UCT
UNIVERSIDAD CATÓLICA DE TRUJILLO

REVISTA CIENTÍFICA
YACHAQ

Ciberseguridad y calidad de vida digital en una empresa de Trujillo

Cybersecurity and digital quality of life in a Trujillo company

Alexis Enrique Poma Vargas [1]
Universidad Católica de Trujillo Benedicto XVI
Trujillo– Perú
Carmen Liliana Huamán Gonzales[2]
Newmont Yanacocha-Minera Yanacocha SRL
Cajamarca– Perú

Recibido: 20/01/2023
Aceptado: 01/06/2023

DOI https://doi.org/10.46363/yachaq.v6i2.4

RESUMEN

Este articulo tiene como objetivo principal, determinar en qué medida la ciberseguridad permite el desarrollo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022.; además, objetivos específicos como: verificar que exista una gestión de riesgos que permita identificar los riesgos y mitigarlos; asimismo, evaluar si se obtienen excelentes beneficios con la mitigación de riesgos de acuerdo con las evaluaciones establecidas. La metodología es no experimental, mixta y descriptiva; se utilizó la estadística descriptiva e inferencial; asimismo, contó con dimensiones e indicadores de variables; así como, aplicación de instrumen-

1ORCID 0000-0001-5061-7760. Docente de la Universidad Católica de Trujillo Benedicto XVI. contaepv1108@gmail.com

2 ORCID 0000-0001-9768-2498. Jefa del Área de Bienestar Social y Calidad de Vida. Newmont Yanacocha. lilianagonzales425@gmail.com

tos según las técnicas, como el cuestionario y guía de entrevista, aplicados a una población y muestra de treinta y cinco colaboradores; también, aplicación de matrices tanto de TIC, como Gestión de Riesgos en Ciberseguridad y Calidad de Vida Digital, para detectar riesgos presentados en la institución en relación a vulnerabilidad de protección de datos. Al respecto, según los resultados obtenidos, se evidenció que existen ataques cibernéticos a empresas a nivel internacional, nacional y local; no siendo la empresa Jama Café –Restaurant, la excepción; asimismo, existe un destaque en ciberseguridad, con 42.86% en integridad de información; en relación a calidad de vida digital en 42.86% correspondiente a asequibilidad del Servicio de Internet, existiendo una protección en cuanto a la información de datos informáticos en la empresa; así como, la aplicación de medidas correctivas en forma oportuna en el caso de presentarse riesgos con la finalidad de mitigarlos.

PALABRAS CLAVE: Sistemas Informáticos; Hackers; Protección de datos.

ABSTRACTS

The main objective of this article is to determine to what extent cybersecurity allows the development of an optimal digital quality of life in the company Jama-Café Restaurant, period 2022.; In addition, specific objectives such as: verify that there is risk management that allows risks to be identified and mitigated; likewise, evaluate if excellent benefits are obtained with the mitigation of risks according to the established evaluations. The methodology is non-experimental, mixed and descriptive; descriptive and inferential statistics were used; likewise, it had dimensions and indicators of variables; as well as, application of instruments according to the techniques, such as the questionnaire and interview guide, applied to a population and sample of thirty-five collaborators; Also, application of ICT matrices, such as Cybersecurity Risk Management and Digital Quality of Life, to detect risks presented in the institution in relation to data protection vulnerability. In this regard, according to the results obtained, it was evidenced that there are cyber attacks on companies at an international, national and local level; not being the company Jama Café -Restaurant, the exception; Likewise, there is a highlight in cybersecurity, with 42.86% in integrity of information; in relation to quality of digital life in 42.86% corresponding to affordability of the Internet Service, there is protection regarding the information of computer data in the company; as well as the application of corrective measures in a timely manner in the event of risks with the purpose of mitigating them.

KEY WORDS: Computer Systems; Hackers; Data Protection.

INTRODUCCIÓN

En la actualidad, el concepto de ciberseguridad se ha vuelto un boom a nivel internacional, y es que las empresas han optado por asegurar sus sistemas en contra de los ataques cibernéticos; por lo que es considerada, como uno de los desafíos más importantes de la era digital. El crecimiento global de las redes y la información, impulsado por la innovación tecnológica, ha permitido a la sociedad crear prosperidad y mejorar la calidad de vida.

Al respecto, la ciberseguridad cuenta con cinco dimensiones, siendo estas: Integridad de información, disponibilidad de información, autenticidad, trazabilidad y acceso de datos. En este contexto, Perú ha conseguido subir este 2021 cuatro (4) puestos, lográndose constatar que mejoró en ciberseguridad, posicionándose en el puesto 67 a nivel global en este aspecto.

Por otro lado, el referirse a calidad de vida digital, se considera a un término que determina el bienestar digital correspondiente a las personas o denominados ciudadanos de un territorio a lo cual se refleja en función de cinco (5) aspectos de mayor relevancia, tal como lo indica RPP (2021). En este contexto, internet es ahora parte de muchas vidas a nivel mundial, usado por muchas empresas. Es por ello que, los usuarios pasan en promedio de siete (7) horas conectado, como consecuencia de sus compromisos laborales y tras la llegada del teletrabajo debido a la pandemia o; del mismo modo, teniendo en cuenta las aficiones a las redes sociales, cuya oferta amplia el entorno virtual y más que todo la información digitalizada, que permite atraer a las personas sobre un producto o servicio. Es por ello que, existen cinco (5) aspectos que definen la calidad de vida digital, los cuales son: Accesibilidad a Internet, Infraestructura electrónica, Calidad de Internet, Digitalización del servicio público y Seguridad electrónica.

Al respecto, el Perú se encuentra situado en uno de los más bajos puestos de Sudamérica en el Índice de Calidad de Vida Digital, elaborado por Surfshark. Es de indicar que, se encuentra en el (7) sétimo puesto de (9) nueve países quienes han sido analizados en la región (Venezuela no participa), figurando en el puesto 68 a nivel mundial, dentro de un total de 110 países los cuales han sido evaluados.

Además, si se habla del Índice de Calidad de Vida Digital; se considera (5) cinco pilares, siendo estos: asequibilidad del servicio de Internet, calidad de internet, infraestructura digital, ciberseguridad y gobierno digital.

En merito a ello, el presente trabajo se justifica desde el punto de vista de la seguridad de datos, a través del cual se

pretende, resguardar la información en cuanto a aspectos financieros, administrativos, marketing, entre otros.

Desde el punto de vista Empresarial, por cuanto se pretende evidenciar que los sistemas informáticos de resguardo como cámaras de seguridad, son necesarias en la medida de detección de infiltraciones presenciales en la empresa, a fin de introducir algún elemento infeccioso en las computadoras.

Existen antecedentes de trabajos de investigación que avalan el presente trabajo, tales como:

Según Vilcarromero y Vílchez (2018) en su tesis de Maestría en Gestión Pública titulada Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones, indicaron que el objetivo principal, fue el de Proveer al área del SOC, un marco de ciberseguridad para generar una solución que le permita implantar, operar, monitorear, revisar y mejorar los controles de ciberseguridad, con el fin de ser un SOC de referencia y llegar a ser competitivo en el mercado. Al respecto, se tiene que Seguridad de la Información, es el término más utilizado en los últimos tiempos ya que la información se considera como un activo que brinda valor al negocio; por lo que se necesitan tener un adecuado manejo para protegerla frente a las amenazas y vulnerabilidades que está expuesta, tal como lo señala Themelis y Ann Sime (2019). La información puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente. (Gestión, 2019).

