Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2025,
Volumen 9, Número 5.

https://doi.org/10.37811/cl_rcm.v9i5

CONFIANZA CERO APLICADA A UN HOSPITAL MEXICANO: UNA PROPUESTA DE IMPLEMENTACIÓN

ZERO TRUST APPLIED TO MEXICAN HOSPITAL: AN IMPLEMENTATION PROPOSAL

José Antonio Zárate Urgell
Universidad Americana de Europa (UNADE), México

Richard de Jesús Gil Herrera
Universidad Internacional de La Rioja (UNIR), España

DOI: https://doi.org/10.37811/cl_rcm.v9i5.20194

Confianza Cero Aplicada a un Hospital Mexicano: Una Propuesta de Implementación

José Antonio Zárate Urgell [1]
a-zarateu@choapas.tecnm.mx
https://orcid.org/0000-0003-1442-0121
TecNM Campus Las Choapas (ITS-Choapas) y Universidad Americana de Europa (UNADE)
Las Choapas, Veracruz, México

Richard de Jesús Gil Herrera
richard.dejesus@unir.net
https://orcid.org/0000-0003-4481-7808
Universidad Internacional de La Rioja (UNIR)
Logroño, España

RESUMEN

En el sector de la salud, proteger los datos sensibles de los pacientes es fundamental para garantizar la continuidad de los servicios médicos. Este estudio presenta la implementación de una arquitectura de Confianza Cero (Zero Trust, ZT) en un hospital público de Veracruz, México, con el objetivo de mejorar la protección de datos y la integridad del sistema. Confianza Cero es un modelo de seguridad que no confía automáticamente en ningún usuario o dispositivo, requiriendo una verificación continua. La implementación resultó en una reducción del 50% en violaciones de datos, autenticación multifactor (MFA) exitosa en el 90% de los accesos, microsegmentación de red y capacitación del personal, lo que generó una mejora del 40% en la respuesta a incidentes. Estos resultados demuestran que Confianza Cero es una estrategia eficaz para la seguridad de la información en el ámbito sanitario, fortaleciendo la protección de los datos médicos, mitigando amenazas internas y externas, y asegurando el cumplimiento normativo. A pesar de los desafíos iniciales relacionados con la complejidad y la capacitación, los resultados respaldan la inversión de tiempo y recursos necesaria para su implementación exitosa. El estudio aporta un marco de Confianza Cero escalable para hospitales públicos, que integra políticas granulares, monitoreo continuo, alineado con la transición hacia un sistema de salud más digitalizado y seguro.

Palabras clave: ZT, confianza cero, ciberseguridad, implementación, hospital público

[1] José Antonio Zárate Urgell.
Correspondencia: a-zarateu@choapas.tecnm.mx

Zero Trust Applied to Mexican Hospital: An Implementation Proposal

ABSTRACT

In the healthcare sector, safeguarding sensitive patient data is critical to ensure the continuity of medical services. This study presents the implementation of a Zero Trust (ZT) architecture in a public hospital in Veracruz, Mexico, aiming to enhance data protection and system integrity. Zero Trust is a security model that does not automatically trust any user or device, requiring continuous verification. The implementation resulted in a 50% reduction in data breaches, successful multi-factor authentication (MFA) in 90% of access, network micro-segmentation, and staff training, leading to a 40% improvement in incident response. These outcomes demonstrate that Zero Trust is an effective strategy for healthcare information security, strengthening medical data protection, mitigating internal and external threats, and ensuring regulatory compliance. Despite initial challenges in complexity and training, the results support the investment in time and resources needed for its successful deployment. The study contributes a scalable Zero Trust framework for public hospitals, integrating granular policies, continuous monitoring, and contextual trust algorithms, aligned with the transition to a more digitalized and secure healthcare system.

