ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη ασφάλειας πληροφοριακών συστημάτων σε φορείς ή επιχειρήσεις

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΠΑΡΑΣΚΕΥΗΣ ΓΕΡΟΥ

(ΑΕΜ: 2816)

Επιβλέπων : Δ. ΒΕΡΓΑΔΟΣ

Καστοριά, Μάρτιος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη ασφάλειας πληροφοριακών συστημάτων σε φορείς ή επιχειρήσεις

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΠΑΡΑΣΚΕΥΗΣ ΓΕΡΟΥ (ΑΕΜ: 2816)

Επιβλέπων : **Δ. ΒΕΡΓΑΔΟΣ**

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδιότητα Μέλους	Ιδιότητα Μέλους	Ιδιότητα Μέλους

Καστοριά, Μάρτιος 2024

Ευχαριστίες

Περίληψη

Η μελέτη που ακολουθεί επικεντρώνεται στην ποιοτική ανασκόπηση και στην ποσοτική ανάλυση του βαθμού ασφάλειας των πληροφοριακών συστημάτων σε φορείς ή επιχειρήσεις. Πρόκειται για ένα μείζον ζήτημα, καθότι το πρόβλημα της ασφάλειας των πληροφοριακών συστημάτων είναι κάτι που απασχολεί την πληροφορική από τα πρώτα της βήματα. Από την αρχή, οι προγραμματιστές και οι μηχανικοί λογισμικού αντιμετώπιζαν την ανάγκη να προστατεύσουν τα συστήματα από διάφορες απειλές, όπως κακόβουλο λογισμικό, ανεπιθύμητη παρέμβαση και παραβιάσεις ασφαλείας. Με την εξέλιξη της τεχνολογίας και τη διάδοση των πληροφοριακών συστημάτων σε ευρύτερους κύκλους χρηστών, οι κίνδυνοι ασφάλειας έχουν γίνει ακόμη πιο προβληματικοί. Η σύνδεση με το διαδίκτυο και η χρήση διαδικτυακών υπηρεσιών έχουν δημιουργήσει νέους τρόπους επίθεσης και αυξημένες πιθανότητες παραβίασης της ασφάλειας.

Κύριο θέμα διερεύνησης της μελέτης είναι ο βαθμός διασφάλισης των πληροφοριακών προγραμμάτων που χρησιμοποιούν τόσο οι δημόσιοι φορείς, όσο και οι επιχειρήσεις. Σκοπός της μελέτης είναι η παρουσίαση των χαρακτηριστικών στοιχείων των πληροφοριακών συστημάτων, περιλαμβάνοντας στοιχεία που αφορούν το εννοιολογικό περιεχόμενο τους, τις κατηγορίες, τις δυνατότητες και τα οφέλη που προσδίδουν γενικότερα. Επιπρόσθετος σκοπός είναι η παρουσίαση των μεθόδων εξασφάλισης της λειτουργίας τους, αναδεικνύοντας την πολιτική, τους κανόνες, τη διαδικασία, τη σκοπιμότητα και το σχεδιασμό ασφάλειας τους. Ακόμη, βασικός σκοπός της μελέτης είναι η πραγματοποίηση πρωτογενούς ποσοτικής έρευνας σε φορείς και επιχειρήσεις (δείγμα) σχετικά με τις πολιτικές ασφαλείας που εφαρμόζουν στα πληροφοριακά συστήματα τους.

Η επίτευξη των παραπάνω επιτυγχάνεται με την βιβλιογραφική ανασκόπηση (δευτερογενή έρευνα) που παραθέτει δεδομένα και υλικό μέσα από άλλες μελέτες και έρευνες που δημοσιεύθηκαν σε επιστημονικά περιοδικά. Όσον αφορά την μελέτη αυτή και τον σκοπό της κρίθηκε ως αναγκαία η διεξαγωγή πρωτογενούς έρευνας προς ένα δείγμα φορέων και επιχειρήσεων, έτσι ώστε να προσδιορίσουν τον βαθμό

εφαρμογής των πολιτικών ασφαλείας στα πληροφοριακά τους συστήματα. Η έρευνα αυτή απευθύνεται στο δείγμα με την συμβολή ενός ερωτηματολογίου.

Λέξεις – Κλειδιά

πληροφοριακά συστήματα, χρήση, ασφάλεια, πολιτικές, διαδικασία, σχέδιο

Abstract

The following study focuses on the qualitative review and the quantitative analysis of the degree of security of information systems in agencies or businesses. This is a major issue, as the problem of information systems security is something that has concerned IT since its earliest stages. Since the beginning, software developers and engineers have faced the need to protect systems from various threats, such as malware, unwanted interference, and security breaches. With the development of technology and the spread of information systems to wider circles of users, security risks have become even more problematic. Connecting to the internet and using online services has created new avenues of attack and increased potential for security breaches.

The main subject of investigation of the study is the degree of assurance of the information programs used by both public bodies and businesses. The purpose of the study is the presentation of the characteristic elements of information systems, including elements concerning their conceptual content, categories, possibilities and the benefits they provide in general. An additional purpose is to present the methods of ensuring their operation, highlighting their policy, rules, procedure, feasibility and security design. Also, the main purpose of the study is to carry out primary quantitative research on institutions and companies (sample) regarding the security policies they apply to their information systems.

The achievement of the above is achieved with the bibliographic review (secondary research) which cites data and material through other studies and research published in scientific journals. With regard to this study and its purpose, it was deemed necessary to carry out a primary survey to a sample of organizations and businesses, so as to determine the degree of implementation of security policies in their information systems. This research is addressed to the sample with the contribution of a questionnaire.

Key Words

information systems, use, security, policies, process, design

Πίνακας Περιεχομένων

Λίστα Πινάκων

Λίστα Διαγραμμάτων

Εισαγωγή

Η εργασία που ακολουθεί διαρθρώνεται σε τέσσερα κεφάλαια τα οποία φέρουν συγκεκριμένο τίτλο και υποκεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζονται όλες οι πληροφορίες που αφορούν τα πληροφοριακά συστήματα, ξεκινώντας από την ανάλυση του όρου, τις κατηγορίες τους, τον σκοπό που εκτελούν, τα οφέλη και τα προβλήματα που πρόκειται να επιφέρουν, αλλά και το βαθμό αναγκαιότητας τους για πολλές επιχειρήσεις.

Στο δεύτερο κεφάλαιο πλαισιώνονται στοιχεία που αφορούν την ασφάλεια των πληροφοριακών συστημάτων, προσδιορίζοντας τις πολιτικές τους, τις οδηγίες, τις διαδικασίες και το σχέδιο ασφαλείας. Ακόμη, προσδιορίζεται η σκοπιμότητα της ασφάλειας των πληροφοριακών συστημάτων και τα χαρακτηριστικά των πολιτικών, ως προς τα είδη, τις μορφές, τους άξονες και τις μεθόδους υλοποίησης τους.

Στο τρίτο κεφάλαιο παρατίθενται οι πληροφορίες για την μεθοδολογία έρευνας, προσδιορίζοντας τη μέθοδο που χρησιμοποιήθηκε, τον ερευνητικό σκοπό, το δείγμα που συμμετείχε, το ερευνητικό εργαλείο και τις μεθόδους ανάλυσης.

Στο τέταρτο κεφάλαιο παρατίθενται τα αποτελέσματα της πρωτογενούς έρευνας με τη συμβολή πινάκων και διαγραμμάτων, η σύνοψη τους, οι ερευνητικοί περιορισμοί και οι προτάσεις για μελλοντική έρευνα.

Η εργασία ολοκληρώνεται με τη συγγραφή των γενικών συμπερασμάτων.

1. Πληροφοριακά Συστήματα

1.1 Εννοιολογικό περιεχόμενο

Ένα Πληροφοριακό Σύστημα (ΠΣ) είναι ένα σύνολο διαδικασιών, δεδομένων, εργαλείων και τεχνολογιών που σχεδιάζονται και χρησιμοποιούνται για τη συλλογή, την αποθήκευση, την επεξεργασία, τη διάδοση και την ανάκτηση πληροφοριών με σκοπό την υποστήριξη λήψης αποφάσεων, τη διαχείριση διαδικασιών και την επίτευξη στόχων ενός οργανισμού. Σε απλούστερους όρους, αποτελεί ένα σύστημα που διαχειρίζεται πληροφορίες με σκοπό τη βελτίωση της αποτελεσματικότητας και της απόδοσης των οργανισμών. Αυτός ο ορισμός εφαρμόζεται ευρέως σε διάφορους τομείς, συμπεριλαμβανομένων της τεχνολογίας, της βιομηχανίας, της επιστήμης και πολλών άλλων (Zemmouchi-Ghomari, 2021).

Ουσιαστικά, ένα ΠΣ αποτελείται από διαδικασίες, τεχνολογίες και ανθρώπινους πόρους που συλλέγουν, αποθηκεύουν, επεξεργάζονται και διαχειρίζονται πληροφορίες με σκοπό την υποστήριξη της διοίκησης και της λήψης αποφάσεων σε μία επιχείρηση. Αυτό επιτυγχάνεται μέσω της παροχής ακριβών, εγκαίρων και συνολικών πληροφοριών που απαιτούνται για τη λήψη αποφάσεων και τον έλεγχο των δραστηριοτήτων της επιχείρησης. Ένα ΠΣ μπορεί να καλύπτει ευρύ φάσμα λειτουργιών και δραστηριοτήτων, από τη διαχείριση επιχειρηματικών δεδομένων μέχρι τη διαχείριση προσωπικού και την επικοινωνία με τους πελάτες (Ming et al., 2021).

Αυτό το είδος των συστημάτων είναι σχεδιασμένο για να συλλέγει, να αποθηκεύει, να επεξεργάζεται και να παρέχει πληροφορίες από διάφορες πηγές σε μια οργάνωση. Τα δεδομένα μπορεί να προέρχονται από εσωτερικούς και εξωτερικούς πόρους, όπως εφαρμογές λογισμικού, βάσεις δεδομένων, αρχεία, αισθητήρες και άλλες πηγές (Zemmouchi-Ghomari, 2021). Το ΠΣ στη συνέχεια επεξεργάζεται αυτά τα δεδομένα και τα παρουσιάζει στους χρήστες με τρόπο που είναι εύκολος να κατανοηθεί και να χρησιμοποιηθεί για τη λήψη αποφάσεων. Η ικανότητα να ενοποιεί δεδομένα από διάφορες πηγές είναι σημαντική για να διασφαλιστεί ότι οι αποφάσεις λαμβάνονται με βάση ολοκληρωμένες και ολοκληρωμένες πληροφορίες (Ming et al., 2021).

Ένα ολοκληρωμένο Πληροφοριακό Σύστημα (ΠΣ) που συνδυάζει τόσο ανθρώπινους πόρους, όσο και μηχανικούς πόρους για την παροχή πληροφοριών που υποστηρίζουν τις δραστηριότητες μιας επιχείρησης. Το ΠΣ αυτό χρησιμοποιεί μηχανολογικό εξοπλισμό και λογισμικό για την ανάλυση, τον προγραμματισμό, τον έλεγχο και τη λήψη αποφάσεων (Dusmanescu and Bradic-Martinovic, 2011). Σημαντικό στοιχείο αυτού του ΠΣ είναι η χρήση μιας τράπεζας δεδομένων, η οποία αποθηκεύει και διαχειρίζεται τις πληροφορίες που απαιτούνται για τη λήψη αποφάσεων. Με τη χρήση αυτής της τράπεζας δεδομένων, το ΠΣ μπορεί να προσφέρει ακριβείς και ενημερωμένες πληροφορίες που απαιτούνται για την ανάλυση της κατάστασης της επιχείρησης και τη λήψη στρατηγικών αποφάσεων. Με άλλα λόγια, το ΠΣ αυτό αξιοποιεί τόσο την τεχνολογία όσο και τον ανθρώπινο παράγοντα για την αποτελεσματική λήψη αποφάσεων και τη διαχείριση των επιχειρηματικών δραστηριοτήτων (Moussa and El Arbi, 2020).

Το ΠΣ συνήθως συλλέγει δεδομένα από διάφορες πηγές, συμπεριλαμβανομένων εξωτερικών πηγών όπως αγορές, ανταγωνιστές, και εσωτερικών πηγών όπως επιχειρησιακές συναλλαγές και διαδικασίες. Αφού συλλέξει τα δεδομένα, το ΠΣ τα επεξεργάζεται με σκοπό τον εντοπισμό των σημαντικών πληροφοριών και τη διάταξή τους σε τρόπο που είναι εύκολος να κατανοηθεί από τα διευθυντικά στελέχη. Το ΠΣ παρέχει τις επεξεργασμένες πληροφορίες στους διευθυντές ή τους χρήστες σε μορφή που είναι κατανοητή και χρήσιμη για τη λήψη αποφάσεων (Zemmouchi-Ghomari, 2021). Επιπλέον, το ΠΣ μπορεί να παρέχει εργαλεία και μέσα στα διευθυντικά στελέχη για τη δημιουργία περαιτέρω αναλύσεων και πληροφοριών που απαιτούνται για τη λήψη αποφάσεων. Αυτή η διαδικασία βοηθά τα διευθυντικά στελέχη να ενημερώνονται και να λαμβάνουν αποφάσεις βασισμένες σε δεδομένα και πληροφορίες που είναι ακριβή, ενημερωμένα και συνολικά (Zhang, 2017).

Σημαντικό χαρακτηριστικό του ΠΣ είναι η εστίασή του στην υποστήριξη της λήψης αποφάσεων και των επιχειρησιακών διαδικασιών της επιχείρησης (Moussa and El Arbi, 2020). Επίσης, αναγνωρίζεται η σημασία του να υπάρχει κοινή κατανόηση και ορισμός μεταξύ των χρηστών, του τμήματος του ΠΣ και της διοίκησης της επιχείρησης, προκειμένου να επιτευχθούν τα καλύτερα δυνατά αποτελέσματα από τη χρήση του ΠΣ (Alotaibi, 2022). Συνεπώς, το ΠΣ αντιπροσωπεύει ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης σε μία επιχείρηση, παρέχοντας σημαντική πληροφόρηση και ενισχύοντας την αποτελεσματικότητά της (Zemmouchi-Ghomari, 2021).

1.2 Κυριότερες κατηγορίες ΠΣ

Τα ΠΣ μπορούν να διακριθούν σε διάφορες κατηγορίες ανάλογα με διάφορα κριτήρια, συμπεριλαμβανομένου του είδους της επεξεργασίας των δεδομένων και των αποδεκτών χρηστών ή στελεχών της επιχείρησης (Taherdoost, 2022). Μερικές κοινές κατηγορίες περιλαμβάνουν:

- **Τα Συστήματα Επεξεργασίας Συναλλαγών (TPS)** είναι συστήματα πληροφορικής που χρησιμοποιούνται για την εκτέλεση και τη διαχείριση μεγάλου όγκου συναλλαγών μιας επιχείρησης. Αυτές οι συναλλαγές μπορεί να αφορούν πωλήσεις, αγορές, παραγγελίες, πληρωμές και άλλες επιχειρηματικές δραστηριότητες που απαιτούν καταγραφή, επεξεργασία και αποθήκευση δεδομένων (Al-Mamary et al., 2014; Taherdoost, 2022).

- **Τα Συστήματα Διαχείρισης Πληροφοριών (Management Information Systems, MIS)** είναι συστήματα πληροφορικής που σχεδιάζονται για να συλλέγουν, να αποθηκεύουν, να επεξεργάζονται και να αναφέρουν πληροφορίες που αφορούν τις λειτουργικές δραστηριότητες ενός οργανισμού. Τα MIS χρησιμοποιούνται σε όλα τα επίπεδα διαχείρισης ενός οργανισμού και παρέχουν στους διαχειριστές τις πληροφορίες που χρειάζονται για τη λήψη αποφάσεων (Al-Mamary et al., 2014; Taherdoost, 2022).

- **Τα Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems, DSS)** είναι συστήματα πληροφορικής που σχεδιάζονται για να βοηθήσουν τους διαχειριστές και τους λήπτες αποφάσεων στην ανάλυση των πληροφοριών και τη λήψη καλών αποφάσεων. Τα DSS συνήθως παρέχουν εργαλεία για την ανάλυση των δεδομένων, τη δημιουργία μοντέλων, τη διεξαγωγή προσομοιώσεων και την αξιολόγηση των εναλλακτικών λύσεων (Al-Mamary et al., 2014; Taherdoost, 2022).

- **Τα Συστήματα Υποστήριξης Διευθυντικών Στελεχών (Executive Support Systems, ESS)** είναι συστήματα πληροφορικής σχεδιασμένα ειδικά για τους επικεφαλής και τους υψηλόβαθμους διευθυντές σε μια επιχείρηση. Τα ESS παρέχουν τη δυνατότητα στους διευθυντές να λαμβάνουν γρήγορες αποφάσεις

με βάση τα στρατηγικά στοιχεία και τις ανάγκες της επιχείρησης (Σπηλιώτη, 2022).

- **Τα Συστήματα Αυτοματισμού Γραφείου (Office Automation Systems, OAS)** είναι συστήματα πληροφορικής που σχεδιάζονται για να βελτιστοποιούν και να αυτοματοποιούν τις καθημερινές διαδικασίες και εργασίες σε ένα γραφείο ή μια επιχείρηση. Τα OAS προσφέρουν ένα ευρύ φάσμα λειτουργιών και υπηρεσιών που βοηθούν στην ομαλή λειτουργία του γραφείου και στην αποτελεσματική διαχείριση των εργασιών (Σπηλιώτη, 2022).

Κάθε κατηγορία ΠΣ έχει τον δικό της στόχο και την αντίστοιχη επεξεργασία δεδομένων που αντιστοιχεί στις ανάγκες και τις λειτουργίες των διαφορετικών τομέων μιας επιχείρησης (Taherdoost, 2022).

1.2.1 Λειτουργίες και ΠΣ

Οι λειτουργίες ενός ΠΣ είναι οι δραστηριότητες που εκτελεί προκειμένου να επεξεργαστεί, να αποθηκεύσει, να διαχειριστεί και να παρουσιάσει πληροφορίες (Alter, 2008). Αυτές οι λειτουργίες περιλαμβάνουν:

- *Συλλογή Δεδομένων*: Αφορά τη συλλογή όλων των αναγκαίων δεδομένων από διάφορες πηγές, είτε εσωτερικές είτε εξωτερικές της επιχείρησης.
- *Αποθήκευση Δεδομένων*: Τα δεδομένα που συλλέγονται αποθηκεύονται σε κατάλληλες βάσεις δεδομένων ή άλλες μορφές αποθήκευσης (Chuma, 2020).
- *Επεξεργασία Δεδομένων*: Τα δεδομένα υφίστανται επεξεργασία για τη μετατροπή τους σε χρήσιμες πληροφορίες. Αυτή η επεξεργασία μπορεί να περιλαμβάνει ανάλυση, υπολογισμούς, συγκρίσεις και άλλες διαδικασίες.
- *Διαχείριση Δεδομένων*: Περιλαμβάνει τον έλεγχο της ποιότητας των δεδομένων, τη διαχείριση της ασφάλειας των δεδομένων και τη διαχείριση της πρόσβασης σε αυτά.

- *Παρουσίαση Πληροφοριών*: Τέλος, οι πληροφορίες παρουσιάζονται σε μορφές που είναι κατανοητές και χρήσιμες για τους χρήστες, όπως αναφορές, γραφήματα, διαγράμματα κ.λπ. (Singh and Kaur, 2012).

Αυτές οι λειτουργίες εκτελούνται από το ΠΣ, προκειμένου να διασφαλιστεί ότι οι πληροφορίες που παρέχονται είναι ακριβείς, ενημερωμένες και χρήσιμες για τους χρήστες του συστήματος (Vargas et al., 2019).

1.2.2 Διοίκηση και ΠΣ

Η διοίκηση συνδέεται στενά με τα ΠΣ, καθώς αποτελούν ουσιαστικό εργαλείο για τη λήψη αποφάσεων, την οργάνωση και τον έλεγχο των δραστηριοτήτων της επιχείρησης (Berisha – Shaqiri, 2014). Παρακάτω παρουσιάζεται το πώς συνδέονται η διοίκηση και τα ΠΣ:

- **Υποστήριξη Λήψης Αποφάσεων**: παρέχουν τις απαραίτητες πληροφορίες και αναλύσεις που χρειάζεται η διοίκηση για να λάβει αποφάσεις. Αυτές οι πληροφορίες μπορούν να προέλθουν από διάφορα τμήματα της επιχείρησης και να είναι σχετικές με την οικονομική κατάσταση, τις πωλήσεις, την παραγωγή, τις αποθήκες και άλλες λειτουργίες.

- **Οργάνωση Επιχειρησιακών Διαδικασιών**: μπορούν να βοηθήσουν στην οργάνωση και την αυτοματοποίηση των διαδικασιών της επιχείρησης. Αυτό μπορεί να περιλαμβάνει την εφαρμογή συστημάτων ERP (Enterprise Resource Planning) για την ολοκληρωμένη διαχείριση των πόρων της επιχείρησης.

- **Έλεγχος και Παρακολούθηση**: επιτρέπουν στη διοίκηση να παρακολουθεί τις επιδόσεις της επιχείρησης μέσω δεικτών απόδοσης και αναφορών. Αυτό επιτρέπει την έγκαιρη αντίδραση σε προβλήματα και τη λήψη αποφάσεων για τη βελτίωση των επιδόσεων.

- **Επικοινωνία και Συνεργασία**: Τα ΠΣ επιτρέπουν στη διοίκηση να επικοινωνεί και να συνεργάζεται εύκολα με άλλα μέλη της οργάνωσης, ανεξαρτήτως του τοποθετημένους ή γεωγραφικούς περιορισμούς (Karim, 2011).

Συνολικά, τα ΠΣ παρέχουν την υποστήριξη που απαιτείται για τη διοίκηση των διαδικασιών και των αποφάσεων της επιχείρησης, ενισχύοντας την αποτελεσματικότητα και την αποδοτικότητά της (Santos and Estender, 2014).

1.2.3 Διαλειτουργικά και διεπιχειρησιακά ΠΣ

Τα διαλειτουργικά και διεπιχειρησιακά ΠΣ αποτελούν ένα είδος συστημάτων που επιτρέπουν στις επιχειρήσεις να επικοινωνούν, να αλληλεπιδρούν και να συνεργάζονται μεταξύ τους. Αυτά τα συστήματα βοηθούν στη δημιουργία ενός ολοκληρωμένου περιβάλλοντος διαλειτουργικότητας και συνεργασίας μεταξύ επιχειρήσεων ή οργανισμών (Awan and Khan, 2016). Παρακάτω παρατίθεται ο τρόπος με τον οποίο λειτουργούν αυτά τα συστήματα:

- **Διαλειτουργικότητα**: Τα διαλειτουργικά ΠΣ επιτρέπουν σε διαφορετικά συστήματα και εφαρμογές να επικοινωνούν και να ανταλλάσσουν πληροφορίες μεταξύ τους. Αυτό μπορεί να γίνει μέσω προτύπων ανταλλαγής δεδομένων και πρωτοκόλλων επικοινωνίας.

- **Διεπιχειρησιακή Συνεργασία**: Τα διεπιχειρησιακά ΠΣ επιτρέπουν σε διαφορετικές επιχειρήσεις ή οργανισμούς να συνεργάζονται και να μοιράζονται πληροφορίες για την επίτευξη κοινών στόχων ή για τη βελτίωση της απόδοσής τους (Chulkov, 2017).

