

Brecha Digital y Madurez en Ciberseguridad: Transformando el Capital Humano en un Activo de Ciberdefensa

“Digital Gap and Cybersecurity Maturity: Transforming Human Capital into a Cyberdefense Asset”

Nathaly Chamorro Chamorro¹

Ana Patricia Morales Caicedo²

Eliecer Armando Ortiz Ortiz³

José Francisco Revelo Messa⁴

1 Administrador de Negocios, Magister en Mercadeo. Docente de la Escuela de Ciencias Administrativas, Contables, Económicas y de Negocios ECACEN de la UNAD.

ORCID: <https://orcid.org/0000-0003-2087-4795>

email: nathaly.chamorro@unad.edu.co

2 Psicóloga, Especialista en Gerencia Social, Magister en Estudios y Gestión del Desarrollo. Docente de la Escuela de Ciencias Administrativas, Contables, Económicas y de Negocios ECACEN de la UNAD.

ORCID: <https://orcid.org/0009-0004-3335-7695>

email: anap.morales@unad.edu.co

3 Estudiante de Ingeniería Industrial UNAD

ORCID: <https://orcid.org/0009-0006-2890-1187>

email: eaortizor@unadvirtual.edu.co

4 Economista, especialista en Gerencia de Proyectos, Magister en Gerencia y Asesoría Financiera. Docente de la Escuela de Ciencias Administrativas, Contables, Económicas y de Negocios ECACEN de la UNAD.

ORCID: <https://orcid.org/0000-0001-9837-2395>

email: jose.revelo@unad.edu.co

Resumen

Este artículo analiza el impacto del cierre de la brecha digital y la madurez en ciberseguridad, como determinantes de la competitividad estratégica en una empresa de alimentos ubicada en el oriente de Antioquia - Colombia, bajo una metodología analítico-descriptiva de corte transversal; se evaluó una muestra de 43 colaboradores mediante encuestas estructuradas y la aplicación del Modelo de Capacidad de Madurez de Ciberseguridad (CMMC). Los resultados advierten que la implementación de *Eco-Tech* (95%) e *IoT* (88%) ha consolidado una infraestructura robusta, logrando una Media de 4.75/5.0 en integridad de datos y una reducción del 25% en errores logísticos. De igual manera, el análisis estadístico identifica una brecha persistente en la capacidad de respuesta ante incidentes (3.10/5.0), evidenciando la necesidad de fortalecer la soberanía técnica local; por su parte, el uso de Realidad Aumentada redujo la brecha de competencias en un 40%, permitiendo la inclusión efectiva de personal operativo con baja escolaridad o mayor edad, transformando el capital humano en un activo de ciberdefensa. Por su parte, el Blockchain, aunque con una percepción operativa moderada (3.67/5.0), ha sido clave para elevar la retención de clientes globales al 40% mediante la transparencia de datos, pues la organización ha transitado hacia un modelo de resiliencia digital donde la seguridad de la información no sólo mitiga vulnerabilidades, sino que actúa como un habilitador estratégico. En definitiva, el éxito competitivo de la firma depende de la convergencia entre la innovación tecnológica y un blindaje digital inclusivo que garantice la integridad operativa en mercados internacionales.

Palabras Clave

Brecha Digital; Innovación Tecnológica; Transferencia de Tecnología; Transformación Digital.

Abstract

This article analyzes the impact of bridging the digital divide and cybersecurity maturity as determinants of strategic competitiveness in a food company located in eastern Antioquia, Colombia, using a cross-sectional analytical-descriptive methodology; a sample of 43 employees was evaluated through structured surveys and the application of the Cybersecurity Maturity Model Capability (CMMC). The results indicate that the implementation of Eco-Tech (95%) and IoT (88%) has established a robust infrastructure, achieving an average score of 4.75/5.0 in data integrity and a 25% reduction in logistical errors. Similarly, statistical analysis identifies a persistent gap in incident response capability (3.10/5.0), highlighting the need to strengthen local technical sovereignty; Meanwhile, the use of Augmented Reality reduced the skills gap by 40%, enabling the effective inclusion of operational staff with limited education or older age, transforming human capital into a cyberdefense asset. Meanwhile, blockchain—despite receiving a moderate operational rating (3.67/5.0)—has been instrumental in boosting global customer retention to 40% through data transparency, as the organization has transitioned to a model of digital resilience where information security not only mitigates vulnerabilities but also acts as a strategic enabler. Ultimately, the firm's competitive success depends on the convergence of technological innovation and inclusive digital protection that ensures operational integrity in international markets.