Jama-Café Restaurant, es una empresa dirigida a la preparación y comercialización de variedades de alimentos gastronómicos, el cual tiene como dispositivos de pago: Yape, paypal, cuentas bancarias y efectivo. Al respecto, existe una problemática la cual es controlar que dichos dispositivos, sean seguros con la finalidad de que no existan sustracciones de dinero a través de transferencias ilegales, que perjudiquen los ingresos del restaurante. Asimismo, es el proteger las transferencias de dinero que, se realizan a través de los citados medios, por cuanto en muchas ocasiones, pueden existir infecciones de virus o extracción de información a través de ataques cibernéticos. Por este motivo, la calidad de vida digital se ve reflejada en la medida que tanto el colaborador como el cliente, se sientan seguros de que las transacciones e información financiera que se tenga a la fecha, no tenga ninguna variante y es más que, no haya tenido manipulación alguna por softwares dañinos, que intervengan en algún momento para extraer datos económicos de la empresa Jama.

En este sentido, Andina (2018), Akamai (2019) y Cepal (2022), quienes afirman

que, es necesario la incorporación de las dimensiones dentro de una herramienta de análisis de riesgos que permitan de esta manera asegurar el rendimiento económico de una empresa a través de la protección de datos digitales e información, en este caso lo aplicó Jama, dando la seguridad de que exista medios de pagos seguros a través de las redes y de mecanismos de control seguros.

El presente trabajo se justifica desde el ámbito de la ciberseguridad Cepal (2022) porque va a permitir que las herramientas de control de riesgos sean capaces de ser aplicadas, con la finalidad de obtener resultados, para que el restaurante este protegido contra ciberataques de cualquier naturaleza.

En este sentido su objetivo principal es determinar en qué medida la ciberseguridad permite el desarrollo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022. Objetivos específicos tales como: verificar que exista una gestión de riesgos que permita identificar los riesgos y mitigarlos en su momento, en los sistemas informáticos; asimismo, evaluar si la ciberseguridad y la calidad de vida digital obtienen excelentes beneficios con la mitigación de riesgos de acuerdo a las evaluaciones establecidas.

Se consideró la teoría de la Cibernética, a través del cual Mena (2022), indicó que la seguridad de la información y la utilización de las tecnologías permite un avance significativo en el desarrollo de la potencialidad de ejecución de los trabajos efectuados en las empresas, en el contexto que su aplicación permitirá la confianza de contar en todo momento con elementos ayuden a fomentar el control tecnológico y con ello la investigación sobre aspectos riesgosos que puedan aparecer.

Al respecto, según El Peruano (2019) y Colsof (2022) el paradigma de la ciberseguridad se acrecentará a medida que pasa al tiempo lo que a su vez hará que sus exigencias sean más rigurosas y complejas. Es decir que se vincula con la cultura de los datos, lo que hará que la estrategia de negocio en ciberseguridad sea un primordial plan de acción de ahora en adelante para toda gran empresa (VASS, 2021), en este sentido Jama –Café Restaurant trata de incorporar un mecanismo de seguridad a través de softwares sofisticados con la compra de licencias, motivo por el cual el problema indicado deberá ser evaluado a través de sus respectivas tomas de decisiones y de la revisión de dichos sistemas de seguridad; a fin de controlar las transacciones financieras.

Según Poggy, N. (2019), Martínez (2020), León, J. Á. Q. (2021), León et al. (2022), En el caso de la doctrina, la Ciberseguridad desde el punto de vista doctrinal y estratégico según lo estable-

ce Poma, A. y Vargas, R. (2019) y Martin, L. (2021) y Berdud, Chacón y Martinelli (2021) puede ser protectiva, correctiva, disuasoria, preventiva y prospectiva, la adopción de una forma progresiva de estas doctrinas genéricas, supone un impacto en la organización de los recursos en forma de sistemas y en las estructuras, planes, misiones y perfiles de las organizaciones de Ciberseguridad de las empresas y los gobiernos; por tanto Jama-Café restaurant toma la opción de ingresar al paradigma de la Globalización.

Al respecto se ha considerado la siguiente hipótesis de investigación: La ciberseguridad permite el desarrollo significativo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022; asimismo la hipótesis nula: la ciberseguridad no permite el desarrollo significativo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022

METODOLOGÍA

El estudio es de diseño no experimental y descriptivo; así como, enfoque mixto, en este sentido, Sampieri (2018) indica que, dichos estudios son bastantes útiles para estudiar cómo se manifiestan los fenómenos y sus respectivos componentes. Se utilizó las técnicas de la encuesta, la entrevista y análisis documentario, con la finalidad de recolectar información a través del cuestionario, la guía de entrevista, ficha electrónica y documentación de la propia empresa, respectivamente.

El método utilizado para esta investigación fue el hipotético deductivo, a través del cual se define como el razonamiento que combina la reflexión racional con la observación de la realidad; en otras palabras, es aquel que parte de una hipótesis, la cual es sustentada, por el desarrollo teórico de una determinada ciencia que, por lo tanto, siguiendo las reglas lógicas de la deducción, se encarga de permitir llegar a nuevas conclusiones y predicciones empíricas; entonces, a su vez son sometidas a verificación. Es tipo aplicada y práctica, en el sentido que, se justificó por la atención a la elaboración de los instrumentos y se determinó la ejecución de ellos en el trabajo de campo. (Sampieri, 2018).

Con relación a la Población y Muestra (ver tabla 1) se ha considerado al personal de Jama-Café Restaurant el cual consta de treinta y cinco (35) trabajadores; a los cuales se les ha aplicado preguntas a través de la técnica de la encuesta, cuyo instrumento es el cuestionario; a fin de que indiquen según su experiencia, cómo se desarrolla los procedimientos de aplicación de ciberseguridad y calidad de vida digital en la empresa.

Asimismo, se ha aplicado la técnica de la entrevista con su instrumento guía de entrevista a los treinta y cinco (35) colaboradores, quienes también proporcionan información respecto a estas variables, con la finalidad de contrastar si efectivamente dichos procedimientos cumplen con la protección de los datos informáticos y económicos en la empresa Jama-Café Restaurant.

Se revisó material documentario de la empresa y de esta forma el material bibliográfico correspondientes a fuentes confiables como son las revistas, periódicos digitales y reportes anuales. Por otro lado, se utilizó la ficha electrónica lecturas, para extraer resúmenes de las citadas fuentes, relacionadas al tema de ciberseguridad y calidad de vida digital. Se contó con la información proporcionada por la web de Kaspersky (2022), quien cuenta con datos actualizados a la primera semana de octubre del 2022.

Autores como Pontifica Universidad Javeriana (2022), UNESCO (2022), Smartsheet (2022) y Kaspersky (2022) consideran unas dimensiones mejor estructuradas dentro de una herramienta de gestión empresarial cuya denominación es Gestión de Riesgos de seguridad de la información para empresas, o como se les denominaría en otras palabras Matriz de Gestión de Riesgos en Ciberseguridad y Calidad de Vida Digital, tales dimensiones se describen a continuación: Gestión y Planificación en Ciberseguridad, Ciberseguridad en las TIC en el desarrollo empresarial, Desarrollo Técnico y Profesional, Cultura Digital, Recursos e Infraestructura TIC; así como, Calidad de vida digital en Empresa y Sociedad.

