Alinto

Libro blanco

El correo electrónico: ¿el eslabón débil de Office 365?

Resumen

Introducción

La transformación digital está más que nunca en el centro de las preocupaciones de las empresas. Cada organización está desplegando proyectos de desmaterialización, rediseño de procesos, lugar de trabajo digital, espacios colaborativos, etc. En la mayoría de las empresas, esto implica **el despliegue de Office 365, ahora llamado Microsoft 365**.

Pero la tecnología sigue siendo un campo de juego formidable para los ciberdelincuentes. Entre las diferentes formas de ataques, están **el ransomware, el spam o los correos electrónicos de phishing...**. Son amenazas graves para las empresas, que pueden tener serias consecuencias en su negocio.

Muy a menudo, estos ataques provienen de correos electrónicos fraudulentos. Y Outlook, de la suite Office 365, no se salva. ¿Qué soluciones hay -de Microsoft u otras- para mejorar la seguridad? ¿Cómo puede proteger su correo electrónico? ¿Es posible ir acompañado de un partner? Respondemos a todas estas preguntas en nuestro libro blanco.

Adopción de Microsoft 365 en las empresas: el estado de la cuestión

Microsoft 365 es una suite escogida por las empresas por sus numerosas aplicaciones, su practicidad y también por el lugar que ocupa en el mercado. Sin embargo, tras meses de uso, muchas organizaciones se dan cuenta de que estas herramientas se utilizan poco o mal. **Por lo tanto, el retorno de la inversión no está necesariamente ahí**. En este artículo, hemos decidido ofrecerle cifras y un informe sobre la adopción real de Office 365 y las razones de los fracasos.

Adopción de Office 365: las cifras

La suite de Microsoft se lanzó en su forma actual, basada en suscripción, hace casi diez años. Reúne una serie de aplicaciones que responden a las necesidades diarias y de negocio de las empresas: las herramientas históricas (Word, Excel, PowerPoint, etc.), y los nuevos servicios web (OneDrive, Yammer, etc.). En 2019, la suite Office 365 tenía **155 millones de usuarios activos**. A principios de 2020 pasó a llamarse Microsoft 365.

Según un informe de Forrester, la implantación de Office 365 puede generar un retorno de la inversión del 162% en tres años, siempre que la suite se utilice correctamente. El estudio de Microsoft 365 Report informa que el **88% de los responsables de la toma de decisiones de TI han desplegado completamente Microsoft 365 en su empresa**. Según un artículo de la JDN, el 80% de las empresas del CAC40 lo tienen. La razón principal de esta elección es la flexibilidad de la oferta para responder a la complejidad de las organizaciones.

Sin embargo, las cifras deben tratarse con precaución. El informe de Microsoft indica que la mayoría de las empresas aún no han adoptado el paquete de software en todas sus funcionalidades, especialmente en lo que respecta a la seguridad. Entonces, ¿cuándo se considera que una herramienta ha sido adoptada? ¿Es sólo estar conectado a Microsoft? Si es así, el 100% de los usuarios lo utilizan, porque están conectados al correo electrónico. Pero la adopción efectiva es más compleja: lo es cuando la transformación que provoca es real y concreta, con nuevos modos de colaboración, por ejemplo.

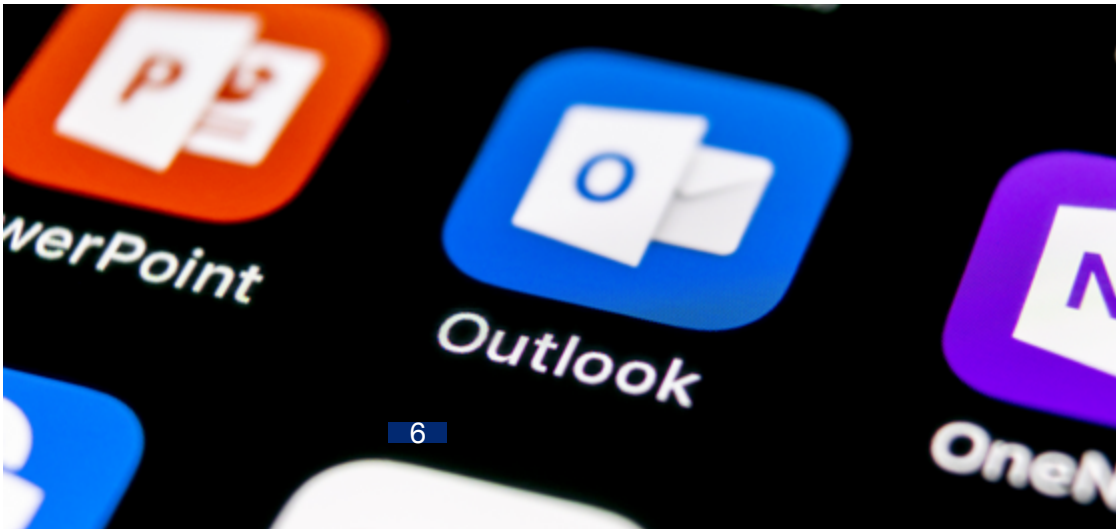
Uso de Office 365: las aplicaciones más populares

