Acronis

Soluciones de ciberprotección para los desafíos del sector sanitario en el siglo XXI

Cómo pueden los profesionales técnicos de la salud proteger los datos confidenciales en la era de las ciberamenazas

El sector de la atención sanitaria está sufriendo una transformación digital fundamental, que implica pasar de los métodos anticuados de almacenamiento de información de pacientes a la adopción de nuevas aplicaciones de diagnóstico y tratamiento, que consumen gran cantidad de datos. Al mismo tiempo, los centros de atención sanitaria se enfrentan a una presión enorme para que incrementen los beneficios, cumplan las normativas de privacidad, optimicen la atención al paciente y mejoren la interoperabilidad entre contribuyentes, proveedores, socios de prestación de servicios, instituciones académicas y pacientes.

El ingente volumen de datos sanitarios de carácter confidencial aumenta y se distribuye por múltiples ubicaciones físicas, dispositivos informáticos y redes (incluidas las nubes públicas y privadas). A esta avalancha de datos, se une la importante incorporación de nuevas aplicaciones de atención sanitaria, como las de teleasistencia, supervisión remota de pacientes y formación por realidad virtual y asistida. Otras tecnologías emergentes, como la inteligencia artificial, el aprendizaje automático, el Internet de las cosas (IoT) y blockchain, complican aún más el puzle, mientras que cada vez hay más usuarios que exigen acceder a esos datos.

Entre tanto, la industria está asediada por las nuevas ciberamenazas, como las violaciones de privacidad, ataques de ransomware y campañas de cryptojacking. Nunca antes ha sido tan difícil garantizar la disponibilidad, accesibilidad y privacidad de los datos del sector sanitario.

Los ciberdelincuentes y actores en nombre de estados hostiles intensifican sus ataques contra el sector sanitario, ya que saben que el malware, y en concreto el ransomware, es particularmente eficaz cuando el acceso a datos sensibles es cuestión de vida o muerte.

Esto explica la avalancha de ataques de ransomware de perfil alto contra hospitales en los últimos años, como los que afectaron al National Health Service en Reino Unido, y a los hospitales estadounidenses Hancock Health, Adams Memorial Hospital, MedStar Health, Erie County Medical, y muchos otros. Las fugas de datos en el sector suelen ocupar titulares, con noticias de robos de cientos de millones de historias médicas y extractos de pagos confidenciales de pacientes.

Además, la industria está también en el punto de mira de los organismos reguladores centrados en las normativas de protección de la privacidad, como la Health Insurance Portability and Accountability Act (HIPAA) de Estados Unidos, el Reglamento general de protección de datos de la Unión Europea, y las normas de protección de la privacidad estatales de Estados Unidos, como la California Consumer Privacy Act (CCPA). Las compañías también se enfrentan al riesgo de infringir las normativas del sector de tarjetas de crédito, como Payment Card Industry Data Security Standard (PCI DSS).

La mayor dependencia de los datos electrónicos del paciente incrementa la importancia de la disponibilidad continua. Además de la amenaza evidente para la seguridad del paciente que representan las interrupciones del funcionamiento, el coste incurrido puede ser tan alto que ponga en riesgo la viabilidad de las instituciones sanitarias. Según el documento "Downtime Cost Calculator for Data Center Disaster Recovery Planning, 28 February 2014" (Calculadora del coste del tiempo de inactividad para la planificación de la recuperación ante desastres en centros de datos, 28 de febrero de 2014) de Gartner, el coste medio del tiempo de inactividad en todo tipo de empresas es de 5600 dólares por minuto, o casi 300 000 por hora. Information Technology Intelligence Consulting informa de que **al 98 % de las empresas, una sola hora de inactividad les cuesta más de 100 000 dólares y a las grandes empresas una cantidad que oscila entre 1 y 5 millones de dólares.**

Mientras tanto, los departamentos de TI de las instituciones sanitarias se enfrentan a los mismos retos que cualquier otro sector: la mayor complejidad de las infraestructuras, la dificultad de contratar y retener a personal cualificado, la migración continua de las aplicaciones a nubes privadas y públicas, la proliferación de dispositivos móviles, como los smartphones y tablets, la llegada de los sensores del IoT, los dispositivos de seguimiento de activos y las cámaras web, así como la necesidad de realizar análisis casi en tiempo real sobre datos nuevos.