Keywords: ZT, zero trust, cybersecurity, implementation, public hospital

Artículo recibido 22 agosto 2025

Aceptado para publicación: 25 septiembre 2025

INTRODUCCIÓN

La expansión del acceso a Internet a través de innumerables dispositivos, intensificada por la pandemia de COVID-19, ha aumentado las vulnerabilidades en las infraestructuras de ciberseguridad. Según IBM, el 83% de las organizaciones experimentan al menos una violación de datos, un evento que cuesta un promedio de $ 4.45 mil millones. El compromiso de credenciales es el vector de violación más común, con detecciones que tardan aproximadamente 243 días y la contención alrededor de 84 días. La industria de la salud sufre el mayor impacto, con costos promedio que alcanzan los $ 10.10 millones por robo de datos, lo que lo convierte en el sector más afectado por duodécimo año consecutivo.

(“IBM: Average Cost of a Healthcare Data Breach Increases toAlmost $11 Million,” 2023)

La creciente interconectividad en los sistemas sanitarios, agravada por la pandemia de COVID-19 y el teletrabajo, ha aumentado significativamente los riesgos de ciberataques, como ransomware y fugas de datos sensibles.

(“Teletrabajo durante la pandemia de COVID-19: riesgos yestrategias preventivas,” n.d.)

Como se destaca en la presente investigación sobre ciberseguridad en salud, solo el 10% del personal del Hospital IMSS-BIENESTAR en Veracruz-México, conocía el modelo Zero Trust (ZT). Esto subraya la necesidad crítica de capacitación y concientización sobre ciberseguridad dentro de las instituciones de atención médica. El costo promedio de las violaciones de datos en el sector de la salud es de $ 10.10 millones, el más alto entre todas las industrias analizadas. Un ejemplo llamativo es el ataque de ransomware WannaCry de 2017, que interrumpió 80 de los 236 hospitales del Reino Unido, provocando pérdidas de 92 millones de euros. Estos incidentes enfatizan la necesidad urgente de medidas sólidas de ciberseguridad en los sistemas de salud digital. (“IBM Helps Customers Adopt a Zero Trust Approach to Security”, s/f)

En 2020, el Instituto Nacional de Estándares y Tecnología (NIST) definió los componentes lógicos de una arquitectura de confianza cero (ZTA). Según el NIST, un usuario solicita acceso al sistema desde un estado que no es de confianza y, mediante la aplicación de políticas de control, pasa a un estado de confianza en relación con recursos empresariales específicos. [(Edwards, 2020)

La transformación digital en la atención médica, evidenciada por la modernización de los registros médicos y el monitoreo remoto de pacientes, ha aumentado la exposición a los ciberdelincuentes. En

una entrevista, Dula Hernández de Palo Alto Networks México destacó que la digitalización del sector ha aumentado su vulnerabilidad, con ataques de ransomware que aumentaron en un 70% en México. Hernández subraya el imperativo de reforzar la ciberseguridad en los servicios de salud y adoptar arquitecturas Zero Trust. (“Zero Trust for Healthcare Organizations Overview”, s/f)

Este citado estudio tiene como objetivo abordar las vulnerabilidades de ciberseguridad en el Hospital IMSS-BIENESTAR mediante el diseño de una arquitectura Zero Trust adaptada a su infraestructura y requerimientos regulatorios.

La metodología combina enfoques cualitativos y cuantitativos, incluida una revisión sistemática de las implementaciones de Zero Trust en la atención médica, el análisis de la infraestructura del hospital y el uso de inventarios del sistema y registros de acceso.

Los resultados demostraron una reducción del 50% en las violaciones de datos, la implementación exitosa de la autenticación multifactor (MFA) en el 90% de los accesos, la microsegmentación de la red y la capacitación del personal, lo que llevó a una mejora del 40% en la respuesta a incidentes. La conclusión subraya que Zero Trust fortalece la protección de datos médicos, mitiga las amenazas internas y externas y garantiza el cumplimiento normativo, a pesar de los desafíos iniciales en complejidad y capacitación.

La principal contribución es un marco escalable de Zero Trust para hospitales públicos, integrando políticas granulares, monitoreo continuo y algoritmos de confianza contextual, alineados con la transición hacia un sistema de salud más digitalizado y seguro.