En relación a los métodos estadísticos, se pudo validar los cuestionarios de ciberseguridad y calidad de vida digital, con el apoyo de 5 expertos en la materia; así como, determinar una confiabilidad de los instrumentos cuestionarios con un Alfa de Cronbach de 0.98 para la variable independiente; así como, un valor de 0.96 en lo correspondiente a la variable dependiente, lo que implicó un nivel de excelencia en relación a la elaboración de los Ítems de los citados cuestionarios de las variables del informe motivo del estudio. (Javeriana, 2022).

Del mismo modo, se validó por los citados expertos las guías de entrevista, con la finalidad de que se aplique a los colaboradores que conformaron la muestra.

También se utilizó Matriz de TIC Ciberseguridad y Calidad de Vida Digital de la empresa Jama-Café Restaurant con la finalidad de identificar los niveles de manejo de las herramientas de ciberseguridad y calidad de vida digital en la empresa.

Al respecto, se puedo evidenciar que, a través de esta investigación, se consiguió proporcionar información suficiente, lo cual también servirá para futuras investigaciones.

Para finalizar, se utilizó como métodos estadísticos, el proceso de recolección de datos, presentación a través de tablas, síntesis y análisis de datos con la finalidad de obtener un nuevo conocimiento de lo que se está investigando; tal como, lo señala Smartsheet (2022); lo que dio lugar a su justificación a través del manejo de datos cuantitativos y cualitativos a la vez, según lo establecido por el citado autor Smartsheet (2022).

Tabla 1

Distribución de la Población y Muestra de Colaboradores correspondiente a la empresa Jama Café Restaurant, Período 2022.

Colaboradores			
Cargo	**Hombres**	**Mujeres**	**Total**
Empleados	17	16	33
Administrador	0	1	1
Gerente	1	0	1
Total	**18**	**17**	**35**

Nota. *El citado cuadro representa la cantidad de colaboradores de la empresa Jama-Café Restaurant.*

Fuente. Staffing Plan o Manual de Organización y Funciones del Restaurant aprobado en el periodo 2022.

RESULTADOS

Según los resultados obtenidos en la presente investigación y de acuerdo con el objetivo general, el cual es determinar en qué medida la ciberseguridad permite el desarrollo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022, se ha podido identificar hechos que a través de la aplicación de los cuestionarios respectivos; así como, del diagnóstico que se presentó como respuesta al análisis documental entregado por parte de la empresa.

Es de precisar que, se ha efectuado un óptimo tratamiento estadístico de la información; puesto que, al aplicarse las técnicas e instrumentos requeridos para la presente investigación, ha permitido de esta forma mostrar a los interesados en investigación los procedimientos necesarios a realizarse para la obtención de los resultados esperados, a través de tablas y figuras.

Al respecto, tomando como herramienta de investigación el uso de la plataforma de Kapersky (2022), se pudo determinar que:

El ataque cibernético a nivel internacional se ve reflejado conforme a la siguiente tabla:

Tabla 2
Virus generadores de ataques cibernéticos a nivel internacional en empresas

Arriba-On Access Scan VIRUS	En la última semana PORCENTAJE (%)
Dangeruos 0bject .Multi.Generic	9.97%
Trojan.WinLINK.Agent.gen	3.34%
Trojan.Win32.Agent.gen	3.16%
Trojan.Win32.Agentb.bqvr	2.59%
Trojan.Script.Generic	2.39%
Worm.Python.Agent.gen	2.13%
Worm.Python.Agent.c	2.02%
Trojan.Win32.AutoRun.gen	1.86%
Virus.Win32.Pioneer.cz	1.79%
Trojan.Win32.Miner.bcbma	1.61%

Nota: Se evidencia los virus más letales que han atacado a 25 de noviembre de 2022, a los sistemas informáticos de las empresas distribuidas en el mundo.

De la información presentada en la tabla 2, el 9.97% de los ataques cibernéticos a nivel mundial ha sido efectuado por el virus Dangeruos 0bject. Multi.Generic, siguiéndole los virus Trojan.WinLINK.Agent.gen con un 3.34% y Trojan.Win32.Agent.gen con un 3.16%; siendo muy significativos en relación a los toros virus que se verifican en la citada tabla.

Al respecto, Los países más atacados por a nivel mundial según la información proporcionada por Kapersky (2022) se muestra en la siguiente tabla 3:

Tabla 3
Países mayormente atacados cibernéticamente a nivel mundial

PAÍS	PORCENTAJE (%)
Afganistán	9.22%
Algeria	8.32%
Burundi	8.27%
Benín	8.16%
Ruanda	7.93%
Guinea-Bisáu	7.88%
Guinea Ecuatorial	7.76%
Togo	7.76%
Chad	7.56%
Camerún	7.55%
Birmania	7. 54%
República Democrática del Congo	7.41%
República Centroafricana	7.40%
Turkmenistán	7.37%
Bangladés	7.31%

Nota: Se evidencia los países internacionales más atacados al 25 de noviembre de 2022, a los sistemas informáticos de las empresas distribuidas en el mundo.

De la información presentada en la tabla 3, los países de Afganistán 9.22%, Algeria 8.32%, Burundi 8.27% y Benín 8.16% son los más atacados cibernéticamente a nivel mundial, siguiéndole los demás países con un porcentaje significativo.

Países de América del Sur mayormente atacados cibernéticamente se muestran en la siguiente tabla:

Tabla 4
Países de América del Sur donde las empresas con mayormente atacadas cibernéticamente

Países de América del Sur	Porcentaje (%)
Bolivia	3.85%
Venezuela	3.74%
Brasil	3.02%
Uruguay	3.02%
Perú	3.02%

Nota: Se evidencia los países de América del Sur más atacados al 25 de noviembre de 2022, a los sistemas informáticos de las empresas distribuidas en el mundo.

De la información presentada en la tabla 4, los países de Bolivia 3.85%, Venezuela 3.74%, Brasil 3.02%, Uruguay 3.02% y Perú 3.02%, son los más atacados en América del Sur.

Para cumplir con la evaluación del objetivo general, se aplicó el cuestionario a los trabajadores de Jama-Café Restaurant, evidenciándose los siguientes resultados:

Tabla 5
Problemas más frecuentes que afectan los sistemas informáticos de la empresa Jama-Café Restaurant

Amenazas	Muestra	Porcentaje (%)
Troyanos o caballos de Troya. Bankers o troyanos bancarios, Backdoors o puertos traseros, Keyloggers o capturadores de pulsaciones, Dialers o marcadores telefónicos, Rogueware.	8	22,86%
Adware o software publicitario	4	11,43%
Herramientas de intrusión.	4	11,43%
Virus	6	17,14%
Archivos sospechosos detectados heurísticamente, Técnica empleada por los antivirus para reconocer códigos maliciosos que no se encuentran en la base de datos de virus del antivirus.	5	14,29%
Spyware o programas espía.	2	5,71%
Gusano o worm	2	5,71%
Otros. Exploit, Rootkits, Scripts, Lackers o Scareware, Jakes o bromas.	4	11,43%
Total	**35**	**100,00%**

Nota: Se reflejan las respuestas indicadas por los colaboradores de la citada empresa, sobre los virus informáticos que más hayan atacado a los sistemas informativos de la empresa Jama-Café Restaurant.

