ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.1773

Cybersecurity Vulnerabilities in Companies: A Case Study

***Abstract*– Cyber risk refers to the dangers associated with the use of information and communication technologies, stemming from criminal activities. These risks can be perpetrated by both individuals and organizations. Many companies lack the technical knowledge necessary to effectively protect themselves against such attacks, placing them in a vulnerable position. However, adopting a proactive and resilient approach enables them to manage these risks more effectively. The objective of this study is to assess the level of cybersecurity in companies and analyze the cyber risks to which they are exposed, using an instrument called ECM2 to measure cybersecurity practices and obtain precise data for a comprehensive evaluation. Through a case study methodology, companies from different sectors and sizes were analyzed and compared, revealing that both multinational technology firms and small market service enterprises are vulnerable and face high levels of cyber risk due to deficiencies in their policies for mobile device usage.**

***Keywords*—Cybersecurity, cyber risk, cyber resilience, cyber vulnerability.**

Vulnerabilidades en la Seguridad Cibernética de Empresas: Un Estudio de Casos

Tamara Howell[1]; Javier Rojas-Segura[2]; Jose Martinez-Villavicencio[3]; Cesar Rodriguez Bravo[4]
[1,2,3]Tecnológico de Costa Rica, Costa Rica, tamarahowell@estudiantec.cr, jarojas@tec.ac.cr, jomartinez@tec.ac.cr, [4]Kyndryl, Inc, Costa Rica, cesarrod@kyndryl.com

Resumen– ***El riesgo cibernético se refiere a los peligros asociados con el uso de tecnologías de información y comunicación, derivado de actividades delictivas. Estos riesgos pueden ser perpetrados tanto por individuos como por organizaciones. Muchas de estas empresas carecen del conocimiento técnico necesario para protegerse eficazmente contra estos ataques, lo que las sitúa en una posición vulnerable. Sin embargo, adoptar una postura proactiva y resiliente les permite gestionar estos riesgos de manera más efectiva. El objetivo de este estudio es comprender el nivel de ciberseguridad en las empresas y analizar el riesgo cibernético al que están expuestas, utilizando un instrumento denominado ECM² para medir las prácticas de ciberseguridad y obtener datos precisos que permitan una evaluación exhaustiva. Mediante la metodología de estudio de casos se analizaron y compararon empresas de diferentes sectores y tamaños, comprendiendo que tanto empresas transnacionales del sector tecnológico, como pequeñas empresas de servicios de mercado, son vulnerables y presentan un nivel de riesgo cibernético alto, dadas sus falencias en las políticas de uso de dispositivos móviles.***

Palabras clave-- Ciberseguridad, riesgo cibernético, resiliencia cibernética, vulnerabilidad cibernética

I. Introducción

En el contexto empresarial moderno, caracterizado por la globalización y la competencia, las organizaciones en general confían cada vez más en las tecnologías de información y comunicación (TIC); por ello, resulta crucial implementar políticas de seguridad, dado que estas políticas han demostrado ser clave en mejorar la competitividad de las empresas [1]. El riesgo asociado a la ciberseguridad ha captado un interés significativo en las últimas décadas [2] y cada vez es más común que su operatividad, la integridad de sus datos y la continuidad de sus negocios se vean comprometidas por estos ataques. A pesar de la importancia que tiene protegerse contra estas amenazas, muchas organizaciones todavía carecen del conocimiento técnico necesario para implementar medidas de seguridad adecuadas. Ref. [3] comenta que la decisión de una empresa de invertir en la gestión del riesgo de ciberseguridad y en su mejora continua probablemente también contribuya a aumentar su resiliencia. La tecnología ha transformado profundamente la sociedad, impulsando el desarrollo humano. Hoy en día, la digitalización ha facilitado un crecimiento acelerado en el uso de las tecnologías de la información y la comunicación, lo cual ha incrementado el riesgo de ciberataques que ponen en peligro la seguridad de la cadena de suministro a nivel global [4]. Esta falta de preparación las deja expuestas a una amplia gama de riesgos, que pueden tener consecuencias graves, no solo para las propias empresas, sino también para la economía en general. La literatura revela que las empresas son especialmente vulnerables a los ciberataques, los cuales pueden ser perpetrados por individuos o grupos con intenciones delictivas, políticas o personales. En muchos casos, las empresas no cuentan con el personal especializado en ciberseguridad ni con la infraestructura tecnológica que les permita defenderse adecuadamente. Esto las deja en una situación delicada, donde cualquier incidente de seguridad podría impactar su estabilidad y seguridad. Ante este panorama, el objetivo de este estudio es comprender el nivel de ciberseguridad en las empresas y analizar el riesgo cibernético al que están expuestas. Para lograrlo, se aplicó un enfoque basado en estudios de casos, seleccionando empresas de distintos sectores económicos y tamaños. El análisis se realizó utilizando el Modelo de Madurez en Ciberseguridad de [5], denominado ECM², que determinó el estado real, en que se encuentran las empresas en materia de ciberseguridad, independientemente del tamaño o sector [6]. Además, se busca identificar sus prácticas actuales y los puntos débiles, fomentando una mayor conciencia sobre la importancia de la ciberseguridad en el entorno empresarial. Este tema es relevante porque los ciberataques representan una amenaza constante, especialmente para las empresas, que juegan un rol crucial en la economía. En un mundo donde las tecnologías de la información se globalizan rápidamente, estas organizaciones se vuelven más vulnerables a diversos riesgos. Esta investigación arrojó datos precisos sobre el nivel de preparación cibernética de las empresas, identificando sus áreas de mayor vulnerabilidad y evaluando sus prácticas de ciberseguridad. Estos resultados permiten a las empresas fortalecer sus defensas frente a los ciberataques, beneficiando no solo a ellas mismas, sino también a sus colaboradores, clientes y, de manera más amplia, al mercado. Asimismo, las agencias gubernamentales y los organismos reguladores pueden utilizar estos hallazgos para diseñar políticas y programas que apoyen de manera más efectiva a las empresas en el ámbito de la ciberseguridad.

