J. Strateg. Manag. Stud. Vol. 16, No. 64, Winter 2025, PP: 53-71 ISSN (Print): 2228-6853 (Online): 2676-6744

Journal of Strategic Management Studies

Homepage: https://www.smsjournal.ir/?lang=en

Original Research Article 10.22034/smsj.2025.495881.2099

Presenting an organizational security model on the path to business sustainability using thematic analysis method

Mohammad Saber Shahrestani*, MA. graduated, Malik Ashtar University of Technology, Tehran, Iran
Hosein Vahidi, Assistant Professor, Department of Industrial Engineering, Malik Ashtar University of Technology, Isfahan, Iran
Fatemeh Nabavinezhad, MA. graduated, Malik Ashtar University of Technology, Tehran, Iran

ARTICLE INFO

Article History
Received: 12 December 2024
Revised: 10 March 2025
Accepted: 17 May 2025

Keywords
Business sustainability, business security, organizational sustainability, organizational security, organizational threats.

Corresponding Author Email:
saber.shahrestani@mut.ac.ir

ABSTRACT

In recent years, numerous studies have been conducted in the field of business, growth and survival of organizations. However, given the complex conditions and dynamic environment of today's world, there has been little research on organizational security that helps business development. Organizational security refers to a set of measures, policies and processes that are designed to protect the assets, information and human resources of an organization, and it can be said that these factors are among the most important components of maintaining the survival of the organization. The purpose of the present study is to develop a model so that organizations can identify various threats, including theft of organizational secrets and information, loss of human resources, loss of customers, financing, etc., which threaten the organization and its sustainability in every aspect, and take preventive measures accordingly. The present study was conducted as a qualitative-applied developmental research with an exploratory nature, which was conducted in the field with a semi-structured interview method from 56 experts in different fields in a targeted manner, and the content analysis method was used to extract the pattern and finalize it. Theoretical saturation of the sampling adequacy point was considered. The results showed that 127 initial codes were extracted from the review and analysis of the interview data based on the principles of repetition, emphasis, and importance, which were categorized into 37 sub-themes and 6 main themes including physical security, cyber security, operational security, financial security, human resource security, and legal security and compliance.

How to cite this article:
Shahrestani, M.S., Vahidi, H., & Nabavi Nezhad, F. (2025). Presenting an organizational security model in the path of business sustainability by the method of content analysis. *Journal of Strategic Management Studies*, 64(16), 53-71. (In Persian with English abstract). https://doi.org/10.22034/smsj.2025.495881.2099

J. Strateg. Manag. Stud., Vol. 16, No. 64, Winter 2025
Web**:** http://smsjournal.ir
Doi: **10.22034/smsj.2025.495881.2099**

EXTENDED ABSTRACT

Introduction

In the contemporary volatile, uncertain, complex, and ambiguous (VUCA) business environment, the pursuit of organizational sustainability has transcended traditional performance metrics. While substantial scholarly attention has been directed toward organizational growth strategies and competitive advantage, a critical lacuna remains in the literature: the fundamental role of "organizational security" as a foundational pillar for strategic development. Organizational security is not merely a defensive function; it encompasses a comprehensive ecosystem of policies, risk-mitigation processes, and strategic measures designed to safeguard an organization's tangible and intangible assets, intellectual capital, sensitive information, and human resources. As organizations operate within increasingly complex supply chains and digital landscapes, they face an unprecedented array of threats—ranging from industrial espionage and cyber-attacks to the attrition of critical talent and complex financial volatility. Surprisingly, many organizations treat security as a peripheral, technical concern rather than a strategic imperative. This study seeks to bridge this gap by proposing a holistic framework that enables organizations to identify, assess, and neutralize multifaceted threats. By conceptualizing security as an integrated strategic capability, this research provides a roadmap for organizations to transition from reactive protection to proactive resilience, thereby ensuring long-term viability and sustained competitive positioning in a turbulent marketplace.

Methodology

The current study employs a qualitative, applied-developmental research design, characterized by its exploratory nature. Given the complexity of organizational security and the need for deep, context-specific insights, a field-based approach was adopted. Data collection was facilitated through in-depth, semi-structured interviews conducted with a panel of 56 high-level experts. These participants were selected through purposeful sampling from six distinct, mission-critical domains, ensuring a multidisciplinary perspective—including information technology, human resources, financial management, legal affairs, and operational management. The analytical phase of the study adhered to the rigorous systematic content analysis methodology established by Braun and Clarke (2006). This process involved a multi-stage coding procedure: initial open coding to capture raw concepts, followed by axial coding to identify relationships, and finally, selective coding to synthesize core thematic categories. To ensure the reliability and validity of the research, the principle of theoretical saturation was strictly observed, ensuring that data collection continued until no new conceptual insights emerged from the participants' discourse. This iterative process allowed for the transformation of granular data into a robust, conceptually grounded model of organizational security.

Results and Discussion

The rigorous thematic analysis of the interview transcripts yielded 127 initial codes, which were subsequently refined and integrated into 37 sub-themes and 6 overarching dimensions of organizational security. These dimensions—Physical Security, Cybersecurity, Operational Security, Financial Security, Human Resource (HR) Security, and Legal Compliance—collectively form the bedrock of the proposed security model. The findings indicate that these dimensions are highly interdependent. For instance, while cyber security protects digital infrastructure, it is inextricably linked to HR security (e.g., mitigating insider threats) and operational security (e.g., ensuring business continuity in the event of system failures). Financial security, on the other hand, acts as the overarching framework that sustains these measures, while legal compliance provides the normative boundary. The study posits that security should no longer be viewed as a siloed function. Instead, the extracted themes suggest that organizational resilience is a systemic property emerging from the integration of these six areas. Leaders who prioritize this multidimensional security posture are better positioned to mitigate risks such as intellectual property theft, hacking, talent poaching, and financial mismanagement, all of which pose existential threats in the modern era.

J. Strateg. Manag. Stud., Vol. 16, No. 64, Winter 2025
Web**:** http://smsjournal.ir
Doi: **10.22034/smsj.2025.495881.2099**

Conclusion

In the current global economic landscape, the traditional focus on gaining competitive advantage is insufficient if an organization lacks foundational security. This research highlights that negligence in any of the identified security domains—whether physical, cyber, operational, financial, human, or legal—can serve as a primary catalyst for organizational failure. The proposed organizational security model serves as a strategic imperative, advocating for a shift toward a culture of integrated security. By proactively embedding these security dimensions into the core strategy, organizations can enhance their agility and ensure business continuity despite external shocks. Furthermore, the model provides practical insights for decision-makers to align their security investments with broader strategic goals, such as project stability, resource optimization, and regulatory alignment. Ultimately, this study asserts that organizational security is the prerequisite for growth. Only by creating a hardened, secure, and compliant internal environment can an organization successfully navigate the complexities of today's market, securing not only its assets but its future.

Keywords: Business sustainability, Business security, Organizational sustainability, Organizational security, Organizational threats

مطالعات مدیریت راهبردی، دوره ۱۶، شماره ۶۴، زمستان ۱۴۰۴، صفحه: ۵۳ تا ۷۱ شاپای چاپی: ۶۸۵۳-۲۲۲۸ شاپای الکترونیکی: ۶۷۴۴-۲۶۷۶

مطالعات مدیریت راهبردی

Homepage: https://www.smsjournal.ir

مقاله پژوهشی 10.22034/smsj.2025.495881.2099 OPEN ACCESS

ارائه الگوی امنیت سازمان در مسیر پایداری کسب وکارها به روش تحلیل مضمون

محمدصابر شهرستانی*، فارغ التحصیل کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، تهران، ایران

حسین وحیدی، استادیار، گروه مهندسی صنایع دانشگاه صنعتی مالک اشتر، اصفهان، ایران

فاطمه نبوی نژاد، فارغ التحصیل کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، تهران، ایران

اطلاعات مقاله

سابقه مقاله

تاریخ دریافت: ۱۴۰۳/۱۰/۰۵

تاریخ بازنگری: ۱۴۰۳/۱۲/۲۰

تاریخ پذیرش: ۱۴۰۴/۰۲/۲۷

واژه‌های کلیدی

پایداری کسب‌وکار،
امنیت کسب‌وکار،
پایداری سازمانی،
امنیت سازمانی،
تهدیدهای سازمانی