- **Διαλειτουργικές Εφαρμογές**: Αυτές οι εφαρμογές συνδυάζουν λειτουργίες από διάφορα συστήματα ή εφαρμογές, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε πληροφορίες και λειτουργίες από διαφορετικές πηγές με ένα ενιαίο διεπαφικό περιβάλλον.

- **Πλατφόρμες Σύνδεσης (Middleware)**: Οι πλατφόρμες σύνδεσης λειτουργούν ως ενδιάμεσο λογισμικό που επιτρέπει την επικοινωνία και τη συνεργασία μεταξύ διαφορετικών συστημάτων και εφαρμογών (Σπηλιώτη, 2022).

Με αυτόν τον τρόπο, τα διαλειτουργικά και διεπιχειρησιακά ΠΣ επιτρέπουν στις επιχειρήσεις να ανταλλάσσουν πληροφορίες, να συνεργάζονται και να επιτυγχάνουν

συναλλαγές με άλλους οργανισμούς με αποτελεσματικό και αποδοτικό τρόπο (Monteiro and Pinto, 2019).

1.3 Σκοπός των ΠΣ

Τα ΠΣ έχουν πολλούς σκοπούς και λειτουργίες που εξυπηρετούν διάφορους τομείς και ανάγκες των οργανισμών (Sudirman et al., 2014). Οι βασικοί σκοποί των ΠΣ περιλαμβάνουν:

Α) Υποστήριξη Λήψης Αποφάσεων

Ένας από τους κύριους σκοπούς των ΠΣ είναι να παρέχουν τις απαραίτητες πληροφορίες και αναλύσεις που υποστηρίζουν τη διαδικασία λήψης αποφάσεων στο επίπεδο της διοίκησης (Almazán et al., 2017). Η υποστήριξη λήψης αποφάσεων αποτελεί έναν σημαντικό σκοπό των ΠΣ. Τα ΠΣ παρέχουν τις απαραίτητες πληροφορίες, αναλύσεις και εργαλεία που υποστηρίζουν τη διαδικασία λήψης αποφάσεων στις επιχειρήσεις (Hayati et al., 2021). Οι βασικοί τρόποι με τους οποίους υποστηρίζουν τη λήψη αποφάσεων περιλαμβάνουν:

- *Παροχή Επιχειρηματικών Πληροφοριών*: συλλέγουν, αναλύουν και παρέχουν επιχειρηματικές πληροφορίες από διάφορες πηγές όπως εσωτερικές βάσεις δεδομένων, εξωτερικές πηγές, αναλύσεις αγοράς κ.λπ. Αυτές οι πληροφορίες βοηθούν τους διοικητικούς φορείς να λαμβάνουν ενημερωμένες αποφάσεις.

- *Αναλυτικές Αναφορές και Δείκτες Απόδοσης*: δημιουργούν αναλυτικές αναφορές και δείκτες απόδοσης που παρέχουν ενδείξεις για την τρέχουσα κατάσταση της επιχείρησης και την απόδοσή της σε διάφορους τομείς, βοηθώντας τους διαχειριστές να εκτιμήσουν τις επιπτώσεις των αποφάσεών τους.

- *Προβλέψεις και Προβληματισμός*: Μέσω της ανάλυσης δεδομένων και της χρήσης προηγμένων αλγορίθμων, μπορούν να παράγουν προβλέψεις σχετικά με μελλοντικές τάσεις και εξελίξεις, επιτρέποντας έτσι στη διοίκηση να προετοιμαστεί εγκαίρως για πιθανά σενάρια.

- *Συστηματική Διαχείριση Πληροφοριών*: βοηθούν στη συστηματική οργάνωση και διαχείριση των πληροφοριών, εξασφαλίζοντας ότι οι αποφάσεις λαμβάνονται με βάση τα συγκεκριμένα δεδομένα και τις ανάγκες της επιχείρησης (Σπηλιώτη, 2022).

Οι παραπάνω τρόποι αποτελούν μόνο μερικά παραδείγματα του πώς τα ΠΣ υποστηρίζουν τη διαδικασία λήψης αποφάσεων στις επιχειρήσεις (Almazán et al., 2017). Είναι κρίσιμης σημασίας για την επιτυχία και την ανταγωνιστικότητα της επιχείρησης να έχουν πρόσβαση σε αξιόπιστες και εύχρηστες πληροφορίες κατά τη λήψη αποφάσεων (Sudirman et al., 2014).

Β) Βελτίωση της Αποδοτικότητας και της Αποτελεσματικότητας

Τα ΠΣ βοηθούν στη βελτίωση της απόδοσης των διαδικασιών και των επιχειρηματικών διαδικασιών μέσω της αυτοματοποίησης, της βελτιστοποίησης των ροών εργασίας και της αποτελεσματικής χρήσης των πόρων (Almazán et al., 2017). Η βελτίωση της αποδοτικότητας και της αποτελεσματικότητας είναι σημαντικοί στόχοι για κάθε επιχείρηση και τα ΠΣ συμβάλλουν σημαντικά σε αυτούς τους στόχους με διάφορους τρόπους (Sudirman et al., 2014), συμπεριλαμβανομένων:

- *Αυτοματοποίηση Διαδικασιών*: επιτρέπουν την αυτοματοποίηση ρουτίνας διαδικασιών και εργασιών, μειώνοντας τον ανθρώπινο κόπο και τον χρόνο που απαιτείται για την ολοκλήρωσή τους.

- *Βελτίωση Ροών Εργασίας*: βοηθούν στη βελτίωση των ροών εργασίας με την απλοποίηση και την επιτάχυνση της επικοινωνίας και της συνεργασίας μεταξύ των μελών της ομάδας.

- *Διαχείριση Πόρων*: παρέχουν εργαλεία διαχείρισης πόρων όπως ανθρώπινο δυναμικό, χρηματοοικονομικά, και υλικά, βοηθώντας την επιχείρηση να αξιοποιεί αποτελεσματικά τους πόρους της.

- *Επικοινωνία και Συνεργασία*: διευκολύνουν την επικοινωνία και τη συνεργασία μεταξύ των τμημάτων και των μελών της επιχείρησης, ενισχύοντας την αποτελεσματικότητα και την απόδοση της οργάνωσης.

- *Πρόσβαση σε Πληροφορίες*: επιτρέπουν την άμεση πρόσβαση σε πληροφορίες και δεδομένα, εξασφαλίζοντας ότι οι αποφάσεις λαμβάνονται με βάση τις πλέον ενημερωμένες πληροφορίες (Σπηλιώτη, 2022).

Με τη συνολική συνεισφορά τους, τα ΠΣ ενισχύουν την απόδοση και την αποτελεσματικότητα των επιχειρήσεων, επιτρέποντάς τους να λειτουργούν πιο αποτελεσματικά και αποδοτικά σε έναν ανταγωνιστικό και δυναμικό επιχειρηματικό κόσμο (Sudirman et al., 2014).

Γ) Υποστήριξη Λειτουργιών Επιχειρήσεων

Τα ΠΣ παρέχουν λειτουργίες όπως η διαχείριση πελατών, η διαχείριση αποθεμάτων, η λογιστική, η διαχείριση ανθρώπινου δυναμικού κ.ά., που βοηθούν στην ομαλή λειτουργία της επιχείρησης. Η υποστήριξη των λειτουργιών της επιχείρησης αποτελεί βασικό στόχο τους. Αυτό σημαίνει την παροχή εργαλείων και λειτουργιών που καλύπτουν τις ανάγκες της καθημερινής λειτουργίας της επιχείρησης (Sudirman et al., 2014). Οι λειτουργίες που υποστηρίζονται από τα ΠΣ μπορεί να περιλαμβάνουν:

- *Διαχείριση Πελατών (CRM)*: Τα συστήματα CRM παρέχουν εργαλεία για τη διαχείριση των πελατών, την παρακολούθηση των δραστηριοτήτων τους, τις επικοινωνίες και τις πωλήσεις, με σκοπό τη βελτίωση της εξυπηρέτησης τους και την αύξηση των πωλήσεων.

- *Διαχείριση Αποθεμάτων και Προμηθειών*: Αυτά τα συστήματα επιτρέπουν την παρακολούθηση και τον έλεγχο των αποθεμάτων, τη διαχείριση των παραγγελιών προμηθειών και την αυτοματοποίηση της διαδικασίας εφοδιαστικής αλυσίδας.

- *Οικονομική Διαχείριση (ERP)*: Οι εφαρμογές ERP παρέχουν ολοκληρωμένες λύσεις για τη διαχείριση των οικονομικών λειτουργιών της επιχείρησης, συμπεριλαμβανομένης της λογιστικής, των οικονομικών αναλύσεων, της διαχείρισης των πληρωμών και του τραπεζικού ταμείου.

- *Διαχείριση Ανθρώπινου Δυναμικού (HRM)*: Οι εφαρμογές HRM παρέχουν λύσεις για τη διαχείριση του προσωπικού, συμπεριλαμβανομένων της απασχόλησης, των αποδοχών, των κατάρτισης και των επιδόσεων.

- *Διαχείριση Έργων και Εργασιών*: Τα συστήματα αυτά βοηθούν στην οργάνωση, την παρακολούθηση και τη διαχείριση των εργασιών και των έργων της επιχείρησης (Σπηλιώτη, 2022).

Με την υποστήριξη αυτών των λειτουργιών, τα ΠΣ βοηθούν τις επιχειρήσεις να λειτουργούν αποτελεσματικά και να επιτυγχάνουν τους στόχους τους με μεγαλύτερη αποτελεσματικότητα (Almazán et al., 2017).

Δ) Ενίσχυση της Ανταγωνιστικής Θέσης

Τα ΠΣ μπορούν να βοηθήσουν τις επιχειρήσεις να ανταγωνιστούν αποτελεσματικά στην αγορά παρέχοντας σημαντικές πληροφορίες για την αγορά, τους πελάτες και τους ανταγωνιστές (Altamony et al., 2012). Η ενίσχυση της ανταγωνιστικής θέσης αποτελεί έναν σημαντικό στόχο για κάθε επιχείρηση και τα ΠΣ παίζουν ένα κρίσιμο ρόλο σε αυτόν τον τομέα (Elnagar and Osei-Bryson, 2021). Οι τρόποι με τους οποίους συνεισφέρουν στην ενίσχυση της ανταγωνιστικής θέσης μιας επιχείρησης περιλαμβάνουν:

- *Ανάλυση Δεδομένων και Εξαγωγή Γνώσης*: μπορούν να αναλύουν μεγάλα σύνολα δεδομένων και να εξάγουν σημαντική πληροφορία και γνώση για την αγορά, τους πελάτες, τους ανταγωνιστές και τις τάσεις της αγοράς.

- *Βελτίωση της Ανταπόκρισης*: μπορούν να βοηθήσουν την επιχείρηση να ανταποκριθεί ταχύτερα στις αλλαγές της αγοράς και στις ανάγκες των πελατών.

- *Καινοτομία και Εξέλιξη Προϊόντων*: Μέσω της ανάλυσης δεδομένων και της έρευνας και ανάπτυξης, τα ΠΣ μπορούν να συμβάλουν στη δημιουργία νέων προϊόντων και υπηρεσιών που ανταποκρίνονται στις ανάγκες της αγοράς.

- *Ενίσχυση της Επικοινωνίας με τους Πελάτες*: Τα συστήματα CRM μπορούν να βοηθήσουν στην ανάπτυξη σχέσεων με τους πελάτες, παρέχοντας εξατομικευμένες υπηρεσίες και επικοινωνία με τους πελάτες σε πραγματικό χρόνο.

- *Βελτίωση της Ποιότητας και της Παραγωγικότητας*: Μέσω της αυτοματοποίησης και της βελτίωσης των εργασιών, τα ΠΣ μπορούν να βελτιώσουν την ποιότητα των προϊόντων και υπηρεσιών και να αυξήσουν την παραγωγικότητα της επιχείρησης (Σπηλιώτη, 2022).

Με την αξιοποίηση των ΠΣ για την ενίσχυση της ανταγωνιστικής θέσης, οι επιχειρήσεις μπορούν να επιτύχουν μεγαλύτερη αγορά μεριδίου, καινοτομία και ανάπτυξη, και μακροπρόθεσμη αειφορία (Elnagar and Osei-Bryson, 2021).

Ε) Καινοτομία και Ανάπτυξη

Τα ΠΣ επιτρέπουν στις επιχειρήσεις να εφαρμόζουν καινοτόμες ιδέες, νέες διαδικασίες και να αναπτύσσονται διαρκώς για να προσαρμοστούν στις αλλαγές της αγοράς και του περιβάλλοντος (Arici et al., 2022). Η καινοτομία και η ανάπτυξη αποτελούν κρίσιμους παράγοντες για την επιτυχία και την ανταγωνιστικότητα μιας επιχείρησης. Ακόμη, διαδραματίζουν σημαντικό ρόλο στην υποστήριξη αυτών των δύο πτυχών, παρέχοντας εργαλεία και πόρους για τη δημιουργία και την καινοτόμο ανάπτυξη (Jerome et al., 2023). Επίσης, συμβάλλουν στην υποστήριξη αυτών των διαδικασιών και τη διευκόλυνση της καινοτομίας και της ανάπτυξης με τους ακόλουθους τρόπους:

- *Ανάλυση Δεδομένων και Εξαγωγή Γνώσης*: αναλύουν μεγάλα σύνολα δεδομένων για την ανίχνευση τάσεων και προτύπων, παρέχοντας έτσι βάση για καινοτόμες ιδέες και προσεγγίσεις.

- *Σύστημα Διαχείρισης Ιδεών*: διαχειρίζονται τη διαδικασία καταγραφής, αξιολόγησης και εφαρμογής νέων ιδεών από το προσωπικό της επιχείρησης.

- *Συνεργατικά Εργαλεία*: Πλατφόρμες συνεργασίας και εργαλεία τηλεργασίας μπορούν να συνδράμουν στην ανάπτυξη ιδεών από διαφορετικά τμήματα και ομάδες εργασίας.

- *Αυτοματοποίηση Διαδικασιών*: Η αυτοματοποίηση διαφόρων διαδικασιών μπορεί να απελευθερώσει το χρόνο και τους πόρους που μπορούν να επενδυθούν στην καινοτομία.

- *Διαχείριση Έργων*: Τα συστήματα διαχείρισης έργων μπορούν να βοηθήσουν στην οργάνωση και την παρακολούθηση των καινοτόμων έργων (Σπηλιώτη, 2022).

Συνολικά, η χρήση ΠΣ μπορεί να διευκολύνει τη διαδικασία της καινοτομίας και της ανάπτυξης, επιτρέποντας στις επιχειρήσεις να είναι ευέλικτες, αποτελεσματικές και προσαρμοστικές στις αλλαγές της αγοράς (Arici et al., 2022). Αυτοί είναι μερικοί από τους κύριους σκοπούς που εξυπηρετούν τα ΠΣ στο πλαίσιο της επιχειρηματικής δραστηριότητας (Awamleh and Ertugan, 2021).

1.4 Οφέλη και προβλήματα

Τα ΠΣ προσφέρουν πληθώρα οφελών για τις επιχειρήσεις και τους οργανισμούς. Ανάμεσα στα κυριότερα οφέλη περιλαμβάνονται:

- *Βελτίωση της Παραγωγικότητας*: αυτοματοποιήσουν εργασίες και διαδικασίες, εξοικονομώντας χρόνο και ανθρώπινους πόρους και βελτιώνοντας την αποτελεσματικότητα.

- *Βελτίωση της Αναλυτικής Διαδικασίας*: παρέχουν εργαλεία για την ανάλυση δεδομένων, επιτρέποντας στους διαχειριστές να λαμβάνουν αποφάσεις βασισμένες σε πληροφορίες και αναλύσεις.

- *Βελτίωση της Λήψης Αποφάσεων*: παρέχουν πρόσβαση σε πληροφορίες που είναι απαραίτητες για τη λήψη αποφάσεων σε όλα τα επίπεδα της επιχείρησης.

- *Βελτίωση της Επικοινωνίας*: επιτρέπουν την επικοινωνία και την κοινοποίηση πληροφοριών εντός και εκτός της επιχείρησης.

- *Βελτίωση της Ανταγωνιστικής Θέσης*: μπορούν να βοηθήσουν την επιχείρηση να παρακολουθεί τους ανταγωνιστές της και να προσαρμόζεται στις αλλαγές της αγοράς.

- *Βελτίωση της Διαχείρισης Ρίσκου*: μπορούν να παρέχουν αναλύσεις και πληροφορίες που επιτρέπουν στους διαχειριστές να αντιληφθούν και να διαχειριστούν αποτελεσματικά το ρίσκο.

- *Ενίσχυση της Ασφάλειας Πληροφοριών*: μπορούν να παρέχουν μηχανισμούς προστασίας για την ασφάλεια των πληροφοριών και των δεδομένων της επιχείρησης.

- *Εξοικονόμηση Χρημάτων*: Μέσω της αυτοματοποίησης διαδικασιών και της αποτελεσματικής διαχείρισης των πόρων, τα ΠΣ μπορούν να συμβάλουν στην εξοικονόμηση κόστους (Σπηλιώτη, 2022).

Αυτά τα οφέλη αναδεικνύουν τη σημασία των ΠΣ στην αποτελεσματική λειτουργία και την ανάπτυξη μιας επιχείρησης (Jerome et al., 2023).

Α) Βελτίωση της Παραγωγικότητας

Η βελτίωση της παραγωγικότητας αποτελεί ένα από τα κύρια οφέλη που προσφέρουν τα ΠΣ στις επιχειρήσεις (Jerome et al., 2023). Αυτό επιτυγχάνεται μέσω διάφορων τρόπων:

- *Αυτοματοποίηση Διαδικασιών*: επιτρέπουν την αυτοματοποίηση εργασιών και διαδικασιών που προηγουμένως απαιτούσαν ανθρώπινη εργασία, μειώνοντας έτσι τον χρόνο και τους πόρους που απαιτούνται για την ολοκλήρωσή τους.

- *Βελτιωμένη Πρόσβαση σε Πληροφορίες*: παρέχουν τη δυνατότητα γρήγορης και εύκολης πρόσβασης σε πληροφορίες, εξαλείφοντας τον χρόνο που θα απαιτούνταν για την αναζήτησή τους με παραδοσιακούς τρόπους.

- *Βελτιωμένη Οργάνωση Εργασιών*: επιτρέπουν την αποτελεσματικότερη οργάνωση και διαχείριση των εργασιών μέσω εργαλείων και λειτουργιών διαχείρισης έργων.

- *Αυξημένη Ακρίβεια και Αποτελεσματικότητα*: Η χρήση ΠΣ μπορεί να βοηθήσει στην αύξηση της ακρίβειας και της αποτελεσματικότητας στην εκτέλεση διαφόρων εργασιών και διαδικασιών.

- *Βελτιωμένη Επικοινωνία και Συνεργασία*: Τα ΠΣ διευκολύνουν την επικοινωνία και τη συνεργασία μεταξύ των μελών μιας οργάνωσης, βοηθώντας στην επίτευξη κοινών στόχων (Σπηλιώτη, 2022).

Συνολικά, η βελτίωση της παραγωγικότητας είναι ένα σημαντικό όφελος που προσφέρουν τα ΠΣ, καθώς βοηθούν τις επιχειρήσεις να εκτελούν τις εργασίες τους αποτελεσματικά και αποδοτικά (Awamleh and Ertugan, 2021).

Β) Βελτίωση της Αναλυτικής Διαδικασίας

Η βελτίωση της αναλυτικής διαδικασίας είναι ένα από τα σημαντικότερα οφέλη που προσφέρουν τα ΠΣ. Αυτό επιτυγχάνεται μέσω διάφορων τρόπων:

- *Ανάλυση Δεδομένων και Αναφορές*: παρέχουν εργαλεία για την ανάλυση δεδομένων και τη δημιουργία αναφορών, επιτρέποντας στους διαχειριστές να

αναλύουν τις επιχειρηματικές επιδόσεις, να ανιχνεύουν τάσεις και να προβλέπουν μελλοντικές εξελίξεις.

- *Εξελιγμένα Εργαλεία Ανάλυσης*: με τη χρήση ΠΣ, οι επιχειρήσεις μπορούν να χρησιμοποιήσουν εξελιγμένα εργαλεία ανάλυσης όπως δείκτες απόδοσης, μοντέλα πρόβλεψης, και τεχνικές δεδομένων mining για την ανάλυση μεγάλων όγκων δεδομένων.

- *Αναλυτική Εξερεύνηση Δεδομένων*: οι πληροφοριακές πλατφόρμες επιτρέπουν την αναλυτική εξερεύνηση των δεδομένων, παρέχοντας στους χρήστες τη δυνατότητα να ανακαλύπτουν πρότυπα και τάσεις που δεν είναι εύκολα αντιληπτά με άλλους τρόπους ανάλυσης.

- *Διαχείριση Αποθεμάτων και Προμηθειών*: η ανάλυση δεδομένων μπορεί να βοηθήσει στην αποτελεσματική διαχείριση των αποθεμάτων και των προμηθειών μέσω της πρόβλεψης της ζήτησης, της αξιολόγησης των προμηθευτών και της βελτιστοποίησης των επιπέδων αποθεμάτων.

- *Ανάπτυξη Στρατηγικών Αποφάσεων*: η ανάλυση δεδομένων παρέχει την αναγκαία πληροφορία για τη λήψη στρατηγικών αποφάσεων, όπως η επιλογή νέων αγορών ή προϊόντων, η ανάπτυξη νέων στρατηγικών πωλήσεων, και η προσαρμογή στις αλλαγές της αγοράς (Σπηλιώτη, 2022).

Συνολικά, η βελτίωση της αναλυτικής διαδικασίας μέσω των ΠΣ επιτρέπει στις επιχειρήσεις να λαμβάνουν πιο ενημερωμένες και εύστοχες αποφάσεις βασισμένες στην ανάλυση των δεδομένων και των πληροφοριών που διαθέτουν (Jerome et al., 2023).

Γ) Βελτίωση της Λήψης Αποφάσεων

Η βελτίωση της λήψης αποφάσεων είναι ένα από τα κύρια οφέλη που προσφέρουν τα ΠΣ (Awamleh and Ertugan, 2021). Αυτό επιτυγχάνεται μέσω διάφορων τρόπων:

- *Ενίσχυση της Αναλυτικής Δυνατότητας*: παρέχουν εργαλεία για την ανάλυση δεδομένων και τη δημιουργία αναφορών, βοηθώντας τους διαχειριστές να έχουν πλήρη εικόνα της κατάστασης της επιχείρησης και του περιβάλλοντος της αγοράς για τη λήψη ενημερωμένων αποφάσεων.

- *Επίλυση Προβλημάτων*: αναγνωρίζουν προβλήματα και τάσεις στα δεδομένα, παρέχοντας τις απαραίτητες πληροφορίες για τη λήψη αποφάσεων που να τα αντιμετωπίζουν.

- *Υποστήριξη Προγραμματισμού και Πρόβλεψης*: παρέχουν εργαλεία για τον προγραμματισμό και την πρόβλεψη μελλοντικών γεγονότων, βοηθώντας τη διοίκηση να λαμβάνει προληπτικά μέτρα και να προσαρμόζει τις στρατηγικές της.