II. Estado del Arte

Ref. [7] indica que el riesgo cibernético se define como el conjunto de posibles amenazas y vulnerabilidades que surgen como consecuencia directa de la utilización de TIC, fenómeno que abarca desde empresas unipersonales hasta organizaciones multinacionales. Estas empresas se exponen a desafíos únicos en un panorama digital en constante evolución, lo cual desencadena cambios significativos en sus modelos de negocios por el uso de tecnología digital [8]. Estas

organizaciones y la sociedad en general, dependen cada vez más de las TIC, esto hace necesario que establezcan políticas de seguridad como una forma de protección, ya que se ha comprobado que estas tienen un impacto significativo en el aumento de los niveles de competitividad [9]. Ref. [10] indica que durante el primer trimestre de 2024, el sistema operativo Windows dominaba el mercado global de computadoras personales con una cuota del 73,5%, esta adopción masiva ha mejorado significativamente la eficiencia en diversas industrias, sin embargo, a medida que se incrementa el uso de estas tecnologías, los ciberdelincuentes también están aprovechando las vulnerabilidades de las aplicaciones y sistemas operativos, lo que presenta desafíos tanto para investigadores como para las fuerzas del orden. Los desafíos se ven exacerbados por la aparición constante de nuevos riesgos de seguridad, que dificultan a los investigadores mantenerse al día con las actualizaciones frecuentes, haciendo que tanto las aplicaciones como los sistemas operativos se vuelvan desconocidos para ellos.

Además, la creciente complejidad de las amenazas cibernéticas obliga a las autoridades a desarrollar nuevas estrategias para enfrentar un panorama de seguridad en constante evolución. Ref. [11] destaca que el crecimiento tecnológico actual, como la implementación de redes 5G y Wifi6, ha llevado a un aumento global en los ataques cibernéticos. Por lo que es relevante diseñar estrategias para detectar y corregir tempranamente las vulnerabilidades en los sistemas evaluados.

Aunque no es posible desarrollar un sistema completamente impenetrable, es factible crear planes de mitigación que permitan una rápida corrección ante cualquier situación que comprometa la integridad de la aplicación. Ref. [12] señala que, para proteger a las corporaciones, es fundamental lograr una resiliencia adecuada frente a ciertos niveles de amenazas. No obstante, la resiliencia cibernética de las corporaciones multinacionales suele ser insuficiente, y en el contexto de la integración de la cadena de suministro digital, las posibles consecuencias son aún mayores. Esta situación podría mejorarse significativamente si la alta dirección adopta de manera efectiva los estándares, procesos y recursos existentes. La resiliencia cibernética requiere no solo una planificación consciente, sino también una acción constante por parte del proveedor de seguridad y de la propia corporación multinacional. Ref. [13] comenta que ante estos desafíos, especialmente la susceptibilidad a incidentes de ciberseguridad, las empresas de comercio electrónico están invirtiendo cada vez más en estrategias de ciber resiliencia. Estas estrategias son esenciales para garantizar una gestión eficaz de incidentes e incluyen capacidades para la detección, contención, erradicación y recuperación rápida, con el fin de mantener el rendimiento operativo y la productividad. Implementar estas estrategias requiere un equilibrio cuidadoso entre ciberseguridad, flexibilidad, agilidad y escalabilidad para mantener una ventaja competitiva y eficiencia operativa.

Ref. [14] indicó que se estaban llevando a cabo numerosos ataques con sospechas de participación de organizaciones criminales y estados, incluso es común que los ataques interfieran con los procesos democráticos de otros países, también realizar ataques a gran escala que exploten vulnerabilidades en las cadenas de suministro, sistemas de control industrial y otras infraestructuras, afectando diversas actividades económicas y sociales, así como la seguridad nacional.

También se han visto ataques realizados mediante infraestructuras altamente anónimas, lo que ha resultado en un aumento significativo de ataques indiscriminados, [15] indicó que en los últimos 10 años, los atacantes han creado una gran cantidad de sitios web de phishing debido al rápido crecimiento de Internet. Estos sitios intentan engañar a los usuarios para que revelen información personal, como detalles de cuentas bancarias y contraseñas, al aparentar ser sitios de empresas confiables.

Según [16], las PYMEs son particularmente vulnerables y menos maduras en términos de riesgo y resiliencia cibernética, se estimó que los daños causados por el cibercrimen costaron al mundo 6 billones de dólares anualmente para 2021, un aumento significativo con respecto a los 3 billones del año anterior. El gasto global en productos y servicios de ciberseguridad superó el 1 billón de dólares durante 2021. Por lo tanto, la preparación en ciberseguridad está emergiendo como una competencia crítica para la supervivencia y el crecimiento organizacional. Las PYMEs enfrentan muchos de los mismos problemas de ciberseguridad que las grandes empresas, pero carecen de los recursos adecuados para abordar los riesgos de manera efectiva.

Ref. [17] afirmó que la falta de personal y habilidades en ciberseguridad continuará aumentando en América Latina y el Caribe. Por lo tanto, es crucial que el ecosistema de ciberseguridad en la región trabaje de manera integral y coordinada para enfrentar una combinación única de desafíos y problemas, avanzando siempre desde la formulación de soluciones hasta la implementación de acciones concretas. Las entidades también mencionan que el panorama de amenazas y riesgos está en constante expansión tanto a nivel global como en América Latina y el Caribe. Con los beneficios de la transformación digital también viene el peligro del riesgo cibernético [7], por lo que futuras investigaciones deben de enfocarse en la evaluación de este riesgo [18]. Los ciberdelincuentes aprovechan cada oportunidad para explotar vulnerabilidades en personas y organizaciones mediante la tecnología, adaptando rápidamente nuevas tecnologías y métodos de ataque, y cooperando estrechamente entre sí, entre 2018 y 2022, entre el 52,0% y 62,0% de las organizaciones percibieron un incremento en los ataques respecto al año anterior [17] .

Es crucial que las empresas conozcan el nivel de riesgo cibernético al que están expuestas, ya que manejan datos sensibles que, en caso de ser comprometidos, pueden perjudicar sus operaciones diarias, su rendimiento financiero y su reputación. La gestión del riesgo de ciberseguridad contribuye significativamente a la resiliencia organizacional, y las turbulencias del mercado y la tecnología son factores

importantes que impulsan los esfuerzos de las organizaciones en relación con la gestión de riesgo [19].

