TRABAJO DE GRADO
Opción Seminario-Diplomado.

Recomendaciones para la selección y auditoría de proveedores de outsourcing TI: Estrategias de ciberresiliencia, Zero Trust y sostenibilidad en la nueva EPS

Corporación Universitaria Remington.
Nombre de la facultad: Ingeniería
Nombre del programa académico: Ingeniería de Sistema

Jenny Jimenez Torres
Profesor Jorge Mauricio Sepúlveda Castaño
Opción de Trabajo de grado Seminario-Diplomado.
2026.

Agradecimiento

Quiero agradecer a la corporación Universitaria Remington por brindarme la oportunidad proporcionarme los recursos académicos, profesores con excelente formación profesional para capacitarme y ensañarme los pilares de tan importante carrera que se ha desarrollado en su punto mas alto en la actualidad, he terminado esta etapa tan importante en mi vida acompañados de un excelente cuerpo académico que me guiado y corregido en mi aprendizaje, llevándome más allá de mis expectativas. Permitiendo que culminara mi proceso formativo en mi opinión personal satisfactoriamente, culmino con agradecimiento profundo por proporcionarme y capacitarme con la mejor calidad para contribuir para mi maravilloso logro.

Tabla de Contenidos

Resumen

En este trabajo se establece un marco técnico integral de sugerencias para seleccionar y auditar proveedores de outsourcing TI que prestan sus servicios en el sector salud colombiano, tomando como caso de estudio a la NUEVA EPS colombiana. La exploración surge a partir de la necesidad de fortalecer la gobernanza TI ante el aumento de ciberamenazas y la complejidad de la infraestructura hibridas que común mente se manejan, donde la gestión de datos sensibles de millones de afiliados depende de terceros **(Superintendencia Nacional de Salud, 2024)**. Se examina como la evolución del outsourcing TI es una herramienta que pueden ser amoldada al modelo de negocio, en donde se puede requerir que las entidades de salud trasciendan los modelos de control tradicionales, Dando como alternativa la integración de ciberresilencia en donde su foque es prevenir y la trasparencia operativa que son fundamentales para garantizar la prestación ininterrumpida de servicios médicos que presta la entidad **(The Health Policy Partnership, 2024)**.

Las recomendaciones propuestas se centran en la implementación de una matriz de selección y pautas de auditoria continúa basadas en los principios de "confianza cero" (Zero trust) y responsabilidad ambiental (ESG). Los resultados demuestran que el uso de accesos Just-in-Time minimiza drásticamente la superficie de ataque al eliminar privilegios permanentes de proveedores externos **(NIST, 2020)**, a la mano de poder exigir al proveedor que tenga centros de datos con neutralidad de carbono asegurando la alineación con las normativas globales de sostenibilidad ambiental **(Green Software Foundation, 2024)**. A partir de lo anterior, se examina una preceptiva que no solamente mejore la seguridad de la información conforme a estándares como el ISO 27001, sino que además establezca a NUEVA EPS como un modelo de eficiencia energética y de innovación en el entorno digital sanitario **(ISO/IEC, 2023)**.

Palabras clave:

Outsourcing TI, Nueva EPS, Zero Trust, Auditoría Continua, ESG, Sector Salud, ciber-resiliencia, accesos Just-in-Time, PUE, MFA.

Pregunta Orientadora

¿De qué manera la integración de criterios de ciberresiliencia, accesos Just-in-Time y sostenibilidad ambiental en los procesos de selección y auditoría de proveedores de outsourcing TI, garantiza la continuidad del servicio y la protección de datos críticos en la Nueva EPS para el año 2026?

1 MARCO CONCEPTUAL Y CONTEXTUAL

1.1. Selección y Auditoría en la Era de la Confianza Digital

Para 2026, el outsourcing de TI en salud ha evolucionado de la simple reducción de costos a la gestión de la resiliencia operativa. La selección debe ser un proceso de debida diligencia técnica, mientras que la auditoría debe ser un mecanismo de verificación de cumplimiento normativo y ético **(ISACA, 2025; Superintendencia Nacional de Salud, 2024).**

1.1.2 Responsabilidad Corporativa

La integración de criterios ESG en el proceso de auditoría permite que la Nueva EPS lidere la transformación hacia una salud digital verde, alineada con las exigencias globales de sostenibilidad y eficiencia energética **(Green Software Foundation, 2024)**. Asimismo, la implementación de un monitoreo constante mediante auditorías continuas supera la efectividad de

los modelos anuales tradicionales, permitiendo un control proactivo ante cualquier desviación en los niveles de servicio o SLA **(ISACA, 2025; Piattini & Del Peso, 2021)**.