- *Βελτιωμένη Πρόσβαση σε Πληροφορίες*: η εύκολη πρόσβαση σε πληροφορίες μέσω των ΠΣ επιτρέπει στους διαχειριστές να λαμβάνουν αποφάσεις βασισμένες σε συγκεκριμένα δεδομένα και αναλύσεις.

- *Καλύτερη Κατανόηση των Αναγκών της Αγοράς*: μέσω της ανάλυσης δεδομένων από τα ΠΣ, οι επιχειρήσεις μπορούν να κατανοήσουν καλύτερα τις ανάγκες και τις προτιμήσεις των πελατών, βοηθώντας τους να λαμβάνουν αποφάσεις που να ανταποκρίνονται σε αυτές (Σπηλιώτη, 2022).

Κατά συνέπεια, η χρήση ΠΣ επιτρέπει στις επιχειρήσεις να λαμβάνουν πιο ενημερωμένες, ολοκληρωμένες και ακριβείς αποφάσεις που βασίζονται σε δεδομένα και αναλύσεις (Cuillier, 2022).

Δ) Βελτίωση της Επικοινωνίας

Η βελτίωση της επικοινωνίας είναι ένα από τα σημαντικότερα οφέλη που προσφέρουν τα ΠΣ. Αυτό επιτυγχάνεται μέσω διάφορων τρόπων:

- *Αυξημένη Διαθεσιμότητα Πληροφοριών*: διευκολύνουν την πρόσβαση σε πληροφορίες, επιτρέποντας στους εργαζομένους να αποκτούν πρόσβαση σε αναλυτικές αναφορές, δεδομένα πελατών και άλλες πληροφορίες που είναι σημαντικές για την εκτέλεση των καθηκόντων τους.

- *Επικοινωνία σε Πραγματικό Χρόνο*: διευκολύνουν την επικοινωνία σε πραγματικό χρόνο μεταξύ των μελών μιας ομάδας ή των διαφόρων τμημάτων της επιχείρησης, επιτρέποντας τη γρήγορη ανταλλαγή πληροφοριών και την άμεση αντίδραση σε αλλαγές.

- *Βελτιωμένη Ομαδική Εργασία*: Μέσω των ΠΣ, οι εργαζόμενοι μπορούν να συνεργάζονται εύκολα και να μοιράζονται πληροφορίες με άλλα μέλη της ομάδας, ανεξαρτήτως της γεωγραφικής τους τοποθεσίας.

- *Διευκόλυνση Επικοινωνίας με Πελάτες και Προμηθευτές*: Οι πληροφοριακές πλατφόρμες διευκολύνουν την επικοινωνία με πελάτες και προμηθευτές μέσω ηλεκτρονικού ταχυδρομείου, διαδικτυακών πλατφορμών και άλλων εργαλείων, βελτιώνοντας την απόκριση σε ερωτήματα και αιτήματα.

- *Διαχείριση Έργων και Προθεσμιών*: επιτρέπουν τη διαχείριση έργων και προθεσμιών μέσω εργαλείων όπως ηλεκτρονικά ημερολόγια και συστήματα παρακολούθησης έργων, βοηθώντας στην αποφυγή καθυστερήσεων και την αποτελεσματική διαχείριση του χρόνου (Σπηλιώτη, 2022).

Συνολικά, η βελτίωση της επικοινωνίας μέσω των ΠΣ βελτιώνει τη συνεργασία, την απόδοση και την αποτελεσματικότητα σε μια επιχείρηση, καθιστώντας την πιο ανταγωνιστική και επιτυχημένη (Jerome et al., 2023).

Ε) Βελτίωση της Ανταγωνιστικής Θέσης

Η βελτίωση της ανταγωνιστικής θέσης είναι ένα σημαντικό όφελος των ΠΣ (Awamleh and Ertugan, 2021) και περιλαμβάνει τα ακόλουθα:

- *Ανάλυση της Αγοράς και των Ανταγωνιστών*: επιτρέπουν τη συλλογή, την ανάλυση και την ερμηνεία δεδομένων σχετικά με την αγορά και τους ανταγωνιστές, προσφέροντας στην επιχείρηση σημαντικές πληροφορίες για τη λήψη στρατηγικών αποφάσεων.

- *Καινοτομία και Διαφοροποίηση*: Η χρήση ΠΣ επιτρέπει στις επιχειρήσεις να αναπτύσσουν καινοτόμες υπηρεσίες και προϊόντα, να προσφέρουν βελτιωμένες εμπειρίες στους πελάτες και να διαφοροποιούνται από τους ανταγωνιστές τους.

- *Ανταπόκριση στις Ανάγκες των Πελατών*: Με τη βοήθεια των ΠΣ, οι επιχειρήσεις μπορούν να αντιλαμβάνονται και να ανταποκρίνονται γρήγορα στις μεταβαλλόμενες ανάγκες και προτιμήσεις των πελατών τους.

- *Βελτιωμένη Ποιότητα Υπηρεσιών*: Η χρήση των ΠΣ επιτρέπει την αυτοματοποίηση και βελτίωση διαδικασιών, με αποτέλεσμα την παροχή υψηλότερης ποιότητας υπηρεσιών στους πελάτες.

- *Ενίσχυση της Αποτελεσματικότητας και Απόδοσης*: επιτρέπουν στις επιχειρήσεις να λειτουργούν με μεγαλύτερη αποτελεσματικότητα και απόδοση, βελτιώνοντας την απόδοση των διαδικασιών και την αποδοτικότητα των πόρων (Σπηλιώτη, 2022).

Γενικότερα, η χρήση των ΠΣ συμβάλλει στην ανάπτυξη της ανταγωνιστικής θέσης των επιχειρήσεων, επιτρέποντας τους να προσαρμόζονται στις αλλαγές της αγοράς, να καινοτομούν και να παρέχουν ανώτερης ποιότητας υπηρεσίες στους πελάτες τους (Cuillier, 2022).

ΣΤ) Βελτίωση της Διαχείρισης Ρίσκου

Η βελτίωση της διαχείρισης του ρίσκου είναι ένα σημαντικό όφελος των ΠΣ (Awamleh and Ertugan, 2021). Αυτό επιτυγχάνεται με τους ακόλουθους τρόπους:

- *Αναγνώριση Κινδύνων*: βοηθούν στον εντοπισμό και την αναγνώριση διαφόρων ειδών κινδύνων που επηρεάζουν την επιχείρηση, όπως οι αγοραίοι κίνδυνοι, οι χρηματοοικονομικοί κίνδυνοι, οι κίνδυνοι ασφάλειας δεδομένων και άλλοι.

- *Αξιολόγηση Ρίσκου*: Μέσω της συλλογής και ανάλυσης δεδομένων, τα ΠΣ μπορούν να βοηθήσουν στην αξιολόγηση του επιπέδου των κινδύνων που αντιμετωπίζει η επιχείρηση και στην κατάταξή τους κατά προτεραιότητα.

- *Παρακολούθηση και Ενημέρωση*: παρέχουν τη δυνατότητα συνεχούς παρακολούθησης των κινδύνων και των αλλαγών στο περιβάλλον της επιχείρησης, καθώς και την άμεση ενημέρωση της διοίκησης για πιθανούς κινδύνους που απαιτούν δράση.

- *Διαχείριση Κρίσεων*: μπορούν να στηρίξουν την αποτελεσματική διαχείριση κρίσεων, παρέχοντας στη διοίκηση σημαντικές πληροφορίες και εργαλεία για τη λήψη γρήγορων και αποτελεσματικών αποφάσεων.

- *Εφαρμογή Στρατηγικών*: Με βάση τις πληροφορίες που παρέχουν τα ΠΣ, οι επιχειρήσεις μπορούν να αναπτύξουν και να εφαρμόσουν στρατηγικές για τη μείωση των κινδύνων και την αντιμετώπισή τους.

Συνολικά, τα ΠΣ βελτιώνουν τη διαχείριση του ρίσκου εντοπίζοντας, αναλύοντας και διαχειρίζοντας τους κινδύνους που επηρεάζουν την επιχείρηση, βοηθώντας την να προστατευτεί και να αποκτήσει ανταγωνιστικό πλεονέκτημα (Jerome et al., 2023).

Ζ) Ενίσχυση της Ασφάλειας Πληροφοριών

Η ενίσχυση της ασφάλειας των πληροφοριών αποτελεί ένα ζωτικής σημασίας πλεονέκτημα των ΠΣ. Αυτό επιτυγχάνεται με διάφορους τρόπους:

- *Προστασία Δεδομένων*: μπορούν να υιοθετήσουν μέτρα προστασίας όπως κρυπτογράφηση, δικαιώματα πρόσβασης και λογισμικό ασφαλείας για να προστατεύσουν τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση.

- *Ανίχνευση και Αποτροπή Παραβιάσεων*: μπορούν να υλοποιήσουν μηχανισμούς ανίχνευσης παραβιάσεων και επιθέσεων, που επιτρέπουν την άμεση αντίδραση και αποτροπή απειλών στην ασφάλεια των πληροφοριών.

- *Εκπαίδευση Προσωπικού*: Η εκπαίδευση του προσωπικού σχετικά με τις βέλτιστες πρακτικές ασφαλείας των πληροφοριών είναι ουσιώδους σημασίας για την αντιμετώπιση απειλών.

- *Εφαρμογή Πολιτικών Ασφαλείας*: μπορούν να εφαρμόσουν πολιτικές ασφαλείας, οι οποίες καθορίζουν τους κανόνες και τις διαδικασίες που πρέπει να ακολουθούνται για την προστασία των πληροφοριών.

- *Επικύρωση και Πιστοποίηση*: μπορούν να υλοποιήσουν μηχανισμούς επικύρωσης και πιστοποίησης για να επιβεβαιώσουν ότι οι διαδικασίες και οι πρακτικές ασφαλείας πληρούν τα πρότυπα και τις απαιτήσεις ασφάλειας (Σπηλιώτη, 2022).

Έτσι, η ενίσχυση της ασφάλειας των πληροφοριών μέσω των ΠΣ είναι κρίσιμη για την προστασία ευαίσθητων πληροφοριών και την πρόληψη δυνητικών κινδύνων ασφαλείας (Cuillier, 2022).

Η) Εξοικονόμηση Χρημάτων

Η χρήση ΠΣ μπορεί να οδηγήσει σε εξοικονόμηση χρημάτων με πολλούς τρόπους (Awamleh and Ertugan, 2021):

- *Αυτοματοποίηση Διεργασιών*: μπορούν να αυτοματοποιήσουν διάφορες εργασίες και διαδικασίες, ελευθερώνοντας το προσωπικό για άλλες εργασίες και μειώνοντας το κόστος ανθρώπινου δυναμικού.

- *Βελτιστοποίηση Αποθηκευτικού Χώρου*: συμβάλουν στην αποτελεσματική διαχείριση των δεδομένων και τη μείωση των δαπανών σε αποθηκευτικό χώρο.

- *Βελτιστοποίηση Παραγωγικότητας*: Μέσω αναλύσεων και βελτιστοποιήσεων που προσφέρουν τα ΠΣ, η παραγωγικότητα της επιχείρησης μπορεί να αυξηθεί, μειώνοντας το κόστος ανά μονάδα παραγωγής.

- *Βελτιστοποίηση Διαχείρισης Αποθεμάτων*: συντελούν στην καλύτερη διαχείριση των αποθεμάτων, μειώνοντας τα κόστη αποθήκευσης και την υπερβολική αγορά αποθεμάτων.

- *Βελτιστοποίηση Ενεργειακής Απόδοσης*: η εφαρμογή των ΠΣ μπορεί να συμβάλει στη μείωση της ενεργειακής κατανάλωσης μέσω της αυτοματοποίησης και της βελτιστοποίησης διαδικασιών (Σπηλιώτη, 2022).

Με τη συνολική βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των διαδικασιών της επιχείρησης, τα ΠΣ μπορούν να συμβάλουν σημαντικά στη μείωση των δαπανών και την εξοικονόμηση χρημάτων (Awamleh and Ertugan, 2021). Παρά τα πλεονεκτήματα που προσφέρουν τα ΠΣ, υπάρχουν και ορισμένα προβλήματα που μπορούν να προκύψουν:

- *Ασφάλεια και Προστασία Δεδομένων*: Η ασφάλεια των δεδομένων είναι συχνά ένα μεγάλο πρόβλημα, καθώς υψηλού επιπέδου δεδομένα μπορεί να είναι ευάλωτα σε κυβερνοεπιθέσεις και παραβιάσεις ασφαλείας.

- *Συμβατότητα και Ενσωμάτωση*: Ορισμένα ΠΣ μπορεί να μην είναι συμβατά με άλλα συστήματα ή να δυσκολεύουν την ενσωμάτωση νέων τεχνολογιών ή λογισμικού.

- *Κόστος Εγκατάστασης και Συντήρησης*: Η εγκατάσταση και η συντήρηση ΠΣ μπορεί να είναι δαπανηρές, ειδικά για μικρομεσαίες επιχειρήσεις.
- *Εκπαίδευση Προσωπικού*: Η ανάγκη για εκπαίδευση του προσωπικού στη χρήση νέων τεχνολογιών και ΠΣ μπορεί να απαιτεί σημαντικούς πόρους και χρόνο.
- *Διακοπές Λειτουργίας*: Οι διακοπές στη λειτουργία του ΠΣ λόγω τεχνικών προβλημάτων ή κυβερνοεπιθέσεων μπορεί να έχουν σοβαρές επιπτώσεις στην επιχείρηση.
- *Εξάρτηση από Τεχνολογία*: Η υπερβολική εξάρτηση από τα ΠΣ μπορεί να δημιουργήσει ευαισθησία σε περιβαλλοντικούς κινδύνους και κυβερνοαπειλές (Σπηλιώτη, 2022).

Η αντιμετώπιση αυτών των προβλημάτων απαιτεί προσεκτικό σχεδιασμό, εκπαίδευση και συνεχή βελτίωση των συστημάτων και των διαδικασιών (Gashi Shatri, 2020).

1.5 Αναγκαιότητα χρήσης των ΠΣ από τις επιχειρήσεις

Η χρήση των ΠΣ από τις επιχειρήσεις είναι ουσιώδης για πολλούς λόγους:

- *Αποτελεσματικότητα και Απόδοση*: βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης των επιχειρήσεων μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων.
- *Ανταγωνιστική Θέση*: επιτρέπει στις επιχειρήσεις να είναι πιο ανταγωνιστικές στην αγορά, προσφέροντας καλύτερες υπηρεσίες και προϊόντα σε πιο αποτελεσματικό κόστος.
- *Λήψη Αποφάσεων*: παρέχει στη διοίκηση την απαραίτητη πληροφόρηση για τη λήψη αποφάσεων που βασίζονται σε δεδομένα και αναλύσεις.
- *Επικοινωνία και Συνεργασία*: επιτρέπει την εύκολη επικοινωνία και συνεργασία εντός και εκτός της επιχείρησης, βελτιώνοντας την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών της ομάδας.

- *Διαχείριση Δεδομένων*: βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες.

- *Εκσυγχρονισμός Διαδικασιών*: επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών, μειώνοντας τον χρόνο και το κόστος παραγωγής.

- *Παροχή Αξίας στους Πελάτες*: μέσω της αποτελεσματικής διαχείρισης της πληροφορίας, οι επιχειρήσεις μπορούν να προσφέρουν υψηλότερη ποιότητα προϊόντων και υπηρεσιών στους πελάτες τους (Σπηλιώτη, 2022).

Ο ανταγωνισμός αποτελεί έναν καθοριστικό παράγοντα για τη βιωσιμότητα μιας επιχείρησης στον χώρο των επιχειρήσεων. Η κατανόηση και η αντιμετώπιση του ανταγωνισμού αποτελούν σημαντικά θέματα μελέτης για πολλούς ερευνητές και επιχειρήσεις, καθώς η αντιμετώπισή του επηρεάζει την απόδοση και την επιτυχία της επιχείρησης στην αγορά (Cuillier, 2022).

2. Ασφάλεια Πληροφοριακών συστημάτων

2.1 Πολιτική Ασφάλειας ΠΣ

2.1.1 Έννοια

Η "πολιτική" σε έναν οργανισμό αναφέρεται στο σύνολο των οδηγιών, των γενικών προσανατολισμών και των αρχών που καθορίζουν τον τρόπο λειτουργίας της επιχείρησης (Kamariza, 2017). Αποτελεί την κατευθυντήρια γραμμή για τη λήψη αποφάσεων σχετικά με διάφορα θέματα που αφορούν τη λειτουργία της επιχείρησης, είτε αυτά αφορούν τις εσωτερικές του διαδικασίες είτε τις εξωτερικές του σχέσεις (Ifinedo, 2012). Η πολιτική περιλαμβάνει συχνά γενικές προτάσεις και δηλώσεις που ορίζουν τις βασικές αξίες, τους στόχους και τις προτεραιότητες της επιχείρησης (Kamariza, 2017). Επίσης, καθορίζει τους κανόνες, τις διαδικασίες και τις πρακτικές που πρέπει να ακολουθούνται από τα μέλη της επιχείρησης κατά την εκτέλεση των καθηκόντων τους. Οι πολιτικές είναι σημαντικές για την επίτευξη συνέπειας, συνοχής και αποτελεσματικότητας στη λειτουργία της επιχείρησης, καθώς καθορίζουν το πλαίσιο εντός του οποίου λαμβάνονται οι αποφάσεις και δρομολογείται η δράση (Lopes and Oliveira, 2015).

Η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής. Αποσκοπεί στην προστασία των υπολογιστικών συστημάτων, των δεδομένων και των δικτύων τους από απειλές και επιθέσεις που μπορούν να προκαλέσουν ζημία, δυσφήμιση, ή ακόμα και κλοπή ή καταστροφή δεδομένων (Njenga, 2016). Ανάμεσα στις δράσεις που αναλαμβάνονται για την ασφάλεια περιλαμβάνονται οι κρυπτογραφικές τεχνικές, οι προστατευτικές πολιτικές και διαδικασίες, οι μηχανισμοί ανίχνευσης και αποκατάστασης επιθέσεων (IDS/IPS), η εκπαίδευση του προσωπικού, και η διαχείριση των αδυναμιών (vulnerability management). Επίσης, η ασφάλεια ΠΣ εξετάζει τα μέτρα προστασίας ενάντια σε διάφορες μορφές επιθέσεων, όπως οι κακόβουλοι κώδικες (malware), οι κυβερνοεπιθέσεις και οι ατυχείς ανθρώπινες πράξεις (π.χ. αφήνοντας τον υπολογιστή ανοιχτό χωρίς επιτήρηση) (Σταματινός, 2015).

Η πολιτική ασφάλειας των ΠΣ αποτελεί ένα σημαντικό μέρος της συνολικής ασφάλειας ενός οργανισμού και έχει ως στόχο την προστασία από απειλές και επιθέσεις.

Η πολιτική ασφάλειας προσδιορίζει τον σκοπό και τους βασικούς στόχους της ασφάλειας των ΠΣ (Ifinedo, 2012). Περιλαμβάνει τις κατευθυντήριες γραμμές, τις διαδικασίες και τους κανόνες που πρέπει να ακολουθούνται για την επίτευξη των στόχων ασφάλειας. Καθορίζει τους ρόλους και τις ευθύνες των διαφόρων μερών της επιχείρησης σχετικά με την ασφάλεια των ΠΣ (Njenga, 2016). Η πολιτική ασφάλειας συνήθως τεκμηριώνεται σε ένα έγγραφο που είναι προσβάσιμο σε όλα τα μέλη της επιχείρησης και περιγράφει λεπτομερώς τις απαιτούμενες πρακτικές και διαδικασίες για την ασφάλεια. Η κατανόηση και η συμμόρφωση με αυτές τις κατευθυντήριες γραμμές αποτελούν ζωτικό μέρος της διαχείρισης (Alshaikh et al., 2015).

Η πολιτική ασφάλειας των ΠΣ ορίζει τους στόχους, τις οδηγίες, τις διαδικασίες και τους ρόλους που απαιτούνται για την προστασία των ΠΣ της επιχείρησης. Μέσα από αυτήν προσδιορίζονται οι στόχοι ασφάλειας του ΠΣ, όπως η προστασία από μη εξουσιοδοτημένη πρόσβαση, η διασφάλιση της ακεραιότητας των δεδομένων και η διαθεσιμότητα των υπηρεσιών (Maynard and Ruighave, 2010). Ακόμη, η πολιτική ασφάλειας περιλαμβάνει τις κατευθυντήριες γραμμές και τις διαδικασίες που πρέπει να ακολουθούνται για την ασφαλή λειτουργία του ΠΣ, συμπεριλαμβανομένης της διαχείρισης πρόσβασης, των αντιμέτρων ασφαλείας και των διαδικασιών αντιμετώπισης παραβιάσεων (Προκόπος, 2014). Επίσης, καθορίζει ποιοι είναι υπεύθυνοι για την υλοποίηση των διαφόρων πτυχών της πολιτικής ασφαλείας, όπως οι διαχειριστές συστημάτων, οι αναλυτές ασφαλείας και οι χρήστες. Με αυτόν τον τρόπο, η πολιτική ασφάλειας ορίζει το πλαίσιο εργασίας για την ασφαλή λειτουργία των ΠΣ της επιχείρησης (Ifinedo, 2012).

Η πολιτική ασφάλειας είναι νομικά δεσμευτική και απαιτεί τη συμμόρφωση όλων των μελών της επιχείρησης με τις οδηγίες, τις διαδικασίες και τα μέτρα που καθορίζονται σε αυτήν (Kamariza, 2017). Οι χρήστες πρέπει να είναι ενήμεροι για τις προϋποθέσεις ασφαλείας και να τις εφαρμόζουν στην καθημερινή τους εργασία. Η μη συμμόρφωση μπορεί να έχει σοβαρές συνέπειες, συμπεριλαμβανομένων πειθαρχικών μέτρων έως και δικαστικών κυρώσεων σε περιπτώσεις σοβαρής παράβασης. Επιπλέον, η συμμόρφωση με την πολιτική ασφάλειας είναι σημαντική για τη διατήρηση της ασφάλειας και της ομαλής λειτουργίας της επιχείρησης (Alshaikh et al., 2015).

2.1.2 Οδηγίες, διαδικασίες και σχέδιο ασφαλείας

Οι πολιτικές ασφάλειας ορίζουν τους γενικούς στόχους και τις κατευθυντήριες αρχές για την ασφάλεια των ΠΣ, ενώ οι οδηγίες προσφέρουν κατευθυντήριες γραμμές για την εφαρμογή αυτών των στόχων (Nord et al., 2020). Ειδικότερα, οι οδηγίες που περιλαμβάνονται στην πολιτική ασφάλειας παρέχουν κατευθύνσεις και προτάσεις για την ασφαλή λειτουργία και χρήση των ΠΣ. Αυτές οι οδηγίες μπορεί να αφορούν τον τρόπο δημιουργίας και χρήσης των κωδικών πρόσβασης, την αποθήκευση και μεταφορά ευαίσθητων δεδομένων, τη χρήση λογισμικού ασφαλείας, την ανίχνευση και αντιμετώπιση πιθανών απειλών ασφαλείας, και άλλα σχετικά θέματα (Njenga, 2016). Ο σκοπός τους είναι να καθοδηγήσουν τους χρήστες και το προσωπικό της επιχείρησης στην ασφαλή συμπεριφορά και διαχείριση των πληροφοριών και των ΠΣ (Kamariza, 2017).