Sobrevivir en esta situación exige un nuevo enfoque de la protección de los datos que se base en los cinco vectores de la ciberprotección:

SALVAGUARDA

Garantía de que siempre hay disponible una copia fiable de sus datos.

ACCESIBILIDAD

Disponibilidad permanente de los datos desde cualquier lugar y en cualquier momento.

PRIVACIDAD

Control de quién tiene visibilidad y acceso a sus datos.

AUTENTICIDAD

Creación de una prueba incontestable de que una copia es una réplica exacta del original.

SEGURIDAD

Protección de los datos, aplicaciones y sistemas contra las amenazas maliciosas.

Este documento examina estos principios de ciberprotección contrastados con los siete desafíos principales para el sector de la asistencia sanitaria:

1. **Solucionar** las fugas de datos
2. **Protegerse** frente a las amenazas de malware, como el ransomware y el cryptojacking
3. **Cumplir** los requisitos de las normativas
4. **Migrar** las aplicaciones esenciales y el almacenamiento a las nubes privadas y públicas
5. **Ofrecer** disponibilidad constante de los datos
6. **Incorporar** dispositivos móviles
7. **Fortalecer** la protección de datos sin aumentar la complejidad de la infraestructura

EL ESTADO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN SANIDAD

La protección y la seguridad de los datos sigue siendo una prioridad máxima para las organizaciones del sector sanitario. En su estudio sobre las violaciones de la seguridad, la empresa de ciberseguridad Protenus descubrió que en el sector sanitario el ritmo de los ataques era de más de un incidente al día en 2017.

Ese mismo año, se filtraron 5,6 millones de historias médicas, y una institución tardaba de media 308 días en descubrir un incidente.

Para restringir el número de violaciones de datos médicos se necesitan capas de seguridad de la infraestructura de TI alrededor de los sistemas físicos, las máquinas virtuales, los servicios en la nube y los dispositivos móviles. Entre las medidas básicas, se incluyen la protección antimalware en los endpoints, las defensas frente a amenazas externas a las redes mediante firewalls y la segmentación de la red mediante redes vLAN o definidas por software, con el fin de limitar la propagación de los ataques por las redes internas. Es fundamental contar con protección de datos en forma de copia de seguridad y recuperación ante desastres, para prevenir ataques que dañen, destruyan o bloqueen el acceso a los datos confidenciales. Esto requiere copias de seguridad y almacenamiento seguras, de ser posible, cifradas, tanto in situ como en la nube.

AMENAZAS DE MALWARE

Según la mayoría de los investigadores de seguridad, las dos amenazas de malware más generalizadas que sufre el sector sanitario en los últimos años son el ransomware y el cryptojacking.

El ransomware infecta los servidores, equipos de sobremesa y dispositivos móviles (normalmente cuando el usuario hace clic en un enlace o adjunto malicioso en un mensaje de phishing), cifra los datos que encuentra y, a continuación, solicita un pago online a cambio de la clave de descifrado que permite desbloquear los archivos de las víctimas. Al carecer de medidas para detectar y bloquear los ataques de ransomware, o la posibilidad de restaurar los datos desde una copia de seguridad reciente, muchas instituciones de atención médica han sufrido interrupciones que ponen en riesgo la vida de los pacientes y cuestan millones de dólares en pérdidas de productividad y costes de reparación.