En cuanto al uso, está claro que, a pesar de la integración de Office en la nube, **los usuarios se aferran a las viejas prácticas**: crear documentos localmente, compartir archivos por correo electrónico... Lógicamente, los usuarios deberían prescindir del correo electrónico, al menos para intercambiar o compartir documentos internamente. OneDrive permite generar enlaces seguros para compartir. Así que no aprovechan realmente los puntos fuertes de la suite.

En detalle, las aplicaciones más utilizadas en el tercer trimestre de 2019 son :

- Outlook / Exchange: **59 %**
- Equipos: **41 %**
- Skype Empresarial: **23 %**

Vemos que a las aplicaciones verdaderamente colaborativas les cuesta despegar. Esto se debe a que muchos usuarios desconocen a qué aplicaciones tienen acceso (el 47% según el Informe de Microsoft 365), así como las ventajas que aportan.



ROI Office 365: Warum klemmt es?

En realidad, **la adopción de la suite Office 365 no es tan evidente como las empresas usuarias quieren hacer creer**.

He aquí algunas cifras que lo demuestran:

- **El 34%** de los usuarios son reacios a cambiar
- **El 47%** no sabe a qué aplicaciones tiene acceso
- **El 29%** carece de tiempo para formarse

Las empresas deben supervisar constantemente el uso de sus equipos para acompañarlos en la dirección correcta. Y ahí es donde radica el problema. No basta con desplegar guías que expliquen cómo hacer las cosas, sino que hay que crear escenarios, mostrar y convencer a la gente de las ventajas de la suite colaborativa. Se trata de **iniciar un verdadero proceso de transformación interna**, y pocas empresas lo hacen. Consideran que, si los usuarios se conectan a su correo electrónico y a algunas aplicaciones de vez en cuando, es una implantación exitosa. Sin embargo, el retorno de la inversión no está a la altura de sus expectativas. Y por una buena razón, ¡el precio de las licencias ha aumentado un 10% en 2019!

Para una mejor adopción de Office 365, he aquí algunos consejos:

- Poner la suite en el centro de la transformación digital de la empresa
- Implicar a la dirección fijando objetivos
- La dirección también debe ser usuaria de las soluciones para dar ejemplo

Si bien la adopción de Microsoft 365 es una realidad cuantitativa, su adopción “cualitativa” por parte de los usuarios corporativos aún no es óptima. Aunque la suite tiene todas las cualidades necesarias para el trabajo colaborativo seguro en papel, se encuentra con los obstáculos que ponen los usuarios, que pueden ralentizar **el proceso de transformación digital de las organizaciones**.

Office 365: ¿qué cambia para el correo electrónico?

El correo electrónico es una herramienta central para una empresa. Si se estropea, todo el negocio se resiente. Y si no tiene un BCP (Business Continuity Plan), es todo un hándicap.

En 2018, el 56% de las empresas utilizaban la suite Office 365 (ahora Microsoft 365). Para recibir correos electrónicos, estas empresas tienen que pasar por el servidor Exchange, que proporciona acceso a los correos electrónicos, el calendario y los documentos almacenados en los servidores. Por ello, por razones de simplicidad, muchas organizaciones optan por equiparse con los servicios integrales del editor. A menudo a costa de la seguridad. Esto es lo que analizaremos en este artículo.

¿Cuáles son las características del correo electrónico de Office 365?