ایمیل نویسنده مسئول

Saber.shahrestani@mut.ac.ir

چکیده

در دنیای امروز که با پیچیدگی‌ها و چالش‌های فراوانی روبرو است، حفظ امنیت سازمانی به عنوان یکی از ارکان کلیدی در بقای هر سازمان اهمیت ویژه‌ای دارد. امنیت سازمانی نه تنها به حفاظت از اطلاعات و دارایی‌های فیزیکی سازمان می‌پردازد، بلکه تأمین امنیت منابع انسانی، مالی و حتی تطابق با قوانین و مقررات نیز به عنوان عوامل ضروری برای تضمین موفقیت و پایداری بلندمدت سازمان‌ها شناخته می‌شود. با توجه به تهدیداتی نظیر هک اطلاعات، سرقت‌های فیزیکی، دستبرد به منابع انسانی و مشکلات مالی، سازمان‌ها باید تدابیر امنیتی مناسبی را برای مقابله با این خطرات اتخاذ کنند. این تدابیر شامل استراتژی‌های مختلف از جمله امنیت فیزیکی، امنیت سایبری، امنیت عملیاتی، امنیت مالی، امنیت منابع انسانی و پیروی از قوانین و مقررات است. عدم توجه به هر یک از این جنبه‌ها می‌تواند منجر به مشکلات جدی برای سازمان‌ها شود که ممکن است در نهایت به بحران و حتی شکست سازمان منجر گردد. هدف از تحقیق حاضر، تدوین الگویی است که به سازمان‌ها کمک کند تا بتوانند تهدیدهای گوناگونی نظیر سرقت اسرار و اطلاعات سازمانی، از دست دادن منابع انسانی، کاهش یا ریزش مشتریان، چالش‌های تأمین مالی و سایر مخاطراتی را که بقای سازمان را در معرض خطر قرار می‌دهند، شناسایی کرده و اقدامات پیشگیرانه‌ی متناسب با آن‌ها را اتخاذ نمایند. این تحقیق از نوع توسعه‌ای–کاربردی است و به روش کیفی با رویکردی اکتشافی انجام شده است. گردآوری داده‌ها به‌صورت میدانی و از طریق مصاحبه‌های نیمه‌ساختاریافته با ۵۶ نفر از خبرگان حوزه‌های مختلف و به‌صورت هدفمند صورت گرفته است. برای تحلیل داده‌ها و تدوین الگوی نهایی، از روش تحلیل مضمون استفاده شده و اشباع نظری به عنوان معیار کفایت نمونه‌گیری در نظر گرفته شده است. نتایج نشان داده‌اند که تعداد ۱۲۷ کد اولیه براساس اصول تکرار، تأکید و اهمیت از بررسی و تحلیل داده‌های حاصل از مصاحبه استخراج شده‌اند که در ۳۷ مضمون فرعی و ۶ مضمون اصلی شامل امنیت فیزیکی، امنیت فضای مجازی، امنیت عملیاتی، امنیت مالی، امنیت منابع انسانی و امنیت قانونی و امتثال دسته‌بندی شده‌اند.

استناد به این مقاله: شهرستانی، محمدصابر؛ وحیدی، حسینعلی؛ نبوی نژاد، فاطمه. (۱۴۰۴). ارائه الگوی امنیت سازمان درمسیر پایداری کسب وکارها به روش تحلیل مضمون. مطالعات مدیریت راهبردی،۶۴(۱۶)، ۷۱-۵۳.

۱. مقدمه

در دنیای امروز، امنیت سازمانی به‌عنوان یکی از ارکان اساسی موفقیت و پایداری کسب‌وکارها شناخته می‌شود. با این حال، عواملی همچون بی‌ثباتی مدیریتی، ضعف در نظام شایسته‌سالاری، تمرکز صرف بر کمّیت و سایر چالش‌های ساختاری، موجب شده‌اند که طراحی نظام‌مند امنیت سازمانی تاکنون مورد توجه جدی قرار نگیرد [۱۷]. مفهوم امنیت از پیچیدگی‌های متعددی برخوردار است؛ این پیچیدگی‌ها ناشی از گستره‌ی معنایی آن و مرزهای نامشخصش در حوزه‌هایی نظیر امنیت اقتصادی، امنیت ملی، امنیت انسانی و امنیت اطلاعات است. در گذشته، امنیت بیشتر به‌عنوان مفهومی عینی و قابل سنجش در نظر گرفته می‌شد، اما امروزه، این مفهوم عمدتاً ذهنی و وابسته به برداشت‌ها و تصمیم‌گیری‌های بازیگران مختلف تلقی می‌گردد. این تغییر نگرش، به‌ویژه در دنیای پیچیده و پویای امروز، موجب شده است که ابعاد گوناگون امنیت با رویکردی جامع‌تر مورد بررسی قرار گیرد.

با گسترش مفهوم امنیت در قرن حاضر، امنیت سازمانی به‌عنوان یکی از ابعاد حیاتی آن، شایسته‌ی توجهی ویژه است. امنیت سازمانی صرفاً به حفاظت از دارایی‌های فیزیکی و اطلاعاتی محدود نمی‌شود، بلکه نهادینه‌سازی فرهنگ امنیتی، مدیریت ریسک و ارتقاء آگاهی سازمانی در تمامی سطوح را نیز در بر می‌گیرد. در این راستا، شناسایی تهدیدات و آسیب‌پذیری‌های احتمالی سازمان، گامی ضروری به شمار می‌آید تا با تدوین و اجرای تدابیر مناسب، بتوان از موجودیت و پایداری سازمان در برابر مخاطرات گوناگون محافظت کرد.

فام و همکاران (۲۰۱۹) بر اهمیت امنیت سازمانی تأکید کرده و آن را به‌عنوان یکی از ارکان کلیدی در مدیریت مؤثر سازمان‌ها معرفی کرده‌اند [۲]. این موضوع نشان می‌دهد که در دنیای امروز، توجه به امنیت سازمانی نه تنها یک ضرورت، بلکه استراتژی‌ای کلیدی برای دستیابی به موفقیت و پایداری در بازار رقابتی به شمار می‌رود. با در نظر گرفتن پیچیدگی‌های موجود، ارزیابی و بهبود مستمر سیاست‌های امنیتی سازمان‌ها امری حیاتی است تا بتوانند با چالش‌های نوظهوری نظیر حملات فضای مجازی، رفتارهای غیرقابل پیش‌بینی کارکنان، سوءاستفاده از دسترسی‌ها و تغییرات شتاب‌زده‌ی فناوری مقابله کنند.

به‌طور سنتی، تحقیقات مرتبط با امنیت سازمانی بر جنبه‌های کلیدی‌ای متمرکز بوده‌اند که برای حفظ امنیت مؤثر در یک سازمان، حیاتی به شمار می‌روند. این مؤلفه‌ها شامل تدوین سیاست‌های امنیتی.[۲۵]، آموزش کارکنان در زمینه‌های مرتبط با امنیت . [۹] و نیز تضمین حمایت مدیریت ارشد از این ابتکارات [۱۰] می‌باشند.در فضای پرتلاطم و توأم با عدم‌قطعیت کسب‌وکارهای امروزی، بنگاه‌ها برای بقا و پیشی گرفتن از رقبا، نه تنها باید توانایی انطباق مستمر با تغییرات تدریجی را داشته باشند، بلکه باید بتوانند گسست‌های ناگهانی را نیز به‌سرعت شناسایی کرده و تغییرات بنیادین را به‌درستی مدیریت نمایند . [۱۵]. در این مسیر، لازم است جنبه‌های مکملی نیز در سیاست‌های امنیتی سازمان مورد توجه قرار گیرند.به‌عنوان نمونه، "انطباق امنیت فناوری اطلاعات" یکی از این جنبه‌هاست که مجموعه‌ای از تکنیک‌ها و فرآیندها را در بر می‌گیرد. این رویکرد کارکنان را تشویق می‌کند تا با آگاهی و دقت بیشتر، با سامانه‌ها و اطلاعات سازمانی تعامل داشته باشند. این نوع انطباق، سه هدف اساسی را دنبال می‌کند: (۱) کاهش یا پیشگیری از حوادث امنیتی ناشی از سهل‌انگاری کارکنان، (۲) مقابله با رفتارهای مجرمانه‌ی سایبری و سوءاستفاده از سیستم‌های رایانه‌ای، و (۳) ترویج رفتارهای حمایتی و اجتماعی در حوزه‌ی امنیت اطلاعات در میان پرسنل[۲۲]

با این حال، بررسی‌های انجام‌شده نشان می‌دهد که پژوهشگران کمتر به ارتباط میان امنیت سازمانی و پایداری کسب‌وکار پرداخته‌اند. از این‌رو، پژوهش حاضر با محدودیت‌هایی مواجه بوده است؛ از جمله، کمبود منابع نظری مرتبط با موضوع امنیت سازمانی در راستای پایداری کسب‌وکار، ضرورت بازنگری مکرر در الگوی نهایی پژوهش، و نیز تعدد مفاهیم اولیه که فرایند پالایش نظری را پیچیده‌تر ساخته است.

همچنین نوآوری تحقیق حاضر بدین جهت است که تا کنون به موضوع امنیت سازمانی درراستای پایداری کسب‌وکار پرداخته نشده است و براساس نتایج تحقیق میتوان راهکارهای پایداری کسب‌وکار را به بهترین شکل ممکن توسعه داد.

هدف از این تحقیق، ارائه یک الگوی مؤثر است که به سازمان‌ها کمک کند تا به‌صورت نظام‌مند و جامع به تهدیداتی که میتواند بقای سازمان را از هر حیث با خطر مواجه کند، پاسخ دهند.