Οι διαδικασίες, από την άλλη πλευρά, παρέχουν συγκεκριμένες οδηγίες και βήματα που πρέπει να ακολουθηθούν για την υλοποίηση των οδηγιών και την εφαρμογή των μέτρων ασφαλείας (Προκόπος, 2014). Οι διαδικασίες παρέχουν λεπτομερείς οδηγίες και βήματα για την εφαρμογή των οδηγιών που περιλαμβάνονται στην πολιτική ασφαλείας. Αυτές οι διαδικασίες μπορεί να περιγράφουν πώς να δημιουργήσει και να διαχειριστεί κάποιος τους κωδικούς πρόσβασης, πώς να αντιμετωπίσει ενδεχόμενες παραβιάσεις ασφάλειας, πώς να εκτελέσει αναλύσεις και να αναφέρει παραβιάσεις ασφάλειας (Lopes and Oliveira, 2015). Είναι σχεδιασμένες για να διευκολύνουν την καθημερινή εφαρμογή των αρχών και των κανόνων που περιγράφονται στην πολιτική ασφαλείας της επιχείρησης. Μαζί αυτά τα στοιχεία σχηματίζουν ένα πλήρες πλαίσιο για την προστασία της ασφάλειας των ΠΣ (Σταματινός, 2015).

Το Σχέδιο Ασφάλειας αναπτύσσει και εφαρμόζει τις αρχές και τις κατευθυντήριες γραμμές που ορίζονται στην Πολιτική Ασφάλειας. Αυτό περιλαμβάνει τον προσδιορισμό των απαιτήσεων ασφάλειας, την επιλογή κατάλληλων μέτρων προστασίας, και την εφαρμογή τους στα ΠΣ της επιχείρησης (Kamariza, 2017). Το Σχέδιο Ασφάλειας αποτελεί ένα σημαντικό εργαλείο για τη διασφάλιση της προστασίας των πληροφοριακών πόρων και τη διατήρηση του επιπέδου ασφαλείας που καθορίζεται από την πολιτική ασφαλείας (Njenga, 2016). Επιπλέον, το Σχέδιο Ασφάλειας περιλαμβάνει τα παρακάτω στοιχεία:

- *Ανάλυση Κινδύνων (Risk Analysis)*: Αξιολόγηση των δυνητικών κινδύνων για την ασφάλεια των ΠΣ, όπως αναγνώριση αδυναμιών και πιθανών απειλών.

- *Κατηγοριοποίηση των Δεδομένων (Data Classification)*: Καθορισμός των επιπέδων εμπιστευτικότητας και ευαισθησίας των δεδομένων και των μέτρων προστασίας που απαιτούνται για κάθε κατηγορία.

- *Πολιτικές Ασφαλείας Συστήματος (System Security Policies)*: Συγκεκριμένες κατευθυντήριες γραμμές για τη χρήση, τη διαχείριση και την ασφάλεια των ΠΣ.

- *Εκπαίδευση και Ευαισθητοποίηση (Training and Awareness)*: Εκπαίδευση των εργαζομένων σχετικά με τις πρακτικές ασφάλειας και ευαισθητοποίησή τους για τις απειλές ασφάλειας.

- *Σχέδιο Αντιμετώπισης Περιστατικών (Incident Response Plan)*: Οδηγίες για την αντιμετώπιση πιθανών περιστατικών ασφάλειας και την ανάκτηση από αυτά.

- *Παρακολούθηση και Αναθεώρηση (Monitoring and Review)*: Μέτρα για τη συνεχή παρακολούθηση της αποτελεσματικότητας των μέτρων ασφάλειας και την αναθεώρηση του Σχεδίου Ασφάλειας όταν απαιτείται (Σταματινός, 2015).

2.1.3 Σκοπιμότητα των ΠΣ

Η ανάπτυξη και η εφαρμογή της πολιτικής ασφάλειας απαιτεί συνεργασία και συντονισμό μεταξύ των διαφόρων τμημάτων και επιπέδων της επιχείρησης (Lopes and Oliveira, 2015). Πέραν του ότι αφορά το ΠΣ, επίσης επηρεάζει τις λοιπές λειτουργίες και τις επιχειρηματικές διαδικασίες της επιχείρησης, καθώς η ασφάλεια των πληροφοριών είναι ένας ζωτικός παράγοντας για την επιτυχή λειτουργία και την προστασία των επιχειρηματικών συμφερόντων (Kamariza, 2017). Επίσης, η πολιτική ασφάλειας πρέπει να ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της (Nord et al., 2020).

Η δημιουργία και η εφαρμογή μιας πολιτικής ασφάλειας για τα ΠΣ είναι κρίσιμη για τους οργανισμούς. Η πολιτική ασφάλειας βοηθάει στην αναγνώριση και προστασία από διάφορες απειλές, όπως κυβερνοεπιθέσεις, κακόβουλο λογισμικό και άλλες μορφές κυβερνοεγκληματιών. Πολλοί οργανισμοί διαχειρίζονται ευαίσθητα δεδομένα, όπως

προσωπικές πληροφορίες πελατών και εταιρικά μυστικά. Η πολιτική ασφάλειας βοηθά στην προστασία αυτών των δεδομένων από μη εξουσιοδοτημένη πρόσβαση (Alshaikh et al., 2015).

Οι πελάτες εμπιστεύονται τις εταιρείες με τα προσωπικά τους δεδομένα. Μια ισχυρή πολιτική ασφάλειας δείχνει στους πελάτες ότι η εταιρεία λαμβάνει σοβαρά την προστασία των πληροφοριών τους (Nord et al., 2020). Μία παραβίαση της ασφάλειας μπορεί να έχει καταστροφικές επιπτώσεις στη φήμη μιας εταιρείας ή μιας οργάνωσης. Η πολιτική ασφάλειας βοηθά στην αποτροπή τέτοιων παραβιάσεων και στη διατήρηση της εμπιστοσύνης του κοινού (Σταματινός, 2015). Υπάρχουν νόμοι και κανονισμοί που απαιτούν από τις επιχειρήσεις να διατηρούν υψηλά πρότυπα ασφάλειας για την προστασία των προσωπικών δεδομένων και των πληροφοριών που διαχειρίζονται. Οι κανονισμοί αυτοί ποικίλουν ανάλογα με τη γεωγραφική περιοχή και τον τομέα δραστηριότητας της επιχείρησης (Kamariza, 2017).

Αναλυτικότερα, η σκοπιμότητα των ΠΣ έχει ως εξής:

Α) Καθοδήγηση για την επιλογή και υλοποίηση των μέτρων ασφάλειας

Η αντιμετώπιση προβλημάτων ασφάλειας στα ΠΣ μιας επιχείρησης ή ενός οργανισμού είναι σημαντική και συχνά απαιτεί τη χρήση κατάλληλων μεθόδων ασφάλειας (Pakusadewa et al., 2020). Ωστόσο, η απλή αγορά προϊόντων ασφάλειας χωρίς την ανάλογη οργανωτική υποδομή και προετοιμασία μπορεί να οδηγήσει σε ανεπαρκή προστασία και ανταποκρίνεται στην πρόκληση της αποτελεσματικής χρήσης των προϊόντων ασφάλειας (Njenga, 2016). Παρακάτω αναφέρονται τα βήματα που μπορούν να βελτιώσουν την αποτελεσματικότητα της αντιμετώπισης προβλημάτων ασφάλειας:

- *Αξιολόγηση των αναγκών*: Πριν από την αγορά οποιουδήποτε προϊόντος ασφάλειας, είναι σημαντικό να καθοριστούν σαφώς οι ανάγκες της επιχείρησης και να γίνει ανάλυση των απειλών που αντιμετωπίζει.

- *Σχεδιασμός συνολικής στρατηγικής ασφάλειας*: Αντί να βασιστεί μόνο στην αγορά προϊόντων, ο οργανισμός πρέπει να αναπτύξει μια συνολική στρατηγική ασφάλειας που περιλαμβάνει τόσο τεχνικά όσο και οργανωτικά μέτρα.

- *Εκπαίδευση και ευαισθητοποίηση του προσωπικού*: Το προσωπικό πρέπει να εκπαιδευθεί για τις βέλτιστες πρακτικές ασφάλειας και να είναι ενημερωμένο για τις απειλές ασφάλειας που μπορεί να αντιμετωπίσει.

- *Διαδικασίες και πρωτόκολλα αντίδρασης*: Πρέπει να δημιουργηθούν διαδικασίες και πρωτόκολλα για την άμεση αντιμετώπιση προβλημάτων ασφάλειας, συμπεριλαμβανομένης της ανίχνευσης, της απόκρισης και της αποκατάστασης (Σταματινός, 2015).

Με αυτόν τον τρόπο, η αγορά προϊόντων ασφάλειας γίνεται μέρος μιας ευρύτερης προσέγγισης που συνδυάζει την τεχνολογία, το προσωπικό και τις διαδικασίες για τη δημιουργία μιας ολοκληρωμένης προστασίας των πληροφοριών και των ΠΣ (Nord et al., 2020).

Η προστασία των ΠΣ απαιτεί μια ολοκληρωμένη προσέγγιση που συνδυάζει τεχνικά, διοικητικά και οργανωτικά μέτρα ασφάλειας. Η εναρμόνιση αυτών των μέτρων είναι ζωτικής σημασίας για την αποτελεσματική προστασία της επιχείρησης (Kamariza, 2017). Αν η υλοποίηση των μέτρων ασφάλειας δεν είναι συνεπής, υπάρχει κίνδυνος τόσο από την άποψη της ασφάλειας όσο και της αποδοτικότητας. Συγκεκριμένα, η έλλειψη συνέπειας μπορεί να οδηγήσει σε διάφορα προβλήματα (Pakusadewa et al., 2020). Η υλοποίηση πολλαπλών μέτρων προστασίας για την ίδια απειλή μπορεί να οδηγήσει σε υπερβολική προστασία και υπερβολικό κόστος, ενώ η έλλειψη κατάλληλων μέτρων για συγκεκριμένες απειλές μπορεί να αφήσει το σύστημα ευάλωτο. Η εφαρμογή μέτρων ασφάλειας που έχουν αντικρουόμενους στόχους μπορεί να δημιουργήσει συγκρούσεις και ασυμβατότητες, που ενδέχεται να μειώσουν την αποτελεσματικότητα τους ή να προκαλέσουν ανεπιθύμητες επιπτώσεις (Lopes and Oliveira, 2015). Για να αποφευχθούν αυτά τα προβλήματα, η συνεκτική στρατηγική ασφάλειας πρέπει να συντονίζει τις δράσεις και τα μέτρα που λαμβάνονται σε όλα τα επίπεδα της επιχείρησης και να εξασφαλίζει ότι είναι αναλογικά με τις απειλές και τις ανάγκες ασφάλειας (Alshaikh et al., 2015).

Β) Επικοινωνία και την διαπραγμάτευση μεταξύ των εμπλεκόμενων μερών

Η διαχείριση της ασφάλειας των ΠΣ εμπλέκει πολλούς διαφορετικούς φορείς εντός και εκτός της επιχείρησης. Κάθε φορέας έχει έναν συγκεκριμένο ρόλο και ευθύνες στην εξασφάλιση της ασφάλειας των ΠΣ. Οι χρήστες των ΠΣ έχουν την ευθύνη να τηρούν τις

πολιτικές ασφαλείας και να ακολουθούν τις κατευθυντήριες γραμμές για την ασφαλή χρήση των συστημάτων (Kamariza, 2017).

Οι διαχειριστές των ΠΣ έχουν την ευθύνη να διαχειρίζονται και να συντηρούν τα συστήματα με ασφάλεια, να εφαρμόζουν ενημερώσεις λογισμικού και να προβαίνουν σε διαμόρφωση των ρυθμίσεων ασφαλείας (Lopes and Oliveira, 2015). Οι υπεύθυνοι ασφάλειας αναλαμβάνουν τον σχεδιασμό, την εφαρμογή και την παρακολούθηση των πολιτικών ασφαλείας, καθώς και τη διαχείριση αντιμετώπισης περιστατικών ασφαλείας (Nord et al., 2020). Τα διοικητικά στελέχη έχουν την ευθύνη να υποστηρίζουν την υλοποίηση πολιτικών ασφαλείας, να διαθέτουν τους αναγκαίους πόρους και να διατηρούν μια κουλτούρα ασφάλειας εντός της επιχείρησης. Η συνεργασία μεταξύ όλων αυτών των φορέων είναι απαραίτητη για τη διασφάλιση ότι τα ΠΣ παραμένουν ασφαλή και προστατευμένα (Pakusadewa et al., 2020).

Η επικοινωνία και η συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ. Οι διαφορετικοί φορείς μπορεί να έχουν διαφορετικές απόψεις, εμπειρίες και γνώσεις σχετικά με την ασφάλεια, αλλά η εποικοδομητική επικοινωνία και η συνεργασία μπορούν να συμβάλουν στην επίλυση προβλημάτων και στην εφαρμογή βέλτιστων πρακτικών (Nord et al., 2020).

Οι φορείς πρέπει να συνεργαστούν για να αντιληφθούν και να αξιολογήσουν τις απειλές που αντιμετωπίζουν τα ΠΣ. Οι ενδιαφερόμενοι φορείς πρέπει να συμφωνήσουν σε κοινές πρακτικές και πολιτικές για την ασφάλεια των ΠΣ. Η ανοιχτή επικοινωνία επιτρέπει την ανταλλαγή γνώσεων και εμπειριών μεταξύ των διαφόρων φορέων, πράγμα που μπορεί να οδηγήσει σε βελτίωση της ασφάλειας (Pakusadewa et al., 2020). Σε περιπτώσεις επείγουσας ανάγκης ή κρίσεων ασφαλείας, η αποτελεσματική επικοινωνία και συνεργασία είναι απαραίτητες για την ταχεία αντίδραση και αντιμετώπιση του προβλήματος. Συνολικά, η καλή επικοινωνία και συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι ουσιαστική για την επίτευξη των κοινών στόχων ασφάλειας των ΠΣ (Manuscript, 2020).

Η πολιτική ασφάλειας αποτελεί ένα σημαντικό έγγραφο που ορίζει τους στόχους και τα μέτρα για την ασφάλεια. Επομένως, μπορεί να λειτουργήσει ως σημείο αναφοράς για την επικοινωνία και τη διαπραγμάτευση μεταξύ των εμπλεκομένων φορέων (Lopes and Oliveira, 2015). Αυτό το έγγραφο παρέχει ένα κοινό πλαίσιο αναφοράς για τη συζήτηση

και την κατανόηση των αναγκών και των προτεραιοτήτων σχετικά με την ασφάλεια των ΠΣ. Μέσω αυτής της διαδικασίας, μπορεί να δημιουργηθεί μια κοινή αντίληψη για τη σημασία της ασφάλειας και να επιτευχθεί συναίνεση σχετικά με τις καλύτερες πρακτικές και τις δράσεις που απαιτούνται (Σταματινός, 2015).

Γ) Καθορισμός και εξασφάλιση των απαραίτητων πόρων για την ασφάλεια των ΠΣ

Η προστασία των ΠΣ ενός οργανισμού είναι αναγκαία αλλά και δαπανηρή. Οι σύγχρονοι οργανισμοί πρέπει να επενδύουν σημαντικά ποσά σε μέτρα ασφαλείας για να προστατεύσουν τα ΠΣ από εσωτερικές και εξωτερικές απειλές. Αυτό περιλαμβάνει τόσο το κόστος απόκτησης και εφαρμογής τεχνολογικών λύσεων ασφαλείας, όπως προηγμένα λογισμικά ασφαλείας και υλικού, όσο και το κόστος για τη δημιουργία και τη συντήρηση διαδικασιών ασφαλείας (Nieles et al., 2017).

Επιπλέον, απαιτείται η εκπαίδευση και η επιμόρφωση του προσωπικού, καθώς και η ανάθεση σημαντικών πόρων για την ανάπτυξη και την εφαρμογή πολιτικών ασφαλείας (Manuscript, 2020). Επιπλέον, η εμπλοκή έμπειρου και εξειδικευμένου προσωπικού είναι απαραίτητη για την επίτευξη μέγιστης αποτελεσματικότητας στην προστασία των ΠΣ. Αυτοί οι πόροι πρέπει να ενσωματωθούν στο γενικό προϋπολογισμό της επιχείρησης και να διατηρούνται σε σταθερά επίπεδα για τη διασφάλιση της ασφάλειας (Nord et al., 2020).

Η ασφάλεια τους πράγματι απαιτεί ολοκληρωμένη διαχείριση και προσέγγιση ως ένα αυτόνομο έργο μέσα στον οργανισμό. Από την αρχή της διαδικασίας, πρέπει να αναγνωρίζονται οι ενδιαφερόμενοι φορείς και να λαμβάνονται υπόψη τα συμφέροντά τους (Pakusadewa et al., 2020). Η χρονοπρογραμματισμένη δράση και οι δεσμευμένοι πόροι είναι ουσιώδεις για την αποτελεσματική υλοποίηση των ασφαλιστικών μέτρων. Η ενεργή συμμετοχή της διοίκησης είναι καίρια, καθώς μπορεί να διασφαλίσει όχι μόνο την κατανόηση και την υποστήριξη για τους στόχους της ασφάλειας, αλλά και την ανάθεση των αναγκαίων πόρων για την επίτευξή τους. Η διοίκηση μπορεί επίσης να δώσει την απαραίτητη έμφαση στη σημασία της ασφάλειας των ΠΣ σε όλη την οργάνωση και να ενθαρρύνει τη συνεργασία και τον συντονισμό μεταξύ των διαφόρων τμημάτων και ενδιαφερομένων φορέων (Safa et al., 2017).

Η ανάπτυξη μιας συνεκτικής και ολοκληρωμένης πολιτικής ασφάλειας είναι κρίσιμη για την αποδοτική διαχείριση της ασφάλειας σε έναν οργανισμό. Μέσω αυτής

της πολιτικής, καθορίζονται οι στόχοι, οι οδηγίες και οι διαδικασίες που πρέπει να ακολουθηθούν για την προστασία των ΠΣ (Alshaikh, 2018). Αυτό εξασφαλίζει όχι μόνο την ασφάλεια των ΠΣ, αλλά και τη συμμόρφωση με τους νόμους, τους κανονισμούς και τις βέλτιστες πρακτικές ασφαλείας. Επιπλέον, η πολιτική ασφάλειας δημιουργεί ένα πλαίσιο εντός του οποίου η διαχείριση της ασφάλειας μπορεί να γίνει πιο συντονισμένη και αποτελεσματική, ενισχύοντας έτσι την υποστήριξη και την προστασία των πληροφοριακών πόρων της επιχείρησης (Elvin and Johansson, 2017).

Δ) Προσδιορισμός της σημασίας της ασφάλειας των ΠΣ και κουλτούρα ασφάλειας

Η ανάπτυξη μιας κουλτούρας ασφάλειας ανάμεσα στα μέλη ενός οργανισμού είναι ζωτικής σημασίας για την αποτελεσματική προστασία των ΠΣ. Αυτό επιτυγχάνεται μέσω της εφαρμογής μιας πολιτικής ασφάλειας που υπογραμμίζει τη σημασία της ασφάλειας σε όλα τα επίπεδα της επιχείρησης (Limaye, 2013). Η δέσμευση της διοίκησης δημιουργεί μια αίσθηση ευθύνης και αφοσίωσης στην ασφάλεια σε ολόκληρο το προσωπικό (Nieles et al., 2017). Οι χρήστες των ΠΣ κατανοούν τη σημασία της προστασίας των πληροφοριών και συμμετέχουν ενεργά στην εφαρμογή των ασφαλείας μέτρων. Μέσω αυτής της συλλογικής αντίληψης και συμμετοχής, δημιουργούνται οι προϋποθέσεις για μια δυναμική και αποτελεσματική αντιμετώπιση των απειλών και των προβλημάτων ασφαλείας (Artur, 2020).

Η κουλτούρα ασφάλειας αναφέρεται στις πεποιθήσεις, τις αξίες, τις συμπεριφορές και τις πρακτικές που επικρατούν σε έναν οργανισμό σχετικά με την ασφάλεια των πληροφοριών και των ΠΣ του. Η καλή κουλτούρα ασφάλειας είναι ζωτικής σημασίας για την επιτυχημένη προστασία των δεδομένων και των πληροφοριών της επιχείρησης (Nord et al., 2020).

Η κουλτούρα ασφάλειας παίζει κρίσιμο ρόλο στην αποτελεσματική αντιμετώπιση των απειλών κατά των ΠΣ. Αν και η πολιτική ασφάλειας προσδιορίζει τους κανόνες και τις διαδικασίες για την προστασία των ΠΣ, η κουλτούρα ασφάλειας καθορίζει το πώς αυτές οι πολιτικές εφαρμόζονται και αποτυπώνονται στην καθημερινή συμπεριφορά των ανθρώπων που εργάζονται με τα ΠΣ (Kozhusko et al., 2019). Η κουλτούρα ασφάλειας ενθαρρύνει τους χρήστες να είναι επιφυλακτικοί και επιδεξιότεροι στην αντιμετώπιση νέων απειλών που ενδέχεται να προκύψουν και δεν έχουν καλυφθεί από την πολιτική ασφάλειας (Willie, 2023). Οι χρήστες που μοιράζονται κοινές αντιλήψεις και γνώσεις σχετικά με τη σημασία και τους στόχους της ασφάλειας είναι πιο πιθανό να

αναγνωρίσουν και να αντιμετωπίσουν απειλές αποτελεσματικά (Khando et al., 2021). Επιπλέον, η κουλτούρα ασφάλειας διευκολύνει τη συνεργασία και την επικοινωνία μεταξύ των χρηστών και των υπεύθυνων ασφάλειας, βοηθώντας στην αποτελεσματική αντιμετώπιση των απειλών (Blum, 2020). Όταν η ασφάλεια αντιμετωπίζεται ως κοινός στόχος και υποστηρίζεται από όλα τα μέλη της επιχείρησης, η απόκριση σε ενδεχόμενες απειλές γίνεται πιο αποτελεσματική και αποδοτική (Kozhusko et al., 2019).

Ε) Τήρηση νομικών υποχρεώσεων

Το νομικό και κανονιστικό πλαίσιο που διέπει τη λειτουργία ενός οργανισμού επηρεάζει σημαντικά τις πολιτικές ασφάλειας των ΠΣ και τα μέτρα προστασίας που πρέπει να ληφθούν. Σε πολλές περιπτώσεις, η εφαρμογή πολιτικής ασφάλειας είναι νομική υποχρέωση για τους οργανισμούς, και η μη συμμόρφωσή τους μπορεί να έχει νομικές συνέπειες (Pakusadewa et al., 2020).

Για παράδειγμα, ο Νόμος 2472 του 1997 για την Προστασία του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στην Ελλάδα, ο οποίος εναρμονίζεται με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) της ΕΕ, καθιστά υποχρεωτική τη λήψη μέτρων προστασίας για τα ευαίσθητα προσωπικά δεδομένα των ασθενών σε νοσοκομεία και άλλους φορείς υγείας. Η μη συμμόρφωση με αυτές τις νομικές απαιτήσεις μπορεί να οδηγήσει σε σημαντικές κυρώσεις και πρόστιμα. Επομένως, η ανάπτυξη πολιτικών ασφάλειας πρέπει να λαμβάνει υπόψη το συγκεκριμένο νομικό πλαίσιο και να προσαρμόζεται ανάλογα, ώστε να εξασφαλίζεται η συμμόρφωση με τις ισχύουσες νομοθετικές απαιτήσεις (Σταματινός, 2015).