El cryptojacking es un tipo de ciberataque menos patente, pero que va en aumento. Ese malware infecta las máquinas de los centros médicos con zombis de redes de bots que intentan conseguir criptomoneda en nombre de los ciberdelincuentes. El malware solo roba recursos de sus víctimas (ciclos informáticos, memoria, electricidad y refrigeración), pero el coste de la energía y el desgaste de los sistemas aumentan. Además, el malware de criptominería suele inyectar en el sistema que infecta otras amenazas, como el ransomware.

REQUISITOS DE CUMPLIMIENTO DE NORMATIVAS

La vigilancia de los organismos reguladores sobre el sector sanitario ha contribuido a que se convierta en un objetivo de preferencia para los ciberdelincuentes que distribuyen malware y ransomware. El riesgo de incumplir las normativas cuando los datos confidenciales de los pacientes son bloqueados por un ransomware impulsa a las víctimas a pagar rápidamente el rescate para poder recuperar el acceso a los datos.

Por segundo año consecutivo, los ataques de ransomware han representado **más del 70 % de todos los incidentes de malware en el sector de la sanidad,** según el informe de Verizon "2019 Data Breach Investigations Report".

MIGRACIÓN DE LAS APLICACIONES Y EL ALMACENAMIENTO

Como ocurre en la mayoría de los sectores, la sanidad está en medio de un largo proceso de migración de sus aplicaciones y datos fundamentales a una combinación de infraestructura de nube pública y privada. El objetivo es recortar gastos, cambiar activos fijos amortizables por costes de servicios previsibles, y mejorar la accesibilidad de los datos y la posibilidad de compartir desde cualquier ubicación o dispositivo. Sin embargo, muchas instituciones se enfrentan a dificultades para trasladar con seguridad el almacenamiento y los recursos de protección de datos a la nube, garantizando al mismo tiempo la privacidad de los datos y cumpliendo las normativas.

Por segundo año consecutivo, los ataques de ransomware han representado más del 70 % de todos los incidentes de malware en el sector de la sanidad, según el informe de Verizon "2019 Data Breach Investigations Report".

DISPONIBILIDAD DE LOS DATOS

En el sector sanitario es evidente la importancia de la gran disponibilidad de los datos de forma continua: la salud y la vida de los pacientes a menudo dependen de ello.

Desde el punto de vista de la copia de seguridad y la recuperación, esto requiere que los profesionales de TI presten especial atención a dos parámetros: el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de restauración (RTO). El RPO define cuánta información se puede permitir perder una institución en un momento dado, y determina con qué frecuencia debe crear copias de seguridad de sus datos esenciales. El RTO refleja la cantidad de tiempo de inactividad que puede soportar una institución entre el momento de la incidencia de datos y la recuperación correcta. La mayoría de las instituciones pueden identificar fácilmente qué aplicaciones requieren RPO y RTO más exigentes, y cuáles admiten mayores pérdidas de datos y tiempos de recuperación más prolongados.

Acronis ofrece a las instituciones de atención sanitaria un completo conjunto de soluciones sencillas, extremadamente flexibles y muy integradas, para la ciberprotección, el almacenamiento y la recuperación ante desastres.

RIESGOS DEL BYOD

La llegada a las instituciones sanitarias de los omnipresentes dispositivos propiedad de los empleados ha aportado varias ventajas al sector, como una mejora de la productividad del personal y un aumento de la colaboración. Sin embargo, también presenta problemas para la protección de los datos, ya que ahora hay más probabilidad de que los datos sensibles se almacenen en dispositivos que pueden ser blanco de ataques o robos, o bien extraviarse.

CIBERPROTECCIÓN SIMPLIFICADA

Como ocurre en muchos sectores, en la sanidad los administradores de TI tienen problemas para encontrar profesionales cualificados, por lo que eliminar la complejidad de las operaciones es una prioridad máxima. Esto es especialmente importante en operaciones rutinarias, como la protección de datos. Implementar varios sistemas para gestionar un entorno de TI diverso y necesitar ingenieros muy cualificados para su funcionamiento, no es la situación ideal.