Según tabla 5, el conocimiento en ciberseguridad y calidad de vida digital, por parte de los colaboradores de la citada empresa, indican que el mayor número de problemas cibernéticos a los sistemas informáticos en la empresa, son los Troyanos o caballos de Troya. Bankers o troyanos bancarios, *Backdoors o puertos traseros,* Keyloggers o capturadores de pulsaciones, Dialers o marcadores telefónicos, Rogueware con un 22,86%; así como, la generalización de virus que cubren un 17.14%, del mismo modo, la técnica empleada por los antivirus para reconocer códigos maliciosos que no se encuentran en la base de datos de virus del antivirus que asciende a un 14,29%; siendo los porcentajes más elevados en la citada tabla.

Tabla 6
Estrategias para evitar los ciberataques a través de la ciberseguridad y tener una calidad de vida digital óptima.

Ítem	Muestra	Porcentaje (%)
Nunca dar información confidencial por Internet	10	28,57%
No instales programas si desconoces el fabricante	6	17,14%
Evita conectarte a redes no autorizadas	7	20,00%
Crea contraseñas difíciles de adivinar	8	22,86%
Utiliza un antivirus y un cortafuego.	4	11,43%
Total	**35**	**100,00%**

Nota: Se reflejan las respuestas indicadas por los colaboradores de la citada empresa, sobre los virus informáticos que más hayan atacado a los sistemas informativos de la empresa Jama-Café Restaurant.

Según la tabla 6, se puede evidenciar que las estrategias para evitar los ciberataques son Nunca dar información confidencial por Internet 28.57%, No instales programas si desconoces el fabricante 17.14%, Evita conectarte a redes no autorizadas 20,00%, Crea contraseñas difíciles de adivinar 22.86% y Utiliza un antivirus y un cortafuego 11.43%.

Tabla 7
Funcionalidad de dimensiones de variable independiente Ciberseguridad por prioridad.

Dimensiones	Muestra	Porcentaje (%)
Integridad de Información	15	42,86%
Disponibilidad de Información	5	14,29%
Autenticidad	3	8,57%
Trazabilidad	2	5,71%
Acceso de Datos.	10	28,57%
Total	**35**	**100,00%**

Nota: Se reflejan las dimensiones indicadas correspondientes a Ciberseguridad, por prioridad de la empresa Jama-Café Restaurant.
Fuente Cuestionario de Ciberseguridad.

Según la tabla 7, La funcionalidad por prioridad de las dimensiones de la variable indica que, Integridad de Información es de 42.86%, Disponibilidad de Información es de 14.29%, Autenticidad es de 8.57%, Trazabilidad es de 5.71% y Acceso de Datos es de 28.57%.

Tabla 8
Funcionalidad de dimensiones de variable dependiente Calidad de Vida por prioridad.

Dimensiones	Muestra	Porcentaje (%)
Asequibilidad del servicio de Internet	15	42,86%
Calidad de internet	10	28,57%
Infraestructura digital	4	11,43%
Ciberseguridad	2	5,71%
Gobierno digital.	4	11,43%
Total	**35**	**100,00%**

Nota: Se reflejan las dimensiones indicadas correspondientes a Calidad de Vida, por prioridad de la empresa Jama-Café Restaurant.
Fuente Cuestionario de Calidad de Vida Digital.

Según la tabla 8, La funcionalidad por prioridad de las dimensiones de la variable indica que, Asequibilidad del servicio de Internet es de 42.86%, Calidad de internet es de 28.57%, Infraestructura digital es de 11.43%, Ciberseguridad es de 5.71%, y Gobierno digital es de 11.43%

Tabla 9
Medios de pago permitidos en Jama-Café Restaurant con protección a través de Ciberseguridad

Dimensiones	Muestra	Porcentaje (%)
Pagos a través de trasferencias bancarias por la banca móvil	8	22.86%
Uso de las tarjetas de débito con chip y uso de PIN	8	22.86%
Uso de tarjeta de crédito con el uso del DNI	9	25,71%
Efectivo	10	28,57%
Total	**35**	**100,00%**

Nota: Se reflejan los medios de pagos a utilizar en la empresa Jama-Café Restaurant por parte de los clientes para consumo.

Según la tabla 9, los medios de pago que se utilizan y que están expuestos a la Ciberseguridad son por pagos a través de trasferencias bancarias por la banca móvil 22.86%, el uso de las tarjetas de débito con chip 22.86% y crédito con el uso del DNI 25.71% y efectivo 28.57%.

Tabla 10
Matriz de TIC en Ciberseguridad y Calidad de Vida Digital aplicado en Jama-Café Restaurant

Dimensión	Indicadores	Puntajes	Nivel	Puntaje de Matriz
Gestión y Planificación en Ciberseguridad	Visión en ciberseguridad	50	Intermedio	
	Planificación en ciberseguridad	52	Intermedio	
	Integración de tecnologías	50	Intermedio	
	Coordinación en ciberseguridad	80	Intermedio	
	Recursos y Equipamiento	82	Avanzado	
	Política de uso	60	Intermedio	**Puntaje en Indicadores**
Total puntaje		**374**	**Básico**	**Nivel**
Ciberseguridad en las TIC en el desarrollo empresarial	Grado de Integración en seguridad	40	Básico	**Básico: 01-40**
	Transversalidad en detección de virus	40	Básico	**Intermedio: 41-80**
	Tipos de herramientas digitales	50	Intermedio	**Avanzado: 81-100**
	Colaboración en detección de riesgos	52	Intermedio	
	Procesos de vigilancia de datos	56	Intermedio	**Puntaje en Dimensiones**
Total puntaje		**238**	**Básico**	**Nivel**
Desarrollo Técnico y Profesional	Niveles de formación digital en ciberseguridad	50	Intermedio	**Básico: 01-400**
	Oferta de formación permanente	60	Intermedio	**Intermedio: 401-800**
	Redes y colaboración digital	60	Intermedio	**Avanzado: 801-1000**
	Confianza en el uso de las TIC	70	Intermedio	
	Apropiación de los recursos web	60	Intermedio	
	Demanda de desarrollo profesional	80	Intermedio	
Total puntaje		**380**	**Básico**	
Cultura Digital	Acceso de los medios virtuales	60	Intermedio	
	Acceso de personal confiable	70	Intermedio	
	Espacio institucional en la Web	81	Avanzado	
	Participación en comunidades virtuales	82	Avanzado	

Cultura Digital	Colaboración entre trabajadores	60	Intermedio	
	Actitud hacia las TIC	80	Intermedio	
Total puntaje		**433**	**Intermedio**	
Recursos e Infraestructura TIC	Localización	81	Avanzado	**Puntaje General**
	Intranet	82	Avanzado	
	Soporte técnico	90	Avanzado	**Básico:**
	Internet	90	Avanzado	**01-400**
	Software y contenidos digitales	80	Intermedio	**Intermedio:**
	Variedad de dispositivos	81	Avanzado	**401-800**
	Actualización del equipamiento	81	Avanzado	**Avanzado:**
Total puntaje		**585**	**Intermedio**	**801-1000**
Calidad de vida digital en Empresa y Sociedad	Participación en el diseño e implementación de TIC	82	Avanzado	
	Acceso	82	Avanzado	
	Actores involucrados	83	Avanzado	
	Alfabetización digital comunitaria	90	Avanzado	
	Apoyo de la comunidad hacia la empresa.	90	Avanzado	
Total puntaje		**427**	**Intermedio**	
TOTAL PUNTAJE Y NIVEL GENERAL SEGÚN LA MATRIZ		**402**	**INTERMEDIO**	

Nota: Se reflejan las dimensiones correspondientes a la Matriz de TIC de Ciberseguridad y Calidad de Vida, por prioridad de la empresa Jama-Café Restaurant.

