiración de documentos de forma automática después de cumplir con su objetivo.

Existen numerosas razones que convierten a todas estas funcionalidades en grandes soluciones para las empresas. Entre ellas, garantizar la seguridad de la información, mejorar la gestión y accesos a la misma y permite reaccionar rápidamente frente a robos o modificaciones maliciosas de la información.

¿Qué desventajas tienen las empresas que no digitalizan estos procesos?

- Poca eficiencia en la gestión del tiempo.
- Coste elevado.
- Riesgo de daño o perdida de los documentos.
- Riesgo de alteración o sustracción de documentación confidencial.

Además de las administraciones públicas y otros sectores especialmente regulados o auditados en sus procesos de intercambio de información, todos pueden beneficiarse de la automatización de procesos para promover esa invaluable confianza digital mientras se crea más valor para las organizaciones.

Acerca del analista

Sebastian Miranda, **Analyst, IDC Spain**

Responsable de realizar investigaciones, proporcionar servicios de análisis y consultoría a las principales empresas tecnológicas y end-users en su proceso de transformación digital.

Consultor y analista con experiencia en proyectos de transformación digital y analítica de datos de tecnología, que involucran tanto análisis de mercado, diagnóstico y análisis GAP así como el desarrollo de estrategias de ejecución. Con experiencia en varios países, y una actitud proactiva y dinámica, habilidades de comunicación, sólida formación tanto económica como de análisis.

Sebastian es licenciado en Administración de Empresas y Master en Innovación y Gestión Estratégica por la Universidad Solvay Brussels School of Economics and Management.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor global de inteligencia de mercado, servicios de consulta y acontecimientos para la tecnología de la información, telecomunicaciones y mercados de tecnología de consumo. IDC ayuda a los profesionales de Tecnologías de la Información, ejecutivos de negocio, la comunidad inversionistas toman decisiones basándose en hechos sobre compras de tecnología y la estrategia de negocio. Más de 1100 analistas en IDC proporcionan experiencia global, regional, y local sobre la tecnología y oportunidades de industria y tendencias en más de 110 países por todo el mundo. Durante más de 50 años, IDC ha proporcionado informaciones estratégicas para ayudar a nuestros clientes a alcanzar sus objetivos claves de negocio. IDC es una filial de IDG, líder en los medios de comunicación de tecnología, investigación de mercados y eventos.

IDC España

Serrano 41, 3ª
28001 Madrid
+34 91 787 21 50
Twitter: @IDCSpain
www.idcspain.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright y Restricciones