ANÁLISIS DE BRECHAS DE SEGURIDAD DE LA INFORMACIÓN EN EL FACTOR HUMANO: CASO DE ESTUDIO APLICADO EN EL SECTOR GOBIERNO

INFORMATION SECURITY BREACH ANALYSIS IN THE HUMAN FACTOR: CASE STUDY APPLIED IN THE GOVERNMENT SECTOR

Recebido em: 6 de maio de 2025
Aprovado em: 5 de agosto de 2025
Sistema de Avaliação: Double Blind Review
RCO | a. 17 | v. 2 | p. 295-313 | jul./dez. 2025
DOI: https://doi.org/10.25112/rco.v2.4160

Julián Alberto Uribe Gómez *julianuribe8729@correo.itm.edu.co*
Magister en Gestión Tecnológica por la Universidad Pontificia Bolivariana (Medellín/Colombia).
Docente del Instituto Tecnológico Metropolitano (Medellín/Colombia).

Jorge Iván Brand Ortiz *jorgebrand@itm.edu.co*
Doctor en Gestión de la Tecnología y la Innovación por la Universidad Pontificia Bolivariana (Medellín/Colombia).
Profesor en la Institución Universitaria ITM (Medellín/Colombia).

Javier Mauricio Durán Vásquez *javierduran1237@correo.itm.edu.co*
Magister en TICS por la Institución Universitaria ITM (Medellín/Colombia).
Profesor en la Institución Universitaria ITM (Medellín/Colombia).

Alejandro Salgar Marín *alejandrosalgar2487@correo.itm.edu.co*
Especialista en Desarrollo de software por la Institución Universitaria ITM (Medellín/Colombia).
Profesor en la Institución Universitaria ITM (Medellín/Colombia).

Julián Esteban Murillo Martínez *julianmurillo@medellin.gov.co*
Especialista en Gerencia Financiera por la Universidad Pontificia Bolivariana (Medellín/Colombia).
Asesor de despacho Hacienda Alcaldía de Medellín (Medellín/Colombia).

Revista CONHECIMENTO ONLINE

ISSN: 2176-8501

RESUMEN

Se aborda la importancia de la seguridad de la información en las instituciones públicas, destacando la necesidad de proteger datos sensibles y mitigar las vulnerabilidades que se puedan presentar debido a factores humanos. Se destaca la implementación de modelos de madurez y la influencia de factores individuales, sociales y organizacionales en el comportamiento de ciberseguridad. Se utiliza un modelo explicativo secuencial mixto, combinando enfoques cualitativos y cuantitativos. Se aplicó una encuesta diagnóstica a 228 empleados públicos, evaluando su conocimiento en aspectos de seguridad de la información. La encuesta midió el grado de conocimiento en autenticación, navegación web, correo electrónico, aplicaciones de mensajería, redes sociales, dispositivos móviles, equipos de cómputo, dispositivos domóticos, buenas prácticas financieras y otras amenazas latentes. Los resultados muestran que los empleados tienen altos conocimientos en redes sociales (90%), pero presentan vulnerabilidades en amenazas latentes (48.4%) como ingeniería social. El rol con mayor desempeño es coordinador mientras los técnicos administrativos son más vulnerables. Adicional, con un valor-p de 0.173 se concluye que un mayor tiempo de servicio en la organización no garantiza mayor conocimiento en seguridad de la información. Finalmente, se dispuso un modelo de regresión logística para la predicción de la variable calificación con una precisión del 75%. Se revelan brechas dentro de la organización y se sugiere implementar programas de capacitación y concientización en ciberseguridad siguiendo prácticas de mejoramiento continuo. Además, se recomienda la colaboración entre organizaciones y el uso de tecnologías emergentes para mejorar la detección y mitigación de amenazas.

Palabras clave: seguridad de la información, modelo de madurez, organización pública, análisis cuantitativo.

RESUMO

É abordada a importância da segurança da informação nas instituições públicas, destacando a necessidade de proteger dados sensíveis e mitigar vulnerabilidades que possam surgir devido a fatores humanos. Destacam-se a implementação de modelos de maturidade e a influência de fatores individuais, sociais e organizacionais no comportamento de cibersegurança. É utilizado um modelo explicativo sequencial misto, combinando abordagens qualitativas e quantitativas. Foi aplicada uma pesquisa diagnóstica a 228 servidores públicos, avaliando seu conhecimento sobre aspectos de segurança da informação. A pesquisa mediu o nível de conhecimento em autenticação, navegação web, email, aplicações de mensagens, redes sociais, dispositivos móveis, equipamentos informáticos, dispositivos de domótica, boas práticas financeiras e outras ameaças latentes. Os resultados mostram que os colaboradores possuem alto conhecimento de redes sociais (90%), mas apresentam vulnerabilidades em ameaças latentes (48,4%), como engenharia social. A função com maior desempenho é a de coordenador enquanto os técnicos administrativos são mais vulneráveis. Adicionalmente, com valor p de 0,173, conclui-se que um maior tempo de serviço na organização não garante maior conhecimento em segurança da informação. Por fim, montou-se um modelo de regressão logística para prever a variável rating com precisão de 75%.

Revista CONHECIMENTO ONLINE

ISSN: 2176-8501

São reveladas lacunas dentro da organização e sugere-se a implementação de programas de formação e sensibilização em cibersegurança seguindo práticas de melhoria contínua. Além disso, recomenda-se a colaboração entre organizações e o uso de tecnologias emergentes para melhorar a detecção e mitigação de ameaças.

