Alinto

Libro Blanco

noviembre 2022

SOBERANÍA DIGITAL: ¿CUÁLES SON LOS DESAFÍOS DEL EMAIL PROFESIONAL?

Índice

Introducción	3
Retos de la soberanía digital	4
Soberanía digital: las iniciativas europeas	8
Soberanía y ciberseguridad: ¿están ligados?	14
Los sistemas de correo electrónico profesional presentan riegos.	18
El código abierto al rescate de los servicios de correo profesional	22
Conclusión	26
Sobre Alinto	27

Introducción

La soberanía digital está más que nunca en el centro de las preocupaciones de las empresas. **Plantea cuestiones sobre la protección de datos, la confidencialidad y la independencia de las empresas frente a los proveedores estadounidenses (GAFAM en particular)**.

Se trata de una cuestión importante en un contexto geopolítico tenso (guerra en Ucrania, crisis en Taiwán, etc.), y en el que la mayoría de los ciberataques provienen de países autocráticos como Rusia o China (según el informe Carbon Black[1]). Más que nunca, las empresas europeas necesitan proteger sus datos y centrarse en la soberanía.

Las tecnologías de código abierto ofrecen algunas respuestas. Gracias a la apertura del código, las empresas tienen una visión del funcionamiento de las aplicaciones y, por tanto, del alojamiento, el almacenamiento y la explotación de los datos producidos. Además, están surgiendo varias iniciativas nacionales y europeas para contrarrestar a los gigantes mundiales del sector: reglamento (RGPD), conciencia de la soberanía, evangelización en torno a las tecnologías de código abierto...

El correo electrónico empresarial también se ve afectado. Su exposición a los ciberataques los convierte en una prioridad en términos de seguridad, mientras que su funcionamiento, en términos de enrutamiento y almacenamiento de datos, sigue siendo complejo. Por eso, en este Libro Blanco, hacemos un balance de la soberanía digital, las iniciativas europeas y el papel del código abierto para la seguridad de los sistemas de correo electrónico profesional.

[1] https://www.developpez.com/actu/216086/La-Russie-et-la-Chine-sont-les-deux-principales-origines-des-cyberattaques-dans-le-monde-entier-d-apres-un-rapport-de-Carbon-Black/

Retos de la soberanía digital

Los debates sobre la soberanía digital están en el centro de las estrategias digitales de las empresas. La soberanía no es sólo una moda proteccionista para compensar el retraso digital de Europa. Su objetivo es garantizar la prosperidad e independencia de las empresas protegiendo sus datos, los de sus clientes y los de sus conciudadanos.

En concreto, para las empresas, optar por una solución digital soberana permite hacer frente a tres grandes retos. He aquí algunas explicaciones.

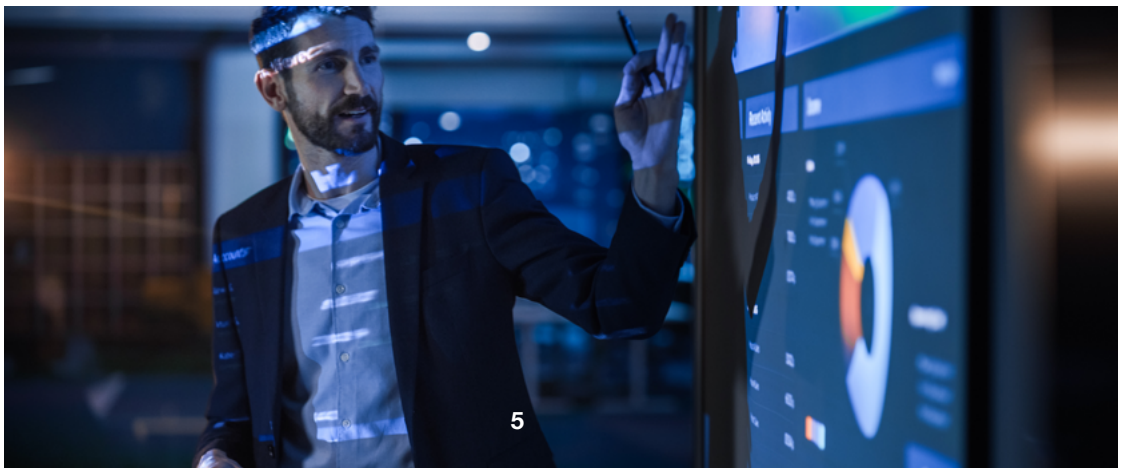
La soberanía para mantener el control de los datos