Outlook es el servicio de correo electrónico empresarial más utilizado. Y por una buena razón, tiene varias características clave:

1. Acceda a **servicios adicionales**: calendario, gestión de tareas y notas, etc.
2. Crear **firmas personalizadas**
3. Comprobación de **varios buzones** simultáneamente
4. Facilitar el **trabajo colaborativo**
5. Enviar un correo electrónico **desde Word**
6. **Perfecta integración** con otros programas ofimáticos de Microsoft
7. Mejorar **la seguridad del correo electrónico**
8. Acceso a la mensajería en **situación de movilidad**
9. Organización de **carpetas y archivos**

Sin embargo, todavía hay agujeros en el sistema, especialmente en el área de seguridad del correo electrónico entrante y saliente. Los paquetes de protección de Microsoft no son gratuitos, y muchas empresas no se acogen a esta opción. Como resultado, muchos sistemas de correo electrónico tienen poca o ninguna seguridad y quedan en manos de los hackers, o al menos son vulnerables. El peligro se acentúa con la introducción masiva y rápida del teletrabajo: sin un marco estricto y un software de seguridad (antispam, antiphishing) para la mensajería, toda la actividad de una empresa se ve amenazada por un simple correo electrónico.

¿Cuáles son las alternativas a Office 365?

Los CIO quieren reducir su **dependencia de Microsoft.** Sin embargo, la sustitución de un eslabón de la cadena como Exchange podría hacer más frágil la vida cotidiana de los usuarios. Y un cambio así no es fácil.

En primer lugar, porque Microsoft opera en el vacío: todas las aplicaciones son interdependientes y las alternativas no siempre son fácilmente interoperables. Por ello, las empresas suelen tomar el **paquete "Outlook, Exchange y Active Directory"** para trabajar, sin buscar otras soluciones.

Por otro lado, los cambios en las herramientas generan limitaciones para los usuarios. Por ello, las organizaciones no quieren alterar sus hábitos.

Sin embargo, existen alternativas para proteger mejor el correo electrónico. Es posible mantener Outlook, por ejemplo, pero **elegir otro servidor de envío que no sea Exchange**. Esto es totalmente transparente para los usuarios, pero permite mejorar la seguridad del correo electrónico y no depender totalmente de Microsoft.

El correo electrónico de Outlook es muy cómodo y totalmente compatible con todas las aplicaciones de Microsoft, lo que mejora la colaboración. Sin embargo, es totalmente posible utilizar proveedores externos para integrar la funcionalidad de Office y hacerla interoperable.

Despliegue de Office 365: ¿cómo garantizar la seguridad del correo electrónico?

Los ataques de ransomware van en aumento y afectan a todos, incluso a las pequeñas empresas. **Estos programas maliciosos suelen introducirse a través de un correo electrónico**. Por lo tanto, no debe tomarse a la ligera el aspecto de la seguridad de su sistema de correo electrónico profesional. Además de concienciar a sus empleados sobre las acciones básicas (no abrir correos electrónicos con objetos o archivos adjuntos extraños, cambiar las contraseñas con regularidad y no utilizar la misma en todas partes, etc.), hay que poner en marcha otras soluciones para **garantizar su seguridad informática**.

En este artículo, echamos un vistazo al estado actual de la seguridad del correo electrónico de Exchange y le damos nuestros consejos sobre cómo proteger su correo electrónico.

Asegurar la mensajería de Exchange: ¿qué cifras y qué problemas?

La mayoría de los ataques de ransomware son oportunistas y se aprovechan de los bajos niveles de madurez digital de las organizaciones. Desde 2018, los ataques se han intensificado y se unen cada vez más a otros programas maliciosos como criptovirus u otros troyanos. Esto facilita que los hackers cifren los datos de la empresa, así como los datos privados, y pidan un rescate para acceder a sus propios datos.

El daño a las empresas suele ir mucho más allá de la pérdida de unos pocos datos:

- parada de producción
- caída de la facturación asociada
- riesgos legales (por ejemplo, con la RGPD)
- daño a la reputación
- pérdida de confianza
- La policia también constata casos de suicidios de empleados a raíz de estafas contra el CEO.

En la guía “Ataques por ransomware, todos los interesados” publicada por el gobierno francés, varias empresas dan testimonio:

- En noviembre de 2019, el **Hospital Universitario de Rouen** ya no pudo acceder a una aplicación empresarial. El departamento de TI descubrió entonces que las estaciones de trabajo y los servidores habían sido encriptados. Era un ransomware.
- En octubre de 2019, el **grupo M6 fue objeto de** un ataque de ransomware, que cortó el acceso a internet, esencial para las emisiones de radio en particular.
- En abril de 2019, **Fleury Michon tuvo** que cortar el acceso a internet de todos los empleados tras un ataque de ransomware. El negocio se detuvo por completo durante tres días y se degradó durante quince días.

