Tendencias en ciberseguridad

Almacenamiento seguro y ubicuo de datos médicos

Los datos médicos de pacientes son información altamente sensible y debe ser almacenada de forma segura para garantizar la privacidad de los pacientes y usuarios. La recopilación de información proveniente de múltiples dispositivos médicos y la disponibilidad de una historia clínica a través de una red clínica dificultan la **integridad y confidencialidad de los datos**. Dicho datos requieren, no sólo de un sistema de almacenamiento cifrado, si no de un mecanismo de transferencia segur, garantizando que la **ubicuidad de los datos personales y clínicos** de los pacientes no ponen en peligro su confidencialidad.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | TECNOLOGÍA

El mantenimiento de la seguridad en las **redes informáticas** y en los datos es una prioridad para el sector sanitario, con la particularidad respecto a otros sectores de que el carácter confidencial y la **sensibilidad de los datos** de los pacientes (que son almacenados en la red), incrementando la necesidad de soluciones de seguridad. La **legislación europea y española** regulan la protección de la privacidad de la información confidencial de los ciudadanos; en el caso de la sanidad, ésta crea la necesidad de disponer de servicios de almacenamiento específicos y adaptados los datos vinculados con la salud de los pacientes. Por este motivo, las soluciones de seguridad tales como aquellas dirigidas a la asesoría legal, el cumplimiento de la ley de protección de datos o firma digital adquieren gran relevancia en el sector, con el objetivo de **prevenir fugas de información**, gestión y control de acceso y modificaciones en bases de datos.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación | Comercialización | Servicios

La protección de la privacidad del historial clínico y otros datos almacenados en los centros sanitarios requiere de la contratación de servicios de seguridad que prevenga la **pérdida de información** e incorpore **controles de acceso** en los servidores de almacenamiento de datos para prevenir riesgos en ciberseguridad y de fuga de información.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en pacientes/centros ●●○	Impacto en proveedores ●○○	Impacto en sistema sanitario ●●●
Un enfoque sistémico de seguridad en los sistemas de almacenamiento de datos médicos fomentará la **mejora en la eficiencia en los sistemas de atención médica** contribuyendo a una mayor exactitud, rapidez y seguridad en el diagnóstico, control y tratamiento de las enfermedades.	La apuesta por la digitalización de la prestación de los servicios médicos y el almacenamiento de los datos digitales exige contar con **sistemas de seguridad de la información** cada vez más potentes y con **proveedores de servicios** que sean capaces de cumplir con los requisitos más ambiciosos.	La adopción de soluciones de seguridad que garanticen la privacidad y confidencialidad de los datos de los pacientes almacenados, contribuye a **reducir la desconfianza** de los ciudadanos en el Sistema Nacional de Salud, aumentando su predisposición a compartir **información sensible**.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN | SOLUCIONES DE CONTROL | SOLUCIONES DE MITIGACIÓN

La seguridad en el almacenamiento de datos médicos requiere la incorporación de **soluciones de prevención de fuga** de información sensible y privada de pacientes. Además, las soluciones de **control de acceso** a la gestión y modificación de bases de datos contribuyen a garantizar la confidencialidad de la información médica almacenada.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | INTRODUCCIÓN | CRECIMIENTO | MADUREZ

La implantación de las TIC en los **sistemas de almacenamiento y gestión de datos** del Sistema Sanitario contribuye al desarrollo de un sistema más moderno, eficiente, flexible y efectivo. La confidencialidad y el carácter sensible de la información que maneja el sector requiere de soluciones de seguridad de la tecnología implantada que aseguren la **integridad y privacidad** de los datos almacenados en la red.

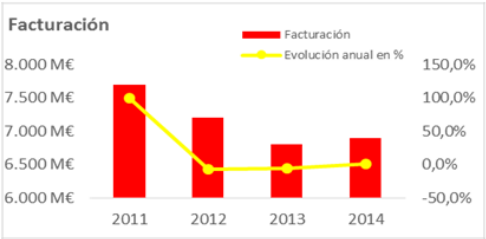
Tendencias en ciberseguridad

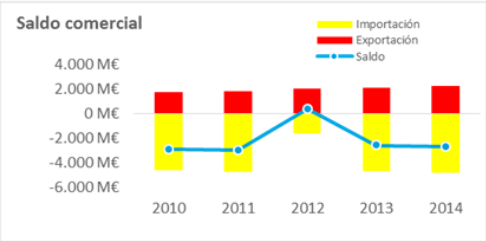
Almacenamiento seguro y ubicuo de datos médicos

ÁMBITO DE APLICACION

Esta tendencia tiene aplicación en las diferentes empresas, que almacenan y gestionan información de carácter confidencial de pacientes, fundamentalmente centros de **salud públicos y privados**. La implantación de estos sistemas permite el acceso a la información clínica de los pacientes desde cualquier dispositivo conectado a la red de la organización **optimizando el servicio** a los usuarios. También puede compartirse de forma segura con otras organizaciones al incluir soluciones de cifrado.

CARACTERIZACIÓN DEL SECTOR





- Históricamente, el **gasto sanitario** en España ha presentado una evolución creciente. Este crecimiento se ha estabilizado según los últimos datos en torno al 9,29% en 2012.
- En los 3.006 centros de salud y 10.116 consultorios de Atención Primaria en funcionamiento en el **Sistema Nacional de Salud**, se atendieron en el 2012, alrededor de 259 millones de consultas médicas al año, lo que supuso una frecuentación por persona de **5,6 visitas** al año.
- Si se tiene en cuenta también la atención a la urgencia fuera del horario ordinario, el número de consultas médicas en **Atención Primaria** fue de 279 millones. Al añadir a la actividad médica la actividad de enfermería el volumen superó los 418 millones de contactos.
- En el **ámbito privado**, el sector hospitalario en España se encuentra **muy fragmentado**. En el año 2011, los cinco grandes grupos hospitalarios representaban solamente el **31% del mercado**, mientras que en países como Alemania o Reino Unido, los cinco grandes grupos representaban el 89% y el 64% del mercado hospitalario privado.

PREVISIONES DE DEMANDA

CRECIMIENTO

- El Departamento de Salud en la Comunidad de Cataluña puso en marcha hace unos años una **plataforma virtual** como herramienta de control y prevención de incidentes médicos.
- Esta plataforma permite que de forma anónima, voluntaria y confidencial, el personal de todos los **hospitales de la red pública** pueden comunicar los incidentes detectados y prevenir que se repita.

CLIENTES

- Hospitales públicos o privados.
- Centros médicos.
- Empresas del sector de la salud.
- Empresas aseguradoras.
- Personal médico.
- Comunidad de pacientes.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | DIFERENCIACIÓN EN PRESTACION DE SERVICIOS | DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

- **Intel Security**, cuenta con soluciones para proteger los dispositivos médicos de forma que sólo se permitan los archivos ejecutables y cambios que estén autorizados y capturar una pista de **auditoría** de los cambios autorizados, facilitando el **cumplimiento de las normativas** y la generación de informes. La protección de lectura/escritura para dispositivos de campo bloquea la visualización y la alteración de los datos del sistema y los archivos de configuración desde cualquier otra aplicación que no sea la original.
- Las soluciones disponibles incluyen McAfee Integrity Control, una solución para dispositivos que ocupa poco espacio, y el software McAfee Embedded Control, diseñado para **fabricantes de dispositivos médicos**.