با توجه به هدف تحقیق به دنبال پاسخ به این سوال هستیم که امنیت سازمانی در پایداری کسب‌وکارها بر اساس چه الگویی برقرار می‌شود؟

۲. مبانی نظری و پیشینه پژوهش

ایداری مفهومی چندبُعدی است که ترکیبی از عوامل محیط‌زیستی، اجتماعی و اقتصادی را در بر می‌گیرد. در این میان، عوامل اقتصادی به‌عنوان اجتناب‌ناپذیرترین مؤلفه، نقش محوری در تحقق پایداری ایفا می‌کنند. مدیریت پایداری، از هر یک از این سه بُعد آغاز می‌شود و می‌تواند به کسب‌وکارها و بنگاه‌های اقتصادی در راستای دستیابی به اهداف کوتاه‌مدت و بلندمدت یاری رساند [۶]. پایداری بر فعالیت‌هایی متمرکز است که هم عملکرد پایدار اقتصادی و مالی، و هم عملکرد پایدار غیرمالی را دنبال می‌کنند؛ از جمله حداکثرسازی اثربخشی در اداره سازمان‌ها و بهره‌برداری از فرصت‌های تجاری، در کنار به حداقل رساندن آسیب‌های زیست‌محیطی و اجتماعی. این رویکرد به‌ویژه بر موفقیت‌های بلندمدت در خلق ارزش برای ذی‌نفعان تمرکز دارد [۱۳]. در حالی که دوره‌ای از شرکت‌ها به ادغام تدریجی شیوه‌های پایدار در عملکرد خود مشغول بودند، اکنون دوره‌ای جدید آغاز شده است؛ دوره‌ای که در آن شرکت‌ها به‌طور فعال در حال تحول‌بخشی به بازار با هدف ارتقاء پایداری هستند. مسیر پایداری کسب‌وکار، از آغاز جنبش‌های مدرن محیط‌زیستی در دهه‌ی ۱۹۷۰ و پایه‌گذاری مقررات زیست‌محیطی، تا به امروز که پایداری به موضوعی راهبردی و بازارمحور تبدیل شده، دگرگونی بزرگی را پشت سر گذاشته است. امروزه بیش از ۹۰ درصد از مدیران عامل اذعان دارند که پایداری برای سودآوری و موفقیت سازمان‌هایشان اهمیت اساسی دارد. در پاسخ به این ضرورت، شرکت‌ها به توسعه‌ی استراتژی‌های پایداری، بازاریابی محصولات و خدمات پایدار، ایجاد موقعیت‌های شغلی همچون مدیر ارشد پایداری، و افشای عملکرد خود از طریق گزارش‌های پایداری به مصرف‌کنندگان، سرمایه‌گذاران، فعالان اجتماعی و عموم مردم روی آورده‌اند [۱۱]. به رغم اهمیت موضوع پایداری کسب‌وکارها، بررسی ها حاکی از آن است که در عمل بسیاری از کسب‌وکارهای ایجاد شده در بخشهای مختلف به دلیل مواجهه با دشواریها و موانع پرشمار اعم از سیاسی -زیرساختی، قانونی، مالی–هزینهای، مهارتی–آموزشی، فنی– جغرافیایی و ارتباطی–اطالع رسانی، از سطح پایداری مناسبی در ابعاد اقتصادی–اجتماعی و زیست محیطی برخوردار نبوده و پایداری آنها با تردیدهای فروانی همراه است [۱۶] به نحوی که بسیاری از این کسب‌وکارها نه تنها در ابعاد اجتماعی و زیست محیطی از عملکرد مناسبی برخوردار نیستند، بلکه در ابعاد اقتصادی و درآمدزایی نیز چندان موفق عمل نکرده و در نتیجه در مدت زمان کوتاهی پس از راه اندازی، دچار شکست شده و فعالیت شان متوقف می‌شود [۲۳].

پیشینه پژوهش:

در بررسی های بعمل آمده در منابع داخلی و خارجی مشاهده گردید موضوع این مقاله به ندرت مورد توجه و بررسی پژوهش گران قرار گرفته است لذا نزدیک ترین موضوعات مرتبط در این بخش آورده می‌شود:

سالاری‌نیا و همکاران (۱۴۰۳) در مقاله‌ای با عنوان «ارائه مدل حکمرانی خوب به منظور پایداری کسب‌وکارهای کشاورزی در استان تهران (مورد مطالعه: بانک کشاورزی)» نشان دادند که از میان مؤلفه‌های مؤثر بر پایداری کسب‌وکار کشاورزی، کنترل فساد (β=۲۷۹/۰) اثرگذارترین مؤلفه است. پس از آن، مؤلفه‌های کیفیت قوانین و مقررات (β=۲۷۴/۰)، حاکمیت قانون (β=۲۷۱/۰)، حق اظهار نظر و پاسخگویی (β=۱۷۲/۰)، اثربخشی دولت (β=۰۴۳/۰) و ثبات سیاسی (β=۰۲۲/۰) به ترتیب در رتبه‌های بعدی اهمیت قرار داشتند [۱۸].

علی‌نژاد و همکاران (۱۴۰۲) در مقاله‌ای با عنوان «مفهوم‌سازی مؤلفه‌های مدل پایداری کسب‌وکارهای زنان در شهرستان بهبهان» به بررسی عواملی پرداختند که بر پایداری کسب‌وکارهای زنان در این منطقه تأثیرگذارند. یافته‌های این پژوهش نشان داد که مؤلفه‌هایی همچون دانش بازار، شرایط خانوادگی، ویژگی‌های فردی و شخصیتی، عوامل اقتصادی، آموزش، سیاست‌های حمایتی، بحران‌های اقتصادی و نوسانات محیطی، از جمله عوامل تعیین‌کننده در پایداری کسب‌وکارهای زنان به شمار می‌روند [۱].

سیف‌الهی انار و اکبری (۱۴۰۲) در مقاله‌ای با عنوان «ارائه الگویی برای پایداری کسب‌وکار مبتنی بر مهارت‌های دیجیتال در همه‌گیری کرونا» مدلی ارائه داده‌اند که بر مبنای آن، مفاهیم به‌صورت نظام‌مند در قالب یک مقوله‌ی محوری، ۲۱ مقوله‌ی اصلی، ۱۲ مقوله‌ی فرعی و ۲۴۱ مفهوم یا کد باز طبقه‌بندی شده‌اند. در نهایت، مدل پارادایمی پایداری کسب‌وکار مبتنی بر مهارت‌های دیجیتال در دوران همه‌گیری کرونا طراحی و ارائه شده است [۱۹]. بر اساس این مدل، عوامل علّی شامل هوش رقابتی، ارزش‌آفرینی هوشمند و ارتقای خودآگاهی هستند. عوامل زمینه‌ای عبارت‌اند از زیرساخت‌های دیجیتالی همگرا و انطباق منابع مالی. در مقابل، عواملی نظیر سنت‌های فرهنگی، نبود تکنیک‌ها و رویه‌های مشخص، و همچنین مسائل امنیتی مرتبط با فناوری‌های دیجیتال به‌عنوان عوامل

مداخله‌گر شناخته شده‌اند. عوامل راهبردی نیز شامل شفافیت، پاسخگویی و جهت‌دهی هوشمند فرایندها می‌باشند.نتیجه‌گیری این پژوهش بر آن است که با به‌کارگیری مؤثر عوامل راهبردی، می‌توان پایداری کسب‌وکارهای مبتنی بر مهارت‌های دیجیتال را در دوران بحران‌هایی نظیر همه‌گیری کرونا تضمین کرد. این پایداری از طریق ارتقای مسئولیت‌پذیری اجتماعی، تقویت اهداف بلندمدت اقتصادی و تلفیق رویکردهای حفاظتی و توسعه‌محور در قبال محیط‌زیست، محقق خواهد شد.

شیرمحمدی و همکاران (۱۴۰۲) به طراحی مدل پایداری کسب‌وکار در صنعت خودرو ایران پرداخته‌اند که نشان می‌دهد دستیابی به پایداری کسب‌وکار در این صنعت مستلزم توجه به سه مقوله اقتصادی، زیست‌محیطی و اجتماعی است [۲۱].

کلابی (۱۳۹۹) در مقاله‌ای با عنوان «مدلسازی عوامل مؤثر بر پایداری مدل‌های کسب‌وکار» نشان داد که عوامل مؤثر بر پایداری مدل کسب‌وکار به ترتیب شامل نوآوری، خلق ارزش مشترک، رهبری مشارکتی، عوامل اقتصادی و حاکمیت شرکتی هستند [۱۲].

شرفی و همکاران (۱۳۹۸) در مقاله‌ای با عنوان «طراحی مدل پایداری کسب‌وکارهای کوچک و متوسط کشاورزی در استان کرمانشاه» به بررسی عواملی پرداختند که پایداری این نوع کسب‌وکارها را تحت تأثیر قرار می‌دهند. یافته‌های آنان نشان می‌دهد که عوامل درون‌سازمانی و برون‌سازمانی، نقش محوری در این زمینه دارند. عوامل درون‌سازمانی شامل متغیرهایی مانند ویژگی‌های فردی و خانوادگی مدیر، عوامل مرتبط با بازاریابی، وضعیت اقتصادی–مالی، شرایط تولیدی و ویژگی‌های محصول، ساختار و ویژگی‌های کسب‌وکار و نیز عوامل ارتباطی و اطلاعاتی هستند. در مقابل، عوامل برون‌سازمانی شامل مؤلفه‌هایی نظیر محیط سیاسی–قانونی، زیرساخت‌های حمایتی و مداخلات ترویجی می‌باشند [۲۰].