De la tabla 10, correspondiente a la Matriz de TIC en Ciberseguridad y Calidad de Vida Digital aplicado en Jama-Café Restaurant, se puede identificar que existen seis (6) dimensiones siendo los niveles siguientes: Gestión y Planificación en Ciberseguridad de básico, Ciberseguridad en las TIC en el desarrollo empresarial de básico, Desarrollo Técnico y Profesional de básico de intermedio, Cultura Digital de intermedio, Recursos e Infraestructura TIC de intermedio; así como, Calidad de vida digital en Empresa y Sociedad de intermedio.

Al respecto como nivel general de la Matriz aplicado a la empresa se ha obtenido un nivel Intermedio, con un puntaje de 402, según lo indica la citada tabla.
En ese sentido, se ha podido responder al objetivo específico 1, el cual es verificar que exista una gestión de riesgos que permita identificar los riesgos y mitigarlos en su momento, en los sistemas informáticos, de acuerdo con el siguiente detalle:

Figura 1.
Matriz de Riesgos Ciberseguridad y Calidad de Vida Digital de la Empresa Jama-Café Restaurant

1. Información de fondo			
Lugar de trabajo:	Jama Café-Restaurant	**La fecha:**	09/11/2022
Título de la evaluación:	**Evaluación de riesgos en Ciberseguridad y Calidad de Vida Digital de la Empresa Jama-Café Restaurant**	**Nombre de la persona que realiza la evaluación:**	Adm. Wilmer Saldaña Canales Dr. Alexis Enrique Poma Vargas

2. Evaluación de riesgos						
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Consecuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*
Gestión y Planificación en Ciberseguridad						
1	Visión en ciberseguridad	Integridad de Información	1	Insignificante	Raro	Control de ingresos a través de plataforma en estado de cuenta.
2	Planificación en ciberseguridad	Disponibilidad de Información,	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.
3	Integración de tecnologías	Autenticidad	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
4	Coordinación en ciberseguridad	Trazabilidad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.
5	Recursos y Equipamiento	Acceso de Datos.	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
6	Política de uso	Integridad de Información	1	Insignificante	Raro	Se han implantado políticas los cuales son de carácter obligatorio sobre uso de tecnología
Ciberseguridad en las TIC en el desarrollo empresarial						
7	Grado de Integración en seguridad	Integridad de Información	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.
8	Transversalidad en detección de virus	Disponibilidad de Información,	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.

2. Evaluación de riesgos						
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Consecuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*
9	Tipos de herramientas digitales	Autenticidad	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.
10	Colaboración en detección de riesgos	Trazabilidad	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes
11	Procesos de vigilancia de datos	Asequibilidad del servicio de Internet	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
Desarrollo Técnico y Profesional						
12	Niveles de formación digital en ciberseguridad	Calidad de internet	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.
13	Oferta de formación permanente	Infraestructura digital	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
14	Redes y colaboración digital	Ciberseguridad	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.
15	Confianza en el uso de las TIC	Gobierno digital.	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
16	Apropiación de los recursos web	Asequibilidad del servicio de Internet	5	Severo	Casi Seguro	Selección y vigilancia de información a través de niveles.
17	Demanda de desarrollo profesional	Calidad de internet	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
Cultura Digital						
18	Acceso de los medios virtuales	Infraestructura digital	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.

2. Evaluación de riesgos						
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Consecuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*
19	Acceso de personal confiable	Ciberseguridad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.
20	Espacio institucional en la Web	Gobierno digital.	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
21	Participación en comunidades virtuales	Integridad de Información	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
22	Colaboración entre trabajadores	Disponibilidad de Información,	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
23	Actitud hacia las TIC	Autenticidad	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
Recursos e Infraestructura TIC						
24	Localización	Trazabilidad	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
25	Intranet	Acceso de Datos.	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
26	Soporte técnico	Asequibilidad del servicio de Internet	3	Moderado	Posible	Selección y vigilancia de información a través de niveles.
27	Internet	Calidad de internet	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
28	Software y contenidos digitales	Infraestructura digital	4	Mayor	Probablemente	Control de identificación de autenticidad de identificación de clientes.
29	Variedad de dispositivos	Ciberseguridad	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.
30	Actualización del equipamiento	Gobierno digital.	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos.

2. Evaluación de riesgos						
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Consecuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*
Calidad de vida digital en Empresa y Sociedad						
31	Participación en el diseño e implementación de TIC	Asequibilidad del servicio de Internet	2	Menor	Insólito	Existe una supervisión sobre el uso de softwares en los sistemas informáticos
32	Acceso	Calidad de internet	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.
33	Actores involucrados	Infraestructura digital	3	Moderado	Posible	Control de identificación de autenticidad de identificación de clientes.
34	Alfabetización digital comunitaria	Ciberseguridad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.
35	Apoyo de la comunidad hacia la empresa.	Gobierno digital.	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.

Nota: Se reflejan las dimensiones correspondientes a la Matriz de Riesgos Ciberseguridad y Calidad de Vida Digital de la Empresa Jama-Café Restaurant

Según figura 1, se ha obtenido resultados significativos de treinta y cinco (35) ítems para la evaluación de riesgos en ciberseguridad y calidad de vida digital; por lo que, se puede identificar consecuencias y probabilidades de riesgos de vulnerabilidad en los sistemas informáticos de la empresa, siendo seis (8) ítems los cuales están en condiciones extremas, diez (10) en condiciones bajas y diecisiete (17) en condiciones medio.

Tabla 11.
Descripciones, niveles y definiciones de consecuencias de que se produzca un riesgo y probabilidades de que se produzca un incidente de ciberataque a los sistemas de información de Jama-Café Restaurant.