La investigación sobre Zero Trust ha logrado un progreso significativo desde que John Kindervag lo propuso por primera vez en 2010. (Nandakumara, 2024) Se han establecido marcos y arquitecturas teóricas, como los definidos por el NIST en su publicación "Zero Trust Architecture" (“Zero Trust Architecture: NIST Publishes SP 800-207”, 2020)

Esto ha mejorado la comprensión y la aplicación del modelo Zero Trust en varios entornos, incluida la atención médica. Estudios como el de Teerakanok (Phiayura & Teerakanok, 2023) han examinado los desafíos y la migración hacia la Arquitectura de Confianza Cero, ofreciendo una base teórica para su implementación. Una brecha clave en la investigación es la falta de estudios sobre la escalabilidad de Zero Trust en múltiples hospitales y contextos.

Los estudios existentes a menudo se centran en casos individuales sin evaluar cómo se puede implementar Zero Trust de manera efectiva en redes más amplias de hospitales y clínicas. Además, se necesita más investigación sobre las mejores prácticas para la capacitación del personal y la gestión cultural para garantizar el éxito de Zero Trust en entornos hospitalarios.

Este estudio tiene como objetivo abordar estas limitaciones y brechas mediante la implementación de un marco de Confianza Cero adaptado a las necesidades específicas de un hospital público en México. Nuestro enfoque combina una revisión de la literatura con un análisis detallado de la infraestructura y los requisitos del hospital, así como la implementación práctica de soluciones basadas en Zero Trust. Los resultados buscan mejorar la comprensión y la eficacia de Zero Trust como estrategia de seguridad en la atención médica.

Objetivos del estudio

Objetivo General

- Desarrollar una propuesta de diseño de seguridad basada en Zero Trust adaptada a las necesidades específicas y a la infraestructura existente del hospital, que se adapte tanto a los usuarios actuales como a las demandas futuras anticipadas.

Objetivos específicos

- Realización de una revisión cualitativa de varias implementaciones de Zero Trust Architecture (ZTA) en el sector de la salud.
- Investigar los requisitos de seguridad y protección dentro de la red interna del hospital, considerando la infraestructura actual y los perfiles de usuario.
- Formular una propuesta de diseño que detalle los pasos de implementación, integrando las mejores prácticas y recomendaciones para la implementación de ZTA para el estudio de caso.

Este estudio empleó un enfoque de métodos mixtos, combinando técnicas cualitativas y cuantitativas para evaluar la efectividad de la implementación de Zero Trust en el Hospital IMSS-BIENESTAR.

Marco teórico

Descripción general de Zero Trust

Zero Trust (ZT) representa un marco de seguridad destinado a mitigar el riesgo de acceso no autorizado al negar la confianza implícita a cualquier usuario o dispositivo, incluso a aquellos dentro del perímetro

de la red. A pesar de los posibles desafíos de usabilidad, los primeros resultados muestran que las organizaciones que implementan la tecnología de la lengua y el calzado pueden lograr ahorros de costos considerables. Según Microsoft, el 76% de las organizaciones han iniciado una estrategia de Confianza Cero, y el 35% afirma que la implementación completa. (Microsoft, s/f)

Originalmente propuesto por John Kindervag en 2010 ("Forrester Pushes 'zero Trust' Model for Security", 2010), ZT se basa en tres principios:

- Acceso seguro a todos los recursos independientemente de su ubicación.
- Aplique controles de acceso granulares en toda la red.
- Inspeccione y registre continuamente todo el tráfico de red.

El objetivo central de ZT es asegurar el acceso a la red a través de una autenticación rigurosa y un control de políticas, asegurando que cada intento de acceso sea verificado y registrado. Un ejemplo de estos principios en acción es cuando un usuario de una red externa solicita acceso a recursos dentro de la red. Se verifica la identidad del usuario; Si la verificación es exitosa, se les permite acceder a los recursos solicitados. Si no es así, se rechaza la solicitud. En cualquier caso, la solicitud del usuario se registra en un archivo de registro. Este monitoreo se lleva a cabo cada vez que el usuario intenta acceder a un recurso, no solo una vez.