El punto de partida de estos ataques suele ser un correo electrónico. Sin emabargo, el asunto de la seguridad del correo electrónico, asi como la infraestructura informática, sigue sin tomarse lo suficientemente en serio. Y las cifras de una encuesta realizada por SoftwareONE lo demuestran:

- **El 44% de los encuestados no utiliza Microsoft Intune** (gestión de dispositivos y aplicaciones móviles);
- **El 37% no utiliza Microsoft Azure Advanced Threat Protection** (identificación, detección e investigación de amenazas avanzadas);
- **El 36% no utiliza Microsoft Azure Information Protection** (protección de documentos).

Todavía hay que avanzar en la lucha contra las amenazas y la anticipación de los ataques.

Protección del correo electrónico: nuestros tres consejos

Para reducir los riesgos y proteger su empresa, hay varias medidas que puede tomar. Sin embargo, si tuviéramos que darle nuestros mejores consejos, elegiríamos los tres siguientes.

1 Sensibilizar a sus empleados

Los ataques de malware a menudo se originan en los correos electrónicos recibidos por un empleado. Por ello, es esencial **recordar a los empleados las buenas prácticas y hace hincapié en el correcto uso del correo electrónico**: no abrir objetos o archivos adjuntos sospechosos o de destinatarios desconocidos, informar de cualquier problema al departamento de informática, etc. No se trata de una defensa absoluta, pero sí de un paso necesario para reducir el riesgo de ataques.

2 Asegurar su SI

Por supuesto, es esencial asegurar su sistema de información. Se trata de gestionar los derechos de acceso a las aplicaciones, particionar el SI para limitar el riesgo de propagación a todas las estaciones de trabajo, mantener las distintas aplicaciones actualizadas, ya que esto mejora su seguridad, y realizar regularmente copias de seguridad de los datos.

3 Optar por soluciones de protección del correo electrónico

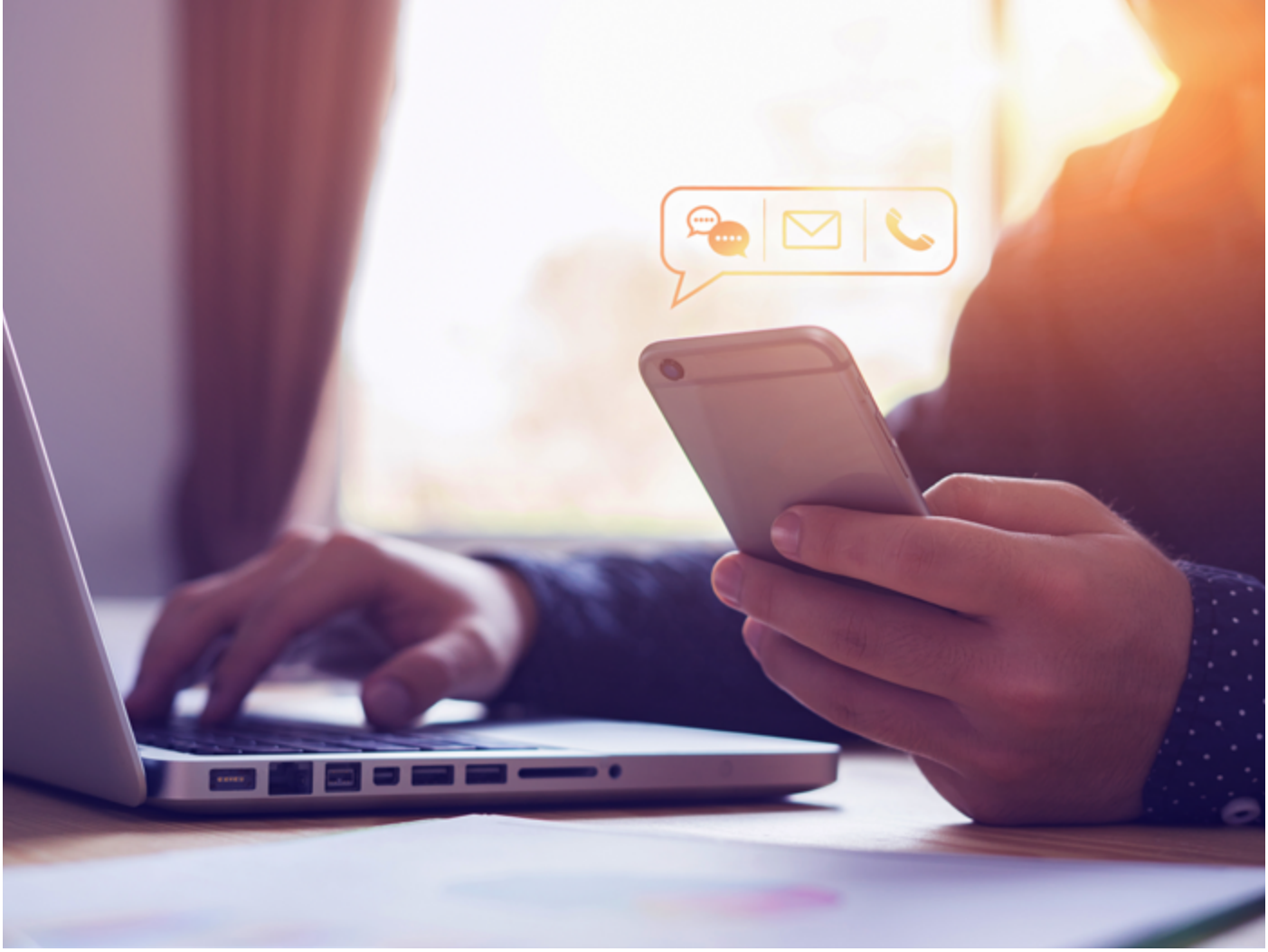
Por último, para garantizar la máxima seguridad de sus correos electrónicos, es importante equipar los puestos de trabajo con programas antispam y antivirus. **Estas herramientas identifican y bloquean los correos electrónicos maliciosos, evitan comprometer el sistema asi como el cifrado de sus datos**. Sin embargo, no son suficientes por sí solas. Para una protección óptima, es importante mantenerlos actualizados, para asegurarse de que no se instalan aplicaciones maliciosas en los servidores, estaciones de trabajo, etc.