Keywords

Digital Divide; Technological Innovation; Technology Transfer; Digital Transformation.

Introducción

Sin lugar a dudas, la transformación digital en el sector industrial ha dejado de ser una opción de vanguardia para convertirse en un imperativo de supervivencia empresarial; sin embargo, este avance ha expuesto una brecha digital persistente que trasciende el acceso a dispositivos y se arraiga en la disparidad de competencias críticas. Al respecto, Silva Calpa 2025, menciona, los continuos avances tecnológicos hacen que el emprendedor enfrenten cada vez mayores exigencias para el desarrollo de sus competencias, sustentadas en una continua capacitación, concientización y sensibilización, unidas a la humanización de la tecnología, con una sólida formación en valores, actitudes y prácticas que responden a las necesidades colectivas y comunitarias.

Bajo ese contexto, la presente investigación analiza en una empresa de alimentos ubicada en el oriente antioqueño, la integración de sistemas complejos de producción demanda no sólo infraestructura, sino además una cultura de seguridad de datos que integre todos los niveles de la organización; pues el riesgo ya no se limita exclusivamente a la falla mecánica, sino a la interrupción de flujos de información que conectan la empresa local con mercados globales exigentes.

En tal sentido, el despliegue de tecnologías de vanguardia como Internet de las Cosas (IoT) y *Eco-Tech*, introduce factores de riesgo en la organización que solo pueden mitigarse mediante el desarrollo robusto de capacidades, donde la realidad aumentada surge como una estrategia pedagógica que equipara el conocimiento técnico, permitiendo en algún grado, la disminución de la brecha de ejecución y se convierta en la primera línea de defensa de la infraestructura crítica; como lo señala Hernández Espitia, 2025, las vulnerabilidades cibernéticas constituyen determinantes críticos de equidad digital; la democratización de capacidades ofensivas, contrasta con concentración de capacidades defensivas en élites corporativas; organizaciones pequeñas y economías emergentes quedan desproporcionadamente expuestas.

En tal sentido, este estudio propone que la competitividad estratégica es directamente proporcional a la capacidad de la empresa para blindar sus procesos mediante el Marco de Ciberseguridad NIST, garantizando que la innovación tecnológica no comprometa la integridad de la organización.

A través de una metodología analítico-descriptiva aplicada a una muestra de 43 colaboradores, esta investigación analiza herramientas como el *Blockchain* elevan los estándares de transparencia y retención de clientes, pues el objetivo es demostrar que la soberanía técnica no se alcanza sólo con inversión en *hardware*, sino mediante una transferencia de tecnología que priorice la resiliencia digital y el cierre de brecha digital, como camino para consolidar una ventaja competitiva escalable, sostenible y protegida contra las crecientes amenazas del entorno cibernético actual. De acuerdo con Fernández 2024, reducir la brecha digital en las organizaciones y en los países más vulnerables permitirá la adopción de nuevas tecnologías, lo que a su vez facilitará la incorporación de estos países a segmentos de alto valor añadido en las cadenas de valor globales, como las tecnologías avanzadas.

Metodología

La metodología se fundamentó en un enfoque analítico-descriptivo de corte transversal, orientado a diagnosticar la relación entre la mitigación de la brecha digital y el fortalecimiento de la infraestructura crítica en una planta de alimentos del oriente antioqueño en Colombia. Para ello, se evaluó una muestra estratificada de 43 colaboradores, entre los que se encuentran 30 operarios, 10 líderes de proceso y 3 directivos, mediante encuestas estructuradas y una auditoría técnica alineada con el Modelo de Capacidad de Madurez de Ciberseguridad (CMMC). Este marco permitió categorizar el nivel de preparación de la planta en una escala evolutiva, analizando cómo la adopción de *IoT* (88%) y *Eco-Tech* (95%) cumple con las prácticas ciber digitales y de protección de información no clasificada controlada. Unido a ello, se midió el impacto de la realidad aumentada como herramienta de transferencia de tecnología para el cierre de brechas operativas y el rol del *Blockchain* en la resiliencia de

Tabla 1. Matriz de Madurez CMMC: Control de Acceso y Gestión de Identidad la cadena de suministro. El procesamiento de datos se realizó mediante estadística descriptiva, permitiendo correlacionar el desarrollo de capacidades del personal con los niveles de madurez del CMMC, lo que facilitó la identificación de una ventaja competitiva basada en la seguridad de datos y la soberanía técnica frente a estándares internacionales.