III. Metodología

Se utilizó la metodología de estudio de casos, seleccionando cinco empresas como unidades de análisis, este número es adecuado para llevar a cabo un análisis detallado y comparativo [20], proporcionando tanto una visión general como una comprensión profunda de las prácticas de ciberseguridad en entornos corporativos complejos. La selección de las empresas se basó en su relevancia dentro del contexto económico y su disposición para participar en el estudio. Con el objetivo de comprender mejor el nivel de ciberseguridad de estas empresas y analizar el riesgo cibernético al que están expuestas, la recolección y análisis de datos permitió medir y comparar estas prácticas mediante indicadores estandarizados.

A. Instrumento de investigación

Se aplicó una encuesta, que mediante una escala Likert de cinco puntos (ver Figura1) midió el nivel de madurez en ciberseguridad de cada empresa utilizando el instrumento ECM^2 [5]. Lo que permitió obtener métricas precisas para evaluar la efectividad de las medidas implementadas y hacer comparaciones entre las distintas empresas, identificando patrones comunes, diferencias significativas y correlaciones entre las prácticas de ciberseguridad de las empresas estudiadas, además de evaluar su preparación frente a posibles ciberataques.

Fig. 1 Escala de Niveles de Riesgo.
Tomado de [5]

Ha diferencia de múltiples instrumentos que se utilizan en la investigación académica, el ECM^2 de [5] fue concebido por *pratitioners* en ciberseguridad, para conocer y evaluar el nivel de ciberseguridad de una empresa u organización, así como el nivel de riesgo asociado al resultado. Ha sido utilizado ampliamente en el análisis y diagnóstico de empresas de diversos sectores y tamaños. Su fortaleza radica en que es fácil de comprender y permite ver de forma clara la situación real y el riesgo cibernético de la empresa.

Para esta investigación el ECM^2 fue validado por académicos de posgrado en Ciberseguridad. Además se midió su fiabilidad mediante el Alfa de Cronbach (Tabla I.)

TABLA I
Estadística de Confiabilidad

Alfa de Cronbach	N. de Ítems
.990	63

B. Diseño de la investigación

Se utilizó el diseño de múltiples casos, donde según [19], el proceso que se utilizó para cada caso se repite en los demás, por lo que la revisión de los casos es similar por haber utilizado el mismo instrumento para la recolección de datos y el proceso en general [21], [22].

De acuerdo con [23], estos son diseños más robustos y poseen mayor validez. En los casos múltiples, además de intentar descubrir patrones, también se profundiza en el plano individual, ya que el análisis tiende a explicar consistencias e inconsistencias entre los casos [20].

C. Identificación de sujeto de estudio

Se seleccionaron cinco empresas que expresaron su disposición a participar de manera voluntaria. La elección de estos sujetos de estudio se basó en su compromiso y en su infraestructura cibernética para el análisis propuesto.

D. Justificación de la unidad de muestra

La elección de cinco empresas como unidad de muestra para el estudio de casos se fundamentó en varias razones. En primer lugar, [24] destacó que los estudios de caso tienen la capacidad de explorar exhaustivamente el contexto y los factores relacionados con eventos humanos y acciones en su ambiente natural. Esto permitió recopilar información de diversas fuentes y durante un periodo prolongado, facilitando un estudio holístico y bien fundamentado. Este enfoque es esencial para comprender la complejidad de la acción social y sus significados, ofreciendo una visión detallada de la dinámica social a lo largo del tiempo y los cambios en los patrones habituales. Por otro lado, [23] sostiene que la investigación mediante estudios de casos es particularmente adecuada cuando los investigadores se centran en preguntas de "cómo" o "por qué". A diferencia de las encuestas o los estudios de modelado, que pueden ser más limitados en alcance, los estudios de caso permiten examinar un conjunto de eventos contemporáneos sobre los cuales el investigador tiene poco o ningún control, brindando así una perspectiva más profunda y contextual. Además, [20] cita el trabajo de [25], quienes analizaron las prácticas de gestión de relaciones con el cliente en cinco grandes empresas del mercado venezolano. Asimismo, [20] señalaron que, aunque un mayor número de casos puede proporcionar un entendimiento más amplio del problema planteado, el número de casos debe ser balanceado con los recursos económicos y el tiempo disponible del investigador. En este sentido, cinco empresas representan un equilibrio viable entre profundidad y factibilidad, permitiendo un análisis comprensivo sin

comprometer la calidad del estudio debido a limitaciones de recursos.

IV. Resultados

Este análisis explora el nivel de madurez cibernética en cinco empresas destacadas de diversos sectores industriales y financieros en Costa Rica. Cada caso brinda una visión detallada sobre la implementación y gestión de políticas de ciberseguridad, control de accesos y planes de contingencia ante incidentes de seguridad digital. A través de esta evaluación, se busca identificar el grado de preparación y los niveles de riesgo de cada organización, contribuyendo a una comprensión integral de su resiliencia frente a posibles amenazas cibernéticas.

A. Caso A

Es una empresa transnacional del sector industrial, dedicada a la manufactura médica, con más de 2.000 empleados en su sede local y con una trayectoria de 20 años de operación en el país.

En cuanto a la actualización, existencia y difusión de políticas, se han registrado puntuaciones de 2, 1 y 3, respectivamente. Con respecto a la política de control de accesos, se encuentran en un nivel 2, indicando que se encuentra definido y el proceso de contingencia en Ciberseguridad en caso de desastres, obtuvo una puntuación de 2, indicando que se encuentra en un nivel definido. Con un nivel promedio de 2,04 con un nivel de riesgo medio (ver Figura 1).