CÓMO PROPORCIONA ACRONIS SOLUCIONES DE CIBERPROTECCIÓN PARA SANIDAD

Acronis ofrece protección frente a las fugas de datos de distintas formas. Acronis Cyber Backup proporciona cifrado de los datos confidenciales en tránsito y en reposo para garantizar que incluso en caso de que una fuga de datos consiga su objetivo, lo ciberdelincuentes no podrán sacar partido de la información que han comprometido.

Acronis Cyber Backup ofrece también la posibilidad de restaurar completamente los datos que han sido manipulados, destruidos o bloqueados en un ciberataque.

Acronis Cyber Cloud Storage protege los datos y copias de seguridad frente a fugas de datos con una formidable variedad de ciberdefensas, incluido su cifrado fuerte (tanto si están en tránsito como en reposo) y el uso de centros de datos en la nube certificados y seguros.

PROTECCIÓN FRENTE A AMENAZAS DE MALWARE, COMO EL RANSOMWARE Y EL CRYPTOJACKING

Acronis Cyber Backup con Acronis Active Protection usa inteligencia artificial y aprendizaje automático para detectar, bloquear y revertir de forma activa los cambios sospechosos en datos, archivos de copia de seguridad y agentes de copia de seguridad. Para ello utiliza la caché. Además, detecta automáticamente y neutraliza los ataques de cryptojacking.

Esto ofrece una defensa inigualable contra dos de las amenazas de malware más serias en el sector sanitario, añadiendo protección para amenazas de día cero para complementar defensas antiguas, como el software antivirus basado en firmas.

Además, Acronis Cyber Backup mejora también su agente de copia de seguridad y sus archivos para luchar contra los ataques de malware, de manera que una fuga de datos no pueda poner en riesgo la capacidad de una institución para recuperarse rápidamente y reanudar su funcionamiento habitual.

CUMPLIMIENTO DE LOS REQUISITOS DE NORMATIVAS

Las funciones de cifrado de Acronis Cyber Backup con Acronis Active Protection y Acronis Cyber Cloud Storage también facilitan los objetivos de cumplimiento de normativas, ya que protegen la privacidad de los datos médicos confidenciales, de manera que aunque el ataque consiga acceder, no logrará su objetivo. Los productos de Acronis tienen muchas otras funciones nativas que, cuando se configuran y utilizan correctamente, ayudan a cumplir las partes relevantes de la HIPAA, así como de la ley Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). Aunque no existe un proceso de certificación o acreditación legalmente reconocido para la HIPAA o la HITECH, **Acronis mantiene un programa de seguridad y cumplimiento diseñado para minimizar las preocupaciones de incumplimiento de estas leyes.** Para obtener más información, visite el centro de recursos de Acronis.

MIGRACIÓN DE LAS APLICACIONES ESENCIALES Y EL ALMACENAMIENTO A LAS NUBES PÚBLICAS Y PRIVADAS

Acronis Cyber Backup simplifica el proceso de migración de las aplicaciones sanitarias a la nube, ya que es compatible con una amplia variedad de servicios, sistemas operativos (físicos y virtuales), cargas de trabajo de aplicaciones (locales y en la nube) y endpoints en la nube. La gama de herramientas de gestión de datos de Acronis Cyber Backup simplifican y facilitan el traslado de las cargas de trabajo entre entornos físicos, virtuales y de la nube, para realizar una migración rápida y sin riesgos a nuevas plataformas, como las nubes privadas, Acronis Cyber Cloud Storage, y las populares ofertas de nube pública de Amazon, Google y Microsoft.

DISPONIBILIDAD CONSTANTE DE LOS DATOS

Acronis Cyber Backup ofrece prácticas funciones que ayudan a las instituciones sanitarias a gestionar de forma inteligente los RTO y RPO en su entorno de aplicaciones, incluidas:

1. Acronis Instant Restore, que proporciona tiempos (RTO) y puntos de recuperación (RPO) casi nulos para la mayoría de las aplicaciones esenciales.
2. Acronis Universal Restore, que ofrece una gran flexibilidad para restaurar un sistema en un hardware sin sistema operativo o en una plataforma diferente, como por ejemplo, de un dispositivo físico a una máquina virtual, cuando sea necesario.
3. La solución integrada Acronis Active Protection, que elimina el tiempo de inactividad y la disminución del rendimiento asociados a los ataques de ransomware y cryptojacking.