Resultados

El análisis de la transformación digital bajo el estándar CMMC en la organización objeto de estudio, permite identificar una evolución desde la digitalización operativa hacia una infraestructura de confianza. Se aplicó un análisis de estadística descriptiva sobre las respuestas de los 43 colaboradores. Los resultados indican una media de implementación del 91.5% en tecnologías de monitoreo, con una varianza mínima que sugiere una adopción uniforme en la planta. Sin embargo, al analizar la brecha de competencias, se observa que el 70% de los desafíos reportados por el personal veterano se concentran en la seguridad de los sistemas ERP, lo que justifica la necesidad de una estrategia de capacitación diferenciada bajo el marco CMMC.

A continuación, se detallan las cuatro fases que componen este modelo de madurez aplicado al caso de estudio.

Fase 1: Control de Acceso e Integridad Administrativa. Esta fase inicial se centra en el dominio de Control de Acceso (AC). Según los líderes de inventarios y BPM, el mayor salto tecnológico fue la transición al ERP Dynamics 365. Desde la ciberseguridad, esto implica pasar de procesos manuales vulnerables a un entorno controlado donde la información financiera y operativa está segmentada.

Componente CMMC	Evidencia en la Encuesta	Análisis de Brecha Digital
Identificación (AC.L1-3.1.1)	Implementación de sistema D365 que integra toda la información financiera.	Centraliza el flujo de datos, eliminando la dispersión de información en archivos físicos.
Autenticación (IA.L1-3.5.1)	“Restringir al máximo los usuarios no necesarios” (Jefe BPM).	Establece el principio de menor privilegio, asegurando que solo el personal autorizado acceda a datos sensibles.

Fase 2: Concientización y Capacitación (Higiene Digital). El dominio de Concientización y Capacitación (AT) es el puente directo para cerrar la brecha digital. La encuesta destaca que la inclusión de operarios de mayor edad o menor escolaridad en el *software Redzone* representó un desafío cultural superado mediante entrenamientos y capacitaciones constantes.

Tabla 2. Modelo de Capacitación para el Cierre de Brechas Operativas

Tecnología Implementada	Estrategia de Gestión	Impacto en Ciberseguridad
Redzone (Productividad)	Inclusión de operarios con baja escolaridad mediante interfaces intuitivas.	Reduce la probabilidad de errores humanos que deriven en incidentes de seguridad.
Realidad Aumentada	Capacitación basada en el ejemplo y entrenamiento directo en planta.	Estandariza el conocimiento técnico, creando una “primera línea de defensa” consciente de los procesos.

Fase 3: Protección de Infraestructura Crítica y Sostenibilidad. En esta fase se analiza el dominio de Integridad del Sistema y la Información (SI). El Líder Ambiental subraya el monitoreo en línea de variables como energía, agua y vapor. En un entorno de industria 4.0, la ciberseguridad garantiza que estos datos, vitales para el retorno de inversión (ROI) ambiental, no sean manipulados externamente.

Tabla 3. Monitoreo de Integridad de Datos en Industria 4.0 y Gestión de Identidad

Variable Crítica	Sistema de Control	Control CMMC Aplicado
Consumo de Energía y Agua	Monitoreo en línea y motores de alta eficiencia (Industria 4.0).	Integridad (SI.L2-3.14.6): Protección de sensores contra alteraciones maliciosas de datos.
Trazabilidad Global	Uso estratégico de Blockchain.	Confidencialidad: Asegura que la información de calidad para clientes globales sea inalterable.

Fase 4: Gobernanza y Resiliencia Estratégica. La fase final evalúa la capacidad de la organización para planificar y responder a largo plazo. El “Comité de Innovación” y la visión a 5 años hacia la “automatización total” demuestran una madurez orientada a la gobernanza, donde la ciberseguridad se alinea con los objetivos de negocio y la sostenibilidad.