B. Caso B

Es una destacada empresa transnacional en el sector industrial, específicamente en la fabricación de tecnología avanzada. Con más de 2.000 empleados en su sede local y una trayectoria de 28 años de operaciones en el país. Esta organización ha consolidado una reputación sólida tanto a nivel nacional como internacional. La empresa recibió en cuanto a la actualización, existencia y difusión de políticas, una calificación de 4 en todos los rubros; al igual que en los rubros de política de control de accesos y de proceso de contingencia en Ciberseguridad en caso de desastres. La empresa ha sido evaluada en términos de su madurez cibernética, obteniendo un promedio de 3,92 lo que es equivalente a un nivel benchamark / mejor práctica de la industria (ver Tabla II)

C. Caso C

Corresponde a una pequeña empresa, de servicios de mercado especializado en consultoría empresarial, con aproximadamente 20 empleados en su sede local y una trayectoria de 5 años operando en el mercado nacional. Los resultados sobre el nivel de madurez cibernética del Caso C revelan un promedio de 2,72 (ver Tabla II), lo que indica que la empresa se encuentra en una fase intermedia de madurez con un nivel definido y un riesgo medio (ver Figura 1) . En el rubro de existencia de políticas, alcanzó un nivel de 2, en actualización de políticas obtuvo una puntuación de 1, indicando que se encuentra en un nivel se riesgo alto y en la difusión de estas políticas su calificación fue de 3, que es un nivel culturalizado. Con respecto a la política de control de accesos, obtuvo una puntuación de 2 y en el proceso de contingencia en Ciberseguridad en caso de desastres, la puntuación fue de 2, por lo tanto se encuentra definida.

D. Caso D

Es una mediana empresa del sector de servicios financieros, especializada en asesoría y gestión financiera para clientes tanto nacionales como internacionales. Con un equipo compuesto por entre 51 y 100 empleados, y más de 40 años de trayectoria en el mercado local, esta organización ha logrado consolidarse como un actor clave en el sector, ofreciendo soluciones personalizadas y adaptadas a las necesidades de sus clientes. En el ámbito de la ciberseguridad, el Caso D con lo que respecta a la existencia, actualización y difusión de sus políticas de seguridad con las calificaciones respectivas de 3 en todos estos rubros. Con respecto a la política de control de accesos, su puntuación fue de un 3 y en el proceso de contingencia en Ciberseguridad en caso de desastres un 2, siendo un nivel culturalizado y definido respectivamente (ver Figura 1). El análisis del nivel de madurez cibernética del Caso D revela un promedio de 2,49 (ver Tabla II).

E. Caso E

Corresponde a una organización líder en el sector financiero nacional, con más de 2.000 empleados y una trayectoria de más de 100 años en el país. Su rol preponderante en el mercado de servicios financieros lo ha posicionado como un referente en la industria. De acuerdo con el análisis de madurez cibernética realizado, el Caso E obtiene un promedio de 3,04, por ende se encuentra en un nivel culturalizado. En los rubros de existencia de políticas, actualización y difusión de ellas; obtuvieron una calificación de 4, 3 y 2 respectivamente indicando que se encuentran entre un nivel de riesgo muy bajo a un nivel medio. Por último, en la política de control de accesos se tiene una puntuación de 4 y en el proceso de contingencia en Ciberseguridad en casos de desastres, la calificación fue de 2.

TABLA II
PROMEDIOS TOTALES Y NIVEL DE RIESGO DE CADA CASO

Caso	*Promedio Total*	*Nivel de Riesgo*
Caso A	2,04	Medio
Caso B	3,92	Bajo
Caso C	1,14	Alto
Caso D	2,49	Medio
Caso E	3,04	Bajo

V. Conclusiones

El análisis realizado sobre la seguridad cibernética en empresas multinacionales reveló importantes hallazgos sobre la gestión de riesgos y las prácticas de protección de datos. A lo largo del estudio, se identificaron vulnerabilidades y se evaluó el grado de preparación de estas organizaciones frente a amenazas cibernéticas. Los resultados destacan la importancia de la implementación de controles internos sólidos y de la adaptación continua a los avances tecnológicos para mitigar posibles riesgos. A continuación, se detallan las conclusiones obtenidas, las cuales proporcionan una visión integral de las fortalezas y áreas de mejora en la ciberseguridad corporativa de las empresas evaluadas.

Con respecto al Caso A, a pesar de su solidez operativa y experiencia en el mercado, presenta una gestión intermedia en cuanto a su nivel de madurez en ciberseguridad, con áreas específicas que requieren una atención prioritaria para mejorar sus procesos y prácticas de seguridad cibernética, esto al poseer un 2,04 como calificación. Las puntuaciones del Caso A (ver Tabla II) sugieren que, si bien la empresa cuenta con políticas establecidas, aún no ha implementado mecanismos eficaces y regulares para garantizar su actualización ni ha logrado asegurar que todos los empleados estén plenamente informados sobre dichas políticas. Por ejemplo, la actualización de políticas parece depender de un enfoque ad-hoc, lo que implica un riesgo significativo para la organización. Este enfoque podría dejar a la empresa vulnerable frente a amenazas emergentes si no se adapta adecuadamente a los cambios en las regulaciones legales o en el entorno de amenazas cibernéticas. En cuanto a la difusión de las políticas, la puntuación de 2 refleja que la comunicación interna en materia de ciberseguridad no está llegando de manera efectiva a toda la organización, limitando la capacidad de la empresa para mitigar riesgos de forma integral y coordinada. Adicionalmente, el Caso A parece carecer de un enfoque estructurado en la adopción de estándares avanzados de *benchmarking* en ciberseguridad. La falta de una actualización continua y estructurada de sus políticas de seguridad puede tener un impacto negativo significativo en su capacidad para responder de manera eficiente ante nuevas amenazas cibernéticas. Para avanzar en su nivel de madurez cibernética, una de las áreas clave de mejora para el Caso A sería la creación de un proceso de revisión y actualización continua de sus políticas, acompañado de una inversión estratégica en la capacitación del personal y en la mejora de los mecanismos de difusión. De esta manera, la empresa podría no solo mantener sus políticas alineadas con las mejores prácticas del sector, sino también asegurar que todo el personal esté debidamente informado y capacitado para implementar dichas políticas de manera efectiva.