La privacidad de los datos se ha hecho un hueco en la agenda de la mayoría de las empresas. Más aún desde la entrada en vigor del RGPD en 2018, que ha acelerado la concienciación en Europa. En efecto, no todos los países ni todas las legislaciones ofrecen la misma protección de datos. Por lo tanto, es esencial **cartografiarlos, garantizar que estén protegidos y sean inaccesibles para personas malintencionadas**.

Para proteger sus datos, las organizaciones disponen de varias soluciones:

- Alojarlos en una nube soberana, ubicada en Europa y gestionada por empresas sujetas a la legislación europea. Existen varias certificaciones al respecto (como SecNumCloud, la certificación más exigente para el alojamiento en Francia)
- Optar por software de código abierto y/o software europeo
- Formar a los empleados en las distintas normativas sobre protección de datos
- Sensibilizar a los empleados sobre la importancia de una buena gestión de los datos.

La soberanía sobre el alojamiento de los datos los protege legalmente de accesos hostiles. Es la base de una buena estrategia de control para las empresas que quieren extraer valor de sus datos, al tiempo que garantizan la confidencialidad a sus clientes.



Soberanía para contrarrestar el cloud act

Desde 2018, el Cloud Act está en vigor en Estados Unidos. Esta ley estipula que las autoridades estadounidenses pueden solicitar a los proveedores de servicios de comunicación sujetos a la jurisdicción de Estados Unidos que les faciliten los datos que estén en su «posesión, custodia o control», con **independencia de la ubicación de dichos datos**. Se trata de una amenaza real para los datos de las empresas europeas alojados por proveedores estadounidenses, incluso en centros de datos con sede en Europa. De hecho, en virtud de esta ley, estos proveedores de servicios pueden explotar los datos, incluso los confidenciales, más allá de los usos inicialmente previstos.

La soberanía digital europea pretende establecer **garantías frente a este acceso ilícito por parte de determinados países** y regular las solicitudes de acceso de autoridades extranjeras, así como las transferencias de datos no personales.

Para ello, se prevén dos reglamentos europeos:

- **La ley de gobernanza de datos:** adoptada en mayo de 2022, será aplicable en septiembre de 2023. Su objetivo es fomentar el intercambio de datos personales y no personales mediante la creación de estructuras de intermediación.

- **El data act:** esta ley, presentada en febrero de 2022, pretende garantizar un mejor reparto del valor resultante del uso de los datos personales y no personales entre los actores de la economía de los datos, especialmente en relación con el uso de objetos conectados y el desarrollo del Internet de las cosas.

Soberanía para contrarrestar la expansión de los GAFAM

Los GAFAM[1] constituyen una gran amenaza para la soberanía digital. El peso económico de estos gigantes digitales estadounidenses es considerable: «la valoración bursátil acumulada de las GAFAM alcanzó los «5,853 billones de dólares» en 2020, es decir, un valor superior al PIB de Japón, la 3ª economía mundial»[2].

Esta dominación no es sólo económica, sino que también afecta a la dependencia digital. De hecho, estas empresas son capaces de procesar y almacenar los datos de ciudadanos y empresas de todo el mundo (centros de datos, sistemas de correo electrónico, clouds, etc.), que se les «confían» de forma más o menos consciente al utilizar servicios o aplicaciones. Conviene recordar de paso que los GAFAM están sujetos a la legislación estadounidense. Están sujetos a la Ley de la Nube (Cloud Act), lo que significa que los datos en su poder pueden ser transmitidos a terceros.

Por tanto, el resto del mundo, y Europa en particular, deben contrarrestar este poder creando un ecosistema verdaderamente soberano. ¿Cómo hacerlo? Cambiando la normativa al respecto, fomentando el uso de software de código abierto y comunicando sobre los retos de la soberanía digital.