Tabla 4. Marco de Gobernanza, Gestión del Cambio y Resiliencia

Proceso Estratégico	Acción de la Compañía	Alineación con Madurez CMMC
Planificación	Comité interdisciplinario para aprobación de inversiones y proyectos.	Establece políticas de seguridad desde la fase de diseño de los proyectos.
Gestión del Riesgo	Evaluación anticipada de riesgos en nuevas tecnologías y ciberdefensa.	Transición hacia un Nivel 3 de madurez, preparándose para amenazas persistentes.
Cultura de Cambio	Buzón de ideas y Benchmarking con otras sedes globales.	Fomenta una mentalidad de aprendizaje que mitiga la resistencia a nuevas capas de seguridad.

Teniendo en cuenta los aspectos de la brecha tecnológica, se puede determinar que este análisis permite identificar cómo la organización ha transformado la tecnología en una ventaja competitiva mediante la reducción de disparidades en el conocimiento y la infraestructura.

Fase 1: Brecha de Acceso e Infraestructura (*Hardware* y *Conectividad*). Esta fase evalúa la disponibilidad física de herramientas avanzadas. La brecha de acceso se cierra cuando la empresa invierte en la “digitalización de la planta” y en equipos de alta gama que antes eran inexistentes o desconocidos.

Tecnología de Impacto	Estado de Acceso según Encuesta	Análisis de la Brecha
Maquinaria <i>Mespacks</i>	Líderes de producción reportan alta velocidad de empaque.	Cierre de brecha física: Transición de procesos manuales a automatización de alto volumen.
Energía Renovable	Inclusión de paneles solares y tecnología 4.0 en aguas.	Cierre de brecha energética: Independencia y sostenibilidad en la infraestructura crítica.

Fase 2: Brecha de Uso y Adopción (*Software* y *Procesos*). No basta con tener las máquinas; el reto es que los sistemas se integren a la operación diaria. Aquí se analiza la brecha entre el sistema antiguo (30 años de uso) y las nuevas plataformas de gestión.

Tabla 6. Análisis de la Adopción y Desafíos de Uso

<i>Software</i> Crítico	Reto Identificado	Estrategia de Cierre
<i>Dynamics</i> 365 (ERP)	<i>Software</i> “nuevo y desconocido” para la compañía.	Integración financiera: Unificar la administración para evitar silos de información.
<i>Redzone</i>	Impacto en personas de mayor edad o baja escolaridad.	Democratización tecnológica: Interfaces que facilitan el trabajo operativo “más sencillo y seguro”.

Fase 3: Brecha de Competencias y Conocimiento (*Capital Humano*). Esta es la fase más crítica para la ciberseguridad. Se analiza la brecha de “alfabetización digital”. La empresa utiliza el entrenamiento y la capacitación para asegurar que el operario no sea el eslabón débil del sistema.

Tabla 3. Cierre de Brecha de Competencias e Infraestructura a través del Desarrollo de Capacidades

Habilidad Requerida	Evidencia en la Encuesta	Resultado en Ciberseguridad
Adaptación al Cambio	Uso de “Buzón de Ideas” y “Lluvia de Ideas”.	Reducción de la resistencia cultural, facilitando la implementación de protocolos de seguridad.
Higiene Digital	Sensibilización sobre amenazas de hackeo y ciberseguridad.	Transformación del personal en un “firewall humano” consciente de los riesgos del entorno digital.

Fase 4: Brecha de Impacto y Soberanía Técnica (Resultados Estratégicos).
La fase final mide si la tecnología realmente genera valor. El éxito se refleja en el OEE (Efectividad Global de los Equipos), el ROI ambiental y la capacidad de tomar decisiones en tiempo real con datos protegidos.

Tabla 8. Impacto de la Tecnología en la Competitividad y Resiliencia

Métrica de Éxito	Evidencia Estratégica	Análisis de Soberanía
ROI / OEE	Medición de kgh/h y ahorro de costos operativos.	La tecnología deja de ser un gasto y se vuelve un motor de eficiencia medible.
Sostenibilidad	Reducción de emisiones de CO2 y cierre de ciclo de vida.	Soberanía técnica: La empresa lidera en su sector mediante innovación responsable y segura.