Palavras-chave: segurança da informação, modelo de maturidade, organização pública, análise quantitativa.

ISSN: 2176-8501

1 INTRODUCCIÓN

La seguridad de la información en las instituciones públicas es crucial para proteger datos sensibles, mantener la confianza y garantizar la seguridad nacional (JEVTIĆ & ALHUDAIDI, 2023; SAMARA, 2023). Abarca la preservación de la integridad, confidencialidad y disponibilidad de los datos al tiempo que se abordan las ciberamenazas más complejas (JEVTIĆ & ALHUDAIDI, 2023). De acuerdo con Hochstetter-Diez et al. (2023) las instituciones públicas están obligadas legalmente a priorizar la seguridad de la información y demostrar una mejora continua. Este mismo autor señala que la implementación de modelos de madurez de seguridad de la información puede ayudar a lograr este objetivo, con la tríada conciencia, infraestructura y gestión propuesta como una guía práctica (HOCHSTETTER-DIEZ et al., 2023). Sin embargo, muchas organizaciones públicas, como por ejemplo las de Ecuador, tienen una baja capacidad de gestión de la seguridad de la información, lo que pone de relieve la necesidad de mejora (IZURIETA et al., 2021). En el sector financiero de Zimbabue, se ha identificado una baja concienciación sobre ciberseguridad y la falta de marcos de protección adecuados, lo que expone a las instituciones a riesgos significativos (MASHIZHA & KANENGONI, 2024). La investigación también revela que los factores individuales, sociales y organizacionales influyen en el comportamiento de ciberseguridad, subrayando la importancia de la concientización y la autoeficacia en seguridad (NASIRI et al., 2024). En los servicios de emergencia de Estados Unidos, las vulnerabilidades críticas, como el *ransomware* y los ataques de *phishing*, amenazan la seguridad pública debido a tecnologías obsoletas y protocolos inconsistentes (GVILAVA, 2023). En Suecia, las autoridades administrativas enfrentan desafíos en la implementación de medidas de ciberseguridad debido a la rápida digitalización y la falta de recursos adecuados (ANDREASSON et al., 2024).

Un aspecto fundamental sobre la seguridad de la información es el conocimiento que poseen los empleados sobre los conceptos y prácticas de seguridad. Esto incluye la comprensión de los tipos de amenazas, como el *phishing* y el *malware*, así como la importancia de las prácticas de contraseñas seguras y las medidas de protección de datos (YUNITA, 2023; OMAR et al., 2021). Por lo tanto, evaluar los niveles de conocimiento es fundamental para identificar las lagunas que deben abordarse mediante programas de formación específicos. Las estrategias eficaces identificadas incluyen la formación de los empleados, la adaptación a las amenazas cambiantes y la integración de la ciberseguridad en las iniciativas de protección y desarrollo (JEVTIĆ & ALHUDAIDI, 2023; SAMARA, 2023). Adicional, es importante considerar la planificación estratégica como esencial para una gestión óptima de la seguridad de la información en las instituciones públicas (IZURIETA et al., 2021).

ISSN: 2176-8501

Por otro lado, las nuevas tecnologías derivadas de la cuarta revolución industrial han permitido que un mayor número de organizaciones públicas y privadas converjan hacia la digitalización, haciendo que sus productos o servicios sean cada vez más accesibles, pero también más vulnerables a las amenazas de seguridad (OLEJNÍČEK et al., 2023). Dichas amenazas representan en mayor medida las conocidas como amenazas cibernéticas tales como ataques de *malware*, *phishing*, ingeniería social, ataques de denegación del servicio (DDoS) y amenazas internas (EFIJEMUE et al., 2023), y es por esta razón que diversos actores reconocen que estas están asociadas a diversos factores humanos debido principalmente a la falta de capacitación, concientización y recursos (OLEJNÍČEK et al., 2023), así mismo a factores técnicos (DE SILVA, 2023), organizacionales, sociales e individuales en el comportamiento en materia de ciberseguridad (NASIRI et al., 2024).

No obstante, diversos autores enfatizan el aspecto humano como uno de los factores de mayor importancia en la ciberseguridad (RIZAL & SETIAWAN, 2024; CHAUDHARY, 2024; LUBIS et al., 2024). A las brechas de ciberseguridad debidas al aspecto humano se le conocen como "error humano", y tal como lo describe Chaudhary (2024) este término es definido como acciones no intencionales o falta de acción, y juega un papel importante en la mayoría de los incidentes cibernéticos y las violaciones de datos. Debido a esto, Blessing (2024) enfatiza que el error humano es el factor más importante en el éxito de los ataques de *phishing*, debido a que los empleados, sin saberlo, hacen clic en enlaces maliciosos o comparten información confidencial (ANDREASSON et al., 2024) o por el contrario son víctimas de ataques de ingeniería social (KARLSSON et al., 2022). Este mismo autor identificó que existe una variabilidad significativa entre los sectores públicos y privados, donde los empleados del sector público generalmente están menos preparados para reconocer los intentos de *phishing* en comparación con sus homólogos del sector privado (BLESSING, 2024). Adicional, Lubis et al. (2024) considera que los aspectos personales de los empleados como carga cognitiva, limitaciones de la racionalidad y apatía respecto a los riesgos aumenta la brecha de seguridad, haciendo a las organizaciones vulnerables frente a las amenazas.