Consecuencia - Evalúe las consecuencias de que se produzca un riesgo según las calificaciones de la fila superior

Descriptor	Nivel	Definición
Insignificante	1	No hay riesgo alguno
Menor	2	Introducción de ataques cibernéticos menores
Moderado	3	Se requiere intervención de especialista para prevención de riesgos.
Mayor	4	Ataque cibernético con ataque de virus malicioso
Severo	5	Robo de información y transferencias económicas

Probabilidad- Evalúe la probabilidad de que se produzca un incidente según las calificaciones de la columna de la izquierda

Descriptor	Nivel	Definición
Raro	1	Puede ocurrir en algún lugar, en algún momento (“una vez en la vida / una vez en 1 año”)
Insólito	2	Puede ocurrir en algún lugar dentro de la empresa durante un largo período de tiempo
Posible	3	Puede ocurrir varias veces en la empresa durante un período de tiempo
Probablemente	4	Puede anticiparse varias veces a lo largo de un periodo de tiempo. Puede ocurrir una vez cada varias repeticiones de la actividad o evento
Casi seguro	5	Propenso a ocurrir regularmente. Se prevé para cada repetición de la actividad de evento

Nota: Utilizando la matriz, calcule el nivel de riesgo encontrando la intersección entre la probabilidad y las consecuencias; así como, el Nivel/calificación de riesgo y acciones

Tabla 12

Matriz de Riesgos y Nivel/calificación de riesgo y acciones en la Empresa Jama-Café Restaurant

Matriz de riesgo

Probabilidad	Consecuencia				
Insignificante		**Menor**	**Moderado**	**Mayor**	**Severo**
Casi seguro	Medio	Alto	Extremo	Extremo	Extremo
Probablemente	Medio	Medio	Alto	Extremo	Extremo
Posible	Bajo	Medio	Medio	Alto	Extremo
Insólito	Bajo	Bajo	Medio	Medio	Alto
Raro	Bajo	Bajo	Bajo	Medio	Medio

Nivel/calificación de riesgo y acciones

Descriptor	Definición
Extremo: (5)	Notificar inmediatamente al Gerente del lugar de trabajo y/o al responsable de la empresa. Deben adoptarse inmediatamente medidas correctoras. Cese de la actividad asociada.
Alto: (4)	Notificar inmediatamente al Gerente del lugar de trabajo y/o al responsable de la empresa. Las acciones correctivas deben tomarse dentro de las 48 horas siguientes a la notificación.
Medio: (2-3)	Notificar al empleado designado, al Administrador. A fin que se designe n personal que realice un seguimiento para que se tomen medidas correctivas en un plazo de 7 días.
Bajo (1)	Notificar al empleado designado, El empleado designado, debe hacer un seguimiento para que se tomen medidas correctivas en un plazo razonable.

Nota: Utilizando la matriz, calcula el nivel de riesgo encontrando la intersección entre la probabilidad y las consecuencias; así como, el Nivel/calificación de riesgo y acciones

Comparando la información de la figura 1, con las tablas 11, 12, se puede identificar que existen ocho (8) ítems los cuales están en condiciones de nivel de riesgo extremo, siendo:

Figura 2.
Niveles de riesgos extremo identificado con la matriz de riesgos de Ciberseguridad y Calidad de Vida en el periodo 2022, en la Empresa Jama-Café Restaurant.

2. Evaluación de riesgos							
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Conse-cuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*	**Nivel**
Gestión y Planificación en Ciberseguridad							
4	Coordinación en ciber-seguridad	Trazabilidad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo
Desarrollo Técnico y Profesional							
12	Niveles de formación di-gital en ciberseguridad	Calidad de internet	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo
16	Apropiación de los recursos web	Asequibilidad del servicio de Internet	5	Severo	Casi Seguro	Selección y vigilancia de información a través de niveles.	Extremo
Cultura Digital							
19	Acceso de personal confiable	Ciberseguridad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo
Recursos e Infraestructura TIC							
28	Software y contenidos digitales	Infraestructura digital	4	Severo	Probablemente	Control de identificación de autentici-dad de identificación de clientes.	Extremo

2. Evaluación de riesgos							
Identificar y enumerar los peligros		**Lista de controles de riesgo actuales**	**Calificación del riesgo**	**Conse-cuencia**	**Probabilidad**	**Enumerar los controles adicionales** *(si los hay - cuando los controles actuales no gestionan adecuadamente el nivel de riesgo)*	**Nivel**
Calidad de vida digital en Empresa y Sociedad							
32	Acceso	Calidad de internet	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo
34	Alfabetización digital comunitaria	Ciberseguridad	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo
35	Apoyo de la comunidad hacia la empresa.	Gobierno digital.	5	Severo	Casi Seguro	No se tiene una seguridad absoluta sobre control de procesos en la red.	Extremo

Nota: Ocho (8) niveles de riesgos identificados con la aplicación de la matriz de riesgos en la empresa Jama-Café Restaurant.

Figura 3.
Consolidado de comentarios de la guía de entrevista aplicado a colaboradores de la empresa.

Número de Colaboradores	Comentario	Resultado
18	Se requirió, se instalen software sofisticados que permitan la detección de virus informáticos con mayor precisión; así como, se utilice estrategias como la verificación semanal de los sistemas informáticos. Del mismo modo, se tiene que identificar al cliente que paga , solicitándole su documento de identidad con la finalidad de que exista una calidad de vida digital óptima en relación a su bienestar y seguridad informática de datos e información.	Seguimiento de medidas correctivas: subsana ítems 4,12,16 y 19, Niveles de riesgos extremo identificado con la matriz de riesgos de Ciberseguridad y Calidad de Vida en el periodo 2022, en la Empresa Jama-Café Restaurant.
17	Se requirió, la revisión generalizada de los implementos de red en los sistemas informáticos, la verificación de las entradas y movimientos efectuados de los pagos; y monitoreos respectivos al personal que utiliza las fuentes de información al momento de efectuar los cobros. Asimismo, proteger la información correspondiente a los colaboradores que trabajan en la empresa y clientes que consumen en el restaurant.	Seguimiento de medidas correctivas: subsana ítems 28, 32,34 y 35, Niveles de riesgos extremo identificado con la matriz de riesgos de Ciberseguridad y Calidad de Vida en el periodo 2022, en la Empresa Jama-Café Restaurant.
35	**Total Colaboradores**	

Nota: Comentarios como resultado de la aplicación de la guía de entrevista al personal de la empresa Jama-Café Restaurant.

Al respecto, según el objetivo específico 2 , el cual fue evaluar si la ciberseguridad y la calidad de vida digital obtienen excelentes beneficios con la mitigación de riesgos de acuerdo a las evaluaciones establecidas, se obtuvo que, de la información obtenida en los comentarios de los treinta y cinco (35) trabajadores, a través de la guía de entrevista, la cual es visualizada en la figura 2; se ha podido conseguir como resultado que para mitigar los riesgos dieciocho (18) personas han considerado se instalen software sofisticados que permitan la detección de virus informáticos con mayor precisión; así como, se utilice estrategias como la verificación semanal de los sistemas informáticos. Del mismo modo, se tiene que identificar al cliente que paga, solicitándole su documento de identidad con la finalidad de que exista una calidad de vida digital óptima con relación a su bienestar y seguridad informática de datos e información. Por otro lado, Diecisiete (17) personas, consideran que es

necesario la revisión generalizada de los implementos de red en los sistemas informáticos, la verificación de las entradas y movimientos efectuados de los pagos; y monitoreos respectivos al personal que utiliza las fuentes de información al momento de efectuar los cobros. En este sentido mitigan los riesgos extremos identificados en la figura 2.