1.2. Marco Normativo

El proyecto se fundamenta en:

- Ley 1581 de 2012: Marco legal colombiano para la protección de datos personales

La **Ley 1581 de 2012** constituye el régimen general para la protección de datos personales en Colombia, desarrollando el derecho constitucional de *Habeas Data* que faculta a todas las personas a conocer, actualizar y rectificar la información recogida sobre ellas en bases de datos o archivos **(Congreso de Colombia, 2012)**. Esta normativa establece principios fundamentales como la libertad, la veracidad y la seguridad, exigiendo que cualquier tratamiento de datos cuente con la autorización previa, expresa e informada del titular. Asimismo, la ley define las obligaciones de los responsables y encargados del tratamiento, garantizando que el manejo de datos sensibles se realice bajo estrictos estándares de confidencialidad y exclusivamente para los fines autorizados **(Ley 1581, 2012; Ministerio de Tecnologías de la Información y las Comunicaciones, 2022)**.

- ISO/IEC 27001:2022

La norma **ISO/IEC 27001:2022** se define como el estándar global para la administración de la seguridad, estableciendo las pautas necesarias para implementar, conservar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Su meta principal es apoyar a las organizaciones en la defensa de su información sensible mediante un método basado en la gestión de riesgos, sustentado en tres pilares esenciales: la confidencialidad, la integridad y la disponibilidad de los datos **(ISO/IEC, 2022)**.

Esta actualización de 2022 introduce modificaciones importantes en las medidas de seguridad para ajustarse a las exigencias del mercado actual y a las amenazas digitales emergentes. Entre los cambios destacados se encuentra la inclusión de controles específicos para la vigilancia de actividades y la protección en la nube, lo que garantiza que las organizaciones operen de manera proactiva frente a incidentes cibernéticos **(ISO/IEC, 2022; Piattini & Del Peso, 2021)**.

.

- Circular 002 de 2024 (Supersalud)

Requerimientos mínimos de ciberseguridad para EPS. La superintendencia nacional de salud es un ente regulador que establece requerimientos en los estándares que se deben implementar sobre seguridad de la información y ciberseguridad, que las entidades de salud en Colombia deben implementar, como las EPS y las IPS **(Superintendencia Nacional de Salud, 2024)**. Tiene como pilar principal proteger la infraestructura delicada del sistema general de seguridad social en la salud frente a situaciones críticas de ciberataque, asegurando la continuidad de la prestación de los servicios y la protección de las historias clínicas de los pacientes. Esta

normatividad exige a las entidades prestadoras de salud implementar políticas de gobierno de datos, efectuar auditorias de vulnerabilidad y contar con planes de respuesta ante ataques cibernéticos, coordinados a sus ves con marcos internacionales para asegurar que la trasformación digital de la salud en el país sea adaptable y confiable **(Ministerio de Salud y Protección Social, 2025; Superintendencia Nacional de Salud, 2024**).

1.3. Contextualización: Nueva EPS

La Nueva EPS opera como el principal asegurador de salud en Colombia. Depende de proveedores externos para la gestión de historias clínicas (HCE) y con ello el procesamiento de autorizaciones, esto exige que estas dependencias externas formalicen estándares de disponibilidad superior o igual 99.9%. La Nueva EPS es una entidad de promotora de salud que está consolidada en el sector de la salud colombiana contando con una de las mayores coberturas en el territorio colombiano, administra la atención de mas de 10 millones de usuarios afiliados en los régimen contributivo y subsidiado **(Ministerio de Salud y Protección Social, 2025)**. Esta gran proporción operativa con lleva a la dependencia total de sistemas digitales híbridos, donde la interoperabilidad de datos y la administración de las historias clínicas se realiza mayormente a través de modelos outsourcing TI **(Google Cloud, 2024)**, Divisando este escenario la entidad actúa como central de información de datos sensibles, lo que lo vuelvo un activo de infraestructura critica nacional, por lo que seleccionar proveedores en TI debe responder a requerimiento estrictos administrativo, esto debe estar alineado a los estándares de la superintendencia nacional de salud **(Supersalud, 2024)**, con respecta a la disponibilidad del servicio y la integridad de los registros clínicos.

Desde un enfoque técnico y de seguridad, la Nueva EPS tienen desafíos en la supervisión de su infraestructura digital, en donde el proveedor administra la atención al usuario desde la nube (App y portales web). Para el año 2026, la implementación de buenas prácticas de seguridad es fundamental, Se debe prevenir cualquier interrupción en el servicio externalizado, puesto que esto impacta directamente a la oportuna atención médica y la seguridad del paciente. Bajo esta primicia, se debe adoptar marcos de gobernanza que exijan a los proveedores externos el cumplimiento debido de los estándares internacionales de ciberresilencia y gobernanza de datos **(ISO/IEC, 2022)**, esto se vuelve indispensable para asegurar que a pesar de externalizar estos servicios TI, la Nueva EPS mantenga la autoridad y el control sobre la privacidad de la información, teniendo en cuenta la continuidad del servicio frente a los incidentes cibernéticos (**The Health Policy Partnership, 2024)**.