Filtrado del correo electrónico: ¿por qué elegir una solución adicional?

En relación con nuestro último consejo, aunque Microsoft ofrezca soluciones de seguridad para el correo electrónico, dotarse de soluciones externas es un plus considerado indispensable por la ANSSI (Agencia Nacional de Seguridad de los Sistemas de Información francesa). En primer lugar, las cifras demuestran que **las empresas no siempre eligen las opciones de seguridad disponibles con Microsoft o no las utilizan**. Esto ya crea un vacío legal.

En segundo lugar, los programas informáticos especializados en el mantenimiento de sistemas de mensajería son el resultado de los continuos esfuerzos de I+D dedicados a estos aspectos y ofrecen soluciones avanzadas. Esto también ayuda a superar las limitaciones de la dependencia de Microsoft, que no es necesariamente infalible en este sentido.

En Alinto proponemos productos que se adaptan a todos los sistemas de gestión de correo electrónico. Más allá de la protección antispam de los correos electrónicos entrantes, también tenemos en cuenta los correos electrónicos salientes, ofreciendo un Plan de Continuidad de Negocio (BCP), cuarentena o funciones de archivo. Todo lo que necesita para mejorar la seguridad de su correo electrónico empresarial. ¿Preguntas ? No dude en ponerse en contacto con nosotros.



Gestión del correo electrónico: ir más allá del correo electrónico

La gestión del correo electrónico es estratégica para una empresa. Y va más allá de enviar y recibir correos electrónicos. El correo electrónico es un **punto de entrada habitual para los ciberataques**. Por ello, la seguridad requiere el despliegue de un software antispam, la implantación de un Plan de Continuidad de Negocio (BCP), pero también un alojamiento seguro. Este es el tema que abordaremos en este nuevo artículo.

#1 - Antispam y antivirus

Para mejorar el filtrado del correo electrónico, es esencial utilizar una **solución antispam y antivirus**. Estas herramientas dan al correo electrónico una puntuación que permite considerarlo como aceptable o como spam, o incluso rechazarlo. Los criterios de evaluación pueden ser configurados por los administradores y adaptados a cada usuario. Algunos ejemplos: peso de la imagen/texto, asunto, remitente, contenido, etc. Pero también criterios más técnicos.