[1] Google, Amazon, Facebook, Apple, Microsoft

[2] https://fr.countryeconomy.com/gouvernement/pib

Soberanía digital: las iniciativas europeas

Para avanzar hacia la soberanía digital europea, es esencial regular el uso, almacenamiento y recogida de datos. Esta necesaria protección de datos sigue suscitando un complejo debate entre los países miembros. Esto no ha impedido que la Unión Europea haya tomado varias iniciativas al respecto. Descodificación.

El Reglamento General sobre la Protección de Datos (RGPD): el punto de partida

El RGPD, que entró en vigor en mayo de 2018, es el primer paso hacia la soberanía digital. Regula el acceso, almacenamiento y uso de los datos personales de los ciudadanos europeos. Para ello, las empresas que posean estos datos deben cumplir varios requisitos (supresión de datos, consulta previa solicitud, nombramiento de un DPO...). El mismo reglamento estipula que los datos personales de la UE sólo pueden transferirse a países que ofrezcan una protección similar y que la UE considere «adecuada».

La legislación estadounidense, por ejemplo, es mucho menos estricta que el RGPD. La Ley de la Nube permite al Gobierno de Estados Unidos acceder a los datos en poder de empresas estadounidenses. Y culturalmente, los estadounidenses consideran que los datos son un activo con el que se puede comerciar. **A pesar de estas diferencias, muchas empresas europeas confían sus datos a grandes proveedores estadounidenses de servicios digitales, especialmente para el alojamiento**. Esto ha llevado a la UE a tomar nuevas iniciativas para regular el mercado de datos.

[1] Consultar https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

El Data Governance Act y el Data Act: para ir más allá

Estos dos textos complementan el RGPD. Su objetivo es desarrollar un mercado único de datos apoyando el acceso a los mismos, su puesta en común y su reutilización, en consonancia con los valores de la UE.

La Ley de Gobernanza de Datos entrará en vigor en septiembre de 2023. Su objetivo es fomentar el intercambio de datos personales y no personales mediante la creación de estructuras de intermediación. Este último definirá claramente las condiciones en las que se pueden reutilizar los datos en poder del servicio público, y así competir en igualdad de condiciones con los agentes del mercado internacional.

La Ley de Datos pretende establecer normas armonizadas para el acceso a los datos generados por los objetos conectados y los diversos servicios relacionados. El objetivo es facilitar el acceso, la gestión y la puesta en común de estos datos.

La Directiva NIS2: soberanía y ciberseguridad

La directiva europea sobre seguridad de las redes de Internet, conocida como NIS 2, tiene por objeto aumentar el nivel de preparación de las empresas y organizaciones sobre los riesgos cibernéticos. Dará lugar a nuevas obligaciones: medidas de seguridad, normas de supervisión, obligación de normas de supervisión, obligación de notificar cualquier ataque a la ANSSI…

Cada país podrá elaborar una lista de organizaciones afectadas por esta directiva, sobre la base de un análisis de riesgos. Se calcula que varios miles de entidades vinculadas a servicios, la industria espacial o la investigación estarán sujetos a esta directiva, actualmente en fase de adopción.

Las autoridades locales: la CNIL y la ANSSI para velar por el respeto de la legislación en Francia

En Francia, dos organismos se encargan de velar por la aplicación de la normativa de protección de datos y de ayudar a empresas y ciudadanos a hacer frente a la ciberamenaza.

La Comisión Nacional de Informática y Libertades (CNIL), a veces llamada la policía digital, es el regulador de los datos personales. Tiene varias misiones:

- **Informar y proteger los derechos:** responde a las solicitudes de información de profesionales y particulares sobre protección de datos. También gestiona sus reclamaciones.
- **Apoyo al cumplimiento:** ofrece una caja de herramientas para ayudar a las empresas a lograr el cumplimiento.
- **Anticiparse e innovar:** participa en el desarrollo de soluciones de protección de la privacidad, asesora a las empresas y contribuye a crear un debate sobre las cuestiones éticas que rodean a los datos.
- **Controlar y sancionar:** vigila la aplicación concreta de la ley.