همچنین، فدایی‌کیوانی و همکاران (۱۳۹۹) در پژوهشی با عنوان «ارائه مدل پایداری کسب‌وکارهای خانوادگی»، با بهره‌گیری از چارچوب مدل پارادایمی، مدلی مفهومی برای تبیین پایداری این دسته از کسب‌وکارها طراحی کرده‌اند. بر اساس یافته‌های این تحقیق، مدل مذکور شامل ۹ مقوله‌ی اصلی و ۲۵ متغیر است. در این مدل، *پایداری کسب‌وکار خانوادگی* به‌عنوان مقوله‌ی محوری شناخته شده و سایر مؤلفه‌ها در دسته‌های زیر تقسیم‌بندی شده‌اند:

- **متغیرهای علّی:** پویایی خانوادگی، اخلاق‌گرایی، سرمایه مالی، سرمایه انسانی و سرمایه اجتماعی؛
- **متغیرهای زمینه‌ای:** ویژگی‌های فردی و مهارت‌های رهبری، توانمندسازی، نهادهای حاکمیتی و ساختار مناسب؛
- **شرایط محیطی:** پایداری زیست‌محیطی، شرایط بازار و حمایت‌های دولتی؛
- **مقوله‌های راهبردی:** اهداف و چشم‌انداز بلندمدت، بهبود مستمر، نوآوری و توسعه کسب‌وکار، ریسک‌پذیری خانوادگی، نرخ بازگشت سرمایه، جانشین‌پروری و توانایی و تمایل جانشین؛
- **مقوله‌های پیامدی:** سودآوری بلندمدت، اشتغال پایدار، انسجام خانوادگی و نقش کسب‌وکار در ارتقاء اقتصاد و رفاه اجتماعی[۸]

وانجیکو نجوگو (۲۰۱۶) در پژوهشی به بررسی عوامل مؤثر بر پایداری شرکت‌های زنان در کشور کنیا پرداخته است. نتایج این مطالعه نشان می‌دهد که عواملی چون فرهنگ سازمانی، دسترسی به منابع مالی، الزامات قانونی و مهارت‌های مدیریتی، نقش کلیدی در پایداری این شرکت‌ها ایفا می‌کنند. نجوگو تأکید کرده است که زنان کارآفرین برای تضمین بقای کسب‌وکار خود، باید مهارت‌های مدیریتی را تقویت کرده، به قوانین موجود پایبند باشند و نیز فرهنگ کاری مناسبی در سازمان خود ایجاد کنند [۲۴].

در همین راستا، دیلیک و موف (۲۰۱۶) در مقاله‌ای با عنوان «شفاف‌سازی معنای کسب‌وکار پایدار: معرفی یک گونه‌شناسی از کسب‌وکار معمول به پایداری واقعی» با مرور ادبیات مرتبط، تیپولوژی‌ای از پایداری کسب‌وکار ارائه کرده‌اند که طیفی از سه سطح را شامل می‌شود:
پایداری کسب‌وکار ۱.۰ که مبتنی بر مدیریت ارزش سهام‌داران به‌صورت محدود است،
پایداری کسب‌وکار ۲.۰ که بر مدیریت همزمان سه‌گانه پایدار (اقتصادی، اجتماعی و زیست‌محیطی) تمرکز دارد،
و نهایتاً پایداری کسب‌وکار ۳.۰ که به عنوان «پایداری واقعی» معرفی می‌شود و با رویکردی تحولی، کسب‌وکار را در خدمت توسعه پایدار جهانی قرار می دهد [۷].

در همین زمینه، کاگنین و همکاران (۲۰۰۵) نیز با معرفی «مدل بلوغ پایداری کسب‌وکار»، مجموعه‌ای از ابعاد کلیدی را که به سازمان‌ها در مسیر دستیابی به توسعه پایدار کمک می‌کند، شناسایی کرده‌اند. این ابعاد عبارت‌اند از: شایستگی‌ها، ارتباطات مؤثر، انگیزش، فناوری، عملیات و استراتژی. به باور ایشان، این عناصر به‌عنوان پایه‌های بلوغ سازمانی، زمینه‌ساز حرکت شرکت‌ها به‌سوی پایداری واقعی هستند [۵].

بررسی مطالعات صورت گرفته نشان میدهد موضوع امنیت سازمانی در راستای پایداری کسب وکار به ندرت توسط محققین داخلی و خارجی بررسی شده و محقق جهت پرکردن شکاف دانشی با توجه به اهمیت موضوع و ارتباط آن با بقای سازمانی خصوصا محیط کسب وکار به این موضوع پرداخته است.

۳. روش‌شناسی پژوهش

پژوهش حاضر یک مطالعه کیفی است که از نظر هدف، در دسته تحقیقات توسعه‌ای-کاربردی و از نظر رویکرد، اکتشافی قرار می‌گیرد. این تحقیق به‌صورت میدانی انجام شده است و داده‌های آن از طریق مصاحبه‌های نیمه‌ساختاریافته جمع‌آوری گردیده است. شرکت‌کنندگان در این پژوهش شامل ۵۶ نفر از خبرگان در دسترس بوده‌اند که در حوزه‌های تخصصی خود، که در جدول ۱ آمده است، فعالیت و تحقیق می‌کنند. برای انتخاب مشارکت‌کنندگان، از روش نمونه‌گیری هدفمند استفاده شده است و اشباع نظری (به معنای عدم استخراج کدهای جدید) به‌عنوان نقطه‌ی کفایت نمونه‌گیری در نظر گرفته شده است. مشخصات مصاحبه‌شوندگان در جدول ۱ ارائه شده است.

جدول۱. اطلاعات جمعیت شناختی مصاحبه شوندگان پژوهش

حوزه تخصص	تعداد کل	جنسیت		سن				وضعیت تحصیلی			تجربه کاری	
*	*	زن	مرد	از ۳۱ تا ۴۰ سال	از ۴۱ تا ۵۰ سال	از ۵۱ تا ۶۰ سال	کارشناسی	کارشناسی ارشد	دکتری	از ۱۱ تا ۲۰ سال	بیشتر از ۲۰ سال
فناوری اطلاعات	۱۰	۳	۷	۴	۵	۱	۴	۴	۲	۹	۱
برنامه‌نویسی کامپیوتر	۱۲	۲	۱۰	۳	۶	۳	۲	۴	۶	۱۰	۲
اقتصاد	۸	۰	۸	۳	۳	۲	۱	۴	۳	۷	۱
منابع انسانی	۱۰	۲	۸	۲	۴	۴	۲	۳	۵	۹	۱
مدیریت کسب‌وکار	۱۰	۳	۷	۳	۴	۳	۲	۴	۴	۹	۱
مهندسی صنایع	۶	۲	۴	۱	۲	۳	۳	۱	۲	۵	۱

با توجه به هدف اکتشافی تحقیق، مصاحبه‌ها با سؤالات باز انجام شد. برای تحلیل داده‌های حاصل از ادبیات تحقیق و متن مصاحبه‌ها، از روش تحلیل محتوای کیفی و رویکرد تحلیل مضمونی بر اساس روش‌شناسی کلارک و برون (۲۰۰۶) استفاده گردید. همچنین، برای پردازش داده‌ها از نرم‌افزار مکس کیودا نسخه ۱۸ بهره‌برداری شد. مراحل شش‌گانه تحلیل مضمون بصورت زیر است [۴]:

۱. آشنایی با داده‌ها ۲. کدگذاری اولیه داده‌ها ۳. جستجوی کدهای گزینشی
۴. شکل گیری مضامین فرعی ۵. تعریف و نامگذاری مضامین اصلی ۶. ترسیم شبکه مضامین

در نهایت، الگوی برآمده از تحلیل مضمون با استفاده از روش بازدید همتایان مورد پرسش از ۹ خبره تأیید ۵ تن از ایشان قرار گرفت.

۴. تحلیل داده‌ها و یافته‌ها

پس از پایان مصاحبه‌ها، متن مصاحبه‌ها مورد بررسی قرار گرفت و با مرور مکرر داده‌ها، در مرحله اولیه کدگذاری انجام شد. در این مرحله، با مطالعه خط به خط متن، نکات مربوط به عوامل مؤثر در تدوین الگوی امنیت سازمانی و الزامات آن به‌عنوان یادداشت‌هایی استخراج گردید. این یادداشت‌ها به‌عنوان داده‌های اولیه در نظر گرفته شدند و مفاهیم از درون آن‌ها استخراج شد. مطابق با دیدگاه شلر و بائرون (۲۰۰۶)، هنگامی که مفاهیم ایجاد می‌شوند، لازم است تحلیل‌گر آن‌ها را تحت عناوینی با قدرت تبیین بیشتر، به‌عنوان مقوله‌ها دسته‌بندی کند. جدول ۳ مفاهیم اولیه استخراج‌شده را نشان می‌دهد.

جدول۲. کدگذاری اولیه مصاحبه ها

ردیف	مفاهیم اولیه	کدهای باز	دفعات تکرار
۱	نظارت و کنترل ورود و خروج	کد ۱	۶
۲	نظارت بر تردد در ساختمان‌ها	کد ۲	۵
۳	محافظت از تجهیزات و اموال سازمان	کد ۳	۶
۴	بررسی منظم ساختمان‌ها	کد ۴	۵
۵	تخصیص مجوزهای دسترسی	کد ۵	۵
۶	نظارت بر دسترسی‌ها	کد ۶	۴
۷	کنترل دسترسی به مناطق حیاتی	کد ۷	۹
۸	بروزرسانی مستمر و دوره ای مجوزها	کد ۸	۷
۹	نگهداری مدارک در مکان های ایمن	کد ۹	۸
۱۰	کنترل دسترسی به اطلاعات حساس	کد ۱۰	۴
۱۱	پشتیبان‌گیری اطلاعات	کد ۱۱	۵
۱۲	نظارت بر انتقال اطلاعات حساس	کد ۱۲	۶
۱۳	نصب سیستم‌های اطفاء حریق	کد ۱۳	۹
۱۴	برنامه‌ریزی جهت مواقع اضطراری	کد ۱۴	۴
۱۵	آموزش کارکنان در خصوص بروز حوادث	کد ۱۵	۵
۱۶	نظارت بر سیستم‌های ایمنی	کد ۱۶	۶
۱۷	نصب دوربین‌های مدار بسته(۳۶۰ درجه)	کد ۱۷	۱۲
۱۸	کنترل دسترسی به پارکینگ‌ها	کد ۱۸	۹
۱۹	نظارت بر امنیت محیط‌های اطراف	کد ۱۹	۱۰
۲۰	برنامه‌ریزی اضطراری برای حوادث در محیط‌های اطراف	کد ۲۰	۳
۲۱	نظارت و کنترل دسترسی به مناطق حیاتی	کد ۲۱	۷
۲۲	محافظت از مخازن داده	کد ۲۲	۴
۲۳	نظارت بر امنیت مناطق حیاتی	کد ۲۳	۶
۲۴	برنامه‌ریزی برای مواقع اضطراری در مناطق حیاتی	کد ۲۴	۳
۲۵	نصب راه بندها و مانع‌های فیزیکی	کد ۲۵	۴
۲۶	نظارت دقیق بر ورود و خروج افراد	کد ۲۶	۵
۲۷	کنترل دسترسی به ورودی‌ها و خروجی‌ها	کد ۲۷	۴
۲۸	نصب دیواره‌های آتش[1]	کد ۲۸	۴
۲۹	استفاده از سیستم‌های تشخیص نفوذ[2]	کد ۲۹	۳
۳۰	استفاده سیستم‌های پاسخ به حوادث[3]	کد ۳۰	۵
۳۱	نظارت و مدیریت شبکه[4]	کد ۳۱	۳
۳۲	رمزگذاری داده‌ها[5]	کد ۳۲	۴
۳۳	امکان بازیابی داده‌ها[6]	کد ۳۳	۵