ΣΤ) Συμβολή στην ανάπτυξη σχέσεων εμπιστοσύνης με πελάτες και εταίρους

Η σημασία της ασφάλειας των ΠΣ είναι πολυδιάστατη και επηρεάζει τη λειτουργία των σύγχρονων οργανισμών σε πολλά επίπεδα. Ειδικότερα, η ασφάλεια είναι κρίσιμη για την ικανότητα της επιχείρησης να λειτουργεί αποτελεσματικά και να εκτελεί τις δραστηριότητές του (Lopes and Oliveira, 2015). Ανεξάρτητα από τον τομέα δραστηριότητας, πολλές λειτουργίες εξαρτώνται από τη σωστή λειτουργία των ΠΣ, όπως η διαχείριση των παραγγελιών, η επικοινωνία με τους πελάτες, η διαχείριση των αποθεμάτων κ.λπ.. Μία παραβίαση ασφάλειας μπορεί να έχει σοβαρές επιπτώσεις, συμπεριλαμβανομένης της διακοπής των υπηρεσιών, της απώλειας δεδομένων και της υπονόμευσης της φήμης της επιχείρησης (Nord et al., 2020).

Επιπλέον, η εφαρμογή μιας πολιτικής ασφάλειας των ΠΣ δεν αποτελεί μόνο μέσο προστασίας, αλλά και πηγή εμπιστοσύνης (Kamariotou and Kitsios, 2023). Οι πελάτες, οι επιχειρηματικοί εταίροι και άλλοι εμπλεκόμενοι θέλουν να είναι βέβαιοι ότι τα προσωπικά τους δεδομένα είναι ασφαλή και ότι ο οργανισμός μπορεί να διαχειριστεί με ασφάλεια τις επιχειρηματικές του συναλλαγές. Μια καλά θεμελιωμένη πολιτική ασφάλειας μπορεί να δημιουργήσει ένα περιβάλλον εμπιστοσύνης που είναι κρίσιμο για την επιτυχία και την ανάπτυξη της επιχείρησης (Nieles et al., 2017).

2.2 Χαρακτηριστικά Πολιτικών Ασφαλείας ΠΣ

2.2.1 Είδη και μορφές πολιτικών ασφαλείας

Οι πολιτικές ασφάλειας μπορούν να διακριθούν σε τεχνικές και οργανωσιακές, ανάλογα με την έμφαση που δίνουν σε διάφορους παράγοντες (Nieles et al., 2017). Παρακάτω παρουσιάζεται κάθε τύπος πιο αναλυτικά:

- **Τεχνικές Πολιτικές Ασφάλειας (Computer-oriented)**: Αυτές οι πολιτικές επικεντρώνονται στην εφαρμογή τεχνικών μέτρων ασφάλειας στα ΠΣ. Περιλαμβάνουν την εγκατάσταση λογισμικού προστασίας, την εφαρμογή πολιτικών πρόσβασης, την κρυπτογράφηση δεδομένων και άλλα τεχνικά μέτρα για την προστασία των πληροφοριών (Kamariotou and Kitsios, 2023). Οι τεχνικές πολιτικές ασφάλειας επικεντρώνονται στην εφαρμογή τεχνικών μέτρων προστασίας προκειμένου να διασφαλιστούν δύο βασικά χαρακτηριστικά ασφάλειας των πληροφοριών (Σταματινός, 2015):
    - *Εχεμύθεια (Confidentiality)*: Αφορά την εξασφάλιση ότι οι πληροφορίες προστατεύονται από την μη εξουσιοδοτημένη πρόσβαση. Οι τεχνικές πολιτικές ασφάλειας προσπαθούν να εξασφαλίσουν ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις ευαίσθητες πληροφορίες, είτε μέσω μέτρων πρόσβασης όπως οι κωδικοί πρόσβασης, είτε μέσω κρυπτογράφησης των δεδομένων (Μπιλάλης κ.α., 2016).

- *Ακεραιότητα (Integrity)*: Αφορά τη διατήρηση της ακεραιότητας των πληροφοριών, δηλαδή την εξασφάλιση ότι οι πληροφορίες δεν έχουν τροποποιηθεί μη εξουσιοδοτημένα ή από ανεξέλεγκτες πηγές. Οι τεχνικές πολιτικές ασφάλειας περιλαμβάνουν μέτρα όπως οι ψηφιακές υπογραφές, οι αλγόριθμοι ελέγχου ακεραιότητας και η δημιουργία αντίγραφων ασφαλείας για την προστασία των δεδομένων από απώλειες ή θέματα συστήματος (Μπιλάλης κ.α., 2016).

Αυτά τα δύο χαρακτηριστικά αποτελούν βασικές αρχές της κυβερνοασφάλειας και η εφαρμογή τεχνικών πολιτικών ασφάλειας επιτρέπει στους οργανισμούς να διαχειρίζονται αποτελεσματικά τους κινδύνους που αφορούν την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών τους (Alotaibi et al., 2016).

- **Οργανωσιακές Πολιτικές Ασφάλειας (Human-oriented)**: Αυτές οι πολιτικές επικεντρώνονται στην ανθρώπινη συμπεριφορά και οργάνωση. Αναζητούν να αλλάξουν συνήθειες και πρακτικές που μπορεί να απειλούν την ασφάλεια των πληροφοριών, όπως η αδιαφορία για προσωπικές κωδικοποιήσεις, η μη συνειδητοποίηση του κινδύνου των κοινωνικών μηχανισμών και η ανεπαρκής εκπαίδευση σχετικά με την κυβερνοασφάλεια (Σταματινός, 2015).

Και οι δύο τύποι πολιτικών είναι σημαντικοί και συμπληρώνονται. Ενώ οι τεχνικές πολιτικές εστιάζουν στην προστασία των συστημάτων, οι οργανωσιακές πολιτικές ασφάλειας επικεντρώνονται στην ανθρώπινη συμπεριφορά και την κουλτούρα ασφάλειας στον οργανισμό (Nieles et al., 2017). Σε συνδυασμό, αυτοί οι δύο παράγοντες συμβάλλουν στην προστασία των πληροφοριών και στην ενίσχυση της κυβερνοασφάλειας της επιχείρησης (Nord et al., 2020).

Οι πολιτικές ασφάλειας συχνά χρησιμοποιούνται για τον καθορισμό κανόνων ελέγχου πρόσβασης και χρήσης στα δεδομένα και τους υπολογιστικούς πόρους (Kamariotou and Kitsios, 2023). Οι κύριοι τρόποι πρόσβασης έχουν ως εξής:

- **Διακριτός Έλεγχος Προσπέλασης (Discretionary Access Control - DAC)**: Στον DAC, οι χρήστες έχουν τη δυνατότητα να ελέγχουν την πρόσβαση στα δεδομένα που δημιουργούν ή που τους έχουν ανατεθεί. Οι ίδιοι οι χρήστες ή

οι ιδιοκτήτες των δεδομένων αποφασίζουν ποιοι άλλοι χρήστες ή ομάδες χρηστών μπορούν να έχουν πρόσβαση σε αυτά.

- **Υποχρεωτικός Έλεγχος Προσπέλασης (Mandatory Access Control - MAC)**: Στον MAC, ο έλεγχος της πρόσβασης γίνεται βάσει κανόνων που καθορίζονται από τους διαχειριστές του συστήματος ή τους διαχειριστές ασφάλειας. Οι χρήστες δεν έχουν τη δυνατότητα να αλλάξουν αυτούς τους κανόνες. Αυτός ο τύπος ελέγχου πρόσβασης συνήθως χρησιμοποιείται σε περιβάλλοντα όπου απαιτείται αυστηρός έλεγχος πρόσβασης, όπως σε κυβερνητικά ή στρατιωτικά συστήματα (Σταματινός, 2015).

Η γλώσσα ACU (Access Control Unit) είναι ένα παράδειγμα γλώσσας που χρησιμοποιείται για τη διαμόρφωση κανόνων πρόσβασης σε δεδομένα. Αυτές οι γλώσσες παρέχουν ένα περιβάλλον προγραμματισμού όπου οι διαχειριστές μπορούν να ορίζουν ποιοι χρήστες ή ομάδες χρηστών έχουν πρόσβαση σε ποια δεδομένα και με ποιους τρόπους (Σταματινός, 2015). Οι γλώσσες αυτές συνήθως προσφέρουν ένα σύνολο εντολών και δομών δεδομένων που επιτρέπουν την περιγραφή πολιτικών πρόσβασης με μεγάλη λεπτομέρεια και ευελιξία. Οι διαχειριστές μπορούν να ορίσουν πολιτικές που καθορίζουν ποιοι χρήστες ή ομάδες χρηστών έχουν πρόσβαση σε ποια δεδομένα, καθώς και τους τρόπους πρόσβασης (π.χ. ανάγνωση, εγγραφή, διαγραφή). Με τη χρήση αυτών των γλωσσών, οι οργανισμοί μπορούν να δημιουργήσουν πολύπλοκες πολιτικές ασφάλειας που προστατεύουν τα δεδομένα τους από μη εξουσιοδοτημένη πρόσβαση και καταχώρηση (Nieles et al., 2017).

Οι πολιτικές ασφάλειας υπολογιστών αποσκοπούν στην προστασία των υπολογιστικών πόρων, συμπεριλαμβανομένων των δεδομένων, και υλοποιούνται κυρίως στο επίπεδο του λειτουργικού συστήματος. Αυτές οι πολιτικές μπορούν να περιλαμβάνουν κανόνες για τον έλεγχο της πρόσβασης στους υπολογιστικούς πόρους, την προστασία από κακόβουλο λογισμικό, την αποτροπή μη εξουσιοδοτημένων πρόσβασης και άλλα θέματα ασφάλειας (Pakusadewa et al., 2020).

Για την περιγραφή αυτών των πολιτικών ασφάλειας μπορούν να χρησιμοποιηθούν διάφορες τυπικές μορφές, όπως οι γράφοι. Οι γράφοι μπορούν να αναπαραστήσουν τις σχέσεις μεταξύ των διάφορων πολιτικών ασφάλειας υπολογιστών, τις εξαρτήσεις μεταξύ τους και τις διαδικασίες εφαρμογής τους (Khando et al., 2021). Με αυτόν τον τρόπο, οι διαχειριστές μπορούν να έχουν μια ολοκληρωμένη εικόνα του συστήματος ασφάλειας και

να λαμβάνουν αποφάσεις για τη βελτίωσή του. Οι γράφοι μπορούν να παρέχουν έναν ευέλικτο τρόπο αναπαράστασης των πολύπλοκων σχέσεων και δομών που αφορούν την ασφάλεια των υπολογιστικών συστημάτων (Kamariotou and Kitsios, 2023).

Η ενσωμάτωση της πολιτικής ασφάλειας στα δίκτυα υπολογιστών είναι ζωτικής σημασίας για τη διασφάλιση της προστασίας των πληροφοριών και των πόρων του δικτύου. Αυτό σημαίνει ότι κάθε οντότητα που αποτελεί μέρος του δικτύου πρέπει να διαθέτει τη δική της πολιτική ασφάλειας, η οποία πρέπει να υλοποιείται αυτόματα (Pakusadewa et al., 2020).

Οι προσεγγίσεις για την ανάπτυξη πολιτικών ασφάλειας δικτύων συχνά χρησιμοποιούν μεθόδους όπως τα Διαγράμματα Ροής Δεδομένων (Data Flow Diagrams - DFD). Αυτά τα διαγράμματα αναπαριστούν τη ροή των δεδομένων σε ένα σύστημα ή ένα δίκτυο, καθώς και τις διαδικασίες που επηρεάζουν αυτήν τη ροή. Μέσω των DFD μπορούν να αναδειχθούν τα σημεία ευπάθειας και να σχεδιαστούν πολιτικές ασφάλειας που να αντιμετωπίζουν αποτελεσματικά αυτούς τους κινδύνους. Με άλλα λόγια, τα DFD παρέχουν ένα πλαίσιο για την κατανόηση της ροής των δεδομένων και την ανάπτυξη αποτελεσματικών πολιτικών ασφάλειας σε ένα δίκτυο υπολογιστών (Σταματινός, 2015).

Οι πολιτικές ασφάλειας ειδικού σκοπού σχετίζονται με συγκεκριμένες εφαρμογές ή περιβάλλοντα και αναπτύσσονται για να αντιμετωπίσουν τα ξεχωριστά ζητήματα ασφάλειας που προκύπτουν σε αυτά τα πλαίσια (Manuscript, 2020). Αυτές οι πολιτικές συχνά προβλέπουν προσαρμοσμένους κανόνες και διαδικασίες ασφαλείας που να ανταποκρίνονται στις ειδικές ανάγκες και απαιτήσεις μιας συγκεκριμένης εφαρμογής ή περιβάλλοντος (Kamariotou and Kitsios, 2023). Για παράδειγμα, μπορεί να αναπτυχθεί μια πολιτική ασφαλείας ειδικού σκοπού για μια ιατρική εφαρμογή που διαχειρίζεται ευαίσθητα δεδομένα υγείας. Αυτή η πολιτική μπορεί να περιλαμβάνει πρόσθετους έλεγχους πρόσβασης, κρυπτογράφηση δεδομένων και ειδικές διαδικασίες αποθήκευσης και ανταλλαγής πληροφοριών που να συμμορφώνονται με τους κανονισμούς περί ασφάλειας υγείας (όπως ο HIPAA στις ΗΠΑ). Επομένως, οι πολιτικές αυτές εστιάζουν στην προσαρμογή των μέτρων ασφαλείας στις συγκεκριμένες ανάγκες και προδιαγραφές της εφαρμογής ή του περιβάλλοντος (Σταματινός, 2015).

Προχωρώντας στις μορφές των ΠΣ έχουν ως εξής:

A) Individual security policies

Οι "Individual security policies" αναφέρονται σε πολιτικές ασφάλειας που εστιάζουν σε συγκεκριμένους χρήστες, υπηρεσίες ή συστήματα. Αυτές οι πολιτικές επικεντρώνονται στις ανάγκες και στις αρμοδιότητες ενός συγκεκριμένου ατόμου ή οντότητας σε έναν οργανισμό. Συνήθως, κάθε χρήστης ή κάθε τμήμα της επιχείρησης μπορεί να έχει τη δική του πολιτική ασφαλείας που να προσαρμόζεται στις ειδικές του ανάγκες και αρμοδιότητες (Manuscript, 2020). Αποδεικνύονται ως απαραίτητες για την καλύτερη διαχείριση των ασφαλείας σε διάφορα επίπεδα και συστήματα ενός οργανισμού (Blum, 2020). Η διατήρηση ξεχωριστών πολιτικών ασφαλείας για διαφορετικές εφαρμογές και συστήματα επιτρέπει την προσαρμογή των πολιτικών σε συγκεκριμένες ανάγκες, απαιτήσεις και απειλές που αφορούν κάθε τομέα (Khando et al., 2021).

Η επιχείρηση διατηρεί μια πολιτική ασφαλείας για το ηλεκτρονικό ταχυδρομείο των υπαλλήλων της, η οποία πιθανόν να εστιάζει σε θέματα, όπως η ασφαλής χρήση του ηλεκτρονικού ταχυδρομείου, οι πολιτικές για τον κωδικό πρόσβασης, οι απαγορεύσεις για την αποστολή ευαίσθητων πληροφοριών μέσω email κ.λπ. (Nieles et al., 2017). Αντίστοιχα, η πολιτική για την πρόσβαση σε δεδομένα και εφαρμογές μπορεί να εστιάζει σε θέματα όπως οι δικαιώματα πρόσβασης, οι περιορισμοί για ευαίσθητες πληροφορίες, οι διαδικασίες αδειοδότησης και παρακολούθησης της πρόσβασης κ.λπ.. Αυτή η προσέγγιση επιτρέπει στην επιχείρηση να διαχειρίζεται καλύτερα τις ασφαλείς πρακτικές και τις προσδοκίες σε διάφορα επίπεδα και τμήματα του (Σταματινός, 2015).

Β) Comprehensive security policies

Από την άλλη πλευρά, οι "Comprehensive security policies" είναι πολιτικές που καλύπτουν ολόκληρο το φάσμα την ασφαλείας ενός οργανισμού. Αυτές οι πολιτικές προσπαθούν να καθορίσουν έναν συνολικό πλαίσιο ασφαλείας που να καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριών και να εφαρμόζεται σε όλα τα επίπεδα και τις δραστηριότητες της επιχείρησης (Manuscript, 2020). Αυτές οι πολιτικές είναι συνήθως πιο γενικές και καλύπτουν θέματα, όπως η διαχείριση των προσβολών, οι διαδικασίες επικοινωνίας ασφαλείας και οι πρακτικές για την πρόληψη και αντιμετώπιση προβλημάτων ασφαλείας. Είναι αλήθεια ότι οι λεπτομερείς πολιτικές ασφαλείας μπορεί να είναι αρκετά μεγάλες και πολύπλοκες λόγω της ανάγκης για εκτεταμένη κάλυψη όλων των πτυχών της ασφάλειας ΠΣ. Ωστόσο, η εκτενής φύση τους είναι συχνά απαραίτητη για την πλήρη και αποτελεσματική προστασία των ΠΣ ενός οργανισμού (Σταματινός, 2015).

Για να γίνουν πιο εύχρηστες, οι πολιτικές ασφαλείας μπορούν να οργανωθούν με τρόπο που να παρέχει εύκολη πρόσβαση στις βασικές πληροφορίες και να διατηρεί μια δομή που να είναι κατανοητή (Manuscript, 2020). Μπορεί επίσης να είναι χρήσιμο να συμπεριληφθούν συνοπτικές ενότητες ή σημεία που να απεικονίζουν τα βασικά σημεία και τις πιο σημαντικές πρακτικές που πρέπει να ακολουθούν οι χρήστες. Επιπλέον, η εκπαίδευση και η ενημέρωση του προσωπικού για τις πολιτικές ασφαλείας είναι ουσιώδης. Οι εργαζόμενοι πρέπει να γνωρίζουν την ύπαρξή τους, τη σημασία τους και πώς να τις εφαρμόζουν στην καθημερινή τους εργασία (Blum, 2020). Αυτό μπορεί να επιτευχθεί μέσω εκπαιδευτικών προγραμμάτων, εκπαιδευτικών υλικών και συστημάτων παρακολούθησης και αξιολόγησης της συμμόρφωσης (Khando et al., 2021). Η ανάγκη για εξατομικευμένες πολιτικές ασφαλείας είναι σημαντική, καθώς οι ανάγκες και οι απαιτήσεις ασφάλειας μπορεί να διαφέρουν ανάλογα με τα διάφορα συστήματα και εφαρμογές της επιχείρησης. Ωστόσο, η δημιουργία και η διατήρηση αυτών των πολιτικών μπορεί να αποτελέσει πρόκληση λόγω του μεγέθους και της πολυπλοκότητας τους (Manuscript, 2020).

Η προσέγγιση της Modular Security Policy μπορεί να αποτελέσει μια λύση σε αυτό το πρόβλημα. Με την υιοθέτηση ενός κεντρικού πλαισίου ασφαλείας που περιλαμβάνει γενικές οδηγίες και προδιαγραφές για την ασφάλεια των ΠΣ, καθώς και των υπευθύνων για την ασφάλεια, η εφαρμογή και η διαχείριση των πολιτικών ασφαλείας μπορεί να γίνει πιο αποτελεσματική και συνεκτική (Pakusadewa et al., 2020). Ταυτόχρονα, η παράλληλη δυνατότητα περαιτέρω αναλύσεων και οδηγιών σε παραρτήματα επιτρέπει την προσαρμογή των πολιτικών σε συγκεκριμένες ανάγκες και εφαρμογές χωρίς να χάνεται η συνολική διαχείριση και εναρμόνιση της ασφάλειας (Nord et al., 2020).

Η χρήση μιας πολιτικής ασφαλείας με μορφή υπερκειμένου σε επιχειρήσεις που διαθέτουν ενδοεπιχειρηματικό δίκτυο επιτρέπει τη δημιουργία ενός ενιαίου εγγράφου που καλύπτει τη γενική πολιτική ασφαλείας της επιχείρησης, ενώ ταυτόχρονα παρέχει τη δυνατότητα πρόσβασης σε λεπτομερείς οδηγίες και διαδικασίες που είναι απαραίτητες για τους συγκεκριμένους χρήστες ή τους υπεύθυνους για την ασφάλεια (Manuscript, 2020). Οι σύνδεσμοι (links) σε παραρτήματα ή επεξηγηματικά κείμενα μπορούν να βελτιώσουν την προσβασιμότητα και την κατανόηση των οδηγιών ασφαλείας από τους χρήστες, ενισχύοντας τη συνολική ασφάλεια. Επιπλέον, αυτή η διαδραστική μορφή επιτρέπει στους χρήστες να βρίσκουν γρήγορα τις πληροφορίες που χρειάζονται χωρίς να χρειάζεται να αναζητούν σε μεγάλα και πολύπλοκα έγγραφα ασφαλείας (Blum, 2020).

2.2.2 Αρχές Διαμόρφωσης Πολιτικών Ασφάλειας

Οι αρχές διαμόρφωσης πολιτικών ασφάλειας αποτελούν τις βασικές κατευθυντήριες αρχές και αξίες που καθορίζουν τον τρόπο με τον οποίο σχεδιάζονται, εφαρμόζονται και διαχειρίζονται οι πολιτικές ασφάλειας σε μία επιχείρηση. Αυτές οι αρχές συμβάλλουν στη δημιουργία ενός ολοκληρωμένου πλαισίου ασφάλειας που προστατεύει τα ΠΣ και τα δεδομένα της επιχείρησης (Manuscript, 2020). Ορισμένες από τις βασικές αρχές διαμόρφωσης πολιτικών ασφάλειας περιλαμβάνουν:

- *Αρχή της ανάγκης*: προσαρμόζονται στις συγκεκριμένες ανάγκες και χαρακτηριστικά της επιχείρησης.
- *Αρχή της αναλογικότητας*: είναι ανάλογες με τους κινδύνους που αντιμετωπίζει ο οργανισμός και τα είδη των πληροφοριών που πρέπει να προστατευτούν.
- *Αρχή της ευελιξίας*: είναι ευέλικτες, ώστε να προσαρμόζονται σε νέες απειλές και αλλαγές στο περιβάλλον λειτουργίας της επιχείρησης.
- *Αρχή της ευθύνης*: Κάθε μέλος της επιχείρησης πρέπει να αναλαμβάνει ευθύνη για την ασφάλεια των πληροφοριών και να συμμορφώνεται με τις πολιτικές ασφαλείας.
- *Αρχή της συνεχούς βελτίωσης*: αναθεωρούνται και βελτιώνονται συνεχώς για να αντιμετωπίζουν αποτελεσματικά τις εξελίξεις στον τομέα της ασφάλειας των πληροφοριών (Σταματινός, 2015).

Αυτές οι αρχές παρέχουν ένα πλαίσιο για τον σχεδιασμό και την υλοποίηση αποτελεσματικών πολιτικών ασφαλείας που ενισχύουν την προστασία των πληροφοριών και των ΠΣ της επιχείρησης (Khando et al., 2021).