De los resultados obtenidos, en la figura 4 se puede identificar que, a través de la matriz de medidas correctivas en ciberseguridad, Jama-Café Restaurant cuenta con medidas automatizables y no automatizables para prevenir y mitigar riesgos, las cuales se describen a continuación:

Figura 4.
Medidas Correctivas aplicadas en Jama-Café Restaurant

Medidas Correctivas	Medidas Correctivas automatizables	Medidas Correctivas no automatizables
Desde el punto de vista Proactivas	Cortafuegos o firewall	• Contraseña • Copias de seguridad de archivos • Partición del disco duro. • Certificados digitales de firma electrónica. • Utilización habitual de permisos reducidos. • DNI electrónico. • Cifrado de documentos o datos. • Uso de máquinas virtuales.
Desde el punto de vista Proactivas y Reactivas	• Programa antivirus. • Actualización del sistema operativo y programas. • Actualizaciones del antivirus.	
Desde el punto de vista Reactivas	• Plugins para el navegador • Programas de bloqueo de ventanas. • Programas de bloqueo de banners. • Programas anti spam. • Programas anti-fraude.	Eliminación de archivos temporales o cookies.

Nota: La figura 4. evidencia las medidas que se utilizan para evaluar los sistemas informáticos de Jama Café restaurant, de acuerdo a las políticas establecidas en la empresa.

En este sentido, según lo indicado por el objetivo general, esta matriz identificó los posibles usos que se pueden dar a una diversidad de elementos como softwares para neutralizar los ataques cibernéticos, en consecuencia, para conseguir que, la ciberseguridad se imponga frente a amenazas digitales, era necesario contar con herramientas proactivas, proactivas y reactivas y reactivas, que permitan de esta forma salvaguardar la información económica y financiera de la empresa Jama-Café Restaurant.

DISCUSIÓN

Al respecto, de los resultados obtenidos en las tablas 2 y 3, viendo los datos informáticos proporcionados por la fuente Kapersky (2022) vemos que a nivel internacional existen países los cuales son atacados cibernéticamente, debido a que no cuentan con recursos sofisticados como el uso de la ciberseguridad y la calidad de vida digital; por eso el país que más ha sufrido daños ha sido Afganistán con 9.22%, teniendo como virus malicioso al Dangeruos 0bject.Multi. Generic con 9.97%.

Perú es considerado como uno de los países latinoamericanos que también es perjudicado con 3.02% de ataque cibernéticos; es decir que las empresas son vulnerables a la aparición de virus informáticos o a sustracciones por los hackers que comúnmente las citadas empresas tienen que afrontar.

En ese sentido viento lo indicado en la tabla 5, se puede apreciar que las amenazas mas grandes que la empresa Jama-Café Rsetaurant tiene que afrontar es la de los Troyanos o caballos de Troya. Bankers o troyanos bancarios, Backdoors o puertos traseros, Keyloggers o capturadores de pulsaciones, Dialers o marcadores telefónicos, Rogueware con un 22.86% del personal que lo confirma; asimismo, los virus los cuales son señalados por el 17.14% de los colaboradores de la empresa.

Es por ello que según la tabla 6, la estrategia que esta empresa Trujillana ha optado es de nunca dar información confidencial por Internet sobre sus clientes y movimientos financieros e informáticos que tienen en la empresa. Del cuestionario aplicado a la citada empresa se ha podido determinar a través de la tabla 7, que existe una funcionalidad por parte de la ciberseguridad en lo concerniente a Integridad de Información es de 42.86%, Disponibilidad de Información es de 14.29%, Autenticidad es de 8.57%, Trazabilidad es de 5.71% y Acceso de Datos es de 28.57%; por otro lado, en relación a la calidad de vida digital según lo indicado en la tabla 8 , se tiene que la funcionalidad por prioridad de las dimensiones de la variable indica que, Asequibilidad del servicio de Internet es de 42.86%, Calidad de internet es de 28.57%, Infraestructura digital es de 11.43%, Ciberseguridad es de 5.71%, y Gobierno digital es de 11.43%

; por tanto según la tabla 9, señala que los pagos más significativos se reflejan en efectivo y uso de tarjeta de crédito con el uso del DNI los cuales reflejan un 28.57% y 25.71% de aceptación, los cuales se encuentran controlados, desde la caja; contándose también con la entrega documentaria del voucher respectivo a través de los medios tecnológicos; asimismo, uso de las tarjetas de débito con chip y uso de PIN; así como, los Pagos a través de trasferencias bancarias por la banca móvil, ambos con un 22.86% de aceptación.

En este caso, la empresa ha optado por contar con ciertas políticas, procedimientos y medidas de seguridad; así como contiene criterios dirigidas a la prevención y a mitigar aquellos riesgos que pueden generar fraudes en el sentido de suplantación de personalidad; por tanto, están obligadas a implantar una serie de recursos sofisticados como son el uso de los PIN o contraseña, puede realizarse los pagos a través de trasferencias bancarias por la banca móvil, el uso de las tarjetas de débito con chip y crédito con el uso del DNI.

Al respecto, Jama-Café Restaurant tiene la preocupación como empresa en el sector Gastronómico, siendo como mantener protegidos los datos personales correspondiente a los clientes y la información sensible de los tantos usuarios, consumidores que confían en esta organización; así como de la propia empresa; por cuanto a optado por aplicar una serie de herramientas como son las matrices que permiten identificar las condiciones en cómo la empresa se encuentra en cuanto a ciberseguridad y a calidad de vida digital.

En ese sentido, la matriz de TIC de Ciberseguridad y calidad de Vida Digital ubicada en la tabla 10 de los resultados, indicó que la empresa Jama–Café Restaurant se encuentra en un Nivel Intermedio en cuanto a protección de datos informáticos; por lo que, en este contexto, también según la figura 1 con las tablas 11, 12; así como, figura 2, la matriz de Gestión de Riesgos identificó los posibles riesgos encontrados por la Ciberseguridad, siendo un total de ocho (8).

Por otro lado, al haberse aplicado la guía de entrevista, se pudo verificar que dio soluciones como medidas preventivas para mitigar dichos riesgos; esto se refleja en el accionar de la figura 3 y 4; donde los jefes y personal que laboran en la empresa solicitaron, se instalen software sofisticados que permitan la detección de virus informáticos con mayor precisión; así como, se utilice estrategias como la verificación semanal de los sistemas informáticos. Del mismo modo, se tiene que identificar al cliente que paga, solicitándole su documento de identidad con la finalidad de que exista una calidad de vida digital óptima en relación a su bienestar y seguridad informática de datos e

información. En ese sentido, también se requirió, la revisión generalizada de los implementos de red en los sistemas informáticos, la verificación de las entradas y movimientos efectuados de los pagos; y monitoreos respectivos al personal que utiliza las fuentes de información al momento de efectuar los cobros. Para lo cual se aplicó la matriz de medidas correctivas con la finalidad de mitigar los riesgos encontrados con la citada matriz de riesgos; dando con ello mayor seguridad a la empresa con ciberseguridad y dando una mejor calidad de vida digital a los colaboradores que trabajan en ella; si no también a los clientes que acuden a consumir en el local.

Para finalizar, de acuerdo con la funcionalidad de ciberseguridad, es considerable su destaque con 42.86% en integridad de información; por otro lado, con calidad de vida digital en 42.86% en Asequibilidad del servicio de Internet. Por consiguiente, existe una protección en cuanto a la información de datos informáticos en la empresa. De esta forma, es necesario afirmar que para la presente investigación se eligió contar con un óptimo tratamiento estadístico de la información.