1 firewall
2 Systems Intrusion Detection
3 Incident Response system
4 Network Monitoring and Management
5 Data Encryption
6 Data Backup and Recovery

ردیف	مفاهیم اولیه	کدهای باز	دفعات تکرار
۳۴	مدیریت داده‌ها	کد ۳۴	۳
۳۵	حمایت از داده‌ها در برابر حملات[1]	کد ۳۵	۴
۳۶	مدیریت دسترسی ها	کد ۳۶	۵
۳۷	تخصیص مجوزها بر اساس نقش افراد[2]	کد ۳۷	۳
۳۸	کنترل دسترسی به اطلاعات حساس	کد ۳۸	۴
۳۹	بروزرسانی مستمر مجوزها	کد ۳۹	۳
۴۰	برنامه‌ریزی جهت پاسخ بموقع به حوادث	کد ۴۰	۳
۴۱	تمرینات پاسخ به حوادث	کد ۴۱	۴
۴۲	بازسازی پس از حادثه[3]	کد ۴۲	۴
۴۳	ارزیابی و یادگیری از حوادث[4]	کد ۴۳	۵
۴۴	برنامه‌ریزی آموزشی	کد ۴۴	۴
۴۵	ایجاد پویش‌های آگاه‌سازی	کد ۴۵	۴
۴۶	ارزیابی دانش و مهارت‌های کارکنان	کد ۴۶	۴
۴۷	ارائه مشاوره و راهنمایی به کارکنان برای بهبود عملکرد و امنیت فضای مجازی	کد ۴۷	۵
۴۸	شناسایی و ارزیابی ریسک‌ها	کد ۴۸	۴
۴۹	برنامه‌ریزی مدیریت ریسک	کد ۴۹	۶
۵۰	کنترل و نظارت بر ریسک‌ها	کد ۵۰	۵
۵۱	بروزرسانی مستمر ریسک‌ها	کد ۵۱	۴
۵۲	ایمن سازی ارتباطات بی‌سیم[5]	کد ۵۲	۳
۵۳	ایمن سازی ارتباطات داخلی	کد ۵۳	۴
۵۴	ایمن سازی ارتباطات خارجی	کد ۵۴	۵
۵۵	کنترل دسترسی به شبکه‌های خارجی[6]	کد ۵۵	۶
۵۶	شناسایی و ارزیابی ریسک‌ها ی عملیاتی	کد ۵۶	۳
۵۷	برنامه‌ریزی مدیریت ریسک عملیاتی	کد ۵۷	۴
۵۸	کنترل و نظارت بر ریسک‌های عملیاتی	کد ۵۸	۵
۵۹	بروزرسانی مستمر ریسک‌ها	کد ۵۹	۵
۶۰	ارزیابی کیفیت فرآیندها	کد ۶۰	۴
۶۱	نظارت و کنترل فرآیندها	کد ۶۱	۳
۶۲	بهبود فرآیندهای عملیاتی	کد ۶۲	۴
۶۳	بکارگیری فناوری اطلاعات در فرآیندها	کد ۶۳	۵
۶۴	برنامه‌ریزی سلامت و ایمنی کارکنان	کد ۶۴	۴
۶۵	ارزیابی ریسک‌های سلامت و ایمنی	کد ۶۵	۳

1 Data Protection against Attacks
2 Role-Based Access Control
3 Post-Incident Recovery
4 Incident Evaluation and Learning
5 Wireless Security
6 External Network Access Control

ردیف	مفاهیم اولیه	کدهای باز	دفعات تکرار
۶۶	تعلیم و آموزش کارکنان در زمینه سلامت و ایمنی	کد ۶۶	۵
۶۷	امکان مراقبتهای پزشکی و بهداشتی در محیط کار	کد ۶۷	۳
۶۸	ایجاد تیم بحران	کد ۶۸	۴
۶۹	برنامه‌ریزی اضطراری در مواقع بحران	کد ۶۹	۴
۷۰	تمرینات اضطراری برای مواقع بحرانی	کد ۷۰	۶
۷۱	ارزیابی کیفیت محصولات	کد ۷۱	۷
۷۲	نظارت و کنترل کیفیت	کد ۷۲	۷
۷۳	بهبود مستمر کیفیت محصولات و خدمات	کد ۷۳	۸
۷۴	بکارگیری فناوری اطلاعات در کیفیت	کد ۷۴	۴
۷۵	نظارت و کنترل زیرساخت‌ها	کد ۷۵	۷
۷۶	محافظت از زیرساخت‌ها	کد ۷۶	۵
۷۷	کنترل دسترسی به زیرساخت‌ها	کد ۷۷	۶
۷۸	بروزرسانی مستمر زیرساخت‌ها	کد ۷۸	۴
۷۹	نظارت و کنترل تراکنش‌ها	کد ۷۹	۴
۸۰	بررسی و تدقیق حسابان	کد ۸۰	۳
۸۱	به‌روزرسانی سیستم‌های مالی	کد ۸۱	۵
۸۲	رمزگذاری اطلاعات مالی	کد ۸۲	۴
۸۳	کنترل دسترسی به اطلاعات مالی	کد ۸۳	۳
۸۴	نظارت بر انتقال اطلاعات مالی	کد ۸۴	۴
۸۵	امکان بازیابی اطلاعات مالی	کد ۸۵	۵
۸۶	نظارت بر بدهی‌ها	کد ۸۶	۵
۸۷	نظارت بر موجودی	کد ۸۷	۶
۸۸	به‌روزرسانی سیستم‌های مدیریت بدهی و موجودی	کد ۸۸	۷
۸۹	ارزیابی ریسک‌های مالی	کد ۸۹	۶
۹۰	تخصیص مجوزهای دسترسی	کد ۹۰	۵
۹۱	کنترل دسترسی به اطلاعات مالی	کد ۹۱	۵
۹۲	بروزرسانی مستمر مجوزها	کد ۹۲	۴
۹۳	نظارت بر منابع مالی	کد ۹۳	۳
۹۴	برنامه‌ریزی منابع مالی	کد ۹۴	۷
۹۵	به‌روزرسانی سیستم‌های مدیریت منابع مالی	کد ۹۵	۱۱
۹۶	ارزیابی ریسک‌های مدیریت منابع مالی	کد ۹۶	۴
۹۷	نظارت بر پرداخت‌ها	کد ۹۷	۴
۹۸	کنترل دسترسی به سیستم‌های پرداخت	کد ۹۸	۴
۹۹	نظارت بر انتقال‌های مالی	کد ۹۹	۵
۱۰۰	بازیابی اطلاعات پرداخت	کد ۱۰۰	۴