1. Εμπλεκόμενοι στην Ανάπτυξη Πολιτικών Ασφάλειας

Η ανάπτυξη πολιτικών ασφάλειας είναι μια διαδικασία που απαιτεί την εμπλοκή διαφόρων εμπλεκομένων μερών εντός μίας επιχείρησης. Αυτοί οι φορείς συμβάλλουν στον σχεδιασμό, την εφαρμογή και τη διαχείριση των πολιτικών ασφαλείας προκειμένου να διασφαλιστεί η αποτελεσματική προστασία των πληροφοριών και των ΠΣ

(Kamariotou and Kitsios, 2023). Ορισμένοι από τους κύριους εμπλεκόμενους στη διαδικασία ανάπτυξης πολιτικών ασφάλειας περιλαμβάνουν:

- *Ηγεσία της επιχείρησης*: Η ανώτερη διοίκηση έχει τον πρωταρχικό ρόλο στην καθοδήγηση και την υποστήριξη της ανάπτυξης πολιτικών ασφαλείας. Η δέσμευσή τους στην ασφάλεια των πληροφοριών είναι κρίσιμη για την επιτυχή υλοποίηση των πολιτικών.

- *Τμήμα Πληροφορικής (IT)*: Οι ειδικοί στον τομέα της πληροφορικής είναι υπεύθυνοι για την ανάπτυξη και την εφαρμογή τεχνικών μέτρων ασφαλείας. Συμβάλλουν επίσης στην παρακολούθηση των συστημάτων για ενδεχόμενες παραβιάσεις ασφαλείας.

- *Νομικό Τμήμα*: Οι νομικοί ειδικοί βοηθούν στη διατύπωση πολιτικών που συμμορφώνονται με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων και ασφαλείας πληροφοριών.

- *Ανθρώπινο Δυναμικό*: Οι υπεύθυνοι ανθρώπινου δυναμικού είναι υπεύθυνοι για την εκπαίδευση του προσωπικού σχετικά με τις πολιτικές ασφαλείας και τις βέλτιστες πρακτικές.

- *Ομάδες Εργασίας Ασφάλειας*: Ορίζονται ομάδες εργασίας από εξειδικευμένους επαγγελματίες που εργάζονται σε συγκεκριμένους τομείς ασφάλειας, όπως η δικτυακή ασφάλεια, η φυσική ασφάλεια και η προστασία από κυβερνοεπιθέσεις (Σταματινός, 2015).

Η ενεργή συμμετοχή και συνεργασία αυτών των μερών είναι ουσιώδης για την ανάπτυξη πολιτικών ασφαλείας που να ανταποκρίνονται στις ανάγκες και τις απαιτήσεις της επιχείρησης (Pakusadewa et al., 2020).

2. Ανάλυση Επικινδυνότητας

Η ανάλυση επικινδυνότητας είναι ένας σημαντικός και κρίσιμος βήματα κατά την ανάπτυξη πολιτικών ασφαλείας. Αυτή η διαδικασία αποσκοπεί στον προσδιορισμό των πιθανών απειλών, ευκαιριών και αδυναμιών που μπορεί να αντιμετωπίσει ένας οργανισμός, ώστε να ληφθούν τα κατάλληλα μέτρα προστασίας (Kitsios et al., 2022). Η ανάλυση αυτή συνήθως περιλαμβάνει τα παρακάτω στοιχεία:

- *Απειλές (Threats)*: Αναφέρονται σε πιθανές καταστάσεις ή ενέργειες που μπορούν να προκαλέσουν ζημιά στην ασφάλεια των πληροφοριών. Αυτές οι απειλές μπορεί να περιλαμβάνουν κυβερνοεπιθέσεις, φυσικές καταστροφές, εσωτερικές απειλές από εργαζόμενους κλπ.

- *Ευκαιρίες (Opportunities)*: Πρόκειται για τις περιστάσεις ή τις συνθήκες που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να προβούν σε επιθέσεις. Οι ευκαιρίες μπορεί να προκύπτουν από αδυναμίες στο σύστημα ασφαλείας, ανθρώπινα λάθη ή ακόμα και καταστάσεις κοινωνικής μηχανικής.

- *Αδυναμίες (Weaknesses)*: Αναφέρονται σε πιθανές ευπάθειες ή ελλείψεις στο σύστημα ασφαλείας που μπορούν να εκτεθούν σε κινδύνους. Αυτές μπορεί να περιλαμβάνουν ελλιπείς πολιτικές, αδύναμους κωδικούς πρόσβασης, μη αναβαθμισμένα λογισμικά κλπ.

- *Κινδύνους (Risks)*: Αφορούν την πιθανότητα της πραγματοποίησης ενός αρνητικού συμβάντος και τις επιπτώσεις που αυτό μπορεί να έχει στον οργανισμό. Οι κίνδυνοι υπολογίζονται λαμβάνοντας υπόψη τις απειλές, τις ευκαιρίες και τις αδυναμίες (Σταματινός, 2015).

Η ανάλυση επικινδυνότητας βοηθά τους οργανισμούς να αναγνωρίσουν τα κύρια σημεία ευπάθειας και να εστιάσουν τις προσπάθειές τους στην ενίσχυση της ασφάλειας σε αυτούς τους τομείς (Kitsios et al., 2022). Η εφαρμογή μεθόδων ανάλυσης επικινδυνότητας, όπως η SBA, η MARION και η CRAMM, στην αξιολόγηση του επιπέδου ασφάλειας των ΠΣ είναι μια καλή πρακτική (Σταματινός, 2015). Αυτές οι μέθοδοι συνήθως περιλαμβάνουν τα ακόλουθα βήματα:

- *Αναγνώριση Κινδύνων*: Ανάλυση των δυνητικών απειλών και αδυναμιών που ενδέχεται να επηρεάσουν την ασφάλεια των ΠΣ.

- Αξιολόγηση *Κινδύνων*: Εκτίμηση της πιθανότητας εκδήλωσης και των επιπτώσεων κάθε κινδύνου.

- *Αντιμετώπιση Κινδύνων*: Ανάπτυξη μέτρων πρόληψης και αντιμετώπισης για τη μείωση των κινδύνων σε αποδεκτά επίπεδα.

- *Διαμόρφωση Πολιτικής Ασφάλειας*: Βασιζόμενη στα αποτελέσματα της ανάλυσης, η πολιτική ασφάλειας προσδιορίζει τα απαιτούμενα μέτρα προστασίας και πρακτικές (Σταματινός, 2015).

Το πλεονέκτημα αυτής της προσέγγισης είναι ότι η πολιτική ασφάλειας είναι πιο εξατομικευμένη και προσαρμοσμένη στις συγκεκριμένες ανάγκες και απειλές που αντιμετωπίζει κάθε οργανισμός. Ωστόσο, η μεθοδολογία αυτή είναι επίσης εξαιρετικά εξαρτημένη από την εμπειρία και τις γνώσεις του αναλυτή και μπορεί να απαιτήσει σημαντικό χρόνο και πόρους για την υλοποίησή της (Blum, 2020).

3. Περιεχόμενο των Πολιτικών Ασφάλειας

Τα έγγραφα πολιτικής ασφάλειας είναι κρίσιμα για την καλή λειτουργία και την προστασία των ΠΣ ενός οργανισμού. Αυτά τα έγγραφα πρέπει να είναι κατανοητά και προσιτά σε όλους τους εμπλεκόμενους, από το ανώτερο επίπεδο διοίκησης έως τους απλούς χρήστες, και πρέπει να παρέχουν τις κατάλληλες κατευθυντήριες γραμμές για την ασφάλεια των ΠΣ (Khando et al., 2021). Τα εν λόγω έγγραφα περιλαμβάνουν συνήθως τα ακόλουθα στοιχεία:

- *Περιγραφή της Πολιτικής*: Περιέχει έναν επισκόπηση των αρχών και των στόχων της πολιτικής ασφάλειας.
- *Καθορισμός Ευθυνών*: Προσδιορίζει τις ευθύνες και τους ρόλους κάθε μέλους της επιχείρησης σχετικά με την ασφάλεια των ΠΣ.
- *Οδηγίες και Διαδικασίες*: Παρέχει λεπτομερείς οδηγίες και διαδικασίες για την αντιμετώπιση πιθανών απειλών και επεισοδίων ασφάλειας.
- *Κανόνες και Πειθαρχικά Μέτρα*: Καθορίζει τους κανόνες που πρέπει να τηρούν οι χρήστες και περιλαμβάνει πιθανά πειθαρχικά μέτρα για παραβάσεις.
- *Διαχείριση Κινδύνων*: Περιλαμβάνει μεθόδους αναγνώρισης, αξιολόγησης και διαχείρισης κινδύνων (Σταματινός, 2015).

Με τη διατήρηση και την τακτική αναθεώρηση αυτών των εγγράφων, ο οργανισμός εξασφαλίζει ότι οι πολιτικές ασφάλειας είναι ενημερωμένες και αποτελεσματικές στην προστασία των ΠΣ (Nord et al., 2020). Μια πολιτική ασφαλείας πρέπει να είναι πλήρης

και συνεκτική, καλύπτοντας όλες τις ανάγκες και τους τομείς ασφαλείας ενός οργανισμού (Kamariotou and Kitsios, 2023). Τα βασικά στοιχεία που πρέπει να περιλαμβάνει μια πολιτική ασφαλείας είναι τα εξής:

- *Στόχοι και αρχές*: Καθορίζει τους βασικούς στόχους και τις αρχές που διέπουν την πολιτική ασφαλείας της επιχείρισης.
- *Περιγραφή του πεδίου εφαρμογής*: Ορίζει το πεδίο εφαρμογής της πολιτικής ασφαλείας, περιγράφοντας τα ΠΣ, τα δεδομένα και τους πόρους που καλύπτονται από αυτήν.
- *Ευθύνες και ρόλοι*: Καθορίζει τις ευθύνες και τους ρόλους των διαφόρων μερών της επιχείρησης σχετικά με την ασφάλεια των ΠΣ.
- *Οδηγίες και διαδικασίες*: Περιέχει λεπτομερείς οδηγίες και διαδικασίες για την ασφαλή χρήση και διαχείριση των ΠΣ και δεδομένων.
- *Πολιτικές πρόσβασης*: Καθορίζει τους κανόνες και τις διαδικασίες πρόσβασης στα ΠΣ και τα δεδομένα.
- *Ανίχνευση και αντίδραση*: Περιέχει οδηγίες για την ανίχνευση ασφαλείας και την αντίδραση σε πιθανές απειλές και επιθέσεις.
- *Εκπαίδευση και ευαισθητοποίηση*: Ορίζει τις απαιτήσεις για εκπαίδευση και ευαισθητοποίηση του προσωπικού σχετικά με την ασφάλεια.
- *Διαχείριση κινδύνων*: Περιλαμβάνει μέτρα για την αναγνώριση, αξιολόγηση και διαχείριση των κινδύνων ασφάλειας.
- *Πολιτικές επιθεώρησης και αναθεώρησης*: Καθορίζει τις διαδικασίες για την τακτική επιθεώρηση και αναθεώρηση της πολιτικής ασφαλείας για ενημέρωση και βελτίωση (Σταματινός, 2015).

2.2.3 Άξονες Διαμόρφωσης Πολιτικών Ασφάλειας

Οι άξονες διαμόρφωσης πολιτικών ασφάλειας περιλαμβάνουν οδηγίες για τον τρόπο επαλήθευσης της ταυτότητας των χρηστών και την ανάθεση πρόσβασης με βάση τα δικαιώματα και τις ευθύνες τους. Ακόμη, περιλαμβάνουν τις οδηγίες για την ασφαλή

αποθήκευση, μεταφορά και επεξεργασία δεδομένων, καθώς και για την αποτροπή μη εξουσιοδοτημένης πρόσβασης (Nord et al., 2020).

Παράλληλα, οι άξονες καθορίζουν τη χρήση κρυπτογράφησης για την προστασία ευαίσθητων πληροφοριών κατά τη μεταφορά και την αποθήκευσή τους. Περιλαμβάνουν τις διαδικασίες για τον εντοπισμό, την αξιολόγηση και τον χειρισμό των κινδύνων για την ασφάλεια των ΠΣ (Blum, 2020). Επιπρόσθετα, καθορίζουν τις διαδικασίες και τα πρωτόκολλα για την αντίδραση σε επιθέσεις και παραβιάσεις της ασφάλειας και περιλαμβάνουν τις οδηγίες για την εκπαίδευση του προσωπικού σχετικά με τις ασφαλείς πρακτικές και την ευαισθητοποίησή τους σε θέματα ασφάλειας. Ταυτόχρονα, καθορίζουν τις διαδικασίες για τη συνεχή παρακολούθηση της ασφάλειας και την αξιολόγηση της αποτελεσματικότητας των μέτρων ασφαλείας (Khando et al., 2021).

A) Personal security

Όσον αφορά στην προσωπική ασφάλεια (personal security), αυτή μπορεί να αποτελεί έναν από τους άξονες ΠΣ, κυρίως όταν συνδέεται με την προστασία των ατομικών δεδομένων και την ασφάλεια των χρηστών του συστήματος (Σταματινός, 2015). Ορισμένοι άξονες ΠΣ που σχετίζονται με την προσωπική ασφάλεια μπορεί να περιλαμβάνουν:

- *Πρόσβαση και Ταυτοποίηση*: Οι κανόνες και οι διαδικασίες που διέπουν την πρόσβαση σε προσωπικά δεδομένα και ταυτοποίησης χρηστών εντός του συστήματος, όπως οι διαδικασίες σύνδεσης (login) και οι ρυθμίσεις απορρήτου.

- *Ασφάλεια Δεδομένων*: Οι πολιτικές και οι μέθοδοι για την προστασία και την ασφαλή αποθήκευση των προσωπικών δεδομένων, καθώς και οι διαδικασίες για τη διαγραφή ή την ανωνυμία δεδομένων όταν δεν απαιτούνται πλέον.

- *Εκπαίδευση και Ευαισθητοποίηση*: Οι διαδικασίες εκπαίδευσης των χρηστών για τους κινδύνους και τις πρακτικές ασφάλειας, καθώς και οι προσπάθειες ευαισθητοποίησης τους για τη σημασία της προσωπικής ασφάλειας.

- *Ανίχνευση και Αντιμετώπιση Παραβιάσεων*: Οι μέθοδοι για τον εντοπισμό και την αντιμετώπιση των παραβιάσεων της προσωπικής ασφάλειας,

συμπεριλαμβανομένων των ανωμαλιών στην κίνηση των δεδομένων ή των προσπαθειών ανεπιτυχούς πρόσβασης (Σταματινός, 2015).

Καθένας από αυτούς τους άξονες απαιτεί την ανάπτυξη συγκεκριμένων πολιτικών και μέτρων προστασίας που εξασφαλίζουν την προσωπική ασφάλεια εντός ενός ΠΣ. Η προσωπική ασφάλεια στον τομέα της πληροφορικής αφορά την προστασία των πληροφοριών και των πόρων από ανθρώπινα λάθη, απάτες, κλοπές ή κατάχρηση από εσωτερικούς ή εξωτερικούς παράγοντες (Blum, 2020). Τα μέτρα ασφάλειας σε αυτήν την κατηγορία περιλαμβάνουν πολιτικές, διαδικασίες και τεχνικές που στοχεύουν στην εκπαίδευση και ευαισθητοποίηση των χρηστών σχετικά με τις απειλές ασφάλειας και τη σωστή συμπεριφορά για την αντιμετώπισή τους (Khando et al., 2021).

Η κατάρτιση των χρηστών σε θέματα ασφάλειας είναι κρίσιμης σημασίας για την εφαρμογή της πολιτικής ασφάλειας στην καθημερινή τους δραστηριότητα. Μέσω της ενημέρωσης και της εκπαίδευσης, οι χρήστες μπορούν να αναγνωρίζουν τις απειλές, να κατανοούν τις σωστές πρακτικές ασφαλείας και να εφαρμόζουν τα κατάλληλα μέτρα προστασίας στις δραστηριότητές τους. Αυτό μπορεί να συμβάλει σημαντικά στη μείωση των πιθανοτήτων επίθεσης και στην ενίσχυση του επιπέδου ασφάλειας (Blum, 2020).

Ο καθορισμός ρόλων και υπευθυνοτήτων για την προστασία των αγαθών του ΠΣ είναι ζωτικής σημασίας για την αποτελεσματική εφαρμογή της πολιτικής ασφαλείας. Κάθε οργανισμός πρέπει να ορίσει σαφώς τους διάφορους ρόλους και τις υπευθυνότητες σχετικά με την προστασία των πληροφοριακών αγαθών του (Khando et al., 2021). Οι βασικοί ρόλοι και οι υπευθυνότητες που μπορεί να καθοριστούν περιλαμβάνουν:

- *Διαχειριστής Ασφάλειας (Security Administrator)*: Υπεύθυνος για τον σχεδιασμό, την εφαρμογή και τη συντήρηση των πολιτικών και των τεχνικών ασφάλειας του συστήματος.

- *Υπεύθυνος Πληροφορικής (IT Manager)*: Υπεύθυνος για τη διαχείριση και την ασφάλεια του ΠΣ σε γενικές γραμμές, συμπεριλαμβανομένης της ανάθεσης καθηκόντων σε άλλα μέλη της ομάδας του.

- *Υπεύθυνος Ασφάλειας Πληροφοριών (Information Security Officer)*: Υπεύθυνος για την ανάπτυξη και την εφαρμογή της πολιτικής ασφάλειας, καθώς και για την παρακολούθηση των απειλών και των επιθέσεων στο ΠΣ.

- *Διαχειριστής Συστήματος (System Administrator)*: Υπεύθυνος για τη διαχείριση, τη συντήρηση και την ασφάλεια των συστημάτων λογισμικού και υλικού.

- *Χρήστες/Εργαζόμενοι*: Έχουν την υποχρέωση να συμμορφώνονται με τις πολιτικές και τα πρότυπα ασφάλειας που έχουν καθοριστεί και να ακολουθούν τις οδηγίες για την ασφαλή χρήση του συστήματος (Σταματινός, 2015).

Η αποτελεσματική ανάθεση ρόλων και υπευθυνοτήτων εξασφαλίζει ότι όλοι οι εμπλεκόμενοι γνωρίζουν τις ευθύνες τους και συμβάλλουν στην προστασία των πληροφοριακών αγαθών. Η επιλογή νέου προσωπικού για θέσεις που αντιμετωπίζουν ευαίσθητα ή κρίσιμα δεδομένα και εφαρμογές απαιτεί προσεκτική διαδικασία για τη διασφάλιση της ασφάλειας των πληροφοριών και της εμπιστοσύνης της επιχείρησης (Khando et al., 2021).

Η βασική ιδέα είναι να εξασφαλιστεί ότι το νέο προσωπικό έχει τις κατάλληλες δεξιότητες, την ακεραιότητα και την ευθύνη για την ασφάλεια των πληροφοριών (Manuscript, 2020). Η συμμόρφωση με το νομικό πλαίσιο αποτελεί ουσιαστικό μέρος της πολιτικής ασφαλείας των ΠΣ. Αυτό περιλαμβάνει την προστασία των προσωπικών δεδομένων, σύμφωνα με τους νόμους περί προστασίας των δεδομένων, καθώς και την προστασία της πνευματικής ιδιοκτησίας (Khando et al., 2021). Παράδειγμα μέτρων που μπορούν να ληφθούν για την επίτευξη αυτής της συμμόρφωσης περιλαμβάνουν:

- *Απόρριψη μη νόμιμου λογισμικού*: Εφαρμογή πολιτικής που να απαγορεύει τη χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο και ενθαρρύνει τη χρήση μόνο νόμιμων άδειων λογισμικού.

- *Ανίχνευση και πρόληψη παραβάσεων*: Εφαρμογή συστημάτων παρακολούθησης και ανίχνευσης παραβάσεων για την πρόληψη αποκλεισμού μη νόμιμης χρήσης λογισμικού ή δεδομένων.

- *Εκπαίδευση του προσωπικού*: Ενημέρωση και εκπαίδευση των εργαζομένων σχετικά με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων και πνευματικής ιδιοκτησίας.

- *Συμμόρφωση με τις πολιτικές άδειας χρήσης λογισμικού*: Εφαρμογή πολιτικής που να επιβάλλει τη συμμόρφωση με τις πολιτικές άδειας χρήσης για το λογισμικό που χρησιμοποιείται στον οργανισμό.

- *Διαδικασίες ανταπόκρισης σε παραβάσεις*: Καθιέρωση διαδικασιών για την αντιμετώπιση παραβιάσεων της πολιτικής ασφαλείας και των νόμων περί προστασίας δεδομένων και πνευματικής ιδιοκτησίας (Σταματινός, 2015).

Η κατάρτιση και ενημέρωση των χρηστών είναι ζωτικής σημασίας για την επιτυχή εφαρμογή των μέτρων ασφαλείας που προβλέπονται στην πολιτική ασφάλειας (Kamariotou and Kitsios, 2023). Μερικές από τις δράσεις που μπορούν να ληφθούν συμπεριλαμβάνουν:

- *Εκπαίδευση των χρηστών*: Προσφορά εκπαιδευτικών προγραμμάτων και σεμιναρίων για τους χρήστες προκειμένου να κατανοήσουν την πολιτική ασφαλείας και τα μέτρα που πρέπει να ακολουθούν.

- *Οδηγίες και εκπαιδευτικό υλικό*: Παροχή οδηγιών και εκπαιδευτικού υλικού σχετικά με τη σωστή χρήση των συνθηματικών, των δικαιωμάτων πρόσβασης και των μεθόδων προστασίας πληροφοριών.

- *Ενημερωτικά μηνύματα*: Αποστολή τακτικών ενημερωτικών μηνυμάτων στους χρήστες για την ανανέωση των συνθηματικών τους και την ανίχνευση απάτης.

- *Δημιουργία επίγειων διαδικτυακών πλατφορμών*: Δημιουργία διαδικτυακών πλατφορμών όπου οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε εκπαιδευτικό υλικό, ερωτήσεις και απαντήσεις, και να λάβουν υποστήριξη σχετικά με την ασφάλεια.

- *Διαχείριση πρόσβασης*: Εφαρμογή πολιτικών που καθορίζουν τους κανόνες πρόσβασης στο σύστημα και τις πληροφορίες, συμπεριλαμβανομένων των πολιτικών αλλαγής κωδικών και των μέτρων διαχείρισης των προσβάσεων (Σταματινός, 2015).

Η διαδικασία αντιμετώπισης και αναφοράς περιστατικών ασφάλειας είναι κρίσιμη για τη διατήρηση της ασφάλειας των ΠΣ ενός οργανισμού (Nord et al., 2020). Οι οδηγίες που καθορίζονται στην πολιτική ασφάλειας πρέπει να περιλαμβάνουν τα εξής:

- *Διαδικασία αντιμετώπισης περιστατικών*: Καθορισμός της διαδικασίας που πρέπει να ακολουθείται όταν ανιχνεύεται ή υποψιάζεται μια παραβίαση ασφαλείας. Αυτό περιλαμβάνει την ταχεία αντίδραση, την απομόνωση του προβλήματος και την επίλυσή του.

- *Κανάλι επικοινωνίας για αναφορά περιστατικών*: Καθορισμός του κατάλληλου καναλιού επικοινωνίας που πρέπει να χρησιμοποιούν οι χρήστες για να αναφέρουν περιστατικά ασφάλειας. Αυτό μπορεί να περιλαμβάνει ειδικούς λογαριασμούς email ή τηλεφωνικές γραμμές υποστήριξης.

- *Ανάλυση περιστατικών*: Καθορισμός των διαδικασιών για την ανάλυση και τον εντοπισμό των αιτιών περιστατικών ασφάλειας, προκειμένου να ληφθούν τα αναγκαία μέτρα πρόληψης στο μέλλον.