Por lo tanto, el propósito de la investigación fue evaluar el nivel de madurez de la seguridad de la información en los colaboradores en una entidad gubernamental, mediante una metodología explicativa secuencial mixta, combinando enfoques cualitativos y cuantitativos apoyado en modelos de regresión logística, con el fin de identificar las áreas, profesiones y cargos con mayores niveles de vulnerabilidad en seguridad de la información y predecir las calificaciones de los colaboradores para la detección de falencias y por ende aportar al mejoramiento del desempeño organizacional en este aspecto. A continuación, serán abordados los factores relacionados con la medición en seguridad de la información, luego el apartado

ISSN: 2176-8501

sobre la metodología llevada a cabo y sus resultados, para finalmente dar paso a las discusiones y conclusiones.

1.1 FACTORES RELACIONADOS A LA MEDICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Evaluar el grado de la seguridad de la información en las organizaciones públicas es una tarea multirelacional que requiere centrarse en varias áreas clave. Estas áreas abarcan conocimientos técnicos, actitudes y comportamientos personales y cultura organizacional, que en conjunto contribuyen a la eficacia de las prácticas de seguridad de la información. Varios autores han estudiado los factores relacionados a la seguridad de la información al interior de las organizaciones, cada uno de ellos responde a contextos específicos, sin embargo, todos discurren en que el comportamiento humano es clave para fortalecer la seguridad (HOFFMAN & SKOVIRA, 2020). Autores como Rizal & Setiawan (2024) identifican 22 áreas de enfoque que incluyen administración de contraseñas, uso de correo electrónico, uso de internet, uso de redes sociales, dispositivos móviles, informes de incidentes, manejo de información, respaldo y actualización, mensajería instantánea y navegación, permisos de acceso, uso de dispositivos de otros, cumplimiento de regulaciones, acción ante las consecuencias, monitoreo del uso de aplicaciones, uso de wifi, hábitos de navegación, política de seguridad de la información, aplicaciones pirateadas y privacidad de seguridad. Baltuttis et al. (2024) proponen 5 categorías de medición: personalidad y actitud, antecedentes en ciberseguridad, conocimientos y habilidades, comportamiento en ciberseguridad, entorno organizacional y forma de trabajar. Zammani & Razali (2016) proponen un modelo de madurez de la seguridad de la información que consta de 3 aspectos, los cuales son personas, organización y procesos con 14 factores de éxito y 57 dimensiones.

Moses et al. (2022) plantea las siguientes dimensiones para evaluar la seguridad de la información: atención de la gerencia, liderazgo, estructura organizacional, organización de procesos, ciclo PHVA, documentación, uso de herramientas, implementación de medidas, gestión de riesgos, mejora continua y conciencia de los empleados, esta última, propuesta por Blessing (2024) incluye diferencias sectoriales, políticas de ciberseguridad, compromiso de los empleados y eficacia de los programas de formación. Por otro lado, Lubis et al. (2024) plantea tres factores, experiencia de privacidad en línea, comprensión de la privacidad en internet y evaluación de la privacidad en internet. Finalmente, Hoffman & Skovira (2020) utilizan un instrumento denominado índice de cultura de seguridad organizacional, allí destacan las actitudes relacionadas con la seguridad de la información en la fuerza laboral, en este índice se destacan las estructuras organizaciones y la diferenciación en los roles de género.

ISSN: 2176-8501

2 METODOLOGÍA

La investigación llevada a cabo emplea un modelo explicativo secuencial mixto, que combina un enfoque cualitativo, mediante un instrumento tipo encuesta en línea de evaluación diagnóstica de defensa individual con retroalimentación de resultados, denominado diagnóstico de defensa individual de seguridad de la información (DDISI), y un enfoque cuantitativo de análisis de datos descriptivo, correlacional y predictivo. Este instrumento fue enviado entre noviembre y diciembre del año 2024 a 228 empleados públicos entre vinculados y contratistas de la Subsecretaría de Tesorería de la Secretaría de Hacienda del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, Antioquia, Colombia. Cuyas áreas están divididas en control y riesgos, inversiones, caja, cobranza y despacho. Dicha encuesta recolecto en total 15.732 respuestas.

La encuesta diagnóstica midió el grado de conocimiento en aspectos relacionados con la seguridad de la información basados en investigaciones de autores mencionados que incluyen, autenticación, navegación web, correo electrónico, aplicaciones de mensajería, redes sociales, dispositivos móviles, equipos de cómputo, dispositivos domóticos, buenas prácticas financieras y otras amenazas latentes.

La investigación identifica en el diagnóstico, basado en los diez factores de seguridad de la información, cuatro tipos de actitudes conductuales, tomadas de Baltuttis et al. (2024) y que hacen referencia al modelo de madurez de la seguridad de la información propuesto por Zammani et al. (2021), las cuales son: novatos ingenuos, examinadores tradicionales, rebeldes flexibles y soldados confiables. Cada una de estas actitudes se explican de la siguiente manera:

- Los novatos ingenuos son el grupo más vulnerable, prestan poca atención a las prácticas de ciberseguridad y confían mucho en los demás. Generalmente son más jóvenes, menos experimentados y, a menudo, carecen de conocimientos sobre ciberseguridad. Con una puntuación de hasta 25% (0.25).
- Los examinadores tradicionales siguen prácticas conservadoras de ciberseguridad y se adhieren estrictamente a las reglas organizacionales, tienen una mentalidad de poca confianza y prefieren una separación clara entre el trabajo y la vida personal. Este grupo tiene una edad promedio y a menudo depende de los departamentos de TI para la ciberseguridad. Con una puntuación hasta 50% (0.50).
- Los rebeldes flexibles exhiben una gran resiliencia y confianza en sí mismos, y cambian con frecuencia entre actividades laborales y personales. Son predominantemente hombres, a menudo trabajan por cuenta propia o en TI, y enfrentan desafíos relacionados con la confusión entre el trabajo y la vida personal. Con una puntuación hasta 75% (0.75).