2. DESARROLLO E IMPLEMENTACIÓN DEL APRENDIZAJE

En esta sección se presentan las herramientas diseñadas para la Nueva EPS, integrando los conceptos de vanguardia discutidos en el seminario.

2.1. Matriz de Selección de Proveedores

Para garantizar que el proveedor sea un aliado estratégico, se aplica la siguiente ponderación de criterios:

Protocolo de Auditoría de Servicios Externalizados

A diferencia de las auditorías anuales, se implementar un modelo de **Auditoría Continua**:

Fase de Planeación: Definición de indicadores de riesgo clave (KRI) automatizados.

Ejecución (Monitoreo 24/7): Uso de tableros de control (*Dashboards*) que consumen telemetría directa de los sistemas del proveedor **(ISACA, 2025).**

Pruebas de Intrusión (*Pentesting*): Realización de simulacros de ataque trimestrales sobre los activos gestionados por el tercero **(ISO/IEC, 2022).**

Tabla 1. *Criterios de Evaluación para Contratación de Outsourcing TI.*

Criterio de evaluación	Peso	Descripción técnica
CiberResiliencia	30%	Capacidad de recuperación (DRP) probada ante Ransomware.
Cumplimiento Zero Trust	25%	Implementación de accesos Just-in-Time (JIT).
Sostenibilidad ESG	20%	Centros de datos con neutralidad de carbono (PUE < 1.2).
Soberanía de Datos	15%	Gestión de llaves de cifrado en control de la Nueva EPS.
Costo Operativo	10%	Modelo financiero OPEX (pago por uso).

Nota. Elaboración propia a partir de los indicadores de eficiencia energética de la **ISO/IEC (2023)**, estándares de ciberseguridad de **NIST (2020)**, los indicadores de sostenibilidad de la **Green Software Foundation (2024)**, los marcos de gobernanza de **ISACA (2025)** y los análisis de infraestructura en salud de **The Health Policy Partnership (2024)**.

2.2. Implementación de Accesos Just-in-Time (JIT)

Se propone eliminar los accesos permanentes de los administradores del proveedor, sustituyéndolos por un protocolo de elevación de privilegios bajo demanda.

Se elimina el concepto de "cuenta compartida" o "acceso permanente" para el proveedor **(NIST, 2020)**.

Tabla 2. *Protocolo Zero Trust: Gestión de Accesos JIT*.

Acción	Requisito de Seguridad	Evidencia de Auditoría
Solicitud de Acceso	MFA Biométrico y ticket aprobado.	Registro en SIEM centralizado.
Duración del Acceso	Máximo 120 minutos por sesión.	Cierre de sesión automático.
Nivel de Privilegio	Lectura/Escritura según rol específico	Reporte de actividad en base de datos.

Nota. Elaboración propia a partir de los controles de gestión de identidades de **NIST (2020)** y los requisitos de registro y supervisión de la norma **ISO/IEC 27001:2022** y los marcos de auditoría continua de **ISACA (2025)**.

2.2.1La Transición al Modelo Zero Trust como Imperativo de Seguridad

Aplicando el esquema de confianza cero, específicamente mediante accesos *Just-in-Time*, es la única estrategia capaz de mitigar el riesgo de movimientos laterales en caso de una intrusión en los sistemas de la Nueva EPS. Al reducir la ventana de exposición de las cuentas de terceros, se protege la integridad de la historia clínica de los afiliados, cumpliendo con creces los estándares de la Ley 1581 de 2012 **(NIST, 2020; Congreso de Colombia, 2012).**

2.3. Auditoría de Sostenibilidad y Eficiencia Energética

La Nueva EPS audita el impacto ambiental de sus activos tecnológicos externalizados mediante los siguientes indicadores:

Tabla 3. *Indicadores de Auditoría ESG para Infraestructura Cloud.*

Indicador	Meta 2026	Método de Verificación
PUE (Power Usage Effectiveness)	>1.15	Telemetría del centro de datos.
Uso de Energías Limpias	100%	Certificados de energía renovable
Economía Circular	Certificado RAEE	Acta de disposición final de hardware

Nota. Elaboración propia a partir de los indicadores de eficiencia energética de la norma **ISO/IEC 30134-2 (2023)** y los estándares de neutralidad de carbono de la **Green Software Foundation (2024)**.