- *Αντιμετώπιση παραβιάσεων*: Καθορισμός των ενεργειών που πρέπει να ακολουθούνται σε περίπτωση παραβίασης της ασφάλειας, συμπεριλαμβανομένων των διαδικασιών ανάκτησης δεδομένων και της ανάκαμψης από το περιστατικό (Σταματινός, 2015).

Β) Φυσικά μέτρα προστασίας

Ένα παράδειγμα φυσικής οχύρωσης ενός οργανισμού μπορεί να είναι η δημιουργία ενός περιβάλλοντος που να περιλαμβάνει τα εξής:

- *Φράγματα και περιφράξεις*: Κατασκευή φραγμάτων, τειχών ή περιφράξεων γύρω από το κτίριο ή το χώρο της επιχείρησης για την προστασία του από την μη εξουσιοδοτημένη πρόσβαση.

- *Πύλες και κλειδαριές*: Χρήση ασφαλών πυλών και κλειδαριών για τον έλεγχο της πρόσβασης σε συγκεκριμένους χώρους του κτιρίου.

- *Συστήματα ανίχνευσης*: Τοποθέτηση αισθητήρων κίνησης και αισθητήρων παραβίασης για την ανίχνευση εισβολών ή ανεπιθύμητων προσπαθειών πρόσβασης.

- *Ασφαλής πρόσβαση*: Χρήση συστημάτων πρόσβασης όπως κάρτες πρόσβασης ή βιομετρικές ταυτοποιήσεις για την επιτροπή σε συγκεκριμένα άτομα.

- *Ελεγχόμενη πρόσβαση στους χώρους*: Καθορισμός περιοχών ελέγχου πρόσβασης, όπως χώροι υψηλής ευαισθησίας ή αποθήκες, με σκοπό την περαιτέρω περιορισμό της πρόσβασης μόνο σε εξουσιοδοτημένα άτομα (Σταματινός, 2015).

Αυτά τα μέτρα συμβάλλουν στην ενίσχυση της φυσικής ασφάλειας ενός οργανισμού και στη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης ή καταστροφής των αγαθών του ΠΣ (Khando et al., 2021). Η ύπαρξη πολλαπλών επιπέδων ασφάλειας αποτελεί σημαντική πρακτική για την προστασία των πληροφοριών και των πόρων ενός οργανισμού. Αυτό το μοντέλο προσφέρει πολλαπλά επίπεδα προστασίας, καθιστώντας δυσκολότερη την εισβολή ή την παράβαση ασφαλείας. Κάθε επίπεδο αντιπροσωπεύει ένα επιπλέον εμπόδιο για τον εισβολέα (Kamariotou and Kitsios, 2023). Μερικά παραδείγματα πολλαπλών επιπέδων ασφάλειας περιλαμβάνουν:

- *Φυσικά μέτρα ασφαλείας*: αφορά τη χρήση φραγμάτων, πυλών και κλειδαριών για την προστασία των φυσικών εγκαταστάσεων.

- *Τεχνικά μέτρα ασφαλείας*: περιλαμβάνουν τη χρήση συστημάτων ανίχνευσης, firewall, λογισμικών antivirus.

- *Οργανωτικά μέτρα ασφαλείας*: Συμπεριλαμβάνουν πολιτικές και διαδικασίες, όπως ο διαχωρισμός των καθηκόντων, ο καθορισμός των ευθυνών και η εκπαίδευση του προσωπικού (Σταματινός, 2015).

Με την πολυεπίπεδη προσέγγιση, ένας εισβολέας θα πρέπει να ξεπεράσει κάθε επίπεδο προστασίας για να προβεί σε παραβίαση. Αυτό καθιστά την εισβολή πολύ πιο δύσκολη και αυξάνει την πιθανότητα ανίχνευσης και αντίδρασης σε ενδεχόμενη απειλή (Khando et al., 2021). Επιπλέον, η πολυεπίπεδη ασφάλεια παρέχει επιπλέον ασφάλεια σε περίπτωση παραβίασης ή διακοπής κάποιου από τα επίπεδα. Με πολλαπλά επίπεδα ασφαλείας, ο εισβολέας πρέπει να ξεπεράσει κάθε επίπεδο για να προβεί σε παραβίαση. Αυτό καθιστά την εισβολή πιο δύσκολη και μειώνει την πιθανότητα επιτυχούς επίθεσης (Kamariotou and Kitsios, 2023).

- *Απορροφά την πίεση από τις απειλές*: Ένα μόνο επίπεδο ασφαλείας είναι ευάλωτο σε επιθέσεις. Η χρήση πολλαπλών επιπέδων ασφαλείας διασπά την πίεση από τις απειλές, καθιστώντας το σύστημα λιγότερο ευάλωτο.

- *Αποτρέπει το σημείο αποτυχίας*: Επειδή καθένα από τα επίπεδα έχει διαφορετικές μεθόδους ασφάλειας και προστασίας, η αποτυχία ενός επιπέδου δεν θα οδηγήσει απαραίτητα στην πλήρη ανακατάληψη του συστήματος (Σταματινός, 2015).

Η πολυεπίπεδη προσέγγιση είναι πολύ πιο ρεαλιστική και εφικτή, καθώς ανταποκρίνεται στην αναπόφευκτη ποικιλία των απειλών και των προκλήσεων που αντιμετωπίζει ένα σύγχρονο ΠΣ (Alkhazi et al., 2022).

Γ) Έλεγχος Πρόσβασης στα ΠΣ

Η εφαρμογή της αρχής "need to know" είναι ζωτικής σημασίας για την αποτελεσματική διαχείριση των δικαιωμάτων πρόσβασης σε ένα ΠΣ. Αυτή η αρχή διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο σε εκείνες τις πληροφορίες και εφαρμογές που είναι απαραίτητες για την εκτέλεση των καθηκόντων τους, μειώνοντας έτσι τον κίνδυνο αποκάλυψης ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένα άτομα (Σταματινός, 2015).

Η καθορισμός των ρόλων και των υπευθυνοτήτων των χρηστών είναι επίσης ουσιώδης για την αποτελεσματική διαχείριση της πρόσβασης. Καθορίζοντας σαφώς τους ρόλους κάθε χρήστη και τις σχετικές τους ευθύνες, μπορεί να εξασφαλιστεί ότι η πρόσβαση παρέχεται μόνο σε εκείνα τα δεδομένα και τις εφαρμογές που είναι σχετικές με την εκάστοτε θέση εργασίας. Αυτό επίσης συνεισφέρει στην ενίσχυση της ασφάλειας των ΠΣ, καθώς μειώνει τον κίνδυνο ανεπιθύμητης πρόσβασης ή κακόπιστων ενεργειών από τους χρήστες (Kamariotou and Kitsios, 2023).

Δ) Διαχείριση υλικού και λογισμικού

Η διαχείριση του υλικού και του λογισμικού αποτελεί κρίσιμο κομμάτι της πολιτικής ασφαλείας ενός οργανισμού. Οι χρήστες πρέπει να έχουν περιορισμένη πρόσβαση σε συσκευές και λογισμικό που δεν απαιτούν για την εκτέλεση των εργασιών τους. Ορισμένες από τις μεγαλύτερες απειλές ασφαλείας προέρχονται από ευπάθειες στο λογισμικό (Khando et al., 2021). Η τακτική εγκατάσταση ενημερώσεων και η διαρκής ενημέρωση για νέες απειλές είναι ουσιώδεις. Η εφαρμογή αυστηρών πολιτικών για τη δημιουργία και τη χρήση δυνατών και μοναδικών κωδικών πρόσβασης σε συσκευές και λογισμικό. Ακόμη, η εφαρμογή πολιτικών που περιορίζουν τη χρήση μη εγκεκριμένων εφαρμογών και λογισμικού. Η δημιουργία συστήματος παρακολούθησης για την

ανίχνευση ανεπιθύμητων δραστηριοτήτων ή απόπειρας παραβίασης. Η εφαρμογή μέτρων εξασφαλίζει την απομόνωση και την κρυπτογράφηση των ευαίσθητων δεδομένων (Kamariotou and Kitsios, 2023).

Ε) Προσαρμογή σε νομικές υποχρεώσεις

Η προσαρμογή σε νομικές υποχρεώσεις αποτελεί σημαντικό κομμάτι της πολιτικής ασφαλείας και περιλαμβάνει τις παρακάτω δράσεις:

- *Συμμόρφωση με Νομοθεσία*: Κατανόηση και τήρηση των νομικών απαιτήσεων που διέπουν την ασφάλεια των ΠΣ, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση.

- *Ανάπτυξη Πολιτικών*: Δημιουργία πολιτικών ασφαλείας που να συμμορφώνονται με τις νομικές υποχρεώσεις και να προστατεύουν τα δεδομένα των χρηστών και των πελατών.

- *Αναθεώρηση και Ενημέρωση*: Συνεχής αναθεώρηση και ενημέρωση της πολιτικής ασφαλείας για να αντικατοπτρίζει τις νέες νομοθετικές απαιτήσεις και αλλαγές στο περιβάλλον λειτουργίας.

- *Εκπαίδευση Προσωπικού*: Εκπαίδευση των εργαζομένων σχετικά με τις νομικές υποχρεώσεις και τις πρακτικές που πρέπει να ακολουθούν για να διασφαλίσουν τη συμμόρφωση.

- *Αναφορά και Παρακολούθηση*: Ανάπτυξη μηχανισμών για την αναφορά παραβιάσεων, καθώς και την παρακολούθηση της συμμόρφωσης και την αντιμετώπιση τυχόν παραβάσεων (Σταματινός, 2015).

ΣΤ) Τρόποι διαχείρισης Πολιτικής Ασφαλείας

Η διαχείριση μιας πολιτικής ασφαλείας περιλαμβάνει την εφαρμογή, την αξιολόγηση και την εξέλιξή της στον χρόνο (Manuscript, 2020). Οι βασικοί τρόποι διαχείρισης μιας πολιτικής ασφαλείας περιλαμβάνουν τα εξής:

- *Καθορισμός Πολιτικής*: Δημιουργία μιας συνολικής πολιτικής ασφαλείας που να καλύπτει τους στόχους, τις αρχές και τις διαδικασίες για την προστασία των ΠΣ και δεδομένων.

- *Εφαρμογή Πολιτικής*: Εφαρμογή της πολιτικής ασφαλείας σε όλα τα επίπεδα της επιχείρησης, από την ανώτερη διοίκηση μέχρι τους απλούς χρήστες.

- *Εκπαίδευση Προσωπικού*: Εκπαίδευση των εργαζομένων σχετικά με την πολιτική ασφαλείας, τις διαδικασίες και τις βέλτιστες πρακτικές που πρέπει να ακολουθούν.

- *Αξιολόγηση και Αναθεώρηση*: Αξιολόγηση της αποτελεσματικότητας της πολιτικής ασφαλείας και αναθεώρηση της όπου χρειάζεται για τη βελτίωσή της.

- *Αντιμετώπιση Παραβιάσεων*: Διαχείριση και αντιμετώπιση περιστατικών ασφαλείας που μπορεί να προκύψουν, συμπεριλαμβανομένης της ανάλυσης των αιτιών και των επιπτώσεων και της λήψης μέτρων για πρόληψη μελλοντικών παραβιάσεων.

- *Συμμόρφωση με Νομικές Υποχρεώσεις*: Παρακολούθηση και συμμόρφωση με τις νομικές υποχρεώσεις που διέπουν την προστασία των πληροφοριών και την ασφάλεια των ΠΣ (Σταματινός, 2015).

Η διαχείριση μιας πολιτικής ασφαλείας απαιτεί συνεχή προσοχή και επιδίωξη βελτίωσης για να διασφαλιστεί η προστασία των πληροφοριών και η αντιμετώπιση των απειλών ασφαλείας (Alkhazi et al., 2022).

Ζ) Οργανωτική δομή

Η οργανωτική δομή ενός οργανισμού παίζει κρίσιμο ρόλο στην αποτελεσματική εφαρμογή μιας πολιτικής ασφαλείας. Η δομή αυτή καθορίζει ποιος είναι υπεύθυνος για την υλοποίηση, την επιτήρηση και τη συμμόρφωση με τις αρχές της πολιτικής ασφαλείας σε όλα τα επίπεδα της επιχείρησης (Kamariotou and Kitsios, 2023). Ορισμένες βασικές αρχές οργανωτικής δομής για την υποστήριξη της πολιτικής ασφαλείας περιλαμβάνουν:

- *Διοικητική Υποστήριξη*: Υπάρχει ανώτερη διοικητική υποστήριξη για την ανάπτυξη, εφαρμογή και συντήρηση της πολιτικής ασφαλείας.

- *Οργανωτική Δομή*: Υπάρχει σαφής καθορισμός των ρόλων, των ευθυνών και των αρμοδιοτήτων για την ασφάλεια των ΠΣ, συμπεριλαμβανομένων των ανώτερων διοικητικών επιπέδων, των διαχειριστών ασφαλείας και των απλών χρηστών.

- *Εκπαίδευση και Ευαισθητοποίηση*: Υπάρχει διαρκής εκπαίδευση και ευαισθητοποίηση του προσωπικού για θέματα ασφαλείας και την πολιτική ασφαλείας της επιχείρησης.

- *Ομάδα Ασφάλειας Πληροφοριών*: Συχνά, υπάρχει μια ειδική ομάδα ασφάλειας πληροφοριών που είναι υπεύθυνη για την εφαρμογή και τη συντήρηση της πολιτικής ασφαλείας.

- *Προνομιούχοι Χρήστες*: Υπάρχουν προνομιούχοι χρήστες που έχουν ειδικά δικαιώματα πρόσβασης και ευθύνες για την ασφάλεια των πληροφοριών.

- *Διαχείριση Κινδύνων*: Υπάρχει διαδικασία διαχείρισης κινδύνων που περιλαμβάνει τον προσδιορισμό, την αξιολόγηση και τη μείωση των κινδύνων ασφάλειας (Σταματινός, 2015).

Μια καλά δομημένη οργανωτική δομή είναι ουσιαστική για την αποτελεσματική εφαρμογή μιας πολιτικής ασφαλείας και την προστασία των πληροφοριών της επιχείρησης (Manuscript, 2020).

2.3 Μέθοδος υλοποίησης πολιτικών ασφαλείας ΠΣ

Η διαμόρφωση μιας ολοκληρωμένης πολιτικής ασφαλείας και η υλοποίηση ενός ολοκληρωμένου συστήματος ασφάλειας πληροφοριών προϋποθέτει την εκτέλεση πολλών βημάτων. Ανάλογα με τις ανάγκες και τα χαρακτηριστικά της επιχείρησης, τα βήματα αυτά μπορεί να παρουσιάζουν μικρές διαφοροποιήσεις (Σταματινός, 2015), αλλά συνήθως περιλαμβάνουν τα ακόλουθα:

1. **Ανάλυση Κινδύνων**: Η ανάλυση κινδύνων αποτελεί ένα κρίσιμο βήμα στην ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας. Κατά τη διαδικασία αυτή, οι οργανισμοί αναγνωρίζουν και αξιολογούν τους πιθανούς κινδύνους που μπορεί να αντιμετωπίσουν σχετικά με την ασφάλεια των πληροφοριών και των συστημάτων τους (Manuscript, 2020). Αυτό περιλαμβάνει τα εξής βήματα:

    - *Αναγνώριση Κινδύνων*: Καταγραφή των δυνητικών κινδύνων που μπορεί να απειλήσουν την ασφάλεια των πληροφοριών, όπως

κυβερνοεπιθέσεις, εσωτερικές απειλές, φυσικές απειλές, ανθρώπινο λάθος κλπ.

- *Αξιολόγηση Κινδύνων*: Αξιολόγηση της πιθανότητας εμφάνισης κάθε κινδύνου και του πιθανού αντίκτυπου του στον οργανισμό. Αυτή η αξιολόγηση βασίζεται σε παράγοντες όπως η πιθανότητα επίθεσης, η ευπάθεια του συστήματος, η αξία των πληροφοριών κλπ.

- *Καταγραφή Ευαίσθητων Περιοχών*: Αναγνώριση των ευαίσθητων περιοχών όπου οι κίνδυνοι μπορεί να είναι πιο υψηλοί ή οι επιπτώσεις πιο σοβαρές, όπως οι βάσεις δεδομένων, οι δικτυακοί κόμβοι, οι ευαίσθητες πληροφορίες κλπ.

- *Ανάπτυξη Πλάνου Διαχείρισης Κινδύνων*: Δημιουργία ενός σχεδίου δράσης για τη διαχείριση και τη μείωση των αναγνωρισμένων κινδύνων. Αυτό μπορεί να περιλαμβάνει την υιοθέτηση τεχνικών ασφαλείας, την εκπαίδευση του προσωπικού, την επιβολή πολιτικών και διαδικασιών ασφαλείας κλπ. (Σταματινός, 2015).

Η ανάλυση κινδύνων αποτελεί κρίσιμο στάδιο για την κατανόηση των απειλών και τη λήψη των κατάλληλων μέτρων για την προστασία των πληροφοριών και των συστημάτων ενός οργανισμού (Manuscript, 2020).

2. **Καθορισμός Πολιτικής Ασφαλείας**: Διαμόρφωση ενός συνόλου αρχών, κανόνων και διαδικασιών που θα καθοδηγούν την ασφάλεια των πληροφοριών. Ο καθορισμός μιας πολιτικής ασφαλείας αποτελεί βασικό βήμα για τη δημιουργία ενός πλαισίου που θα διασφαλίζει την προστασία των πληροφοριών. Αυτό περιλαμβάνει τη διαμόρφωση ενός συνόλου αρχών, κανόνων και διαδικασιών που θα καθοδηγούν τη συνολική προσέγγιση της ασφάλειας των πληροφοριών εντός της επιχείρησης (Kamariotou and Kitsios, 2023). Αυτό μπορεί να περιλαμβάνει τα παρακάτω:

    - *Ανάλυση Αναγκών*: Πριν από τη διαμόρφωση της πολιτικής ασφαλείας, πρέπει να γίνει μια λεπτομερής ανάλυση των αναγκών της επιχείρησης σε ό, τι αφορά την ασφάλεια των πληροφοριών.

- *Καθορισμός Αρχών*: Ορισμός των βασικών αρχών που θα καθοδηγούν την ασφάλεια των πληροφοριών, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

- *Καθορισμός Πολιτικών και Κανόνων*: Διατύπωση συγκεκριμένων πολιτικών και κανόνων που θα προσδιορίζουν τις απαιτήσεις ασφάλειας που πρέπει να τηρούνται από τους εργαζόμενους και τους χρήστες των ΠΣ.

- *Καθορισμός Διαδικασιών*: Καθορισμός των διαδικασιών που πρέπει να ακολουθούνται για την εφαρμογή των πολιτικών και των κανόνων ασφαλείας, καθώς και για τη διαχείριση τυχόν παραβάσεων ασφαλείας.

- *Εκπαίδευση Προσωπικού*: Εκπαίδευση του προσωπικού σχετικά με τις πολιτικές και τις διαδικασίες ασφαλείας και ευαισθητοποίησή τους σχετικά με τους κινδύνους που ενέχονται στην ασφάλεια των πληροφοριών (Σταματινός, 2015).

Με την οριοθέτηση της πολιτικής ασφαλείας, οι οργανισμοί μπορούν να διασφαλίσουν ότι οι αρχές και οι πρακτικές που σχετίζονται με την ασφάλεια των πληροφοριών είναι σαφείς και ότι οι χρήστες των ΠΣ είναι ενημερωμένοι και συμμορφώνονται με αυτές (Alkhazi et al., 2022).

3. **Εκπαίδευση Προσωπικού**: Εκπαίδευση των εργαζομένων σχετικά με τις αρχές και τις διαδικασίες ασφαλείας. Η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών (Manuscript, 2020). Ακολουθούν μερικά σημαντικά στοιχεία που πρέπει να περιλαμβάνει η εκπαίδευση του προσωπικού:

    - *Ανάλυση των Κινδύνων*: Εκπαίδευση των εργαζομένων σχετικά με τους πιθανούς κινδύνους ασφάλειας που μπορεί να αντιμετωπίσει ο οργανισμός, καθώς και τους τρόπους αναγνώρισής τους.

    - *Κανονισμοί και Πολιτικές*: Εξοικείωση του προσωπικού με τους κανονισμούς και τις πολιτικές ασφαλείας που ισχύουν στον οργανισμό και την ανάγκη συμμόρφωσής τους.

- *Πρακτικές Ασφαλείας*: Εκπαίδευση σχετικά με τις βέλτιστες πρακτικές ασφαλείας, συμπεριλαμβανομένων των διαδικασιών πρόληψης των κινδύνων, των μεθόδων προστασίας των δεδομένων και των διαδικασιών αντιμετώπισης περιστατικών ασφαλείας.

- *Ευαισθητοποίηση*: Διαμόρφωση ενός πνεύματος ευαισθητοποίησης στην ασφάλεια πληροφοριών, προβολή παραδειγμάτων και κατανόησης των συνεπειών που μπορεί να έχει η ανεύρεση ασφαλούς πληροφορίας.

- *Ενίσχυση Συνειδητοποίησης*: Προαγωγή μιας συνειδητοποιημένης στάσης έναντι της ασφάλειας πληροφοριών, με έμφαση στην ατομική ευθύνη για την προστασία των δεδομένων και των πληροφοριών της επιχείρησης (Σταματινός, 2015).

Η εκπαίδευση του προσωπικού είναι συνεχής και ανανεώνεται τακτικά για να ανταποκρίνεται στις αλλαγές στο πεδίο της ασφάλειας πληροφοριών και στις νέες απειλές που εμφανίζονται (Alkhazi et al., 2022).

4. **Υλοποίηση Τεχνικών Μέτρων**: Εφαρμογή τεχνικών μέτρων ασφάλειας, όπως firewalls, antivirus λογισμικό, κρυπτογράφηση, κ.λπ.. Η υλοποίηση τεχνικών μέτρων ασφάλειας αποτελεί κρίσιμο στάδιο στην προστασία των πληροφοριών μίας επιχείρησης (Manuscript, 2020). Αυτά τα μέτρα συχνά περιλαμβάνουν:

    - *Firewalls*: Τα firewalls αποτελούν την πρώτη γραμμή άμυνας ενός δικτύου, εμποδίζοντας την μη εξουσιοδοτημένη πρόσβαση από δίκτυα εκτός της επιχείρησης.

    - *Antivirus Λογισμικό*: Το antivirus λογισμικό ανιχνεύει, μπλοκάρει και αφαιρεί κακόβουλο λογισμικό που μπορεί να απειλήσει την ασφάλεια των συστημάτων.

    - *Κρυπτογράφηση*: Η κρυπτογράφηση χρησιμοποιείται για την ασφαλή μεταφορά δεδομένων μέσω δικτύων, καθώς και για την αποθήκευση δεδομένων σε ασφαλή μορφή.

- *Διαχείριση Ταυτότητας και Πρόσβασης*: Τα συστήματα διαχείρισης ταυτότητας και πρόσβασης ελέγχουν την πρόσβαση των χρηστών σε διάφορα επίπεδα των πληροφοριών ανάλογα με τις ανάγκες και τις αρμοδιότητές τους.

- *Ενημερώσεις*: Η εγκατάσταση των τελευταίων ενημερώσεων λογισμικού και παρακολούθηση των ανακοινώσεων ασφαλείας βοηθούν στη διατήρηση των συστημάτων ενημερωμένα και προστατευμένα από ευπάθειες.