ISSN: 2176-8501

- Los soldados confiables son diligentes y atentos en su comportamiento de ciberseguridad, con alta resiliencia y confianza en sí mismos. Son mayores, tienen experiencia y, a menudo, desempeñan funciones de liderazgo y sirven como modelos a seguir en materia de ciberseguridad dentro de sus organizaciones. Con una puntuación hasta 100% (1).

El modelo propuesto para el desarrollo de esta investigación consistió en las siguientes actividades, tal como se observa en la figura 1. Las actividades siguen un ciclo de mejora continua, donde tal y como coinciden los autores Akinyele & Daniel (2024), Moses et al. (2022) y Chaudhary (2024) se debe mantener y mejorar continuamente las medidas de seguridad de la información, siendo este un desafío continuo. Los gobiernos y organizaciones públicas y privadas deben revisar y actualizar periódicamente sus prácticas de seguridad para adaptarse a la evolución de las amenazas, adicional la concientización sobre la seguridad de la información también debe considerarse un proceso continuo que necesita actualizaciones y mejoras periódicas para seguir siendo eficaz.

Figura 1. Modelo de desarrollo de investigación.

Elaboración Autores.

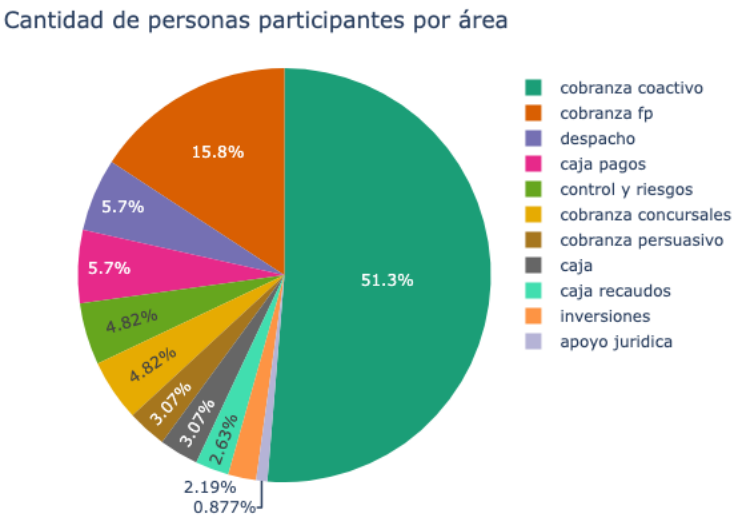
Revista CONHECIMENTO ONLINE
ISSN: 2176-8501

3 RESULTADOS Y ANÁLISIS

3.1 ANÁLISIS DESCRIPTIVOS

De acuerdo a las encuestas recibidas, la distribución de las áreas de la subsecretaria de tesorería estaría dividida tal como se visualiza en la figura 2, siendo las áreas de cobranza coactivo y cobranza facilidades de pago las áreas con mayor número de personas, entre ambas abarcan el 67.1% del total.

Figura 2. Distribución áreas en participación encuesta.



Elaboración Autores.

Al evaluar los conceptos o factores de la encuesta, los resultados, presentados en la figura 3, arrojaron que los colaboradores de la subsecretaria de tesorería tienen altos conocimientos en redes sociales y su gestión y buenas prácticas financieras, ambas puntuaron 90% y 88.6%, un conocimiento medianamente alto en correo electrónico y aplicaciones de mensajería con puntuaciones de 78.6% y 77.5%. En general, de acuerdo a las clasificaciones de nivel de madurez, los colaboradores son clasificados como "soldados confiables".

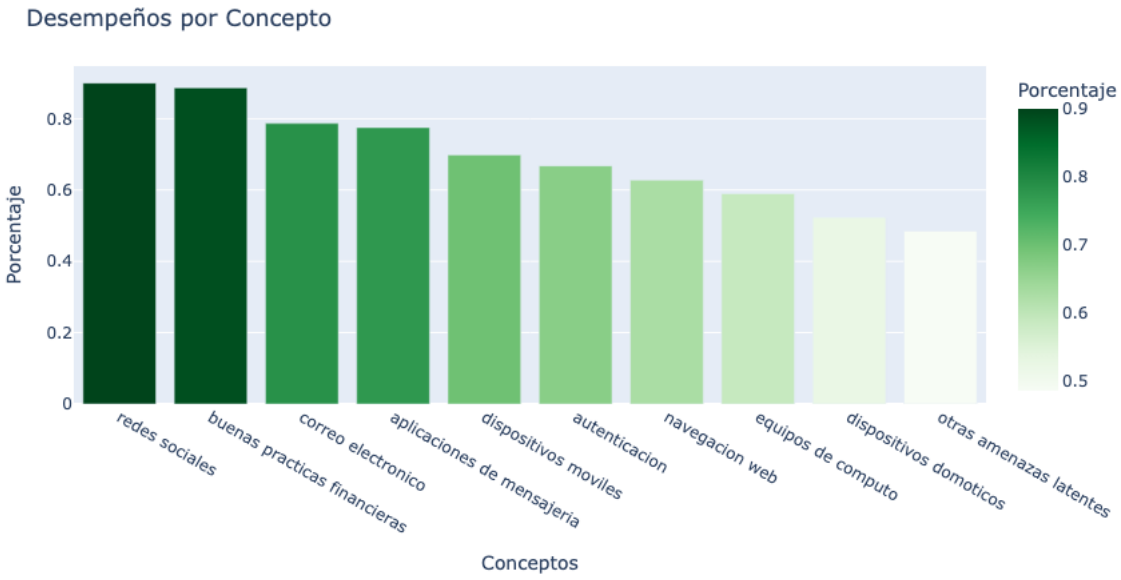
Para los conceptos de dispositivos móviles y autenticación se tiene una puntuación medianamente alta de 69.7% y 66.7% y para los conceptos de navegación web y equipos de cómputo se tiene una puntuación de conocimiento medio de 62.7% y 59.01%, en este mismo grupo, se tiene la categoría