La ANSSI (Agencia Nacional de la Seguridad de los Sistemas de Información), por su parte, proporciona conocimientos y asistencia técnica a las organizaciones en materia de ciberseguridad. Ofrece un servicio de vigilancia, detección, alerta y reacción ante los ataques informáticos.

La acción de los gobiernos europeos: verdaderos prescriptores

Los gobiernos tienen un importante papel que desempeñar en el avance hacia la soberanía digital. Son prescriptores en la elección de soluciones tecnológicas. Sus decisiones contribuyen a promover los conocimientos técnicos de los agentes digitales europeos. Desde hace algunos años, **los gobiernos presionan a las autoridades locales y a las empresas para que recurran a soluciones de código abierto o a software producido por editores locales**.

El desarrollo del ecosistema digital europeo permite así ofrecer una alternativa real a los GAFAM y mantener el control sobre los datos.

La conciencia de los problemas relacionados con la soberanía digital es muy real en Europa. Reglamentos como el RGPD han despertado la atención de los ciudadanos. Los medios de comunicación se hacen eco de escándalos relacionados con fugas de datos o con la obtención de datos sanitarios. Se han tomado iniciativas a escala europea, pero aún no son suficientes para contrarrestar el poder de los gigantes estadounidenses. Sin embargo, **esta normativa muestra el camino hacia soluciones más respetuosas con los datos de nuestros ciudadanos.**

Soberanía y ciberseguridad: ¿están ligados?

En un momento en que los ciberataques son cada vez más numerosos y sofisticados, la ciberseguridad es un requisito previo para la soberanía digital. Los sistemas de información son cada vez más complejos, con interconexiones público-privadas y fronteras a menudo porosas. Al mismo tiempo, el volumen de intercambios de correo electrónico aumenta día a día, lo que ofrece muchos puntos de entrada a las ciberamenazas.

En materia de protección de datos, **ciberseguridad y soberanía son inseparables**. He aquí por qué.

La soberanía digital, el primer paso para la protección de los datos

Como se menciona en el artículo «Soberanía digital: iniciativas europeas», el objetivo de la soberanía es proteger mejor los datos de las organizaciones y los ciudadanos europeos. De hecho, al utilizar los servicios de un socio que afirma ser soberano, uno espera que sólo utilice los datos para los fines especificados y que no los divulgue. Esta garantía está obviamente asegurada por los procesos de control, almacenamiento y tratamiento establecidos, el respeto de la normativa... Pero también por las soluciones tecnológicas utilizadas (alojamiento soberano, software de código abierto...).

La amenaza de ciberataques o revelación de datos es, por tanto, menor cuando se recurre a un proveedor de servicios europeo.

Ciberseguridad: protección frente a amenazas externas

Por definición, la ciberseguridad es un conjunto de medidas destinadas a garantizar la seguridad de los sistemas informáticos y los datos frente a actos malintencionados. Un ciberataque puede afectar gravemente a las empresas. Por tanto, deben ser capaces de hacer frente a un acontecimiento de este tipo y aplicar medidas de seguridad de la SI.

Esto implica, entre otras cosas, el despliegue de software de protección (antivirus, por ejemplo), planes de actualización del sistema (parches), sistemas de autenticación y también la formación de los empleados en buenas prácticas de ciberseguridad.

A menudo, las empresas no son conscientes de que tienen datos sensibles, o piensan que un ataque sólo les ocurre a los demás. Por desgracia, el número de incidentes aumenta constantemente y las técnicas utilizadas por los ciberatacantes son cada vez más sofisticadas. **Las consecuencias pueden ser dramáticas**.

Por ejemplo, como víctima de un ataque de ransomware, el hospital de Corbeil-Essonnes vio algunos datos sensibles (DPI, datos personales, etc.) divulgados en Internet[1] tras su negativa a pagar un rescate.

[1] https://www.liberation.fr/societe/sante/faute-de-rancon-les-donnees-volees-dans-un-hopital-de-lessonne-se-retrouvent-mises-en-ligne-20220925_PMF2MYWN5NAW3BLNDXF7Q34BZY/

No hay soberanía sin ciberseguridad

Cada vez está más claro que **la soberanía digital por sí sola no basta para proteger los datos sin incluir la ciberseguridad**.