En el Caso B, su puntuación de 3,92 refleja un enfoque riguroso y estructurado hacia la ciberseguridad, lo cual es fundamental en un sector tan dinámico y crítico como el tecnológico. Uno de los aspectos más relevantes es su sobresaliente desempeño en la existencia de políticas de ciberseguridad y su actualización periódica. Este compromiso también se extiende al cumplimiento normativo, ya que opera en múltiples jurisdicciones internacionales con regulaciones de protección de datos y seguridad cada vez más estrictas. Las políticas están profundamente arraigadas en la cultura empresarial, y lo más importante, se actualizan de manera regular para mantenerse alineadas con los avances tecnológicos y los cambios en el entorno de amenazas cibernéticas. Este enfoque proactivo permite a la empresa adaptarse rápidamente a nuevas vulnerabilidades o cambios regulatorios, minimizando así los riesgos asociados a la ciberseguridad. El alto nivel de actualización (4) logrado por la empresa indica que se han implementado procesos continuos de revisión de políticas, lo que asegura que estas no solo estén alineadas con las mejores prácticas del sector, sino que también se ajusten a las amenazas emergentes en el panorama global de ciberseguridad. Este enfoque preventivo y anticipatorio permite a la empresa mantener una postura sólida frente a riesgos potenciales, mientras se asegura el cumplimiento normativo con estándares internacionales como el GDPR y el ISO 27001 [26]. Presenta también ciertas áreas de mejora, particularmente en lo que respecta a la difusión de políticas. Aunque las políticas son robustas y se actualizan de manera eficaz, la puntuación obtenida en este ámbito indica que no siempre se comunican de manera eficiente a todos los niveles de la organización. Esto sugiere que existe una oportunidad significativa para mejorar los mecanismos de comunicación interna, asegurando que todos los empleados, independientemente de su nivel o función, estén plenamente informados sobre las políticas vigentes y sobre cómo deben aplicarlas en su trabajo diario. Podría considerar la implementación de campañas de concientización interna más agresivas, así como programas de capacitación específicos para garantizar que las políticas de ciberseguridad se comprendan. Esto le permitiría mantenerse a la vanguardia de las mejores prácticas de ciberseguridad y consolidando su posición como líder en el sector tecnológico.

El Caso C, a pesar de su tamaño relativamente pequeño ha logrado consolidarse en el mercado gracias a su flexibilidad operativa y su enfoque orientado al cliente. No obstante, en el ámbito de la ciberseguridad, el Caso C muestra áreas críticas de mejora que podrían comprometer su estabilidad a largo plazo, especialmente considerando el aumento de las amenazas cibernéticas que afectan tanto a grandes como pequeñas empresas. Aunque se han establecido ciertas políticas de seguridad digital, todavía existen deficiencias importantes en la actualización y difusión de estas políticas, que son esenciales para garantizar la protección adecuada de sus activos digitales y la continuidad de sus operaciones. El verdadero desafío para esta PYME radica en la actualización de políticas, que ha recibido una puntuación de 1, indicando que los mecanismos para revisar y modificar estas directrices no son consistentes ni suficientes para enfrentar las amenazas

emergentes. Además, la difusión de políticas de seguridad dentro de la organización también ha sido identificada como un área de mejora significativa, con una puntuación de 3. Esto sugiere que, aunque las políticas están establecidas, no se comunican de manera efectiva a todos los niveles del personal. Para una PYME como el Caso C, es crucial que todos los empleados, independientemente de su rol, comprendan y apliquen las políticas de seguridad cibernética en sus actividades diarias. La falta de conciencia y capacitación sobre estas políticas podría resultar en errores humanos que comprometan la seguridad de la información, uno de los principales riesgos para las empresas de este tamaño. Una de las recomendaciones clave para el Caso C es instituir un proceso regular de revisión y actualización de políticas, que no solo responda a los cambios en el entorno de amenazas, sino que también se alinee con las mejores prácticas de la industria y las normativas locales e internacionales aplicables a la ciberseguridad. Además, se debe fortalecer la comunicación interna en torno a las políticas de ciberseguridad mediante campañas de concientización y programas de capacitación específicos para todo el personal. Al ser una PYME, el Caso C puede beneficiarse de adoptar soluciones de ciberseguridad escalables y adecuadas a sus necesidades y recursos, como el uso de herramientas automatizadas para la gestión de actualizaciones y la implementación de procedimientos más ágiles y eficientes. A pesar de su tamaño, el Caso C debe entender que las amenazas cibernéticas no discriminan en función del tamaño o la industria, y que una violación de seguridad puede tener consecuencias devastadoras para su reputación y viabilidad financiera. Con un enfoque estratégico en la mejora continua de sus políticas de ciberseguridad y la adopción de tecnologías adecuadas, esta PYME puede posicionarse mejor para enfrentar los retos del entorno digital moderno y proteger sus activos más valiosos.

En el Caso D, ha alcanzado un nivel de madurez 3 en varios factores clave, lo que indica que ha comenzado a integrar políticas de ciberseguridad en su estructura y cultura organizacional de manera más formal. Este avance es un paso crucial para cualquier organización que busca proteger sus activos digitales y garantizar el cumplimiento de las normativas internacionales y locales en materia de seguridad de la información. Sin embargo, a pesar de estos progresos, la empresa sigue enfrentando importantes desafíos en áreas críticas como la existencia y actualización de políticas de seguridad cibernética. La empresa se encuentra actualmente en una fase de transición, en la que ha demostrado tener la capacidad para adoptar políticas formales de ciberseguridad, pero aún no ha logrado consolidarlas de manera óptima. Para alcanzar un nivel de *benchmark* comparable al de empresas más maduras en ciberseguridad, como el Caso B, será necesario que el Caso D realice esfuerzos sostenidos y enfocados en dos áreas prioritarias: la actualización periódica de sus políticas de seguridad y la difusión efectiva de estas políticas entre todos sus colaboradores. Un enfoque recomendado sería la implementación de un proceso estructurado y regular de revisión de políticas, que no solo tome en cuenta los cambios en el entorno de amenazas cibernéticas, sino que también esté alineado con las mejores prácticas internacionales y las regulaciones pertinentes al sector financiero. Además, la empresa debería invertir en programas de capacitación continua para su personal, con el objetivo de asegurar que todos los empleados comprendan y apliquen de manera adecuada las políticas de seguridad, reduciendo así el riesgo de posibles vulnerabilidades. La ciberseguridad no solo es una cuestión técnica, sino también estratégica, y para una empresa con la trayectoria y la importancia del Caso D, la inversión en estos aspectos puede ser determinante para su crecimiento sostenido y la protección de su reputación en el mercado.