ISSN: 2176-8501

sobre dispositivos domóticos, con una puntuación baja de 52.3%, este grupo se clasifica como "rebeldes flexibles".

Finalmente, el concepto con un desempeño inferior en conocimiento corresponde a otras amenazas latentes, lo cual incluye amenazas debidas a ingeniería social, puntuando 48.4%, tiene un nivel de madurez donde los colaboradores se clasifican como "examinadores tradicionales".

Figura 3. Desempeño por concepto medido en la encuesta.



Elaboración Autores.

Por niveles de ocupación en la subsecretaria de tesorería, se encuentran roles más fuertes en aspectos de seguridad de la información y más vulnerables. Tal como se ve en la figura 4, De acuerdo a las encuestas, los roles dentro de la organización con mayor desempeño son coordinador, tecnólogo y líder de programa, con desempeño mediano son profesional universitario, profesional de apoyo, auxiliar administrativo, secretario, líder de proyecto y profesional especializado. Finalmente, los roles con mayor vulnerabilidad son los técnicos administrativos.

Revista CONHECIMENTO ONLINE
ISSN: 2176-8501

Figura 4. Desempeño por rol medido en la encuesta.

Elaboración Autores.

3.2 ANÁLISIS DE CORRELACIONES

Al correlacionar el nivel de madurez, entiéndase grado de conocimiento y conciencia en seguridad de la información con el tiempo de servicio en años de los empleados, las pruebas estadísticas realizadas sobre el conjunto de datos concluyeron que los datos no siguen una distribución normal, dado que el resultado del test de Shapiro da como resultado de valor-p de 0.0018 en cuyo caso si el valor-p es menor a 0.05 indica no normalidad. Por otra parte, los valores p para la correlación de *Pearson* y *Spearman*, dan como resultado 0.173 y 0.361, estos valores indican que no hay correlación significativa entre las variables. Al calcular las pruebas de homogeneidad de la varianza de los datos, se encuentra que el valor-p de la prueba de Levene es igual a 0.527 indicando que las varianzas son iguales, es decir, hay homocedasticidad.

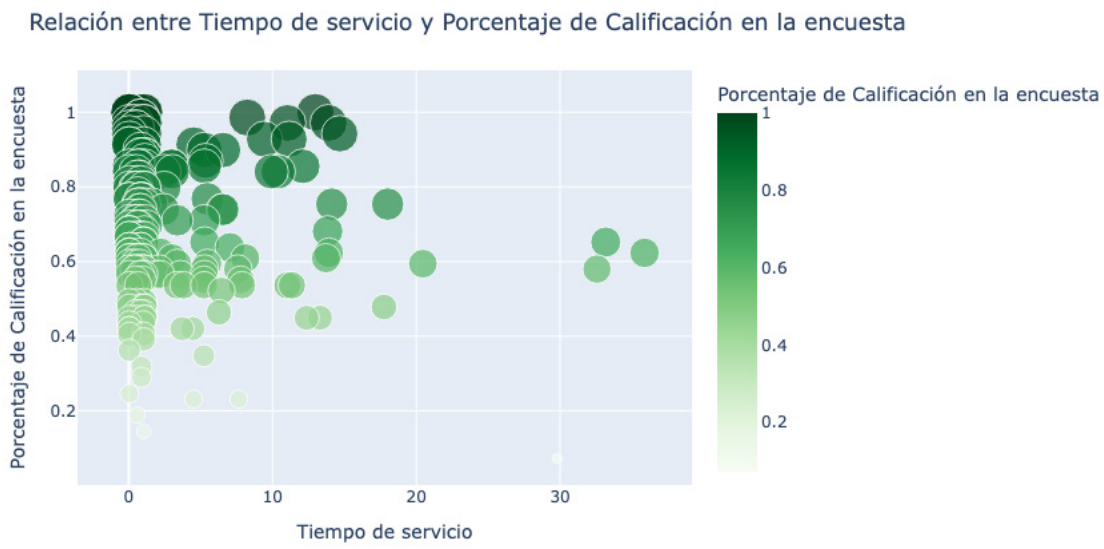
Para el caso del modelo de regresión generado para las variables mencionadas nivel de madurez y tiempo de servicio en años, el análisis de varianza muestra que el valor-p del tiempo de ocupación en años es igual a 0.173, lo cual indica que no hay un efecto significativo y el factor que acompaña a dicha variable tiene como resultado -0.0030, en cuyo caso, el signo negativo significa que el desempeño disminuye con el tiempo, este resultado concluye que no necesariamente tener un mayor tiempo de permanencia en la organización, garantiza un mayor conocimiento en seguridad de la información, este

ISSN: 2176-8501

resultado refuta lo mencionado por Baltuttis et al. (2024) donde su estudio encontró que los empleados mayores demuestran una alta resiliencia a la ciberseguridad, mientras que los más jóvenes presentan un mayor riesgo.