En un ejemplo de los principios de ZT, un usuario de una red externa solicita acceso a los recursos deseados. El usuario accede a Internet desde cualquier parte del mundo utilizando un dispositivo y solicita uno de los recursos que se encuentran dentro de la red. Aquí se verifica la identidad del usuario. Si se verifica, se le permite obtener los recursos deseados; si no, su solicitud es rechazada. En cualquier caso, la solicitud del usuario se registra en un archivo de registro. (Boutin, 2022)

Esta monitorización se realiza en todo momento que el usuario entra en el perímetro de seguridad de la entidad que tiene los recursos solicitados. Para ZT, no es suficiente que el usuario haya verificado una vez, se hace cada vez que el usuario solicita acceso a un recurso.

Descripción general de zero trust

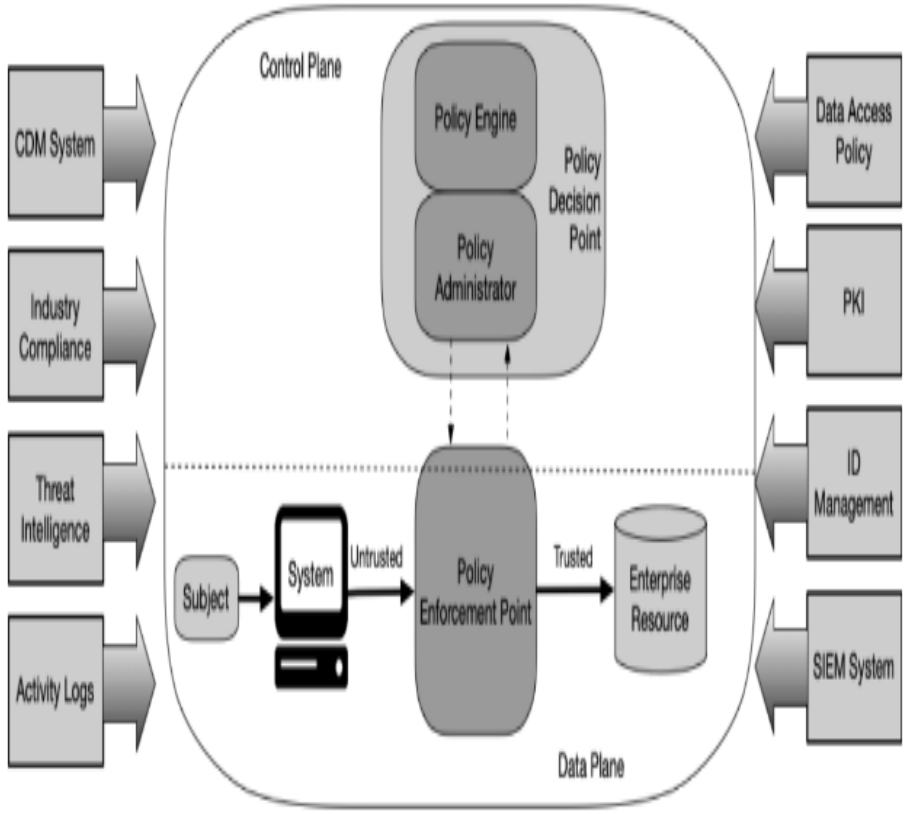
En 2020, el Instituto Nacional de Estándares y Tecnología (NIST) definió los componentes lógicos de una arquitectura de confianza cero (ZTA) en su publicación NIST SP 800-207. De acuerdo con este marco, un usuario accede inicialmente al sistema en un estado que no es de confianza. A través de

políticas de control estrictas, implementadas por puntos de decisión de políticas (PDP) y puntos de aplicación de políticas (PEP), el usuario puede acceder de manera confiable a recursos confidenciales. ("Zero Trust Architecture: NIST Publishes SP 800-207", 2020)

En la Figura 1, se puede observar cómo un usuario solicita acceso al sistema en un estado no confiable y, a través de la política de control, se convierte en confiable para los recursos de la entidad (Plano de datos). En el plano de control, el punto de aplicación de directivas (PEP) envía la solicitud del usuario a través de un recurso del sistema. El administrador de políticas (PA) y el motor de políticas (PE) autorizan o rechazan la solicitud en función de criterios predefinidos y algoritmos de confianza.