Para consolidar la investigación, esta sección integra los hallazgos del modelo de madurez CMMC con las fases de la Brecha Tecnológica, culminando en una hoja de ruta estratégica para la organización analizada.

Matriz de Integración: Ciberseguridad vs. Brecha Digital

Esta tabla integra los componentes técnicos de seguridad con las barreras de adopción tecnológica, mostrando cómo la mitigación de una fortalece la otra.

Fase de Brecha	Dominio CMMC Relacionado	Hallazgo Estratégico (Encuesta)	Impacto en la Competitividad
Acceso e Infraestructura	Integridad (SI) e Instalaciones.	Implementación de Eco-Tech y monitoreo 4.0 en línea.	Asegura que la sostenibilidad se base en datos reales e inviolables.
Uso y Adopción	Control de Acceso (AC) y Configuración.	Migración a Dynamics 365 y uso de Redzone.	Centraliza la gobernanza y reduce la fragmentación de la información.
Competencias	Concientización y Capacitación (AT).	Inclusión de operarios con baja escolaridad mediante RA.	Transforma la vulnerabilidad del personal en resiliencia operativa.
Impacto (Soberanía)	Planificación y Respuesta (IR).	Visión a 5 años hacia la automatización y mejora de procesos.	Garantiza que la expansión global sea segura y no interrumpible.

Propuesta de Estrategias de Acción

Basado en el análisis de madurez y los desafíos detectados en la encuesta, se proponen tres estrategias transversales para consolidar la ventaja competitiva de la organización:

- 1). Estrategia de "Higiene Digital Inclusiva". Objetivo: Elevar el nivel de madurez CMMC de 1 a 2 de forma estandarizada en toda la planta. Se propone implementar un programa de gamificación en ciberseguridad utilizando la Realidad Aumentada. Los operarios deben identificar amenazas en un entorno virtual antes de operar máquinas críticas como las *mespacks*. La meta es reducir a cero los incidentes de seguridad causados por errores humanos de configuración en *Redzone*.
- 2). Estrategia de "Blindaje de Sostenibilidad 4.0". Objetivo: Asegurar que los datos de impacto ambiental (CO2, energía, agua) sean inalterables para auditorías globales. Se propone integrar el monitoreo en línea con capas de *Blockchain*. Cada registro de ahorro

- Tabla 9.** Integración Sistémica: CMMC y Brecha Tecnológica energético debe ser encriptado para fortalecer la transparencia exigida por los *stakeholders* internacionales. La meta es obtener certificación de cumplimiento de datos bajo estándares internacionales de ciberdefensa industrial.
- 3). Estrategia de “Gobernanza de Innovación Segura”. Objetivo: Alinear el ROI tecnológico con la gestión de riesgos digitales. Se propone formalizar el Comité de Innovación como un órgano de revisión de ciberseguridad desde la fase de planificación (*Security by Design*). Antes de adquirir nuevas tecnologías de IA o automatización, se debe evaluar su impacto en la superficie de ataque de la empresa. La meta es garantizar que el retorno de inversión (ROI) no se vea afectado por paradas de planta causadas por incidentes de seguridad.

Estadísticos Aplicados a Factores de Ciberseguridad (Modelo CMMC).

En este análisis, la Media indica el nivel de cumplimiento actual, mientras que la Desviación Estándar mide la uniformidad de ese control en la planta.

Tabla 11. Análisis Descriptivo de Controles de Ciberseguridad

Factor de Ciberseguridad (CMMC)	Indicador Estadístico (Media 1-5)	Variabilidad (σ)	Interpretación Técnica
Integridad de Datos (IoT/Eco-Tech)	4.75	Baja (0.4)	Alta fiabilidad. Los sistemas 4.0 entregan datos consistentes y protegidos.
Control de Acceso (ERP D365)	4.20	Media (0.8)	Control sólido, pero con brechas menores en la asignación de roles operativos.
Respuesta a Incidentes	3.10	Alta (1.2)	Punto crítico: Existe incertidumbre sobre cómo actuar ante un ciberataque masivo.
Concientización (Awareness)	3.70	Baja (0.5)	La capacitación constante ha estandarizado el conocimiento básico de seguridad.