2.3.1Sostenibilidad como Criterio de Selección Técnica

La inclusión de métricas ESG (como el PUE) en la selección de proveedores demuestra que la eficiencia tecnológica y la responsabilidad ambiental son inseparables en 2026. Para la Nueva EPS, contratar proveedores con neutralidad de carbono no solo mejora su reputación corporativa, sino que garantiza una infraestructura más moderna y con menores costos operativos a largo plazo **(Green Software Foundation, 2024; ISO/IEC, 2023)**.

Conclusiones

En primera instancia, se concluye que la implementación de un modelo de "Confianza Cero" (Zero Trust), fundamentado en accesos Just-in-Time, constituye la estrategia más eficaz para mitigar riesgos críticos en la Nueva EPS. Al eliminar los privilegios permanentes para los proveedores de outsourcing, se reduce drásticamente la superficie de ataque y se asegura que el ingreso a las bases de datos de afiliados sea una excepción temporal y estrictamente auditada. Este enfoque no solo protege la privacidad de la historia clínica bajo la Ley 1581 de 2012, sino que garantiza que la entidad mantenga el control total sobre sus activos digitales más sensibles en un entorno de amenazas persistentes para el año 2026 **(NIST, 2020; Congreso de Colombia, 2012)**.

Asimismo, la integración de criterios de sostenibilidad ESG en la selección de proveedores demuestra que la eficiencia tecnológica debe ser inseparable de la responsabilidad ambiental. La exigencia de centros de datos con neutralidad de carbono y un indicador de eficiencia energética (PUE) optimizado permite a la Nueva EPS alinear sus operaciones de TI con los Objetivos de Desarrollo Sostenible. Esta transición no solo favorece el cumplimiento de futuras normativas ambientales en Colombia, sino que también genera una optimización de costos operativos (OPEX) a largo plazo, al priorizar aliados estratégicos que utilizan infraestructuras modernas, limpias y de bajo consumo energético **(ISO/IEC, 2023; Green Software Foundation, 2024)**.

Finalmente, el análisis del caso práctico permite afirmar que la auditoría tradicional de carácter anual ha quedado obsoleta frente a la velocidad de la transformación digital. Para garantizar una gobernanza de TI robusta, es imperativo que la Nueva EPS adopte modelos de

auditoría continúa apoyados en tableros de control en tiempo real y APIs de monitoreo automatizado. Este cambio de paradigma permite una detección temprana de desviaciones en los niveles de servicio (SLA) y una respuesta inmediata ante vulnerabilidades, transformando la función de auditoría en un componente de valor estratégico que asegura la continuidad del servicio de salud y la confianza de millones de usuarios en el ecosistema digital **(ISACA, 2025)**.

Referencias

Asociación de Auditoría y Control de Sistemas de Información [ISACA]. (2025). *Digital Trust Ecosystem Framework*: Auditoría en la era de la IA y el monitoreo continuo. ISACA Press.

Congreso de Colombia. (2012, 17 de octubre). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Google Cloud. (2024). *Keralty y Nueva EPS*: Casos de éxito en la transformación digital de la salud en Colombia. https://cloud.google.com/customers

Green Software Foundation. (2024). *State of Green Software*. https://greensoftware.foundation/

ISO/IEC. (2022). ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardizatio*n. https://www.iso.org/standard/27001

ISO/IEC. (2023). ISO/IEC 30134-2: Key *performance indicators — Power usage effectiveness* (PUE). International *Organization for Standardization.*

Ministerio de Salud y Protección Social. (2025). Informe de gestión y cobertura de las Entidades Promotoras de Salud en entornos digitales. https://www.minsalud.gov.co

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2025). Guía de estándares de IA y ciberseguridad para el sector salud en Colombia.

National Institute of Standards and Technology [NIST]. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Nueva EPS. (2026). Informe anual de sostenibilidad y gobierno corporativo: Retos de la salud digital. https://www.nuevaeps.com.co/informes-corporativos

Piattini, M., & Del Peso, E. (2021). Auditoría de tecnologías y sistemas de información. RA-MA Editorial.

Rodríguez, A. (2026). El fin de la auditoría estática: Modelos de monitoreo continuo en servicios de outsourcing cloud. Revista de Ingeniería de Sistemas Uniremington, 12(1), 15-30.

Superintendencia Nacional de Salud. (2024). Circular externa 002 de 2024: Instrucciones respecto a los requerimientos mínimos de seguridad de la información y ciberseguridad. Ministerio de Salud y Protección Social. https://www.supersalud.gov.co/normatividad/circular-externa-002-de-2024

Superintendencia Nacional de Salud. (2024). Circular única de ciberseguridad y gestión de riesgos para EPS. https://www.supersalud.gov.co

The Health Policy Partnership. (2024). Nuestra salud en la nube: Análisis del papel evolutivo de la tecnología de nube en la atención de salud. https://www.healthpolicypartnership.com/app/uploads/Nuestra-Salud-en-la-Nube.pdf