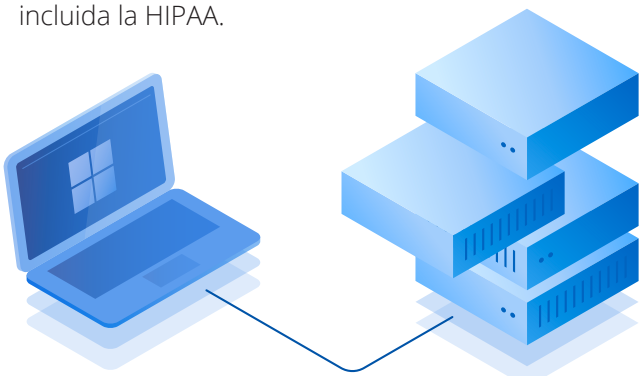
PROTECCIÓN DE DATOS CONFIDENCIALES EN TODOS LOS DISPOSITIVOS

Acronis Files Advanced ayuda a mejorar la atención al cliente y la eficiencia operativa, y al mismo tiempo garantiza el cumplimiento de las exigentes normativas de seguridad, incluida la ley Health Insurance Portability y Accountability Act (HIPAA). Con Acronis Files Advanced, los empleados, partners y contratistas del sector sanitario pueden compartir documentos confidenciales, y colaborar. Mientras tanto, las instituciones conservan el control total de la ubicación, la administración y la privacidad de los datos.

El motor de directivas de Acronis Access Advanced proporciona funciones de administración granular para garantizar el control y el cumplimiento de las normativas sobre contenido, usuarios y dispositivos. Asimismo, la solución garantiza una completa protección y confidencialidad de la información, a través del cifrado integral y seguro de los datos en tránsito y en reposo. Además, Acronis Files Advanced permite a los técnicos prevenir las fugas de información, las violaciones de datos compartidos y las brechas en la seguridad mediante el empleo de controles de directivas centralizados.

Los proveedores de atención sanitaria, el personal médico y los pacientes utilizan Acronis Files Advanced para acceder, editar, crear y compartir datos médicos entre cualquier dispositivo: ordenador de sobremesa, portátil, tablet o smartphone. Los profesionales de la sanidad emplean también la solución para:

- **Proteger** los datos sensibles de pacientes y los documentos administrativos confidenciales (información e investigaciones, contratos con centros académicos y empresas, etc.).
- **Ofrecer** a médicos, investigadores y administradores acceso seguro a datos médicos, y facilitar el intercambio de datos desde cualquier dispositivo.
- **Proteger** las historias de los pacientes, tanto en reposo como en tránsito.
- **Colaborar** de forma rápida y eficaz en la atención al paciente, ya sea de forma interna (en el propio centro de atención sanitaria) o con el exterior (con otros partners).
- **Supervisar** el acceso y uso compartido de archivos de asistencia sanitaria.
- **Cumplir** las estrictas normativas sobre seguridad, incluida la HIPAA.



FORTALECECIMIENTO DE LA CIBERPROTECCIÓN SIN AÑADIR COMPLEJIDAD A LA INFRAESTRUCTURA

Acronis Cyber Backup simplifica y reduce el coste de la ciberprotección en sanidad, proporcionando una sola plataforma que protege todas las cargas de trabajo de las instituciones.

Esta solución permite gestionar las operaciones de almacenamiento, retención, copias de seguridad y recuperación de datos en todos los ámbitos, incluidas las plataformas de nube, virtuales, físicas y móviles, así como las cargas de trabajo de Microsoft, Oracle o Google, entre otras. Además, su intuitiva interfaz y sus eficaces herramientas de supervisión facilitan su uso incluso a los ingenieros informáticos relativamente más inexpertos, de forma que los más experimentados puedan dedicarse a proyectos más estratégicos.