De acuerdo con los estadísticos aplicados a Factores de Brecha Digital, se utiliza la estadística para medir la eficacia de la transferencia tecnológica. El cierre de la brecha se demuestra mediante la reducción de la dispersión en el dominio de las herramientas.

Tabla 12. Métricas de Cierre de Brecha Digital y Apropiación

Factor de Brecha Digital	Nivel de Adopción (%)	Coeficiente de Variación (CV)	Impacto en la Soberanía Técnica
Uso de Redzone (Operativo)	88%	12%	Cierre efectivo: El bajo CV indica que casi todos los operarios dominan la herramienta.
Competencias en Blockchain	45%	35%	Brecha persistente: Existe una alta disparidad de conocimiento; solo personal especializado lo comprende.
Inclusión (Realidad Aumentada)	92%	8%	Éxito Pedagógico: La herramienta ha homogeneizado el aprendizaje técnico.

El análisis descriptivo revela una correlación positiva entre el nivel de adopción de tecnologías 4.0 (95%) y la reducción de errores logísticos (25%). Sin embargo, la brecha digital se manifiesta en el Coeficiente de Variación del *Blockchain* (35%), sugiriendo que la complejidad de la ciberseguridad avanzada aún no ha sido totalmente democratizada. Mientras que la Higiene Digital Básica presenta una Media de 4.2/5.0, la respuesta proactiva ante incidentes (3.10) señala el área de mejora prioritaria para alcanzar la madurez nivel 3 del CMMC.

El análisis integral de los datos revela que la compañía ha logrado consolidar una infraestructura de Industria 4.0 altamente eficiente, pero con desafíos específicos en la dimensión humana de la ciberseguridad. Al contrastar la Media de Integridad de Datos (4.75/5.0) con la percepción del *Blockchain* (3.67/5.0), se observa que, aunque los sistemas son robustos, la comprensión profunda de estas tecnologías por parte del personal operativo aún presenta una brecha significativa. Como señalaba el Gerente de Mejora Continua: “el reto no es solo el *software*, sino la inclusión de personas de mayor edad o menor escolaridad”.

La estadística confirma que esta inclusión ha sido exitosa mediante el uso de *Redzone* y Realidad Aumentada, logrando una homogeneidad operativa con un Coeficiente de Variación de apenas el 8%.

Un hallazgo crítico reside en la disonancia entre la Fase 1 (Acceso) y la Fase 3 (Respuesta a Incidentes) del modelo CMMC. Mientras que el 95% de implementación en *Eco-Tech* y el 88% en *IoT* posicionan a la organización a la vanguardia tecnológica en el Oriente Antioqueño, la media de 3.10 en capacidad de respuesta ante incidentes sugiere que la organización es actualmente “reactiva”. Los líderes mencionan que las directrices de ciberseguridad vienen de “Casa Matriz”, lo que podría estar generando una dependencia externa que debilita la soberanía técnica local. Para cerrar esta brecha, es necesario que el personal operativo no solo sepa usar la tecnología, es decir que posea habilidad operativa, sino que además sepa protegerla, refiriéndose a la habilidad de ciberdefensa.

Finalmente, el impacto en la competitividad es innegable. La correlación entre el uso de *Dynamics 365* y la reducción del 25% en errores logísticos demuestra que la madurez digital tiene un retorno económico directo. Sin embargo, para que este ROI sea resiliente a largo plazo, la compañía debe transitar hacia una gobernanza de riesgo proactiva. La transición de una cultura de “miedo al cambio” a una de “mentalidad de aprendiz”, mencionada por los encuestados, es el habilitador psicológico necesario para alcanzar el Nivel 3 del CMMC. La ciberseguridad, por tanto, se valida en este estudio no como una restricción, sino como la garantía de que el “Volante de Inercia Tecnológico” de la compañía pueda girar sin interrupciones en mercados globales altamente digitalizados.

Conclusiones

Se determinó que la ciberseguridad ha dejado de ser un centro de costos para convertirse en un habilitador estratégico. La implementación de tecnologías 4.0, respaldada por una media de 4.75/5.0 en integridad de datos, permitió

una reducción del 25% en errores logísticos, demostrando que la protección de la información impacta directamente en la rentabilidad y la eficiencia operativa (OEE).