Sin duda, la soberanía digital permite controlar mejor los propios datos. Sin embargo, un entorno de software o unas aplicaciones demasiado abiertas o expuestas permitirán que persistan ciertos fallos. Por tanto, la soberanía no puede disociarse de la ciberseguridad. Esto último requiere inculcar buenas prácticas en las empresas, o construir una oferta cibernética europea que sea una alternativa real a las soluciones de los gigantes estadounidenses.

A la espera de que se despliegue un sistema de este tipo, las empresas no deben descuidar el uso de soluciones de ciberseguridad y deben equiparse con software antivirus, establecer estrategias de copia de seguridad, rodearse de expertos capaces de prestarles apoyo, seguir los consejos de organizaciones de referencia como la ANSSI en Francia y recurrir en la medida de lo posible a soluciones de expertos empresariales locales que trabajen con soluciones de código abierto.

Los sistemas de correo electrónico profesional presentan riegos.

La evolución del trabajo a distancia, la adopción de soluciones en la nube, la hibridación de los sistemas de información... son factores que aumentan la vulnerabilidad de las empresas ante las ciberamenazas. **Si hace unos años los atacantes apuntaban a las infraestructuras, hoy lo hacen a las personas y se apoyan en la falta de vigilancia de los usuarios**. ¿Y qué mejor mejor manera de perpetrar sus ataques que a través del correo electrónico?

Así pues, el correo electrónico empresarial presenta peligros para la protección de los datos corporativos. Afortunadamente, existen soluciones soberanas que ofrecen mayor seguridad. He aquí algunas explicaciones.

Correo electrónico profesional: la primera fuente de ciberataques

Con casi 300.000 millones de correos electrónicos enviados cada día en 2020 en todo el mundo, el correo electrónico es un punto de entrada privilegiado para los ciberataques. Este canal de comunicación permite a las empresas compartir datos e información más o menos sensibles. Estos intercambios son terreno abonado para los ciberdelincuentes. Las cifras así lo atestiguan:

83 % **de los encuestados afirmaron que su empresa había sufrido al menos un ataque de phishing por correo electrónico en 2021.[1]**

Compartir enlaces fraudulentos, enviar archivos adjuntos maliciosos, solicitar datos bancarios, etc. Estas son técnicas utilizadas para atrapar a los destinatarios de correos electrónicos. Sin una mayor concienciación de los empleados y sin las herramientas adecuadas, las empresas se exponen al riesgo de violaciones de datos, cuyas consecuencias pueden ser desastrosas.

[1] Informe «State of the Phish», 2022

Sistemas de correo electrónico y soberanía digital: ¿misión imposible?

¿Cómo evitar los ciberataques? La respuesta no es tan sencilla. Los atacantes son cada vez más astutos, y **el riesgo cero no existe**. Por otra parte, es posible reducir el riesgo y proteger mejor sus datos prestando especial atención a la hora de elegir un proveedor de correo electrónico profesional.

Las soluciones gestionadas por los GAFAM no son soberanas por naturaleza. De hecho, recopilan datos y los almacenan en centros de datos no sujetos a las normas de soberanía europeas. Por lo tanto, no es posible garantizar su confidencialidad ni mantener el control de los mismos como empresa. Además, sus sistemas de correo electrónico son software de código cerrado, lo que refuerza la dependencia de un proveedor, sin transparencia en el tratamiento, en contra de los principios de la soberanía digital.

Sin embargo, existen soluciones y ofrecen alternativas reales: los sistemas de correo de código abierto.

¿Qué debe tener un buen sistema de correo electrónico?

Entre las exigencias de la soberanía y la ciberseguridad, ¿cuál es el correo electrónico empresarial ideal?

El correo profesional ideal y soberano

Es obvio, se trata de un sistema de correo electrónico desarrollado por un editor europeo, o de código abierto. Este último criterio ofrece más transparencia en cuanto al funcionamiento y a la reactividad de una comunidad para corregir posibles fallos. Pero, ¡cuidado! De nada sirve rodearse de un socio local si el anfitrión no cumple todos los requisitos de soberanía.