Finalmente el compromiso del Caso E con la actualización constante, la difusión eficaz de políticas y su enfoque en proteger los activos digitales no solo la han convertido en un referente en el sector financiero, sino que también la preparan para enfrentar los retos del entorno digital en constante cambio. Uno de sus principales logros es la actualización de políticas de ciberseguridad, áreas en las que ha alcanzado niveles culturalizados y con un riesgo bajo. Esto significa que la empresa ha integrado de manera efectiva políticas que no solo están formalmente definidas, sino que son revisadas y adaptadas continuamente para enfrentar las nuevas amenazas del entorno digital. El análisis revela que el Caso E no solo ha establecido políticas formales de seguridad, sino que ha logrado integrarlas completamente en su cultura organizacional. Tener una puntuación total de 3,04, refleja un nivel de riesgo bajo y un factor culturalizado, ya que la organización ha implementado mecanismos de controles eficientes que garantizan que todos los empleados, sin importar su nivel jerárquico o función dentro de la empresa, estén bien informados sobre las políticas de ciberseguridad y los controles respectivos. Además, el personal está debidamente capacitado para aplicar estas políticas en su trabajo diario, lo que reduce significativamente el riesgo de vulnerabilidades internas, uno de los principales desafíos en la gestión de riesgos cibernéticos. Aunque su nivel de madurez es notablemente alto en comparación con otras empresas del sector, el análisis sugiere que aún podría fortalecer algunos aspectos operacionales relacionados con la implementación de herramientas más avanzadas para el monitoreo en tiempo real de amenazas. Si bien la empresa ha adoptado un enfoque proactivo en cuanto a la actualización y difusión de políticas, un área donde podría mejorar sería en la creación de un sistema automatizado y centralizado que permita la detección y respuesta inmediata ante incidentes de seguridad. Esto le permitiría reaccionar con mayor velocidad ante ataques sofisticados que, en el entorno financiero actual, son cada vez más comunes. Otra oportunidad de mejora podría radicar en la gestión de proveedores externos. Como una organización financiera de gran tamaño, el Caso E depende de una red extensa de proveedores de servicios tecnológicos y financieros. Garantizar que estos proveedores cumplan con los

mismos estándares rigurosos de ciberseguridad que la propia empresa es fundamental para minimizar posibles riesgos en la cadena de suministro. Aunque ya se han implementado procesos de control sobre estos terceros, la creación de auditorías regulares más exhaustivas podría ser un paso adicional para fortalecer aún más esta área crítica. Si el Caso E continúa en esta línea de mejora continua, no solo consolidará su posición como líder en ciberseguridad, sino que también servirá como un modelo a seguir para otras empresas del sector que buscan proteger sus activos en un entorno digital cada vez más desafiante.

A. Análisis entre casos de empresas grandes y PYMEs

Las diferencias en la gestión de ciberseguridad entre las empresas grandes y las PYMEs son evidentes, marcadas principalmente por los recursos disponibles y la complejidad organizativa. A continuación un detalle por áreas.

1) Recursos e infraestructura: Las empresas grandes tienen la ventaja de contar con presupuestos que les permiten una mayor inversión en tecnología y talento especializado, algo que queda reflejado en los casos A, B y E. Este grupo de empresas, además, tiene infraestructura tecnológica más robusta, permitiéndoles una respuesta más ágil frente a incidentes cibernéticos. Su capacidad para implementar sistemas de ciberseguridad avanzados y escalables les otorga una ventaja competitiva en un entorno cada vez más digital y vulnerable a los ataques. Además, estas empresas suelen adoptar procesos proactivos de actualización de políticas, asegurando que las medidas de protección se ajusten constantemente a las nuevas amenazas y normativas internacionales.

En contraste, las PYMEs, como en el Caso C, enfrentan limitaciones en la implementación de tecnologías y en la capacidad para adoptar sistemas de ciberseguridad escalables. Su enfoque, generalmente más reactivo que proactivo, les dificulta mantener políticas actualizadas, dejándolas más expuestas a los cambios rápidos en el panorama de amenazas cibernéticas. La falta de recursos no solo afecta la compra de tecnología, sino también la contratación de personal experto, haciendo que muchas de estas organizaciones dependan de soluciones estándar o básicas para su seguridad.

2) Políticas de Ciberseguridad. Definición, actualización y difusión: Las empresas grandes como los Casos A, B y E no solo han desarrollado políticas de seguridad cibernética, sino que han logrado integrarlas de manera efectiva en su cultura organizacional. Esto incluye procesos continuos de revisión y adaptación que les permiten ajustarse a las regulaciones internacionales y a las nuevas amenazas. En el Caso B, por ejemplo, se ha alcanzado un nivel 4 en la difusión de políticas, lo que implica una concientización elevada dentro de toda la organización sobre los riesgos cibernéticos y las medidas preventivas. Además, estas empresas son capaces de ofrecer programas de formación continua que permiten a sus empleados estar al tanto de los protocolos y mejores prácticas en materia de seguridad.

Por otro lado, las PYMEs suelen enfrentarse a retos significativos en la actualización y difusión de sus políticas de ciberseguridad. Aunque los Casos C y D han hecho esfuerzos por desarrollar políticas de seguridad, su capacidad para mantenerlas actualizadas es limitada. El Caso D, por ejemplo, aún se encuentra en un proceso de maduración en cuanto a su estructura de políticas de seguridad, con una puntuación de 2,49 lo que refleja que no ha logrado institucionalizar procesos de actualización ni mecanismos eficientes de difusión. La falta de capacitación regular entre los empleados aumenta la vulnerabilidad de estas empresas ante posibles ataques, ya que el personal no está completamente preparado para reconocer ni responder a las amenazas cibernéticas.