Este marco exige que cada solicitud de acceso sea autenticada y autorizada, transformando una solicitud no confiable en una confiable, siempre que cumpla con las políticas establecidas.

Figura. 1. Componentes lógicos de una arquitectura de confianza cero definida por el NIST. Fuente: (Rose et al., Zero Trust Architecture, 2020)



Estándares para la protección de datos en el cuidado de la salud

La implementación de ZTA requiere el cumplimiento de estándares regulatorios que protegen la información confidencial. Para el sector de la salud, las regulaciones esenciales incluyen:

(“HIPAA y HITECH Requisitos para organizaciones sanitarias|,” n.d.)

HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico): Ley federal de EE. UU. que establece estándares de protección de datos para la información del paciente. (“HIPAA compliance: definición y normativas”, 2021)

HITECH (Tecnología de la Información de Salud para la Salud Económica y Clínica): Regulaciones que respaldan HIPAA a través del desarrollo de registros de salud electrónicos nacionales y hacen cumplir los requisitos de protección de datos. (Office for Civil Rights (OCR), 2009)

GDPR (Reglamento General de Protección de Datos): La directiva de la Unión Europea sobre la protección de datos personales, que garantiza un control estricto sobre el acceso y el uso de los datos. (Stamp, 2024)

Adicionalmente, en México, la protección de datos se rige por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y artículos constitucionales pertinentes. Estos marcos legales son vitales a la hora de implementar una estrategia de Zero Trust en la sanidad. (Diputados, 2011)

Estudio de casos de implementación de zero trust

Estudios recientes e informes de casos ilustran cómo organizaciones y los principales hospitales de EE. UU., han aprovechado la seguridad de la identidad para implementar Zero Trust, protegiendo así los costos, la reputación y los vastos repositorios de datos de pacientes. También muestra un ejemplo de cómo se pueden proteger los costos, la reputación y los miles de registros de pacientes en el hospital líder de EE. UU. a través de la seguridad de la identidad. (“Healthcare and Public Health Cybersecurity”, s/f)

Por ejemplo, Healthfirst implementó Zero Trust para proteger su infraestructura de TI, asegurando que solo los usuarios autorizados pudieran acceder a datos confidenciales. Este enfoque no solo protegió la información confidencial, sino que también mejoró la capacidad de la organización para responder a incidentes de seguridad de manera más efectiva. (Küçükönder & Görçün, 2023)

METODOLOGÍA

Este estudio empleó un enfoque estructurado para implementar Zero Trust en el Hospital IMSS-BIENESTAR, utilizando una metodología de desarrollo de sistemas basada en el ciclo de vida de la cascada. Esta metodología abarcó tres fases principales: análisis, diseño, implementación y pruebas, cada una de las cuales se detalla a continuación:

Fase de análisis: Caso Hospital Bienestar

Para evaluar el panorama de seguridad interna del hospital, se realizó un análisis FODA exhaustivo. Este análisis no solo reveló las fortalezas y debilidades del hospital, sino que también destacó las oportunidades y amenazas externas, identificando así áreas clave para mejorar la seguridad. Se delinearon los requisitos de seguridad específicos, centrándose en las actualizaciones de software, hardware y capacitación del personal para reforzar la postura de ciberseguridad del hospital.