La figura 5 presenta dicha relación entre las variables analizadas en las encuestas en la organización.

Figura 5. Relación entre desempeño y tiempo de ocupación en la organización.

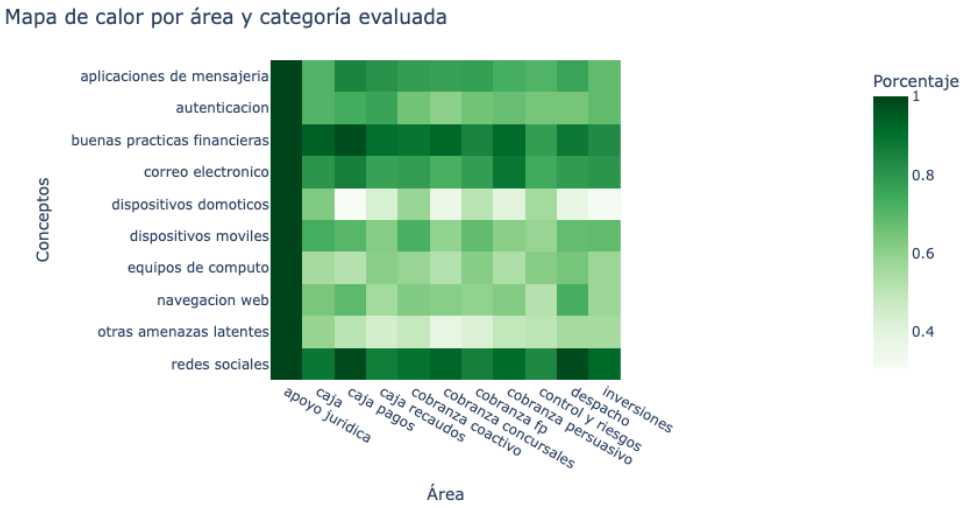


Elaboración Autores.

La figura 6 presenta el mapa de calor que relaciona las áreas de la organización y los conceptos evaluados en la encuesta, esto permite identificar por cada área cuales son los factores con mayor vulnerabilidad y cuales presentan mayor fortaleza. En general, para todas las áreas las redes sociales y las buenas prácticas financieras presentan mayores fortalezas. Por otro lado, los dispositivos domóticos y otras amenazas latentes presentan mayores vulnerabilidades en general para procesos de cobranzas. Por otro lado, se identifica que la área de apoyo jurídico muestra fortalezas transversales significativas en el manejo de la seguridad de la información, en menor medida los procesos de caja y pagos, y las más vulnerables son control y riesgos y cobranza concursales.

Revista CONHECIMENTO ONLINE
ISSN: 2176-8501

Figura 6. Mapa de calor entre áreas y conceptos medidos en la encuesta.



Elaboración Autores.

3.3ANÁLISIS PREDICTIVO

Se planteó un modelo supervisado de aprendizaje de máquina basado en regresión logística, para predecir la probabilidad de obtener una calificación de 1, como función de las variables: pregunta, área, conceptos, género, tiempo de ocupación, ocupación, profesión y tipo de contratación. Del modelo se excluyeron las variables nombre del empleado y la respuesta que tiene por categorías Si o No. En un primer momento se identificó la distribución de la variable respuesta del modelo, la cual es calificación, dando como resultados un 68.03% con valor 1 y 31.96% con valor 0, en un segundo momento se definen los porcentajes de datos de entrenamiento igual al 80% y de prueba igual a 20% para la preparación del modelo.

Una vez se ha entrenado el modelo de predicción, los resultados de la evaluación indican que el modelo de regresión logística muestra una exactitud del 74.74%, lo que indica que clasifica de manera correctamente la mayoría de los resultados, pero esta métrica debe analizarse en conjunto con la matriz de confusión presentada en la tabla 1 para una evaluación más detallada.

ISSN: 2176-8501

Tabla 1. Matriz de confusión del modelo de regresión logística.

Matriz de confusión	Valor predicho negativo	Valor predicho positivo
Valor actual negativo	TN=515	FP=491
Valor actual positivo	FN=304	TP=1837

Elaboración autores.

En la matriz de confusión, observamos 515 verdaderos negativos (TN) y 1837 verdaderos positivos (TP), lo que refleja un buen desempeño en la detección de la clase positiva. Sin embargo, los 491 falsos positivos (FP) reducen la precisión (78.91%), lo que significa que una proporción significativa de las instancias clasificadas como positivas son en realidad negativas. Por otro lado, el modelo tiene una métrica de *recall* alto (85.80%), ya que logra identificar la mayoría de los casos positivos, aunque a costa de algunos falsos positivos. La métrica F1 cuyo resultado es igualmente alto (82.21%) confirma un equilibrio adecuado entre precisión y *recall*. No obstante, la curva ROC cuyo resultado es igual a 0.685 indica que la capacidad del modelo para distinguir entre clases positiva y negativa aún es moderada, lo que sugiere un margen de mejora mediante ajustes en la selección de características, balanceo de clases o afinación del umbral de decisión para optimizar la separación entre categorías.

