Alinto

Confían en nosotros

Establecimientos sanitarios

• SEGURIDAD EMAIL • REPORTING EMAIL • SECTOR PÚBLICO

¿Por qué las instituciones sanitarias necesitan controlar sus sistemas de correo electrónico?

El filtrado de correo de **23 000 buzones de correo** electrónico

Un **despliegue completamente transparente** para los usuarios

Puesta a disposición de **reportings** para la dirección

Las organizaciones públicas, y las instituciones sanitarias en particular, han sido uno de los objetivos favoritos de los ciberpiratas en los últimos años. De hecho, los ataques se han multiplicado, con importantes consecuencias en la actividad de las instituciones públicas y generando a veces costes muy elevados. Por ejemplo, en 2021 se registraron **733 incidentes de seguridad**, entre ellos un centenar de ataques informáticos, en 582 hospitales de Francia*.

Muchos de estos ataques tienen su origen en correos electrónicos fraudulentos. El control específico y reforzado de los correos electrónicos es, por tanto, esencial para reducir los riesgos y garantizar la seguridad de los Sistemas de Información de estas estructuras públicas. Esto es tanto más importante cuanto que las instituciones sanitarias albergan y utilizan datos personales muy sensibles. Más allá del funcionamiento de los hospitales, es también la **confidencialidad de esta información** lo que está en juego.

Por eso es esencial una gestión estricta del sistema de correo electrónico profesional. He aquí lo que está en juego.

*fuente: Ciberataque en el hospital de Corbeil-Essonnes:
« Nous n'avons plus accès à nos bases de données » – TF1 info

Controlar el flujo de correo electrónico: un requisito previo para las instituciones sanitarias

Los hospitales manejan muchos de los llamados datos sensibles, empezando por los datos sanitarios. Por ello, el sistema de email se gestiona in situ: los establecimientos prefieren en general no utilizar el hosting en la nube, ni recurrir a proveedores del tipo GAFAM. El intercambio de datos sensibles suele estar supervisado de manera escrupulosa: los establecimientos sanitarios ejercen un **control total y reforzado sobre el sistema de correo de los empleados**. Y las soluciones implantadas deben cuestionarse periódicamente.

Aunque los hospitales estén equipados desde hace tiempo con programas de protección del correo electrónico, cada cuatro años sondean el mercado y compiten con los distintos editores.

Los dos objetivos principales son **la lucha contra el spam para reducir los correos innecesarios y la protección contra los programas maliciosos** que cada vez están más presentes en los correos electrónicos. Los ciberpiratas son cada vez más ingeniosos, y las soluciones de protección deben ser capaces de anticiparse a estos nuevos modos de ataque para proteger los datos de los hospitales.

Mayor protección e informes personalizados

Al cambiar de solución, los departamentos técnicos quieren beneficiarse de un software que sea al menos tan eficaz como el que ya tienen.

El precio y la funcionalidad también son criterios de selección. Y a veces, necesitan ir más allá con opciones como la posibilidad de **disponer de datos e informes para el análisis**. Si además ofrecen la posibilidad de disponer de informes hechos a medida en tiempo real, es una verdadera ventaja.

Spam bajo control y cuarentena de forma fácil

Sobre todo, es importante que **la implantación sea totalmente transparente para los usuarios** y que el nivel de rendimiento no disminuya.

Al utilizar Alinto, los usuarios corroboran que reciben menos spam que antes, lo que demuestra la eficacia del servicio. Además, valoran muy positivamente la puesta en cuarentena de determinados correos, que filtra la entrega de algunos mensajes, para que no se pierda ninguna información importante. Esto se puede gestionar con un solo clic, mientras que el procedimiento puede ser más complejo con otras soluciones.

Objetivos

- reforzar **la seguridad** de los sistemas de correo profesional
- adaptarse a la evolución de los **ciberataques**
- **disponer de informes** para la dirección

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, etc. a través de varios productos:

- El relay de filtrado de correo electrónico, que inmuniza frente a los riesgos de Internet garantizando un acceso permanente a los emails.
- La pasarela SMTP que permite a los servidores o aplicaciones enviar correos electrónicos para garantizar un tráfico "limpio".
- La solución de correo electrónico independiente de gama alta: compartición de agendas, calendarios y archivos de empleados.

Con oficinas en Francia, Suiza y España, Alinto cuenta con más de 30 empleados y presta 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.

Apoyo eficaz apreciado por el equipo informático

Cleanmail también simplifica el trabajo de los equipos informáticos y la asistencia que prestan internamente a los usuarios.

Las organizaciones sanitarias aprecian especialmente la **flexibilidad de la solución**, que facilita la asistencia a los usuarios. Cuando se encuentran con un problema, las líneas de atención internas pueden configurar listas blancas o negras en unos pocos clics, pueden comprobar los registros para ver si el correo electrónico llegó o no. **Esto es relevante y más eficiente**. Y es una verdadera comodidad para los informáticos.

En cuanto a la formación, dos horas bastan para que los equipos informáticos se familiaricen con la herramienta.

Los agentes sanitarios valoran positivamente la colaboración con los equipos de Alinto. Son reactivos y ágiles, cumplen los plazos y responden a los retos que planeta el sector sanitario. Además, Alinto es una empresa europea, lo que constituye un factor importante para el sector público. Además, dispone de soporte dedicado en España, lo que es un **factor diferenciador**.

Beneficios

- una protección eficaz contra el spam y el malware
- un servicio de **cuarentena ergonómico**
- un **soporte interno** reactivo y de calidad para los usuarios
- un **webmail de seguridad**