Así pues, el sistema de correo ideal se compone de programas informáticos desarrollados en Europa, gestionados por un proveedor de servicios sometido a la legislación europea que los aloja en infraestructuras en Europa, protegidos de acuerdo con las recomendaciones europeas.

El correo profesional ideal y protegido

Un buen sistema de correo electrónico profesional incluye un completo arsenal de seguridad. Las soluciones de seguridad integradas en las versiones estándar de los sistemas de email profesionales (antispam, smtp relay, etc.) son a menudo insuficientes. Muchas empresas no se dotan de soluciones adicionales. **Hasta el día en que sean víctimas**.

Por tanto, un buen sistema de correo electrónico profesional debe incluir las mejores tecnologías para garantizar el filtrado de los emails, pero también su correcta entrega, protegiendo al mismo tiempo la reputación del dominio de correo electrónico. Esto es algo que pocos sistemas de correo electrónico ofrecen por defecto.

Para protegerse de los ciberataques a través del email, el sistema de correo electrónico ideal debe cumplir varios criterios. En primer lugar, se debe elegir un host soberano y, a continuación, un proveedor de correo electrónico europeo. Para ir más lejos, las empresas pueden optar por el código abierto, garantizando así la transparencia del código. Por último, no deben pasarse por alto las soluciones de seguridad adicionales para una protección total del correo electrónico.

El código abierto al rescate de los servicios de correo profesional

El email es una aplicación que forma parte de la vida cotidiana de las empresas. Su uso va más allá del simple intercambio de mensajes. Es una auténtica herramienta de colaboración y un medio de comunicación universal que ahorra tiempo y desmaterializa muchos intercambios.

Por eso es esencial dotarse de una herramienta de correo intuitiva, ergonómica, fiable y segura. Sobre el terreno, GAFAM domina el mercado con sistemas de email integrados en sus suites ofimáticas como Office 365 o Google workspace. Sin embargo, existen alternativas. Entre ellos se encuentran los sistemas de correo de código abierto.

Ventajas de los sistemas de correo de código abierto

La gran ventaja del correo «open source» es que el código está disponible libremente. Su uso no está condicionado a la compra de una licencia, y **las empresas no dependen de un proveedor**. Su integración en el sistema de información puede llevarse a cabo internamente o por un integrador, sin compromiso para este último. La apertura del código también permite adaptarlo a necesidades muy específicas, con un coste menor.

Elegir el código abierto significa beneficiarse de una comunidad de usuarios que enriquecen y mejoran constantemente la solución. Ya se trate de la ergonomía, las funcionalidades o la seguridad, los colaboradores están llenos de ideas y aportan sus competencias para hacer evolucionar la solución y adaptarla a las necesidades de las organizaciones.

Desde el punto de vista del departamento informático, es sobre todo la durabilidad técnica lo que pesa en la balanza. Para los informáticos especializados, **los sistemas de correo de código abierto suelen ser más fáciles de implantar que los de los gigantes tecnológicos, porque recurren a sus conocimientos en la materia**.

Correo electrónico y soberanía digital

La seguridad del correo electrónico empresarial se aborda a distintos niveles. Desde el punto de vista de los datos, hay que preguntarse: ¿dónde se almacenan?, ¿cómo se accede? Las soluciones de código abierto no imponen ninguna norma a las empresas. Así pueden elegir a su proveedor de alojamiento de datos y **asegurarse de que los datos se procesan correctamente**.

Para garantizar la continuidad del servicio, las empresas pueden suscribir un «plan de recuperación de desastres» en caso de incidente, de acuerdo con las condiciones definidas con su proveedor de alojamiento. Optar por un sistema de correo electrónico europeo y de código abierto, combinado con un alojamiento soberano, proporciona una base de seguridad esencial. En concreto, los datos de la empresa no están sujetos a la Cloud Act, la legislación estadounidense que se aplica a las soluciones de correo de los GAFAM.

Por último, **aunque no exista el riesgo cero en materia de ciberseguridad, la prioridad de los piratas informáticos siempre será atacar a los grandes editores**, que tienen una gran cuota de mercado. Este riesgo puede reducirse con un arsenal completo de seguridad email.