Las normas de seguridad pueden evolucionar en función de las necesidades y especificidades de cada empresa. Esta es la ventaja de elegir un conjunto de **servicios de protección de correo electrónico adaptable y fácil de usar** como Alinto Protect. Este filtrado también le permite proteger la reputación de su nombre de dominio y evitar que los destinatarios lo incluyan en sus listas negras

#2 - PCN

Cuando el servicio de mensajería deja de ser accesible, toda la actividad de una empresa se ve afectada. Por lo tanto, es esencial contar con un PCN (Plan de Continuidad de Negocio). Permite **garantizar el acceso a los correos electrónicos gracias a un webmail de respaldo**. Sin embargo, no todos los programas de protección del correo electrónico lo ofrecen. Sin embargo, con el aumento de los ciberataques, esta funcionalidad es esencial.

Un artículo del periódico Le Monde informa que, tras un ciberataque, los empleados extranjeros de Bouygues Construction se encontraron sin trabajo por la falta de acceso a sus correos electrónicos profesionales. Este es el tipo de situación que el relay de correo electrónico seguro Alinto Protect permite evitar gracias a un PCN asegurado y supervisado 24/24. Los usuarios tienen acceso a sus correos electrónicos, incluso en caso de avería, y esto evita un **impacto demasiado grande en la empresa**.

#3 - Cuarentena

Algunos correos electrónicos se consideran a veces como spam aunque el usuario los considere aceptables y quiera recibirlos. Por lo tanto, es esencial contar con una solución que le permita **mantener el control sobre los distintos correos electrónicos** que pasan por el servidor de correo.

Esto es lo que permite el servicio de cuarentena. Los usuarios reciben un resumen de los correos electrónicos en cuarentena y pueden elegir si los reciben o no. La frecuencia del informe es **personalizable por el administrador**.

Con Alinto Protect, los correos electrónicos en cuarentena se conservan durante 30 días, lo que permite a los usuarios mantener el control de su buzón.

#4 - Archivo

Para ir más allá de la simple gestión del correo electrónico, algunas empresas desean beneficiarse de un sistema de archivo de correo electrónico, a menudo para cumplir con **las obligaciones reglamentarias**. Estas características también compensan las incidencias del servidor o la pérdida de datos... También se optimiza el almacenamiento, reduciendo el volumen de correo electrónico directamente en el servidor, lo que a veces lo hace ineficiente.

El servicio de archivo de Alinto conserva una copia no modificable de todos los mensajes durante el periodo establecido. De nuevo, el administrador puede establecer y modificar las reglas por dominio y/o usuarios.

#5 - Alojamiento

La ubicación del alojamiento también es una cuestión delicada para las empresas. Y este problema se ha reforzado desde la aplicación **del RGPD** (Reglamento General de Protección de Datos). Con los gigantes de la web, es difícil saber dónde se alojan los datos. Al utilizar un servicio de retransmisión segura como el de Alinto, las empresas tienen la posibilidad de elegir su alojamiento, en Francia o en Europa.

Los servicios de Alinto se alojan en nubes privadas, en centros de datos de Francia, Suiza, Alemania o España. Los clientes también pueden optar por alojar ellos mismos sus datos. **Se dispone de asistencia y mantenimiento 24 horas al día, 7 días a la semana, durante todo el año**.

Para un mantenimiento más eficaz de la mensajería profesional, se recomienda equiparse con un software que presente las funcionalidades enumeradas en este artículo. Alinto lo ofrece a través de una solución transversal y ágil. Para saber más, ¡está aquí!

Soporte de Microsoft 365: ¿por qué elegir Alinto?

Para evitar que el despliegue del paquete Office 365 fracase y garantizar que la seguridad se sitúe en el centro de su uso, especialmente en lo que respecta a su correo electrónico, usted ha decidido recurrir a un partner.

Sin embargo, es difícil orientarse entre la amplia oferta y proveedores disponibles. En este artículo, le damos cinco criterios para guiarle en su elección.

#1 - Optar por la proximidad

Microsoft es una gran empresa de software, que equipa al **80% de las empresas del CAC40**. Este indicador dice mucho sobre la potencia de la empresa, pero también sobre el número de empleados y la facturación. Si es una PYME o una ETI y necesita un apoyo específico, recurra a un socio de tamaño humano, como Alinto.

Así, se beneficia de un apoyo y un seguimiento personalizados por parte de un equipo que conoce sus problemas y podrá **guiarle en su despliegue**.