Además del análisis FODA, se realizó una revisión sistemática de las implementaciones de Zero Trust en el cuidado de la salud para identificar las mejores prácticas y los posibles desafíos. Esta revisión proporcionó información valiosa sobre cómo otras instituciones de atención médica han adoptado con éxito las arquitecturas Zero Trust, lo que ayudó a informar la estrategia de diseño e implementación de este proyecto.

El análisis incluyó un inventario de sistemas, usuarios y registros de acceso para comprender a fondo el panorama de seguridad del hospital. Este inventario detallado permitió al equipo de investigación trazar un mapa de la infraestructura de seguridad actual del hospital e identificar áreas específicas donde se necesitaban mejoras. Al adoptar un enfoque metódico para comprender los factores internos y externos que afectan la seguridad del hospital, el estudio pudo desarrollar un plan de implementación de Zero Trust específico y efectivo.

Fase de diseño

Con base en los conocimientos de la fase de análisis, diseñamos una infraestructura tecnológica robusta. Mejoramos los servidores de red, las estaciones de trabajo y la seguridad perimetral para alinearnos con los principios de Zero Trust. También desarrollamos un plan estratégico para actualizar el software del hospital para garantizar la compatibilidad con los estándares Zero Trust. Esto implicó identificar y

programar las actualizaciones de hardware necesarias, incluidos los dispositivos de seguridad y los equipos de red, para facilitar la implementación sin problemas de Zero Trust.

Además de estas actualizaciones, creamos políticas de acceso detalladas y estrategias de monitoreo continuo para cumplir con los principios de Zero Trust. Estas políticas tenían como objetivo restringir el acceso a información confidencial en función de las funciones y responsabilidades de los usuarios, reduciendo así el riesgo de acceso no autorizado.

Diseñamos un programa de capacitación integral para que el personal del hospital mejore sus habilidades de ciberseguridad. El objetivo era equipar a los empleados con las habilidades necesarias para apoyar eficazmente la iniciativa Zero Trust. También describimos pasos específicos para implementar la autenticación multifactor (MFA) y la microsegmentación de red para minimizar la superficie de ataque. MFA agrega una capa de seguridad adicional al requerir más verificación que solo una contraseña. La microsegmentación divide la red en partes más pequeñas, lo que limita el movimiento lateral de los posibles atacantes.

Finalmente, planificamos una serie de pruebas para evaluar la efectividad de las mejoras implementadas y garantizar el cumplimiento de los estándares de seguridad establecidos. Estas pruebas tenían como objetivo confirmar que las nuevas medidas de seguridad funcionaban según lo previsto e identificar las áreas que necesitaban un mayor perfeccionamiento.

El diagrama de red actual del hospital muestra una arquitectura de red hospitalaria típica, con un enrutador principal que actúa como puerta de enlace a Internet y varios conmutadores que segmentan la red en áreas funcionales. Se observan múltiples dispositivos conectados, incluidos sistemas de información clínica (HIS), sistemas de comunicación y archivo de imágenes (PACS), equipos médicos y dispositivos IoT. Sin embargo, también revela vulnerabilidades inherentes a esta arquitectura, como un único perímetro de seguridad basado en un firewall, confianza implícita en dispositivos internos, segmentación limitada y configuración de seguridad Wi-Fi considerada "insegura".

La nueva arquitectura Zero Trust propuesta mejora esto con múltiples puntos de control de seguridad, verificación continua de dispositivos y usuarios, microsegmentación granular, autenticación y autorización dinámica basada en atributos, cifrado en reposo y en tránsito, y monitoreo continuo con registro detallado. Esto ofrece una mayor protección contra las brechas de seguridad, reduce el riesgo

de propagación de ataques laterales y proporciona una mayor flexibilidad y adaptabilidad a los cambios del entorno de seguridad. Además, la implementación de Zero Trust demuestra un mayor compromiso con la seguridad de la información y el cumplimiento de regulaciones como HIPAA y GDPR, brindando una mejor experiencia de usuario al permitir políticas de acceso más personalizadas y seguras. Los componentes clave de esta arquitectura incluyen el punto de aplicación de políticas (PEP), el motor de políticas (PE), el motor de confianza y el proveedor de identidades, cada uno con un rol específico en la implementación de políticas de seguridad y la verificación de la identidad y el acceso de usuarios y dispositivos.