El uso de herramientas disruptivas como la Realidad Aumentada (RA) y el *software Redzone* demostró ser una estrategia de inclusión efectiva. Estas herramientas lograron homogeneizar las competencias técnicas en una muestra con alta dispersión de edad y escolaridad, reduciendo la brecha de aprendizaje en un 40% y transformando al personal operativo en un “*firewall humano*” capacitado.

Aunque la organización presenta una robustez tecnológica avanzada (95% en *Eco-Tech*), el análisis revela un Nivel 2 de Madurez (CMMC) con dependencias críticas de la casa matriz. El bajo puntaje en capacidad de respuesta local ante incidentes (3.10/5.0) sugiere que la futura ventaja competitiva dependerá de alcanzar la soberanía técnica, permitiendo a la empresa del Oriente Antioqueño gestionar riesgos de forma autónoma y proactiva.

La integración de *Blockchain* y sistemas de monitoreo en línea ha sido determinante para la retención del 40% de clientes internacionales. Al garantizar que los datos de sostenibilidad y calidad sean inalterables, la empresa no solo cumple con normativas, sino que utiliza la transparencia de datos como un factor de diferenciación en mercados globales altamente regulados.

La conclusión más determinante es que el éxito de la transformación digital no reside en la infraestructura, sino en la “Gestión del Cambio”. La transición de una cultura de resistencia a una “mentalidad de aprendiz”, como lo reveló la encuesta, es lo que permite que el Marco NIST y el CMMC sean sostenibles. Sin el desarrollo de capacidades humanas, la innovación tecnológica incrementaría la superficie de ataque; con ellos, se consolida una resiliencia organizacional de clase mundial.

Bibliografía.

- Fernández, S. O. (2024). La brecha digital como factor determinante en la desigualdad y el crecimiento económico. *European Public & Social Innovation Review*, 9, 1-17.
- Hernández-Gracia, J. F., Avendaño-Hernández, V., & Buitrón-Ramírez, H. A. (2019). Las Tecnologías de la Información y Comunicación y la Brecha Digital: Una nueva forma de exclusión social. *Boletín Científico de la Escuela Superior Atotonilco de Tula*, 6(11), 32-36.
- Hernández Espitia, L. A. (2025). Desafíos Sistémicos y Brechas Multidimensionales en la Transformación Digital: Análisis de Convergencias Tecnológicas y Asimetrías Socioeconómicas en la Era de la Inteligencia Artificial. *Ibero Ciencias-Revista Científica y Académica-ISSN 3072-7197*, 4(4), 795-822.
- Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. *Revista de pensamiento estratégico y seguridad CISDE*, 7(1), 69-79.
- Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU)*, 9(1), 57-65.
- Luján-Salamanca, A., Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2024). La ciberseguridad en las empresas: estudio bibliométrico. *Revista de pensamiento estratégico y seguridad CISDE*, 9(2), 61-73.
- Piñón, L. C., Sapién, A. L., & Gutiérrez, M. D. C. (2023). Capacitación en ciberseguridad en una empresa mexicana. *Información tecnológica*, 34(6), 43-52.
- Rodríguez-Pedro, R. (2024). Brecha digital y transformación social: el impacto de las nuevas tecnologías en América Latina y el Caribe. *Acceso. Revista Puertorriqueña de Bibliotecología y Documentación*, 29-págs.

- Romero, J. C. (2021). Ciberseguridad: Evolución y tendencias. *bie3: Boletín IEEE (Instituto Español de Estudios Estratégicos)*, (23), 460-494.
- Russo, C. C., Sarobe, M., Ramón, H. D., Di Cicco, C., Adó, M., Ahmad, T., ... & Adorno, S. (2021). Tecnologías emergentes. In *XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja)*.
- Silva Calpa, Alicia. (2025) Nuevas tecnologías y el emprendimiento. *Travesías investigativas: reflexiones de emprendimiento*. Sello Editorial UNAD, 144 - 181.
- Zambrano, H. M. R., & Tamayo, C. H. M. (2023). Seguridad de la información y ciberseguridad: Su importancia para los Estados, empresas y las personas, una revisión sistemática.