ردیف	مفاهیم اولیه	کدهای باز	دفعات تکرار
۱۰۱	ارزیابی مستمر سلامت روان کارکنان	کد ۱۰۱	۵
۱۰۲	ایجاد و اجرای دوره‌های آموزشی برای آگاه‌سازی کارکنان در زمینه سلامت روان	کد ۱۰۲	۵
۱۰۳	ایجاد و اجرای برنامه‌های آموزشی برای آگاه‌سازی کارکنان در زمینه امنیت	کد ۱۰۳	۵
۱۰۴	برگزاری پویش های آگاه‌سازی برای افزایش آگاهی کارکنان در برابر تهدیدات امنیتی	کد ۱۰۴	۴
۱۰۵	ارزیابی دانش و مهارت‌های کارکنان در تهدیدات امنیتی	کد ۱۰۵	۶
۱۰۶	مشاوره و راهنمایی به کارکنان در راستای بهبود عملکرد امنیت	کد ۱۰۶	۵
۱۰۷	ارزیابی روان‌داده‌ها	کد ۱۰۷	۷
۱۰۸	نظارت و کنترل روان‌داده‌ها	کد ۱۰۸	۴
۱۰۹	ایجاد و اجرای برنامه‌های پیشگیری برای کاهش روان‌گیری و افزایش روان‌داده‌ها	کد ۱۰۹	۵
۱۱۰	به‌روزرسانی سیستم‌های روان‌داده	کد ۱۱۰	۶
۱۱۱	برنامه‌ریزی دوره‌های آموزشی	کد ۱۱۱	۶
۱۱۲	ارزیابی نیازهای آموزش	کد ۱۱۲	۷
۱۱۳	به‌روزرسانی سیستم‌های آموزشی	کد ۱۱۳	۸
۱۱۴	بررسی و تحلیل قوانین مربوط فعالیت سازمان	کد ۱۱۴	۹
۱۱۵	ارزیابی تأثیر قوانین بر سازمان	کد ۱۱۵	۹
۱۱۶	نظارت بر تغییرات قوانین	کد ۱۱۶	۸
۱۱۷	ایجاد سیاست‌های قانونی	کد ۱۱۷	۹
۱۱۸	نظارت و کنترل سیاست‌ها	کد ۱۱۸	۴
۱۱۹	ارزیابی اثربخشی سیاست‌ها	کد ۱۱۹	۵
۱۲۰	شناسایی و ارزیابی ریسک‌های قانونی	کد ۱۲۰	۴
۱۲۱	بروزرسانی مستمر ریسک‌ها	کد ۱۲۱	۳
۱۲۲	انجام ارزیابی‌های منظم برای بررسی توافق با قوانین و مقررات	کد ۱۲۲	۴
۱۲۳	نظارت و کنترل توافق	کد ۱۲۳	۳
۱۲۴	ارزیابی ریسک‌های عدم توافق	کد ۱۲۴	۵
۱۲۵	بکارگیری افراد خبره جهت نظارت و راهنمایی های دقیق در موارد قانونی	کد ۱۲۵	۴
۱۲۶	برنامه‌ریزی آموزشی جهت توجیه کارکنان در خصوص قوانین و مقررات	کد ۱۲۶	۳
۱۲۷	ایجاد پویش‌های آگاه‌سازی در زمینه رعایت قوانین	کد ۱۲۷	۴

در مرحله بعد مفاهیم اولیه براساس ارتباط، معنا و مفهوم دسته بندی شده و در ۳۷ مضمون فرعی قرار گرفتند، سپس کدهای فرعی مرتبط باهم دسته بندی شده و ۶ مضمون اصلی قرار گرفتند که در جدول ۴ قابل مشاهده می‌باشد.

جدول۳. الگوی جامع امنیت سازمانی

مضامین اصلی	مضامین فرعی	مفاهیم اولیه
امنیت فیزیکی	مراقبت از ساختمان‌ها و اموال	نظارت و کنترل ورود و خروج
		نظارت بر تردد در ساختمان‌ها
		محافظت از تجهیزات و اموال سازمان
		بررسی منظم ساختمان‌ها
	نظارت و کنترل دسترسی	تخصیص مجوزهای دسترسی
		نظارت بر دسترسی‌ها
		کنترل دسترسی به مناطق حیاتی
		بروزرسانی مستمر و دوره ای مجوزها
	نظارت و امنیت مدارک و اطلاعات حساس	نگهداری مدارک در مکان های ایمن
		کنترل دسترسی به اطلاعات حساس
		پشتیبان‌گیری اطلاعات
		نظارت بر انتقال اطلاعات حساس
	ایمنی ساختمان در برابر حوادث غیر مترقبه	نصب سیستم‌های اطفاء حریق
		برنامه‌ریزی جهت مواقع اضطراری
		آموزش کارکنان در خصوص بروز حوادث
		نظارت بر سیستم‌های ایمنی
	نظارت و امنیت پارکینگ‌ها و محیط‌های اطراف	نصب دوربین‌های مدار بسته(۳۶۰ درجه)
		کنترل دسترسی به پارکینگ‌ها
		نظارت بر امنیت محیط‌های اطراف
		برنامه‌ریزی اضطراری برای حوادث در محیط‌های اطراف
	مراقبت از مناطق حیاتی و مخازن داده	نظارت و کنترل دسترسی به مناطق حیاتی
		محافظت از مخازن داده
		نظارت بر امنیت مناطق حیاتی
		برنامه‌ریزی برای مواقع اضطراری در مناطق حیاتی
	حفاظت از ورودی‌ها و خروجی‌های ساختمان ها	نصب راه بندها و مانع‌های فیزیکی
		نظارت دقیق بر ورود و خروج افراد
		کنترل دسترسی به ورودی‌ها و خروجی‌ها
امنیت فضای مجازی	محافظت از شبکه‌ها و سیستم‌های اطلاعاتی	نصب دیواره‌های آتش
		استفاده از سیستم‌های تشخیص نفوذ
		استفاده سیستم‌های پاسخ به حوادث
		نظارت و مدیریت شبکه
	ایمنی داده‌ها و اطلاعات حساس	رمزگذاری داده‌ها

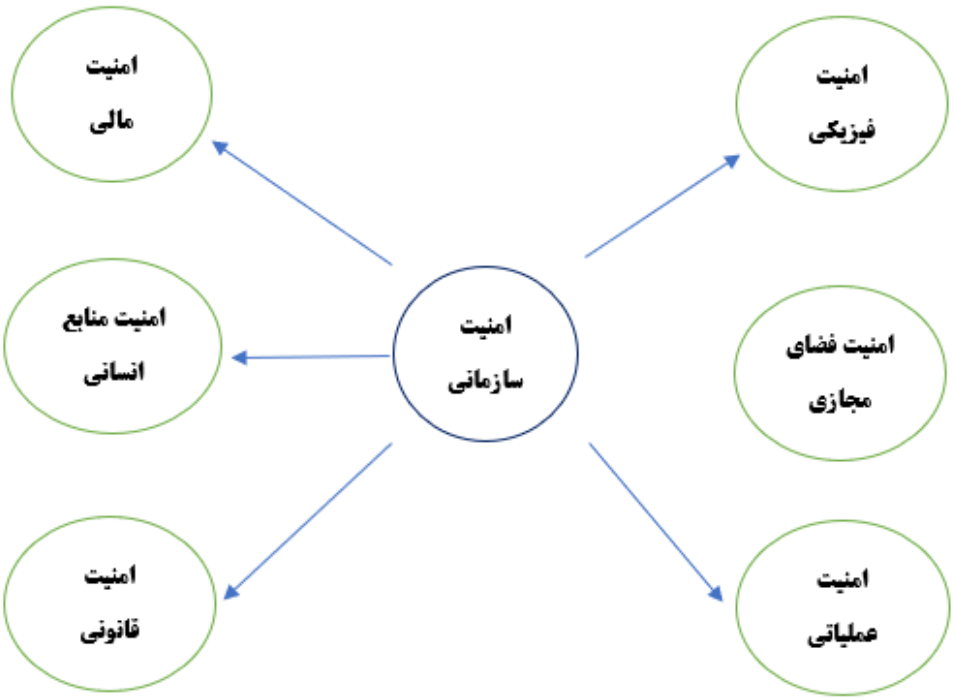
مضامین اصلی	مضامین فرعی	مفاهیم اولیه
		امکان بازیابی داده‌ها
		مدیریت داده‌ها
		حمایت از داده‌ها در برابر حملات
	مدیریت سطح دسترسی و مجوزها	مدیریت دسترسی ها
		تخصیص مجوزها بر اساس نقش افراد
		کنترل دسترسی به اطلاعات حساس
		بروزرسانی مستمر مجوزها
	پاسخ به حوادث امنیتی و بازسازی پس از آن‌ها	برنامه‌ریزی جهت پاسخ بموقع به حوادث
		تمرینات پاسخ به حوادث
		بازسازی پس از حادثه
		ارزیابی و یادگیری از حوادث
	آموزش و آگاه‌سازی کارکنان در زمینه امنیت فضای مجازی	برنامه‌ریزی آموزشی
		ایجاد پویش‌های آگاه‌سازی
		ارزیابی دانش و مهارت‌های کارکنان
		ارائه مشاوره و راهنمایی به کارکنان برای بهبود عملکرد و امنیت فضای مجازی
	مدیریت ریسک‌های فضای مجازی	شناسایی و ارزیابی ریسک‌ها
		برنامه‌ریزی مدیریت ریسک
		کنترل و نظارت بر ریسک‌ها
		بروزرسانی مستمر ریسک‌ها
	امنیت ارتباطات	ایمن سازی ارتباطات بی‌سیم
		ایمن سازی ارتباطات داخلی
		ایمن سازی ارتباطات خارجی
		کنترل دسترسی به شبکه‌های خارجی
امنیت عملیاتی	مدیریت ریسک‌های عملیاتی	شناسایی و ارزیابی ریسک‌ها ی عملیاتی
		برنامه‌ریزی مدیریت ریسک عملیاتی
		کنترل و نظارت بر ریسک‌های عملیاتی
		بروزرسانی مستمر ریسک‌ها
	نظارت بر فرآیندها و فرآیندهای کنترلی	ارزیابی کیفیت فرآیندها
		نظارت و کنترل فرآیندها
		بهبود فرآیندهای عملیاتی
		بکارگیری فناوری اطلاعات در فرآیندها
	اطمینان از سلامت و ایمنی کارکنان	برنامه‌ریزی سلامت و ایمنی کارکنان
		ارزیابی ریسک‌های سلامت و ایمنی