Al analizar el desempeño del modelo a la luz de las categorías de calificación se encuentra que el modelo de clasificación presenta una exactitud de 75%, lo que indica un desempeño general aceptable. Sin embargo, se observa un desequilibrio en el rendimiento entre las dos categorías de calificación. Para la categoría 0 (negativa), la precisión es de 63%, pero el *recall* es bajo (51%), lo que sugiere que el modelo tiene dificultades para identificar correctamente los casos negativos. En contraste, para la categoría 1 (positiva), el *recall* es alto (86%), lo que indica que la mayoría de los casos positivos son detectados correctamente, aunque con un nivel de precisión del 79%. Esto se refleja en la métrica F1, donde la categoría 1 obtiene un 82%, mientras que la categoría 0 solo alcanza 56%, mostrando un desempeño desigual. La media macro de precisión, *recall* y métrica F1 se mantiene en torno a 69%, lo que resalta este desequilibrio. En general, el modelo tiende a favorecer la clasificación de la categoría positiva, estos resultados pueden ser vistos en la tabla 2.

Tabla 2. Clasificación de categorías.

	Precisión	Recall	Métrica F1
Categoría 0	0.63	0.51	0.56
Categoría 1	0.79	0.86	0.82
Exactitud modelo			0.75
Media macro	0.71	0.68	0.69

Elaboración autores.

Revista CONHECIMENTO ONLINE
ISSN: 2176-8501

CONSIDERACIONES FINALES

De acuerdo a los resultados obtenidos, se debe fortalecer en varios frentes, en primer lugar y más importante aspecto encontrado y validado por la literatura implica implementar programas y campañas de capacitación y concientización en materia de ciberseguridad como practica exitosa (DE SILVA, 2023; RIZAL & SETIAWAN, 2024; MOSES et al., 2022; EFIJEMUE et al., 2023; MASHIZHA & KANENGONI, 2024) con mayor relevancia en el sector financiero (NIKANDER et al., 2020), así mismo evaluar y promover la cultura de la ciberseguridad (DE SILVA, 2023; GARCÍA et al., 2024) y fomentar el compromiso para mejorar la cultura de la ciberseguridad (DE SILVA, 2023).

Diversos autores reconocen la importancia de generar una cultura y compromiso de la seguridad de la información al interior de la organización, sin embargo es importante reconocer el papel de la estructura organizacional y su impacto en la promoción y generación de esa cultura, es así como Karlsson et al. (2022) propone que una forma burocrática de cultura organizacional es más efectiva para fomentar el cumplimiento, esta cultura se caracteriza por reglas y estructuras estandarizadas, con un fuerte énfasis en tareas laborales especializadas y gestión jerárquica. Las decisiones se toman en niveles superiores y se espera que los empleados las sigan. Esta cultura promueve la estabilidad y el control al momento de implementar cultura y compromiso con la seguridad de la información organizacional. Y tal como lo indica Maphosa (2023) para una adecuada cultura de la ciberseguridad, se debe invertir en tecnologías de ciberseguridad.

Por otro lado, un desafío identificado al promover programas de cultura de seguridad de la información es referido a la falta de entusiasmo y atención por parte de los empleados (PRÜMMER et al., 2024), esto implica articular estrategias de cultura con otras áreas o actores al interior de la organización, para cumplir los objetivos de cumplimiento, tales como garantizar que los empleados tengan las habilidades y experiencia necesarias en temas de ciberseguridad (AMAN & AL SHUKAILI, 2021), esto finalmente derivara en oportunidades de desarrollo profesional para mantenerse al día con el panorama cambiante de las amenazas cibernéticas.

Finalmente, las estrategias de cultura, concientización y promoción en seguridad de la información deben incluir programas de formación y capacitación especializada periódicos, esto deberá fomentar el aprendizaje continuo de los empleados y la formación (ANDREASSON et al., 2024) con el objetivo de reconocer y responder a las amenazas presentes y futuras proactivamente (AKINYELE & DANIEL, 2024).

La investigación llevada a cabo demostró que existen brechas al interior de la organización en diversas áreas y diversos aspectos medidos, al aplicar la metodología propuesta se espera en futuras

ISSN: 2176-8501

mediciones disminuir las brechas haciendo uso de diversas estrategias propuestas presentadas a lo largo de esta investigación.

Sin embargo, incorporar elementos adicionales en términos de medidas proactivas, colaboración y trabajo conjunto entre organizaciones y uso de tecnologías emergentes como analítica e inteligencia artificial, ayudarían en las labores de detección, identificación, mitigación y monitoreo de amenazas a la seguridad de la información.

CONFLICTO DE INTERÉS

Los autores no presentan conflicto de interés.

AGRADECIMIENTOS

Agradecemos al Señor Secretario de Hacienda del Distrito Especial de Ciencia, Tecnología e Innovación Orlando de Jesús Uribe Villa, por su apoyo en este proyecto.

REFERENCIAS

AKINYELE, D.; DANIEL, S. Building a culture of cybersecurity awareness in the financial sector. [S.l.], 2024.

AMAN, W.; AL SHUKAILI, J. A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. **International Journal of Advanced Computer Science and Applications**, [S.l.], v. 12, n. 8, p. 169–176, 2021.