3) Capacidad del personal y concientización interna: Las empresas grandes tienen una ventaja clara en términos de formación y concientización del personal. El Caso B ha demostrado su capacidad para asegurar que los empleados no solo estén informados, sino también capacitados regularmente sobre las políticas de ciberseguridad, lo que se refleja en su alta puntuación en difusión. Estos programas de formación continua ayudan a crear una cultura organizacional alineada con la seguridad cibernética, donde todos los empleados, independientemente de su posición, entienden su rol en la protección de la organización. Por el contrario, las PYMEs aún luchan por implementar programas de formación regulares debido a limitaciones presupuestarias. Si bien las políticas de seguridad existen, la concientización y el entrenamiento del personal no están al mismo nivel que en las empresas grandes. Esto crea un punto de vulnerabilidad, ya que los empleados son la primera línea de defensa en la mayoría de los incidentes de ciberseguridad. La falta de formación no solo pone en riesgo la seguridad de la empresa, sino que también puede generar costos adicionales en el futuro, como resultado de brechas de seguridad que podrían haber sido prevenidas con una adecuada preparación.

4) Cumplimiento normativo y benchmarking: El cumplimiento de normativas internacionales y la adopción de mejores prácticas son áreas donde las empresas grandes como los Casos B y E destacan. Estas organizaciones no solo cumplen con las leyes locales, sino que también adoptan estándares globales de ciberseguridad, lo que les permite operar con mayor seguridad en el ámbito internacional. Esto no solo reduce el riesgo de sanciones regulatorias, sino que también mejora su reputación ante socios y clientes internacionales. El Caso B, por ejemplo, ha implementado procesos continuos de *benchmarking*, lo que le permite compararse con otras empresas de su sector y asegurarse de que está adoptando medidas de seguridad de vanguardia. En contraste, las PYMEs tienen una menor capacidad para cumplir con las normativas internacionales. Esto se debe, en parte, a la falta de conocimiento y recursos para implementar estándares globales. El Caso D, por ejemplo, ha comenzado a

adoptar algunas mejores prácticas, pero aún no alcanza los niveles de cumplimiento que le permitirían competir con empresas más grandes o internacionalizarse de manera segura. Esto puede representar un obstáculo significativo para su crecimiento y sostenibilidad en un mundo cada vez más interconectado y regulado. Las PYMEs enfrentan limitaciones significativas que obstaculizan su capacidad para protegerse de manera adecuada contra las amenazas cibernéticas. A pesar de que han hecho avances, su capacidad para actualizar, difundir y escalar sus políticas de ciberseguridad sigue siendo limitada. La formación del personal y la adopción de normativas internacionales son áreas críticas que requieren atención si estas empresas desean mejorar su postura de ciberseguridad y competir en un entorno cada vez más digital.

VI. Discusión

De acuerdo con lo previamente analizado, las grandes empresas tienen una mayor capacidad para lograr resiliencia cibernética debido a que disponen de los recursos necesarios para invertir en sistemas avanzados de protección y estrategias de recuperación. Estas organizaciones pueden destinar personal especializado, tecnologías emergentes y la mejora continua de sus políticas de ciberseguridad, lo que les permite estar mejor preparadas para hacer frente a ciberataques y minimizar sus efectos. Acorde a [27] la experiencia de una compañía de seguros global muestra el potencial de las empresas grandes para lograr resiliencia cibernética. Esta empresa destinó $70 millones para un programa integral de ciberseguridad. El gobierno de EE. UU. ha identificado la ciberseguridad como uno de los desafíos económicos y de seguridad nacional más graves que enfrentamos como nación. A nivel mundial, la amenaza de los ciberataques está creciendo tanto en número como en intensidad. Algunas grandes empresas están invirtiendo hasta $500 millones en ciberseguridad, y anualmente se crean más de 100 mil millones de líneas de código en todo el mundo. Muchas compañías reportan miles de ataques cada mes, que van desde los triviales hasta los extremadamente graves.

En contraste, las PYMEs, a pesar de ser altamente vulnerables, suelen carecer de los recursos suficientes para implementar medidas de seguridad robustas. Ref. [28] estima que el 40% de los ataques cibernéticos que resultan efectivos y causan daños significativos afectan a las PYMEs, y el impacto es tan devastador que, en muchos casos, estas empresas no logran recuperarse. Esta falta de recursos hace que las PYMEs sean objetivos más atractivos para los cibercriminales, ya que su infraestructura de seguridad suele ser insuficiente y su capacidad de reacción es limitada.

Por ello, resulta crucial que tanto las grandes empresas como las PYMEs prioricen la inversión en ciberseguridad. Las PYMEs, en particular, deben ser conscientes de la importancia de asignar recursos a esta área, incluso cuando sus presupuestos sean más ajustados, ya que un solo ataque cibernético podría significar el fin de su operación. El fortalecimiento de la gestión del riesgo cibernético es fundamental no solo para proteger la continuidad del negocio, sino también para aumentar la competitividad en un entorno empresarial cada vez más digitalizado.

VII. Limitaciones y Líneas futuras de Investigación

Para un estudio de casos el utilizar una muestra de cinco empresas tiene total validez, tal como se justificó en esta investigación, ya que esto representa un primer acercamiento al tema, sin embargo, si queremos tener datos más significativos para generar política pública y una mayor representatividad, se podrían utilizar otra metodología para analizar muestras más amplias, que permitan entender mejor el nivel de ciberseguridad en las empresas y analizar ampliamente el riesgo cibernético al que están expuestas. Dados los hallazgos de este estudio de casos, cómo líneas futuras de investigación se plantean; profundizar en las prácticas de ciberseguridad de las PYMEs en países en desarrollo, según su nivel de implementación de la transformación digital, ya que este grupo de empresas son altamente vulnerables y carecen de los recursos necesarios para implementar medidas de ciberseguridad robustas. Además, se recomienda, mediante la metodología de casos, estudiar instituciones del sector público, tales como gobiernos locales.

Referencias

[1] E. R. Zuña Macancela *et al.*, "Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro", *Rev. Univ. Soc.*, vol. 11, núm. 4, pp. 487–492, 2019, doi: http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202019000400487&lng=es&nrm=iso&tlng=en.

[2] M. Xu y L. Hua, "Cybersecurity Insurance: Modeling and Pricing", *North Am. Actuar. J.*, vol. 23, núm. 2, pp. 220–249, 2019, doi: 10.1080/10920277.2019.1566076.

[3] T. Aven, "The Call for a Shift from Risk to Resilience: What Does it Mean?", *Risk Anal.*, vol. 39, núm. 6, pp. 1196–1203, 2019, doi: 10.1111/risa.13247.