مضامین اصلی	مضامین فرعی	مفاهیم اولیه
		تعلیم و آموزش کارکنان در زمینه سلامت و ایمنی
		امکان مراقبت‌های پزشکی و بهداشتی در محیط کار
	مدیریت بحران و برنامه‌ریزی اضطراری	ایجاد تیم بحران
		برنامه‌ریزی اضطراری در مواقع بحران
		تمرینات اضطراری برای مواقع بحرانی
	نظارت بر کیفیت محصولات و خدمات	ارزیابی کیفیت محصولات
		نظارت و کنترل کیفیت
		بهبود مستمر کیفیت محصولات و خدمات
		بکارگیری فناوری اطلاعات در کیفیت
	امنیت زیرساخت‌های عملیاتی	نظارت و کنترل زیرساخت‌ها
		محافظت از زیرساخت‌ها
		کنترل دسترسی به زیرساخت‌ها
		بروزرسانی مستمر زیرساخت‌ها
امنیت مالی	نظارت بر تراکنش‌های مالی	نظارت و کنترل تراکنش‌ها
		بررسی و تدقیق حسابان
		به‌روزرسانی سیستم‌های مالی
	ایمنی اطلاعات مالی و داده‌های بانکی	رمزگذاری اطلاعات مالی
		کنترل دسترسی به اطلاعات مالی
		نظارت بر انتقال اطلاعات مالی
		امکان بازیابی اطلاعات مالی
	مدیریت بدهی و موجودی	نظارت بر بدهی‌ها
		نظارت بر موجودی
		به‌روزرسانی سیستم‌های مدیریت بدهی و موجودی
		ارزیابی ریسک‌های مالی
	نظارت بر دسترسی‌ها و مجوزهای مالی	تخصیص مجوزهای دسترسی
		کنترل دسترسی به اطلاعات مالی
		بروزرسانی مستمر مجوزها
	مدیریت منابع مالی	نظارت بر منابع مالی
		برنامه‌ریزی منابع مالی
		به‌روزرسانی سیستم‌های مدیریت منابع مالی
		ارزیابی ریسک‌های مدیریت منابع مالی
	امنیت پرداخت‌ها و انتقال‌های مالی	نظارت بر پرداخت‌ها
		کنترل دسترسی به سیستم‌های پرداخت

مضامین اصلی	مضامین فرعی	مفاهیم اولیه
		نظارت بر انتقال‌های مالی
		بازیابی اطلاعات پرداخت
امنیت منابع انسانی	مدیریت روانشناسی و سلامت روان کارکنان	ارزیابی مستمر سلامت روان کارکنان
		ایجاد و اجرای دوره‌های آموزشی برای آگاه‌سازی کارکنان در زمینه سلامت روان
	آموزش و آگاه‌سازی کارکنان در زمینه امنیت	ایجاد و اجرای برنامه‌های آموزشی برای آگاه‌سازی کارکنان در زمینه امنیت
		برگزاری پویش‌های آگاه‌سازی برای افزایش آگاهی کارکنان در برابر تهدیدات امنیتی
		ارزیابی دانش و مهارت‌های کارکنان در تهدیدات امنیتی
		مشاوره و راهنمایی به کارکنان در راستای بهبود عملکرد امنیت
	نظارت بر روان‌داده‌ها و روان‌گیری	ارزیابی روان‌داده‌ها
		نظارت و کنترل روان‌داده‌ها
		ایجاد و اجرای برنامه‌های پیشگیری برای کاهش روان‌گیری و افزایش روان‌داده‌ها
		به‌روزرسانی سیستم‌های روان‌داده
	توسعه مهارت‌ها و دانش کارکنان	برنامه‌ریزی دوره‌های آموزشی
		ارزیابی نیازهای آموزش
		به‌روزرسانی سیستم‌های آموزشی
امنیت قانونی و امتثال	شناسایی و ارزیابی قوانین و مقررات	بررسی و تحلیل قوانین مربوط فعالیت سازمان
		ارزیابی تأثیر قوانین بر سازمان
		نظارت بر تغییرات قوانین
	برنامه‌ریزی و اجرای سیاست‌های قانونی	ایجاد سیاست‌های قانونی
		نظارت و کنترل سیاست‌ها
		ارزیابی اثربخشی سیاست‌ها
	مدیریت ریسک‌های قانونی	شناسایی و ارزیابی ریسک‌های قانونی
		بروزرسانی مستمر ریسک‌ها
	نظارت بر توافق با قوانین و مقررات	انجام ارزیابی‌های منظم برای بررسی توافق با قوانین و مقررات
		نظارت و کنترل توافق
		ارزیابی ریسک‌های عدم توافق
		بکارگیری افراد خبره جهت نظارت و راهنمایی های دقیق در موارد قانونی
	تعلیم و آموزش کارکنان در زمینه قانونی و امتثال	برنامه‌ریزی آموزشی جهت توجیه کارکنان در خصوص قوانین و مقررات
		ایجاد پویش‌های آگاه‌سازی در زمینه رعایت قوانین

به این ترتیب پس از تعیین تم های فرعی و اصلی، الگوی تدوین شده را در اختیار ۵ خبره قرار گرفت که مورد تایید ایشان قرار گرفت.

شکل ۱. الگوی نهایی



۵. نتیجه‌گیری و پیشنهاد

از دیدگاه صاحب‌نظران مختلف، مفهوم امنیت در زمینه‌های مختلف معانی متفاوتی دارد. به‌عنوان مثال، ترکیب واژه "امنیت" با واژه‌هایی مانند ملی، سازمانی، انسانی، اجتماعی و... هر یک تعابیر خاص خود را دارد. با پیچیده‌تر شدن جهان امروز، ایجاد یک مزیت رقابتی برای سازمان‌ها کافی نیست؛ بلکه ضروری است که امنیت در جنبه‌های مختلف فیزیکی، فضای مجازی، عملیاتی، مالی، منابع انسانی و قانونی سازمان نیز تأمین شود. سهل‌انگاری در هر یک از این عوامل می‌تواند به شکست سازمان منجر شود. زیرا امروزه، تهدیدهایی همچون هک اطلاعات سازمان، دستبرد فیزیکی به دارایی‌ها و از دست دادن نیروی انسانی ماهر می‌تواند سازمان را با چالش‌های جدی مواجه کند. علاوه بر این، با پیش‌بینی صحیح و اتخاذ اقدامات مؤثر در تأمین مالی پروژه‌ها و پیروی از قوانین و مقررات مصوب، می‌توان امنیت سازمان را تقویت کرد.

در نهایت، الگوی امنیت سازمانی به‌طور جامع و در راستای پایداری کسب‌وکار به‌صورت زیر تدوین شده است. همانطور که در جدول ۴ قابل مشاهده است، الگوی جامع امنیت سازمانی شامل ۱۲۷ مفهوم اولیه، ۳۷ مضمون فرعی و ۶ مضمون اصلی است.

در دنیای امروز، سازمان‌ها با چالش‌های متعددی برای بقا مواجه هستند که تهدیدهای امنیتی، یکی از اصلی‌ترین این چالش‌ها به‌شمار می‌روند. با توجه به پیچیدگی و تنوع این تهدیدات، تدوین یک الگوی جامع و نظام‌مند امنیت سازمانی به یک ضرورت تبدیل شده است. الگوی پیشنهادی ما شامل شش تم اصلی است که هر یک به‌طور خاص به جنبه‌های مختلف امنیت سازمان می‌پردازد و به سازمان‌ها کمک می‌کند تا به‌طور مؤثری به تهدیدات پاسخ دهند و پایداری کسب‌وکار خود را تضمین کنند.

امنیت فیزیکی، به‌عنوان یکی از ارکان اصلی این الگو، شامل اقداماتی است که به حفاظت از دارایی‌های فیزیکی و افراد در برابر تهدیدات و خطرات بالقوه پرداخته و محیطی ایمن را برای فعالیت‌های سازمان فراهم می‌کند. این امنیت نه تنها به حفاظت از تجهیزات و زیرساخت‌ها کمک می‌کند، بلکه اعتماد کارکنان و مشتریان را نیز تقویت می‌نماید. از نصب دوربین‌های مداربسته و سیستم‌های کنترل دسترسی گرفته تا نظارت بر کارکنان و اشخاص، تمامی این اقدامات به ایجاد یک محیط ایمن و پایدار برای کسب‌وکار کمک می‌کند.

در کنار امنیت فیزیکی، امنیت سایبری به‌عنوان یکی دیگر از مضامین کلیدی الگو، به حفاظت از اطلاعات و داده‌های دیجیتال سازمان می‌پردازد. با توجه به رشد روزافزون تهدیدات فضای مجازی، از جمله هک‌ها، باج‌افزارها و حملات فیشینگ، سازمان‌ها نیازمند استراتژی‌های امنیت سایبری قوی هستند. این استراتژی‌ها شامل استفاده از نرم‌افزارهای امنیتی پیشرفته، آموزش کارکنان درباره خطرات سایبری و تدوین

سیاست‌های مشخص برای مدیریت داده‌ها و اطلاعات می‌شود. حفاظت از داده‌ها نه تنها به امنیت سازمان کمک می‌کند، بلکه به حفظ اعتبار و اعتماد مشتریان نیز می‌انجامد.

امنیت عملیاتی به بررسی و تأمین امنیت فرآیندها و فعالیت‌های روزمره سازمان اشاره دارد. این مضمون به شناسایی نقاط ضعف در فرآیندها و طراحی راهکارهای مناسب برای کاهش ریسک‌ها می‌پردازد. از مدیریت زنجیره تأمین گرفته تا نظارت بر فعالیت‌های روزمره، امنیت عملیاتی به سازمان‌ها کمک می‌کند تا به‌طور مؤثری از منابع خود استفاده کنند و از بروز مشکلات جلوگیری نمایند. این امر در نهایت به افزایش بهره‌وری و کاهش هزینه‌ها منجر می‌شود.