ANDREASSON, A.; ARTMAN, H.; BRYNIELSSON, J.; FRANKE, U. Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. **Cognition, Technology and Work**, [S.l.], 2024.

BALTUTTIS, D.; TEUBNER, T.; ADAM, M. T. P. A typology of cybersecurity behavior among knowledge workers. **Computers and Security**, [S.l.], v. 140, p. 1–17, 2024.

ISSN: 2176-8501

BLESSING, M. Assessing Employee Awareness and Response to Phishing Attacks in Riyadh's Public and Private Sectors. [S.l.], 2024.

CHAUDHARY, S. Driving behaviour change with cybersecurity awareness. **Computers and Security**, [S.l.], v. 142, 2024.

DE SILVA, B. Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. **International Journal of Information Security and Cybercrime**, [S.l.], v. 12, n. 1, p. 23–29, 2023.

EFIJEMUE, O. et al. Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors. **International Journal on Soft Computing**, [S.l.], v. 14, n. 3, p. 01–16, 2023.

GARCÍA, J. F. et al. Examining cybersecurity culture in Leon city organizations: Insights from 2022. **Revista Chilena de Ingeniería**, [S.l.], v. 32, p. 11, 2024.

GVILAVA, Z. Strengthening Cybersecurity in American Emergency Services: Addressing Critical Vulnerabilities in the Public Safety Sector. [S.l.], 2023.

HOCHSTETTER-DIEZ, J. et al. AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. **Applied Sciences**, [S.l.], v. 13, n. 14, p. 8339, 2023.

HOFFMAN, F.; SKOVIRA, R. J. The Organizational Security Index: A Tool for Assessing the Impact of National Culture on Information Security Attitudes in Slovenia and the United States. **Issues in Information Systems**, [S.l.], v. 21, n. 3, p. 95–104, 2020.

IZURIETA, R. R. et al. Analysis of the Information Security of Public Organizations in Ecuador. 2021 **International Conference on Computational Science and Computational Intelligence** (CSCI), [S.l.], p. 823–829, 2021.

JEVTIĆ, N.; ALHUDAIDI, I. The importance of information security for organizations. **Serbian Journal of Engineering Management**, [S.l.], v. 8, n. 2, p. 48–53, 2023.

KARLSSON, M. et al. The effect of perceived organizational culture on employees' information security compliance. **Information and Computer Security**, [S.l.], v. 30, n. 3, p. 382–401, 2022.

ISSN: 2176-8501

LUBIS, M. et al. Navigating Online Privacy: Insights from Cybersecurity Expert. **Procedia Computer Science**, [S.l.], v. 234, p. 1388–1395, 2024.

MAPHOSA, V. An overview of cybersecurity in Zimbabwe's financial services sector. **F1000Research**, [S.l.], v. 12, p. 1251, 2023.

MASHIZHA, M.; KANENGONI, P. The Adequacy of Cybersecurity in Financial Institutions in Zimbabwe. **International Research Journal of Business Studies**, [S.l.], v. 17, n. 3, 2024.

MOSES, F.; SANDKUHL, K.; KEMMERICH, T. Information security management in German local government. **Communication Papers of the 17th Conference on Computer Science and Intelligence Systems**, [S.l.], v. 32, p. 183–189, 2022.

NASIRI, S. et al. Cybersecurity in Action: Unraveling the Effects of Individual, Social, and Organizational Determinants. **TEHNIČKI GLASNIK**, [S.l.], v. 20, n. 2, p. 1–10, 2024.

NIKANDER, J.; MANNINEN, O.; LAAJALAHTI, M. Requirements for cybersecurity in agricultural communication networks. **Computers and Electronics in Agriculture**, [S.l.], v. 179, p. 1–10, 2020.

OLEJNÍČEK, A. et al. Economic Aspects of Cybersecurity in the Public Sector. **ACTA STING**, [S.l.], v. 12, 2023.

OMAR, S. Z.; KOVALAN, K.; BOLONG, J. Effect of Age on Information Security Awareness Level among Young Internet Users in Malaysia. **International Journal of Academic Research in Business and Social Sciences**, [S.l.], v. 11, n. 19, 2021.

PRÜMMER, J.; VAN STEEN, T.; VAN DEN BERG, B. A systematic review of current cybersecurity training methods. **Computers and Security**, [S.l.], v. 136, p. 1–20, 2024.

RIZAL, M. A.; SETIAWAN, B. Information Security Awareness Literature Review: Focus Area for Measurement Instruments. **Procedia Computer Science**, [S.l.], v. 234, p. 1420–1427, 2024.

SAMARA, N. K. Cybersecurity Requirements for Management Information Systems. **Journal of Information Security**, [S.l.], v. 14, n. 3, p. 212–226, 2023.

ISSN: 2176-8501

YUNITA, A. Research Review on Measuring Information Security Awareness. **Journal of Science and Informatics for Society (JSIS)**, [S.l.], v. 1, n. 2, 2023.

ZAMMANI, M.; RAZALI, R. An empirical study of information security management success factors. **International Journal on Advanced Science, Engineering and Information Technology**, [S.l.], v. 6, n. 6, p. 904–913, 2016.

ZAMMANI, M.; RAZALI, R.; SINGH, D. Organisational Information Security Management Maturity Model. **International Journal of Advanced Computer Science and Applications**, [S.l.], v. 12, n. 9, 2024.