[4] O. Bustillos Ortega, J. Rojas Segura, y J. Murillo-Gamboa, "Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas", *Interfases*, vol. 18, núm. 2, pp. 185–205, dic. 2023, doi: 10.26439/interfases2023.n018.6626.

[5] C. Rodriguez Bravo, "Modelo Madurez Ciberseguridad (ECM2)". 2017. Disponible en: https://es.scribd.com/document/525745224/Modelo-Madurez-Ciberseguridad-Cesar-Rodriguez

[6] M. Soto y L. H. Pérez, "Creación de una plataforma web segura, para automatizar el modelo de madurez en ciberseguridad ECM2 con el fin de facilitar la tarea de determinar el estado real en materia de ciberseguridad a instituciones sin importar su tamaño o sector.", Thesis, Universidad Cenfotec, 2018. Disponible en: https://repositorio.ucenfotec.ac.cr/handle/123456789/xmlui/handle/123456789/381

[7] J. Rojas-Segura et al., "How to evaluate the cyber risk of SMEs? An Academia strategy to create competitive advantages", en Proc. LACCEI int. multi-conf. eng. educ. technol., Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LACCEI2024.1.1.639.

[8] J. Rojas-Segura, M. Faith-Vargas, y J. Martinez-Villavicencio, "Conceptualizing digital transformation using semantic decomposition", *TEC Empres.*, vol. 17, núm. 3, pp. 63–75, dic. 2023, doi: 10.18845/te.v17i3.6850.

[9] O. Bustillos Ortega y J. Rojas Segura, "Protocolo básico de ciberseguridad para pymes", *Interfases*, vol. 16, núm. 2, pp. 168–186, dic. 2022, doi: 10.26439/interfases2022.n016.6021.

[10] A. Raza, M. Hussain, H. Tahir, M. Zeeshan, M. A. Raja, y K.-H. Jung, "Forensic analysis of web browsers lifecycle: A case study", *J. Inf. Secur. Appl.*, vol. 85, p. 103839, sep. 2024, doi: 10.1016/j.jisa.2024.103839.
[11] E. Jhordany Serna Valdivia y J. Mejía Miranda, "Proposal of a Intelligent Agent for Management and Mitigation in Cibersecurity Risk for IoT Environments", en 2020 9th International Conference On Software Process Improvement (CIMPS), oct. 2020, pp. 148–154. doi: 10.1109/CIMPS52057.2020.9390114.
[12] M. J. Lees, M. Crawford, y C. Jansen, "Towards Industrial Cybersecurity Resilience of Multinational Corporations", *IFAC-Pap.*, vol. 51, núm. 30, pp. 756–761, ene. 2018, doi: 10.1016/j.ifacol.2018.11.201.
[13] K. Zkik, A. Belhadi, S. Kamble, M. Venkatesh, M. Oudani, y A. Sebbar, "Cyber resilience framework for online retail using explainable deep learning approaches and blockchain-based consensus protocol", *Decis. Support Syst.*, vol. 182, p. 114253, jul. 2024, doi: 10.1016/j.dss.2024.114253.
[14] Gobierno de Japón, "Cybersecurity for All". Setiembre de 2021. Disponible en: https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[15] M. Nanda, M. Saraswat, y P. K. Sharma, "Enhancing cybersecurity: A review and comparative analysis of convolutional neural network approaches for detecting URL-based phishing attacks", *E-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 8, p. 100533, jun. 2024, doi: 10.1016/j.prime.2024.100533.
[16] S. Morgan, "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021", *Cybercrime Magazine*, junio de 2019. Disponible en: https://cybersecurityventures.com/cybersecurity-market-report/
[17] OEA y CISCO, "Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades". Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, 2023. Disponible en: https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
[18] J. Rojas-Segura, J. Martinez-Villavicencio, y M. Faith-Vargas, "Digital Transformation and Business Model in SMEs: a Bibliometric Analysis", en Proceedings of the LACCEI International Multi-conference for Engineering, Education and Technology, Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LEIRD2024.1.1.280.
[19] S. Durst, C. Hinteregger, y M. Zieba, "The effect of environmental turbulence on cyber security risk management and organizational resilience", *Comput. Secur.*, vol. 137, p. 103591, feb. 2024, doi: 10.1016/j.cose.2023.103591.
[20] R. Hernández-Sampieri y C. Mendoza, *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*, Sexta Edición. Ciudad de México: Mcgraw-Hill México, 2018.
[21] M. B. Gondo, J. M. Vardaman, y J. Amis, "Case Within a Case", en *The Encyclopedia of Case Study Research*, SAGE Publications, 2010, pp. 134–136. https://www.research.ed.ac.uk/en/publications/case-within-a-case
[22] A. J.Mills, G. Durepos, y E. Wiebe, "Authenticity", en *Encyclopedia of Case Study Research*, SAGE Publications, Inc., 2010, pp. 35–36. doi: 10.4135/9781412957397.
[23] R. K. Yin, *Case Study Research and Applications. Design and Methods*, Sixth Edition. Thousand Oaks, CA: SAGE Publications, Inc., 2017.
[24] M. L. Saavedra García, "El estudio de caso como diseño de investigación en las Ciencias Administrativas", *Iberoam. Bus. J. Rev. Estud. Int.*, vol. 1, núm. 1, pp. 72–97, 2017, doi: https://doi.org/10.22451/3002.ibj2017.vol1.1.11005.
[25] R. Puente y M. Cervilla, "Prácticas de la gerencia de relaciones con el cliente (CRM) en empresas venezolanas: un estudio de casos", *Acad. Rev. Latinoam. Adm.*, 2007.
[26] International Organization for Standardization (ISO), "Guidance on Social Responsability ISO 26000:2010". Disponible en: https://www.iso.org/obp/ui#iso:std:iso:26000:ed-1:v1:es
[27] T. Poppensieker y R. Riemenschnitter, "A new posture for cybersecurity in a networked world", Mckinsey & Company, 2018. Disponible en: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world
[28] R. M. Díaz, "Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe". CEPAL, agosto de 2022. Disponible en: https://repositorio.cepal.org/handle/11362/48065