امنیت مالی به حفاظت از منابع مالی و جلوگیری از تقلب‌ها و سوءاستفاده‌های مالی مربوط می‌شود. در دنیای کسب‌وکار، سلامت مالی سازمان یک عامل کلیدی در پایداری و رشد آن است. با اتخاذ تدابیر مناسب، مانند حسابرسی‌های داخلی منظم، نظارت بر تراکنش‌های مالی و تدوین سیاست‌های شفاف مالی، سازمان‌ها می‌توانند از منابع مالی خود به‌طور مؤثر محافظت کرده و از بروز مشکلات مالی جلوگیری نمایند. این اقدام نه تنها به حفظ اعتبار سازمان کمک می‌کند، بلکه به تأمین مالی پروژه‌ها و فعالیت‌های آینده نیز می‌انجامد.

امنیت منابع انسانی به حفاظت از سرمایه انسانی سازمان و مدیریت صحیح نیروی کار مربوط می‌شود. کارکنان، به‌عنوان یکی از ارزشمندترین دارایی‌های هر سازمان، باید در اولویت قرار گیرند. این امنیت شامل ایجاد محیط کار ایمن، ارائه آموزش‌های لازم و تدوین سیاست‌های مناسب برای مدیریت منابع انسانی می‌شود. علاوه بر این، امنیت منابع انسانی به مدیریت ریسک‌های مربوط به استخدام، ترک شغل و مسائل قانونی نیز مرتبط است. ایجاد فرهنگ سازمانی مثبت و حمایت از کارکنان در برابر تهدیدات می‌تواند به افزایش بهره‌وری و رضایت شغلی منجر شود.

نهایتاً، امنیت قانونی و امتثال به رعایت قوانین و مقررات مرتبط با فعالیت‌های سازمان، از اهمیت بالایی برخوردار است. این مضمون به‌ویژه در دنیای امروز که قوانین و مقررات به‌سرعت در حال تغییر هستند، اهمیت بیشتری پیدا می‌کند. سازمان‌ها باید به‌طور مداوم بر تغییرات قانونی نظارت داشته باشند و اطمینان حاصل کنند که تمامی فعالیت‌های آنها با قوانین و مقررات مرتبط مطابقت دارد. این امر نه تنها به جلوگیری از مشکلات حقوقی و مالی کمک می‌کند، بلکه به حفظ اعتبار سازمان در جامعه نیز منجر می‌شود.

در نهایت، این شش مضمون اصلی به‌عنوان اجزای کلیدی الگوی امنیت سازمانی به سازمان‌ها کمک می‌کند تا به‌طور جامع و نظام‌مند به تهدیدات پاسخ دهند. با بهره‌گیری از این الگو، سازمان‌ها می‌توانند محیطی ایمن و پایدار برای فعالیت‌های خود ایجاد کنند و از منابع خود به‌طور مؤثر محافظت نمایند. این رویکرد جامع، به سازمان‌ها این امکان را می‌دهد که نه تنها در برابر تهدیدات فعلی ایمن بمانند، بلکه برای چالش‌های آینده نیز آمادگی لازم را داشته باشند. با توجه به تغییرات سریع در دنیای کسب‌وکار و ظهور تهدیدات جدید، پیاده‌سازی این الگو می‌تواند به بهبود عملکرد و پایداری سازمان کمک کند و در نهایت به موفقیت و رشد پایدار آنها منجر شود.

برهمین اساس پیشنهادات زیر مطرح میگردد:

* لازمه ی موفقیت و بهره مندی در هر یک از مقوله های تعیین شده، بکارگیری افراد خبره در راس واحدهای مربوطه است. مثلا لازم است یک حقوق دان مجرب در راس واحد حقوقی سازمان قرار گیرد تا به بهترین نحو ممکن سازگاری سازمان با قوانین و مقررات موجود را بررسی نماید و.....

* توسعه پایگاه داده های ملی و یا درون سازمانی شرط مهم در حفظ امنیت اطلاعاتی سازمان می‌باشد. بدیهی است هرچه سازمان ها در این امر کوشا باشند با مشکلات و چالش های اندکی مواجه خوهند شد.

* در هر سازمان و یا در واحدهای سازمانی، تشکیل کارگروه هایی جهت بررسی موانع و مشکلات بصورت دوره ای بسیار مفید خواهد بود، لذا مدیریت سازمان باید نسبت به این امر کوشا بوده و بطور مرتب گزارشات کارگروه ها را بررسی نماید.

* توجه لازم به بحث آموزش کارکنان امری ضروری بوده و باید در دستور کار سازمان قرار گیرد. این آموزش ها باید بصورت دوره ای و منظم برای کلیه افراد سازمان برگزار و یادآوری مطالب گذشته و یادگیری مطالب جدید را در پی داشته باشد.

* باتوجه به توسعه روزافزون دانش در حوزه های مختلف، بروزرسانی سیستم های سازمانی در بازه های یک تا سه ساله بسیار سودمند بوده و میتواند نتایج خوبی در پایداری امنیت سازمانی داشته باشد.

منابع

1. Alinajad, F., Akbari, M., & Shiri, N. (2023). Conceptualization of the components of the sustainability model for women's businesses in Behbahan County. Women in Development and Politics, 21(3), 717-741. [In Persian]
2. Alsaif, M., Aljaafari, N., & Khan, A. R. (2015). Information security management in Saudi Arabian organizations. Procedia Computer Science, 56, 213-216. http://dx.doi.org/10.1016/j.procs.2015.07.201
3. Bocken, N. M., Short, S. W., Rana, P., & Evans, S. (2014). A literature and practice review to develop sustainable business model archetypes. Journal of cleaner production, 65, 42-56.
4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.
5. Cagnin, C. H., Loveridge, D., & Butler, J. (2005). Business sustainability maturity model. *Business Strategy and the Environment,* 9(6), 4-6.
6. Doane, D., & MacGillivray, A. (2001). Economic sustainability: The business of staying in business. New Economics Foundation, 1-52.
7. Dyllick, T., & Muff, K. (2016). Clarifying the meaning of sustainable business: Introducing a typology from business-as-usual to true business sustainability. Organization & Environment, 29(2), 156-174.
8. Fadai Kiyani, R., Azizi, M., & Badi' Zadeh, A. (2020). Providing a sustainability model for family businesses. Business Management Quarterly, 13(580), 384-415. [In Persian]
9. Freeman, E. Q. (2000). E-merging Risks. Risk Management, 47(7), 12-12.
10. Hinde, S. (1998). Special feature: Recent security surveys. Computers and Security, 17(3), 207-210.
11. Hoffman, A. J. (2018). The next phase of business sustainability. Stanford Social Innovation Review, 16(2), 34-39.
12. Kalabi, A. M. (2020). Modeling the factors affecting the sustainability of business models. Public Management Research, 13(47), 111-134. [In Persian]
13. Kiron, D., Kruschwitz, N., Haanaes, K., Reeves, M., Fuisz-Kehrbach, S. K., & Kell, G. (2015). Joining forces: Collaboration and leadership for sustainability. MIT Sloan Management Review.
14. Maas, K., Schaltegger, S., & Crutzen, N. (2016). Integrating corporate sustainability assessment, management accounting, control, and reporting. Journal of Cleaner Production, 136, 237-248.
15. Mahmoudzadeh Ahmadinejad, A., Nazemi Ashni, A., & Mahmoudzadeh, E. (2024). A Look to the Future in Startups: A Review of the Most Common Foresight Methods in Business Model Design in Startups. Journal of Standard and Quality Management, 13(4), 141-173. [In Persian] https://doi.org/10.22034/jsqm.2024.412594.1520
16. Malorgio, G., & Marangon, F. (2021). Agricultural business economics: the challenge of sustainability. Agricultural and Food Economics, 9, 1-4.
17. Pham, H. C., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. Journal of Information Security and Applications, 46, 96-107. https://doi.org/10.1016/j.jisa.2019.03.012
18. Salari Nia, M. M., Niknami, M., Sabouri, M. S., & Rafiei, H. (2024). Providing a good governance model for the sustainability of agricultural businesses in Tehran Province (Case study: Agricultural Bank). Agricultural Economics and Development. [In Persian]
19. Seyfollahi Anar, N., & Akbari Arbatani, G. (2023). Providing a model for business sustainability based on digital skills during the COVID-19 pandemic. Scientific-Research Journal of International Business Management, 6(4), 179-198. [In Persian]
20. Sharafi, L., Rezai, R., Mirkezadeh, A. A., & Karami Dehkordi, I. (2019). Designing a sustainability model for small and medium agricultural businesses in Kermanshah Province. Agricultural Promotion and Education Research, 12(2 (Sequential 46)), 11-24. [In Persian]
21. Shirmohammadi, A., Moftahi, H., & Tabaan, M. (2023). Designing a sustainability model for the automotive industry in Iran. Innovation Management in Defense Organizations, 6(3), 129-156. [In Persian]
22. Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. Journal of management information systems, 37(1), 129-161. http://dx.doi.org/10.1080/07421222.2019.1705512
23. Ulvenblad, P., Barth, H., Ulvenblad, P. O., Ståhl, J., & Björklund, J. C. (2020). Overcoming barriers in agri-business development: two education programs for entrepreneurs in the Swedish agricultural sector. The Journal of Agricultural Education and Extension, 26(5), 443-464.
24. Wanjiku Njogu, S. (2016). Factors Affecting Sustainability of Women Enterprises: Insights from Kapsabet Town (KT) Experience, Kenya. Humanities and Social Sciences, 4(4), 90-99.
25. Wood, C. (2000). Integrated approach includes information security. Security, 37(2), 43-44.