Fase de implementación y prueba

La fase de implementación marcó la transición de la planificación a la acción, con mejoras que se implementaron en los servidores de red del hospital para reforzar la seguridad y la eficiencia del sistema. Las estaciones de trabajo se actualizaron meticulosamente para cumplir con los estándares de seguridad Zero Trust, asegurando que cada punto de acceso cumpliera con los criterios de seguridad requeridos. Para protegerse contra amenazas externas, se implementaron medidas avanzadas de seguridad perimetral. Específicamente, la fase de implementación incluyó la implementación de firewalls de próxima generación y la integración de sistemas de gestión de eventos e información de seguridad (SIEM) para mejorar las capacidades de monitoreo. Estas tecnologías fortalecieron la defensa del hospital contra posibles amenazas cibernéticas y proporcionaron información en tiempo real sobre los eventos de seguridad.

A lo largo de esta fase, se administraron encuestas al personal del hospital para recopilar comentarios sobre los cambios implementados e identificar áreas de mejora adicional. Este ciclo de retroalimentación fue fundamental para refinar la arquitectura Zero Trust y garantizar su integración efectiva en el marco operativo del hospital. Además, la capacitación del personal se llevó a cabo en fases, con un enfoque en escenarios prácticos para mejorar los tiempos de respuesta a incidentes y la conciencia general de seguridad. Al equipar al personal con las habilidades y conocimientos necesarios, el hospital reforzó el elemento humano de su postura de seguridad.

Implementación de zero trust

Para implementar Zero Trust en este entorno, es crucial abordar la diversidad de usuarios, la heterogeneidad de los dispositivos y el imperativo de proteger los datos de los pacientes. La implementación incluyó las siguientes medidas:

Firewalls y sistemas SIEM de próxima generación: El hospital implementó firewalls de próxima generación y sistemas integrados de gestión de eventos e información de seguridad (SIEM) para mejorar las capacidades de monitoreo y proporcionar información en tiempo real sobre los eventos de seguridad.

Capacitación del personal: La capacitación del personal se llevó a cabo en fases, con un enfoque en escenarios prácticos para mejorar los tiempos de respuesta a incidentes y la conciencia general de seguridad. Esto garantiza que los empleados estén equipados con las habilidades necesarias para respaldar la iniciativa Zero Trust de manera efectiva.

Autenticación multifactor (MFA) y microsegmentación de red: se describieron pasos específicos para la implementación de MFA y microsegmentación de red para reducir la superficie de ataque. MFA agrega una capa adicional de seguridad al requerir que los usuarios proporcionen una verificación adicional más allá de una simple contraseña, mientras que la microsegmentación de la red divide la red en segmentos más pequeños para limitar el movimiento lateral de los posibles atacantes.

Ciclo de retroalimentación: A lo largo de la fase de implementación, se administraron encuestas al personal del hospital para recopilar comentarios sobre los cambios implementados e identificar áreas de mejora adicional. Este ciclo de retroalimentación fue fundamental para refinar la arquitectura Zero Trust y garantizar su integración efectiva en el marco operativo del hospital.

RESULTADOS

La implementación de Zero Trust en el Hospital IMSS-BIENESTAR resultó en mejoras significativas en las métricas de ciberseguridad:

Reducción de la violación de datos: Se observó una disminución del 50% en los incidentes de violación de datos, lo que demuestra la eficacia de la arquitectura Zero Trust para salvaguardar la información confidencial del hospital. Esta mejora se atribuye a la implementación de políticas de acceso granulares y autenticación multifactor (MFA) para el 90% de los accesos.

Mejora de la respuesta a incidentes: La capacidad de respuesta a incidentes mejoró en un 40% gracias a la implementación de herramientas de monitoreo continuo y análisis de tráfico de red. Esto permitió una detección y mitigación de amenazas más rápida y efectiva.