#2 - Elegir la experiencia en seguridad

Sin embargo, recurrir a un socio de tamaño humano no significa descuidar su **experiencia en materia de seguridad**. Este es un problema importante para las empresas, especialmente con la llegada del teletrabajo y la digitalización de las empresas.

Con Alinto, usted confía en un socio experto en seguridad del correo electrónico desde hace 20 años. El grupo cubre todos los problemas relacionados con el correo electrónico e invierte año tras año en I+D para anticiparse a las tendencias de la seguridad y la lucha contra los hackers.

#3 - Centrarse en la capacidad de respuesta

En relación con la proximidad, recurrir a un socio de tamaño humano le garantiza una mayor **reactividad por parte de** los equipos de asistencia, para responder rápidamente a sus necesidades. Este no es siempre el caso de los socios más grandes, que a veces cobran por la asistencia de nivel 2, y el primer nivel sólo lo gestiona un centro de llamadas con guión.

En Alinto, usted tiene acceso inmediato a los especialistas y nos comprometemos a proporcionar un **servicio supervisado las 24 horas del día, los 7 días de la semana, para garantizar que su negocio esté siempre seguro**. Además, ofrecemos un Plan de Continuidad de Negocio (BCP) en caso de indisponibilidad de su servicio de correo electrónico. Todo ello en un potente paquete de servicios, sin coste adicional.

#4 - Confiar en la objetividad

Para implementar Office 365, ¿por qué no confiar simplemente en Microsoft? Esta suele ser la primera idea que se nos ocurre. Sin embargo, elegir un socio externo le permite obtener **un apoyo objetivo, totalmente centrado en sus necesidades y no en objetivos comerciales**.

En Alinto conocemos los principales servicios de correo electrónico y nuestra solución de protección se adapta a cada uno de ellos. Así que no tenemos ningún interés en recomendar uno sobre otro. Nos basamos en sus necesidades y especificidades, para **ofrecerle la mejor solución**.

#5 - Elección de alojamiento en Francia

Si quiere alojar sus datos en Europa, o incluso en Francia, pero no quiere ocuparse usted mismo, puede confiar el alojamiento a su partner. Segúrese de que sus datos son soberanos porque son muy importantes, ¡lee la letra pequeña!

Nuestros servidores se encuentran en Francia, Suiza, Alemania y España. Actualizamos continuamente nuestra infraestructura para ofrecer la máxima resistencia y seguridad. Nos comprometemos a garantizar un servicio soberano que ofrezca una disponibilidad muy alta.

Ahora tiene todas las cartas en la mano para elegir a su partner y ser apoyado en la implementación de su mensajería segura y el paquete de Office 365. ¿Por qué no hablamos de ello?

Conclusión

El correo electrónico no tiene por qué ser el eslabón más débil de Office 365, siempre que esté bien protegido. Y por eso existen soluciones específicas: tanto por el comportamiento de los usuarios, como por el uso del software de seguridad adecuado.

Sobre Alinto

Fundada en 2000, Alinto es una empresa especializada en el negocio del correo electrónico: servicio de correo electrónico en modo SaaS, antispam, servidor de correo electrónico... a través de varios productos:

- **Alinto Protect:** el relay de correo electrónico seguro que inmuniza contra los riesgos de Internet garantizando el acceso permanente a los correos electrónicos.
- **Alinto Gateway:** El relay de correo SMTP permite a los servidores o aplicaciones enviar correos electrónicos para garantizar un tráfico llamado “limpio”.

Presente en Francia, Suiza y España, Alinto cuenta con más de 30 empleados y proporciona un servicio de calidad a más de tres millones de usuarios. Cada día se envían más de 15 millones de correos electrónicos gracias a sus servicios de correo electrónico.

El grupo Alinto aglutina varias empresas, desde 2016, para posicionarse como uno de los principales actores en la mensajería electrónica. Está compuesta por las siguientes empresas:

- **Cleanmail:** empresa suiza especializada en el filtrado antispam en la nube desde 2002
- **SerenaMail:** especialista español en seguridad del correo electrónico (filtrado de spam).
- **Alinto:** servicios de mensajería segura.

Esto permite al grupo consolidar su posición en el mercado y ampliar su desarrollo internacional.

Lyon (siège)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Paris
31 rue de Reuilly
75012 Paris
+33 141 58 15 33

Madrid
Calle Aniceto Marinas, 48
28008 Madrid
+34 91 005 29 64

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com