También es esencial garantizar que el sistema de correo pueda interactuar con la arquitectura informática de la empresa y comunicarse con otras herramientas. **También en este caso, el código abierto es una alternativa interesante.**

El ejemplo del webmail SOGo

SOGo es una solución de correo web de código abierto que permite compartir calendarios, agendas e emails dentro de una empresa. La solución es completamente abierta y gratuita, si las organizaciones deciden implantarla internamente.

Basado en AJAX, SOGo es un webmail universal y responsivo. Es el componente front-end de la infraestructura de correo electrónico que proporciona a los usuarios una interfaz completa para acceder a la información. Se beneficia de una comunidad de varios miles de colaboradores que enriquecen continuamente la solución.

Para las empresas que deseen beneficiarse de una integración y un soporte completos, Alinto ofrece desde 2022 una versión profesional en la nube de SOGo, con un soporte dedicado y una supervisión 24/7. **La solución es totalmente segura y se basa en el alojamiento soberano**.

El correo electrónico también tiene un papel que desempeñar en el camino hacia la soberanía digital. El código abierto, combinado con ofertas europeas de alojamiento en la nube, es una palanca para lograrlo. Las organizaciones recurren cada vez más a estas tecnologías. Aunque esta transformación lleve tiempo debido a la inercia de los ciclos de vida de las soluciones y las renovaciones del mercado, la tendencia es real.

Conclusión

La soberanía digital se está convirtiendo cada vez más en una prioridad para las organizaciones. Sus motivaciones son numerosas: mantener el control de los datos, fomentar el uso de software europeo o mantener la independencia de los grandes proveedores estadounidenses y mundiales.

Entre las soluciones, los gobiernos europeos están fomentando las iniciativas de código abierto, y las empresas son menos reacias a utilizarlas. Por tanto, les interesa aprovechar esta oportunidad para mantener el control de sus datos. Y esto empieza por el sistema de correo de las empresas y su seguridad.

Sobre Alinto

Fundada en 2000, Alinto es una empresa especializada en el negocio del email: servicios de correo y seguridad en modo SaaS o PaaS, etc. a través de varios productos y principalmente:

- **SOGomail:** servidor de correo seguro y colaborativo todo en uno, que integra el webmail SOGo totalmente responsivo.
- **Cleanmail:** filtrado de correo seguro que protege contra las ciberamenazas garantizando el acceso permanente a los emails.
- **Serenamail:** el relay de correo SMTP permite a los servidores o aplicaciones enviar correos electrónicos para ofrecer un tráfico «limpio».

Alinto, especialista europeo en correo electrónico protegido, trata de responder a las nuevas expectativas del mercado optando por orientarse más activamente hacia el código abierto. Para ello, el editor toma las riendas del webmail de SOGo y su comunidad en 2022, así como las del sistema de filtrado de correo electrónico.

Pero, ¿por qué recurrir al código abierto? Sobre todo, es una cuestión de soberanía digital. Con el código abierto, el código está a disposición de los usuarios y las empresas pueden así mantener el control sobre el alojamiento, el almacenamiento, la explotación y sobre todo la reversibilidad de los datos. Para los equipos de Alinto, el código abierto ofrece a sus clientes y socios la opción de la soberanía digital. Es también la voluntad de ofrecerles una alternativa seria y perenne a GAFAM.

«En nuestra opinión, el código abierto es esencial para dar a los usuarios libertad de elección. Es un elemento importante para la diversidad y para nosotros es una forma de ofrecer a las empresas alternativas a las herramientas de correo de los actores estadounidenses de la nube», explica **Philippe Gilbert, Director General de Alinto**.

Lyon (sede central)
15 quai Tilsitt
FR-69002 Lyon
+33 481 09 01 10

Barcelona
Paseo de Gracia,101-4°1
SP-08008 Barcelona
+34 91 005 29 64

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

Lausana
Rue des Jordils 40
1025 St-Sulpice
Switzerland
Tel: +41 21 695 20 20

Alinto

www.alinto.com