Capacitación del personal: El personal del hospital participó en programas de capacitación en ciberseguridad, mejorando su conocimiento y conciencia de las prácticas seguras. Esto es crucial para mantener una postura de seguridad sólida y evitar el acceso no autorizado debido a errores humanos.

Cumplimiento normativo: La implementación de Zero Trust ayudó al hospital a cumplir con las regulaciones de protección de datos relevantes, como HIPAA y GDPR, fortaleciendo así su reputación y confianza entre los pacientes y las autoridades reguladoras.

CONCLUSIONES

La integración de tecnologías avanzadas en la atención médica se ha vuelto imperativa, particularmente a la luz del aumento del trabajo remoto y los desafíos impulsados por la pandemia. La implementación de Zero Trust, aunque compleja y requiere muchos recursos, es esencial para reforzar la protección de datos y la resiliencia del sistema en entornos hospitalarios. Los beneficios demostrados mejoraron la seguridad de los datos de los pacientes, la respuesta mejorada a las amenazas y el cumplimiento normativo respaldan la inversión sustancial en tiempo y recursos necesarios para su implementación exitosa.

A partir de estos hallazgos, la implementación de Zero Trust en el Hospital IMSS-BIENESTAR ha demostrado que este modelo de seguridad es una estrategia valiosa para proteger la información sensible en el sector salud. A pesar de los desafíos iniciales en términos de complejidad y capacitación, los resultados obtenidos respaldan la inversión en tiempo y recursos necesarios para su implementación exitosa. Estos hallazgos son consistentes con otros estudios de casos en el sector de la salud que han mostrado mejoras en la postura de seguridad a través de la adopción de Zero Trust.

Aunque los resultados son prometedores, es crucial reconocer las limitaciones del estudio, como la implementación experimental en un solo hospital. La investigación futura podría explorar la escalabilidad de Zero Trust en múltiples hospitales y contextos, evaluando su efectividad en diversos entornos con diferentes niveles de recursos.

REFERENCIAS BIBLIOGRÁFICAS

Boutin, C. (2022). NIST Updates Guidance for Health Care Cybersecurity | NIST.

Diputados. (2011). REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. En Gob.mx.

Edwards, J. (2020). Scott Rose on NIST's draft zero trust guidance. En ExecutiveGov.

Forrester pushes "zero trust" model for security. (2010). En Darkreading.com.

Healthcare and public health cybersecurity. (s/f). En Cybersecurity and Infrastructure Security Agency CISA.

HIPAA compliance: definición y normativas. (2021). En Proofpoint.

HIPAA y HITECH Requisitos para organizaciones sanitarias |. (s/f). En Thalesgroup.com.

IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. (2023). En Hipaajournal.com.

IBM helps customers adopt a zero trust approach to Security. (s/f). En IBM Newsroom.

Küçükönder, H., & Görçün, Ö. F. (2023). Healthcare 4.0 and decision-making techniques in the health industry: A systematic literature review. En Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application (pp. 121–134). Springer Nature Singapore.

Microsoft. (s/f). News Microsoft. https://news.microsoft.com/es-xl/microsoft-promueve-zero-trust-en-evento-seguridad-en-el-sistema-financiero/.

Nandakumara, R. (2024). John Kindervag shares zero trust's origin story. En Illumio.com. Illumio.

Office for Civil Rights (OCR). (2009). HITECH act enforcement interim final rule. En HHS.gov. US Department of Health and Human Services.

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. IEEE Access, 11, 19487–19511.

Stamp, N. (2024). What are the 7 main principles of GDPR? En GDPR EU.

Teletrabajo durante la pandemia de COVID-19: riesgos y estrategias preventivas. (s/f). En Europa.eu.

Zero Trust Architecture: NIST publishes SP 800-207. (2020). En CSRC | NIST.

Zero Trust for healthcare organizations overview. (s/f). En Palo Alto Networks.