Por último, el complemento Acronis Disaster Recovery es una sencilla extensión de fácil uso de Acronis Cyber Backup, que permite a las instituciones de atención sanitaria recuperarse inmediatamente tras sufrir un fallo de sistemas informáticos, aplicaciones y datos críticos. Para ello cambia automáticamente a las copias de seguridad que se ejecutan en máquinas virtuales en la nube segura de Acronis. Ofrece conmutación en caso de error para una amplia variedad de plataformas de computación y aplicaciones, como Windows Server, Linux, plataformas de virtualización, como VMware, Hyper-V, KVM, XenServer y Red Hat Virtualization, y aplicaciones Microsoft, como Exchange, SQL Server, SharePoint y Active Directory.

LA ARQUITECTURA EN LA NUBE EXCLUSIVA DE ACRONIS LE OFRECE CONTROL SOBRE SUS DATOS

TODO TIPO DE ADMINISTRACIÓN

Software de administración implementado y controlado de manera independiente, que permite al cliente, proveedor de servicios, proveedor, partner o a un tercero controlar la protección de los datos desde una nube pública, una nube del partner o una nube privada, o bien en las instalaciones del cliente

TODO TIPO DE PROTECCIÓN

- Copia de seguridad
- Almacenamiento
- Recuperación ante desastres
- Sincronización y uso compartido
- Notary/ASign
- Protección frente al ransomware

TODO TIPO DE CARGA DE TRABAJO

- In situ
- Nube
- Aplicaciones
- Virtual
- Nube privada
- Móviles
- Archivos

TODO TIPO DE ALMACENAMIENTO

- Disco, cinta
- Nube del partner
- Nube pública
- NAS, SAN
- Nube privada
- Copia en Acronis

TODO TIPO DE IMPLEMENTACIÓN

- Local
- Nube del partner
- Nube pública
- Nube privada
- Acronis Cloud

TODO TIPO DE RECUPERACIÓN

- Entorno físico
- Virtual
- Móviles
- Aplicaciones
- Archivos
- Nube

CONCLUSIÓN

La combinación de transformación digital rápida, incremento de los volúmenes de datos, aumento de necesidades de interoperabilidad y mayor exigencia por parte de interesados y organismos reguladores contribuye a que el sector sanitario esté viviendo una época complicada. Ofrecer al mismo tiempo protección, accesibilidad, privacidad, autenticidad y seguridad de los datos no es fácil, especialmente si tenemos en frente a ejércitos de ciberdelincuentes decididos a robar los jugosos datos médicos y retenerlos a cambio de un rescate. Las instituciones de atención sanitaria deben permitir el uso de nuevas aplicaciones, reducir los costes y mejorar la situación de los pacientes, todo ello superando muchos retos en el ámbito técnico, como la retención de personal, la migración a la nube y la proliferación de dispositivos móviles y del IoT.

Acronis puede ayudar con una gama de soluciones de ciberprotección, almacenamiento, sincronización y uso compartido de archivos, y recuperación ante desastres, de eficacia probada y optimizadas para el sector sanitario.

Vea cómo la soluciones de ciberprotección de Acronis ya han ayudado a un hospital de Estados Unidos aquí.

Consiga una **prueba gratuita de 30 días de los productos de Acronis** para el sector sanitario aquí:

- Acronis Cyber Backup con Acronis Active Protection — CONSIGA UNA PRUEBA GRATUITA DE 30 DÍAS
- Complemento Acronis Disaster Recovery para Acronis Cyber Backup — CONSIGA UNA PRUEBA GRATUITA DE 30 DÍAS
- Acronis Files Advanced. — CONSIGA UNA PRUEBA GRATUITA DE 30 DÍAS

Acronis

Encontrará más información en **www.acronis.com**