CONCLUSIONES

En mérito al objetivo principal, el cual fue determinar en qué medida la ciberseguridad permite el desarrollo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022, se pudo concluir que, existen ataques cibernéticos a empresas a nivel internacional, nacional y local; no siendo la empresa Jama Café –Restaurant, la excepción.

Al respecto, existe un destaque en ciberseguridad, con 42.86% en integridad de información por cuanto; por otro lado, calidad de vida digital en 42.86% correspondiente a asequibilidad del servicio de Internet, existiendo una protección en cuanto a la información de datos informáticos en la empresa, según datos obtenidos por los cuestionarios. De esta forma, se ha llegado a cumplir con los objetivos propuestos establecidos en el presente artículo.

Por otro lado, según el objetivo específico establecido 1: Verificar que exista una gestión de riesgos que permita identificar los riesgos y mitigarlos en su momento, en los sistemas informáticos, existen ocho (8) riesgos según la identificación de la matriz de riesgos en ciberseguridad y calidad de vida. Asimismo, según el objetivo específico 2: Evaluar si la ciberseguridad y la calidad de vida digital obtienen excelentes beneficios con la mitigación de riesgos de acuerdo a las evaluaciones establecidas; se ha podido identificar que, de la aplicación de la guía de entrevista a los colaboradores de la empresa, de acuerdo a sus comentarios, se pudo controlar los

riesgos, a través de las medidas correctivas necesarias en ese momento.

Para concluir en forma general, efectivamente, según el objetivo general el cual fue determinar en qué medida la ciberseguridad permite el desarrollo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022, se ha podido responder a la hipótesis de investigación en la cual se pudo indicar que la ciberseguridad permite el desarrollo significativo de una calidad de vida digital optima en la empresa Jama-Café Restaurant, periodo 2022, en mérito a la obtención de resultados favorables para la institución, por cuanto dichos resultados han permitido identificar los riesgos y mitigarlos con el apoyo de la ciberseguridad y calidad de vida digital, sus dimensiones e indicadores.

De esta forma, la problemática existente en Jama –Café Restaurant, llega a ser mitigada por cuanto se han tomado las medidas correctivas necesarias como parte de la evaluación presentada en el presente trabajo de investigación, consiguiendo que dicha empresa prevenga en todo sentido, cualquier intento de ataque cibernético y de esta forma que el negocio no sea perjudicado.

REFERENCIAS BIBLIOGRÁFICA

Akamai. (2019). Ciberataques. https://www.akamai.com/es/es/resources/cyber-attacks.jsp

Cepal (2022) Tecnologías Digitales para un nuevo futuro. Archivo PDF. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

Andina (2018) ¿Cuáles son los ciberataques más comunes en el Perú? Disponible en: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

Cepal (2022) Datos y hechos sobre la transformación digital. Archivo PDF. Disponible en: https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf

CiberseguridadTips (2022) Matriz de riesgos: Qué es y cómo se hace. https://ciberseguridadtips.com/matriz-de-riesgos/#:~:text=La%20matriz%20de%20riesgos%20es,de%20una%20empresa%20u%20organizaci%C3%B3n.

Colsof (2022) Ciberseguridad, la primera línea en defensa para las compañías. ARCHIVO PDF.

Mena (2022) Siete de los diez países con mayor calidad de vida digital

están en Europa. Página web. Disponible en: https://es.statista.com/grafico/22883/ranking-de-paises-segun-su-puntuacion-en-el-indice-de-calidad-de-vida-digital/

Berdud, Chacón y Martinelli (2021) Competencia digital y calidad de vida. Página Web. Disponible en: https://www.sindromedownvidaadulta.org/no-39-octubre-2021/competencia-digital-y-calidad-de-vida/

El Peruano. (2019). Ciberataques en crecimiento. Disponible en: https://elperuano.pe/noticiaciberataques-crecimiento74748.aspx

Themelis y Ann Sime (2019) Estudio detallado sobre la Educación del Bienestar Digital: un compendio de prácticas innovadoras y recursos educativos abiertos. Archivo PDF. Disponible en: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/eab5911c-50ac-479e-8070-2e7fa9b942db/DWE-Compendium_Spanish.pdf

Gestión (2019). Radiohead responde a hackers: libera sesiones robadas de música inédita. Disponible en https://gestion.pe/tecnologia/radioheadresponde-hackers-libera-sesiones-robadasmusica-inedita-269828-noticia/

Kapersky (2022) ¿Qué es la Ciberseguridad? https://www.kaspersky.es/resource-center/definitions/what-is-cyber-security

Kapersky (2022) Ciberamenaza Mapa en Tiempo Real. https://cybermap.kaspersky.com/es

León et al. (2022) Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. https://revistas.ulasalle.edu.pe/innosoft/article/view/62/82

León, J. Á. Q. (2021). Ciberseguridad y protección de datos personales en el Perú. Advocatus, (039), 15-21. Enlace: https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/5114

Martin, L. (17 de marzo de 2021) Ciberseguridad Estratégica. Enfoque Doctrinal y Sistémico (1ª Parte). https://www.linkedin.com/pulse/ciberseguridad-estrat%C3%A9gica-enfoque-doctrinal-y-1%C2%AA-luis#:~:text=La%20Ciberseguridad%20desde%20el%20punto,las%20estructuras%2C%20planes%2C%20misiones%20y

Martínez Vásquez, F. (11 de setiembre de 2020) Ciberseguridad y Estado autonómico. https://revistas.comillas.edu/index.php/revistaicade/article/view/12814/12044

Poggy, N. (2019) 24 Estadísticas de Seguridad Informática que Impor-

tan en el 2019. https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

Poma, A. y Vargas, R. (2019) Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. https://revistas.unitru.edu.pe/index.php/SCIENDO/article/view/2692

Pontifica Universidad Javeriana (2022) Proceso Identificación del Riesgo. https://www.javeriana.edu.co/of-organizacion-y-metodos/ident-riesgos/-/asset_publisher/whvzdezcCgB8/document/id/4367161

RPP (29 de setiembre de 2021) Perú entre los peores en Calidad de Vida Digital en América del Sur. https://rpp.pe/tecnologia/mas-tecnologia/peru-entre-los-peores-en-calidad-de-vida-digital-en-america-del-sur-noticia-1360252?ref=rpp

Smartsheet (2022) Descargar plantillas gratuitas de matriz de riesgos personalizables. https://es.smartsheet.com/all-risk-assessment-matrix-templates-you-need

Sampieri (2018) Metodología de la Investigación. Las rutas cuantitativa, cualitativa y mixta. Archivo PDF. https://www.estudiojuridicolingsantos.com/2020/09/metodologia-de-la-investigacion-las.html

UNESCO (2021) Aspectos destacados y resultados destacados. y resultados. https://www.itu.int/net4/wsis/forum/2021/es/Home/Outcomes

VASS (21 de junio de 2021) ¿Por qué han cambiado los paradigmas en Ciberseguridad bancaria? ¿Cuáles son los nuevos retos?. https://vasscompany.com/paradigmas-en-ciberseguridad-bancaria/

Vilcarromero, L. y Vilchez, E. (2018) Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y