- *Εφαρμογή Πολιτικών Ασφαλείας*: Η υλοποίηση πολιτικών ασφαλείας, όπως περιορισμοί πρόσβασης, πολιτικές κωδικών πρόσβασης και περιορισμοί αποθήκευσης δεδομένων, συμβάλλει στην προστασία των πληροφοριών (Σταματινός, 2015).

Οι παραπάνω τεχνικές λύσεις συνήθως εφαρμόζονται σε συνδυασμό μεταξύ τους για να δημιουργήσουν ένα ολοκληρωμένο σύστημα ασφαλείας πληροφοριών (Kamariotou and Kitsios, 2023).

5. **Δημιουργία Διαδικασιών και Πολιτικών**: Ανάπτυξη διαδικασιών για την αντιμετώπιση περιστατικών ασφαλείας και την τήρηση των πολιτικών. Η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών (Kamariza, 2017). Αυτό περιλαμβάνει:

    - *Καθορισμός Διαδικασιών Αντιμετώπισης Περιστατικών*: Δημιουργία διαδικασιών για την άμεση αντίδραση σε περιστατικά ασφαλείας, όπως παραβιάσεις δεδομένων, εισβολές στο δίκτυο, ή άλλες απειλές.

    - *Καθορισμός Πολιτικών Ασφαλείας*: Δημιουργία πολιτικών που καθορίζουν τους κανόνες και τις αρχές για την προστασία των πληροφοριών, συμπεριλαμβανομένων των πολιτικών πρόσβασης, αποθήκευσης και κοινής χρήσης δεδομένων.

    - *Εκπαίδευση και Ευαισθητοποίηση*: Διεξαγωγή εκπαίδευσης και ευαισθητοποίησης του προσωπικού σχετικά με τις πολιτικές και τις διαδικασίες ασφαλείας, καθώς και τις συνέπειες των παραβιάσεων ασφαλείας.

- *Πειθαρχικά Μέτρα*: Καθορισμός των πειθαρχικών μέτρων που θα λαμβάνονται σε περίπτωση παραβίασης των πολιτικών ασφαλείας, συμπεριλαμβανομένων των πιθανών κυρώσεων (Σταματινός, 2015).

Η δημιουργία αυτών των διαδικασιών και πολιτικών βοηθάει στη διασφάλιση ότι οι απειλές ασφαλείας αντιμετωπίζονται με συνέπεια και αποτελεσματικότητα, ενώ επίσης προετοιμάζει το προσωπικό για την αντίδραση σε περιστατικά ασφαλείας με αποτελεσματικό τρόπο (Alkhazi et al., 2022).

6. **Παρακολούθηση και Αξιολόγηση**: Συνεχής παρακολούθηση και αξιολόγηση της αποτελεσματικότητας των μέτρων ασφαλείας. Η παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας αποτελεί κρίσιμο στάδιο για τη διασφάλιση της συνεχούς προστασίας των πληροφοριών και των ΠΣ (Kamariza, 2017). Αυτό περιλαμβάνει:

    - *Παρακολούθηση Συστήματος*: Συνεχής παρακολούθηση των ΠΣ για ανίχνευση ανωμαλιών ή ενδεχόμενων επιθέσεων.

    - *Αξιολόγηση Αποτελεσματικότητας*: Ανάλυση των δεδομένων παρακολούθησης για να αξιολογηθεί η αποτελεσματικότητα των μέτρων ασφαλείας.

    - *Ενημέρωση Πολιτικών*: Εφαρμογή αλλαγών στις πολιτικές και τις διαδικασίες ασφαλείας βάσει των αξιολογήσεων για να βελτιωθεί η ασφάλεια των πληροφοριών.

    - *Εκπαίδευση Προσωπικού*: Εκπαίδευση του προσωπικού σχετικά με τις νέες απειλές και τις αντίστοιχες αλλαγές στις πολιτικές και διαδικασίες ασφαλείας.

    - *Αναθεώρηση Συστήματος*: Αναθεώρηση του συστήματος ασφαλείας και των μέτρων ασφαλείας για να διασφαλιστεί η συνεχής προσαρμογή στις νέες απειλές και τις ανάγκες της επιχείρησης (Σταματινός, 2015).

Η παρακολούθηση και η αξιολόγηση είναι διαδικασίες που επαναλαμβάνονται συνεχώς, προκειμένου να διασφαλιστεί η συνεχής προστασία των πληροφοριών και η αντιμετώπιση των αναδυόμενων απειλών (Pakusadewa et al., 2020).

7. **Προσαρμογή και Βελτίωση**: Προσαρμογή της πολιτικής ασφαλείας και των μέτρων σύμφωνα με τις ανάγκες και τις εξελίξεις στον τομέα της ασφάλειας. Η προσαρμογή και η συνεχή βελτίωση της πολιτικής ασφαλείας και των μέτρων

αποτελεί κρίσιμη διαδικασία για τη διασφάλιση της αποτελεσματικότητας και της ανταπόκρισης τους σε συνεχώς μεταβαλλόμενες απειλές και ανάγκες (Alkhazi et al., 2022). Αυτό περιλαμβάνει τα ακόλουθα:

- *Ανάλυση Κινδύνων και Επίδοσης*: Συνεχής αξιολόγηση του περιβάλλοντος ασφαλείας για την αναγνώριση νέων απειλών και ευκαιριών.
- *Επιθεώρηση της Υφιστάμενης Πολιτικής*: Αξιολόγηση της αποτελεσματικότητας της υφιστάμενης πολιτικής ασφαλείας και των μέτρων ασφαλείας.
- *Αναθεώρηση και Ενημέρωση*: Αναθεώρηση και ενημέρωση της πολιτικής και των μέτρων ασφαλείας για να αντικατοπτρίζουν τις νέες ανάγκες και εξελίξεις.
- *Εκπαίδευση Προσωπικού*: Εκπαίδευση του προσωπικού για τις νέες απειλές και τις αναβαθμισμένες διαδικασίες ασφαλείας.
- *Δοκιμές και Εξασκήσεις*: Εκτέλεση δοκιμών και εξάσκηση σε σενάρια απειλών για να ελεγχθεί η αποτελεσματικότητα των μέτρων και να εκπαιδευτεί το προσωπικό.
- *Συνεχής Βελτίωση*: Εφαρμογή συστηματικών διαδικασιών βελτίωσης, όπως η PDCA (Plan-Do-Check-Act), για τη διαρκή βελτίωση της πολιτικής ασφαλείας και των μέτρων ασφαλείας (Σταματινός, 2015).

Αυτά τα βήματα συνήθως αποτελούν το πλαίσιο για την ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας και την εγκατάσταση ενός ολοκληρωμένου συστήματος ασφάλειας πληροφοριών σε έναν οργανισμό (Kamariotou and Kitsios, 2023).

3. Μεθοδολογία έρευνας

3.1 Μέθοδος συλλογής στοιχείων

Η πραγματοποίηση της παρούσας μελέτης αναδεικνύει πολλά στοιχεία και πληροφορίες που σχετίζονται με τα ΠΣ και τις πολιτικές ασφάλειας τους. Ωστόσο, παρατηρείται ότι δεν υπάρχουν διαθέσιμες πληροφορίες που να αναδεικνύουν τον βαθμό στον οποίο χρησιμοποιούνται οι πολιτικές αυτές σε επίπεδο ελληνικών επιχειρήσεων. Έτσι, για να μπορέσει να διαμορφωθεί ένα πιο εξειδικευμένο αποτέλεσμα και συμπέρασμα που θα περιλαμβάνει πρωτογενή στοιχεία, κρίθηκε αναγκαία η διεξαγωγή μίας νέας έρευνας σε εγχώριο επίπεδο. Ακόμη, παρατηρήθηκε ότι δεν υπάρχουν πολλές ποσοτικές έρευνες που να εξετάζουν με τη χρήση ερωτηματολογίου τον βαθμό συμβολής των πολιτικών ασφαλείας στις ελληνικές επιχειρήσεις. Έτσι, κρίθηκε σημαντικό να διενεργηθεί μία νέα ποσοτική έρευνα για την χρήση των ΠΣ και την εφαρμογή των πολιτικών ασφάλειας στις ελληνικές επιχειρήσεις και τον ρόλο που διαδραματίζουν στην εύρυθμη δραστηριοποίηση τους.

Αναλυτικότερα, παρακάτω διενεργείται μία πρωτογενής ποσοτική έρευνα, η οποία εστιάζει στο να αναδείξει το βαθμό στον οποίο οι ελληνικές επιχειρήσεις έχουν δείξει ενδιαφέρον για τα ΠΣ και τις πολιτικές ασφάλειας τους. Η επιλογή διεξαγωγής της έρευνας αυτής έγκειται στην επιθυμία λήψης δεδομένων και πληροφοριών που έχουν άμεση σχέση με την σημαντικότητα και τον σκοπό των πολιτικών ασφαλείας των ΠΣ που εφαρμόζονται από τις ελληνικές επιχειρήσεις. Στην ουσία πρόκειται για μία έρευνα που βασίζεται στην άντληση στοιχείων μέσα από την χρησιμοποίηση ενός συγκεκριμένου ερευνητικού εργαλείου που είναι το ερωτηματολόγιο. Η έρευνα αυτή απευθύνθηκε προς ένα δείγμα υπευθύνων ελληνικών επιχειρήσεων που δραστηριοποιούνται στον τομέα των υλικών οικοδομής, των τροφίμων και ποτών και των ενδυμάτων.

Η πρωτογενής ποσοτική έρευνα είναι μια μέθοδος επιστημονικής έρευνας που χρησιμοποιείται για τη συγκέντρωση και την ανάλυση ποσοτικών δεδομένων. Σε αντίθεση με την ποιοτική έρευνα που επικεντρώνεται σε παρατηρήσεις, συνεντεύξεις και άλλες μη ποσοτικές μεθόδους, η πρωτογενής ποσοτική έρευνα επικεντρώνεται στη συλλογή αριθμητικών δεδομένων που μπορούν να αναλυθούν με στατιστικές μεθόδους. Οι μέθοδοι πρωτογενούς ποσοτικής έρευνας συχνά περιλαμβάνουν τη δημοσίευση

ερωτηματολογίων, την παρατήρηση συμπεριφοράς ή τη συλλογή δεδομένων μέσω δοκιμών ή πειραμάτων. Η πρωτογενής ποσοτική έρευνα είναι συχνά χρήσιμη για την εξαγωγή στατιστικά αντιπροσωπευτικών συμπερασμάτων από μεγάλα δείγματα και για την εξέταση συσχετίσεων μεταξύ μεταβλητών.

Ο όρος πρωτογενής έρευνα βασίζεται στο γεγονός ότι τα αποτελέσματα που προκύπτουν είναι νέα και δεν προέρχονται από καμία άλλη έρευνα που να σχετίζεται με την συμβολή των πολιτικών ασφάλειας στις ελληνικές επιχειρήσεις. Επιπρόσθετα, χαρακτηρίζεται ποσοτική για το λόγο ότι σημειώνονται οι εκτιμήσεις ενός δείγματος υπευθύνων ελληνικών επιχειρήσεων, οι οποίοι προσδίδουν τον βαθμό στον οποίο είναι σημαντική η εφαρμογή πολιτικών ασφαλείας στην διασφάλιση των πληροφοριών τους.

Ένα από τα κύρια γνωρίσματα της πρωτογενούς ποσοτικής έρευνας που πραγματοποιήθηκε ήταν η διαδικασία οργάνωση της. Συγκεκριμένα, η οργάνωση μιας πρωτογενούς ποσοτικής έρευνας περιλαμβάνει διάφορα βήματα και διαδικασίες που πρέπει να ακολουθηθούν για να διασφαλιστεί η ακρίβεια και η αξιοπιστία των αποτελεσμάτων. Παρακάτω αναφέρονται τα βασικά βήματα για την οργάνωση μιας πρωτογενούς ποσοτικής έρευνας:

- *Καθορισμός του ερευνητικού προβλήματος*: Πρώτο βήμα ήταν ο καθορισμός του αντικειμένου της έρευνας, του στόχου της και των ερωτημάτων που πρέπει να απαντηθούν. Κατά τον καθορισμό αυτών των στοιχείων, υπήρχε σαφής κατανόηση του θέματος που επρόκειτο να ερευνηθεί, αλλά και του στόχου της έρευνας. Επιπλέον, στο πλαίσιο της οργάνωσης της έρευνας διατυπώθηκαν τα κύρια ερευνητικά ερωτήματα που θα οδηγήσουν στην απόκτηση απαντήσεων που θα επιτρέψουν την επίτευξη του στόχου αυτού. Αυτά τα ερωτήματα αναφέρονται στην χρήση και στα οφέλη των ΠΣ, αλλά και στη σημαντικότητα και στην εφαρμογή των πολιτικών ασφάλειας των ΠΣ.
- *Σχεδιασμός της μεθόδου*: Ακολούθησε ο καθορισμός της συγκεκριμένης μεθόδου που θα χρησιμοποιηθεί για τη συλλογή δεδομένων, η επιλογή του δείγματος και ο καθορισμό των μεταβλητών που θα μελετηθούν. Συγκεκριμένα, επιλέχθηκε η πρωτογενής ποσοτική έρευνα μέσω ερωτηματολογίου και προσδιορίστηκε το δείγμα, που αφορά υπεύθυνους ελληνικών επιχειρήσεων. Έπειτα, καθορίστηκαν οι μεταβλητές που κρίθηκε αναγκαίο να μελετηθούν, όπως ο βαθμός χρήσης και οφέλους των

ΠΣ για τις ελληνικές επιχειρήσεις και ο βαθμός συμβολής των πολιτικών ασφάλειας στην διατήρηση τους.

- *Συλλογή δεδομένων*: Σε αυτό το στάδιο επιτεύχθηκε η πραγματοποίηση της έρευνας με την εφαρμογή της επιλεγμένης μεθόδου στο επιλεγμένο δείγμα. Το ερευνητικό εργαλείο - ερωτηματολόγιο διανεμήθηκε στο δείγμα υπεύθυνων ελληνικών επιχειρήσεων δια ζώσης την περίοδο 8 έως 15 Φεβρουαρίου.
- *Ανάλυση δεδομένων*: Τα δεδομένα που συλλέχθηκαν αναλύθηκαν με στατιστικές τεχνικές και εργαλεία για να απαντηθούν τα ερωτήματα της έρευνας. Συγκεκριμένα, χρησιμοποιήθηκαν στατιστικά εργαλεία και εξήχθησαν πίνακες και διαγράμματα.
- *Ερμηνεία και σύνταξη αναφοράς*: Τα αποτελέσματα αναλύθηκαν και ερμηνεύτηκαν κατάλληλα με τη συμβολή πινάκων και διαγραμμάτων.
- *Σύνταξη συμπερασμάτων*: Τέλος, συντάχθηκαν τα συμπεράσματα της έρευνας, βασισμένα στα αποτελέσματα και την ερμηνεία τους.

Κάθε ένα από αυτά τα βήματα απαιτεί προσεκτική σχεδίαση και εκτέλεση για να διασφαλιστεί η ακρίβεια και η αξιοπιστία των αποτελεσμάτων.

3.2 Σκοπός – ερευνητικά ερωτήματα

Ο σκοπός της παρούσας έρευνας πηγάζει μέσα από την επιθυμία διερεύνησης του βαθμού χρήσης και οφέλους των ΠΣ για την δραστηριοποίηση των ελληνικών επιχειρήσεων και του βαθμού εφαρμογής και συμβολής των πολιτικών ασφαλείας των ΠΣ. Είναι μία έρευνα που αποσκοπεί στο να προσδιορίσει μέσα από την οπτική σκοπιά των υπευθύνων των ελληνικών επιχειρήσεων κατά πόσο χρησιμοποιούν τα ΠΣ, τους λόγους που έχουν στραφεί στη χρήση τους και τα πλεονεκτήματα που λαμβάνουν κατά τη χρήση τους. Ακόμη, μέσα από την έρευνα αυτή σκοπός είναι να καταγραφούν οι απόψεις του δείγματος για τη σημαντικότητα και την εφαρμογή των πολιτικών ασφάλειας στα ΠΣ των ελληνικών επιχειρήσεων.

Όλα τα παραπάνω εξετάζονται με γνώμονα τα παρακάτω ερευνητικά ερωτήματα:

α) Χρησιμοποιούν οι ελληνικές επιχειρήσεις τα ΠΣ;

β) Ποια είναι τα οφέλη που αποκομίζουν οι ελληνικές επιχειρήσεις από την χρήση των ΠΣ;

γ) Ποιος ο βαθμός συμβολής των πολιτικών ασφάλειας στην διατήρηση των ΠΣ;

δ) Ποιος είναι ο βαθμός χρήσης και εφαρμογής των πολιτικών ασφάλειας από τις ελληνικές επιχειρήσεις για την διατήρηση των ΠΣ;

Οι απαντήσεις των ανωτέρω ερωτημάτων δίνονται μέσα από την στατιστική επεξεργασία των δεδομένων της πρωτογενούς ποσοτικής έρευνας.

3.3 Δειγματοληψία

Η δειγματοληψία είναι ένα σημαντικό βήμα στην οργάνωση μιας πρωτογενούς ποσοτικής έρευνας και αφορά την επιλογή ενός υποσυνόλου του συνολικού πληθυσμού που θα μελετηθεί. Η διαδικασία αυτή πρέπει να γίνει με προσοχή και να λαμβάνει υπόψη διάφορους παράγοντες για να διασφαλιστεί η αντιπροσωπευτικότητα και η αξιοπιστία των αποτελεσμάτων. Στην παρούσα πρωτογενή ποσοτική έρευνα χρησιμοποιήθηκε η συστηματική δειγματοληψία, για το λόγο ότι επιλέχθηκε αρχικά ένας αριθμός αρχικών μελών του πληθυσμού τυχαία και στη συνέχεια οι υπόλοιποι με γνώμονα το γεγονός ότι είναι υπεύθυνοι ελληνικών επιχειρήσεων που ανήκουν στον τομέα υλικών οικοδομής, τροφίμων και ποτών και ενδυμάτων. Συνολικά, προσεγγίστηκαν 42 επιχειρήσεις σε διάφορα μέρη της Ελλάδας, με αποτέλεσμα το δείγμα να αντιστοιχεί σε 42 υπεύθυνους των εν λόγω επιχειρήσεων. Επιπλέον, η προσέγγιση του δείγματος έγινε δια ζώσης στις εξεταζόμενες επιχειρήσεις.

3.4 Εργαλείο έρευνας

Το εργαλείο της έρευνας είναι το ερωτηματολόγιο, το οποίο είναι ένα από τα πιο δημοφιλή εργαλεία που χρησιμοποιούνται στην έρευνα, ιδίως στον τομέα της

πρωτογενούς ποσοτικής έρευνας. Αποτελεί ένα σύνολο ερωτήσεων που προβάλλονται σε ένα δείγμα ανθρώπων με σκοπό να συλλέξουν πληροφορίες σχετικά με τις απόψεις, τις προτιμήσεις, τις συμπεριφορές ή άλλες μεταβλητές που ενδιαφέρουν τον ερευνητή. Τα ερωτηματολόγια μπορούν να διανεμηθούν σε μεγάλα δείγματα ανθρώπων, επιτρέποντας έτσι τη συλλογή δεδομένων από ευρύ φάσμα ατόμων και περιοχών. Οι συμμετέχοντες μπορούν να δώσουν απαντήσεις με ανωνυμία, πράγμα που μπορεί να τους κάνει πιο πιθανούς να είναι ειλικρινείς και ανοιχτοί στις απαντήσεις τους. Η συγκέντρωση δεδομένων από ερωτηματολόγια μπορεί να είναι γρήγορη και σχετικά οικονομική σε σύγκριση με άλλες μεθόδους. Η ανάλυση των δεδομένων από ερωτηματολόγια μπορεί να γίνει αυτοματοποιημένα, με τη χρήση στατιστικών προγραμμάτων, καθιστώντας τη διαδικασία πιο αποτελεσματική.

Στην προκειμένη περίπτωση, το ερωτηματολόγιο χρησιμοποιήθηκε για να εξυπηρετήσει τις ανάγκες εξέτασης του βαθμού χρήσης και οφέλους των ΠΣ και του βαθμού συμβολής και εφαρμογής των πολιτικών ασφαλείας στα ΠΣ. Απευθύνθηκε σε ένα δείγμα υπευθύνων ελληνικών επιχειρήσεων που φέρουν ένα συγκεκριμένο δημογραφικό προφίλ, το οποίο διαμορφώνεται από το φύλο, την ηλικία, την οικογενειακή κατάσταση, την εμπειρία και νομική μορφή της επιχείρησης, αριθμό εργαζομένων και τομέα δραστηριοποίησης.

Επιπρόσθετα, το ερωτηματολόγιο περικλείει ερωτήσεις που έχουν άμεση σχέση με τα ερευνητικά ερωτήματα της πρωτογενούς ποσοτικής έρευνας, τα οποία έχουν ως εξής:

- Εξέταση ως προς τον βαθμό χρήσης των ΠΣ από τις ελληνικές επιχειρήσεις.
- Διερεύνηση των πλεονεκτημάτων που αποκομίζουν οι ελληνικές επιχειρήσεις από τη χρήση των ΠΣ.
- Προσδιορισμός του βαθμού συμβολής των πολιτικών ασφάλειας στα ΠΣ των ελληνικών επιχειρήσεων.
- Καταγραφή του βαθμού εφαρμογής των πολιτικών ασφάλειας στα ΠΣ των ελληνικών επιχειρήσεων.

Οι απαντήσεις στα ερευνητικά ερωτήματα δίνονται μέσα από την κλίμακα διαβάθμισης, κατά την οποία η επιλογή 1-5 αντιστοιχεί στο είτε στη μορφή «Καθόλου» και στο «Πάρα πολύ». Τα ερωτηματολόγια διανεμήθηκαν εντός των ελληνικών επιχειρήσεων από τις 8 έως τις 15 Φεβρουαρίου.

Η καταχώριση των αποτελεσμάτων πραγματοποιήθηκε αφότου διενεργήθηκε αρχικά μία πολιτική έρευνα σε ένα σύνολο 5 υπευθύνων, προκειμένου να εξεταστεί η αξιοπιστία του.

3.5 Διαχείριση στοιχείων

Η διαχείριση των στοιχείων έγινε μετά την συλλογή και την καταχώριση τους στο στατιστικό πρόγραμμα SPSS. Ακολούθησε η διαδικασία της κωδικοποίησης των δεδομένων και της εξαγωγής πινάκων και διαγραμμάτων, ανάλογα με αυτό που κρίθηκε να εξεταστεί. Τα αποτελέσματα των δημογραφικών στοιχείων δίνονται μέσα από πίνακες συχνοτήτων, ενώ παράλληλα παρατίθενται κυκλικές απεικονίσεις. Ακολουθεί η παρουσίαση των αποτελεσμάτων με ραβδογράμματα, ιστογράμματα και πίνακες συσχετίσεων μεταξύ των μεταβλητών και των δημογραφικών στοιχείων.

4. Αποτελέσματα

4.1 Στατιστική ανάλυση

4.1.1 Έλεγχος αξιοπιστίας

Σε αυτό το σημείο πραγματοποιείται ο έλεγχος αξιοπιστίας του ερωτηματολογίου με σκοπό να αποσαφηνιστεί ο βαθμός στον οποίο τα ερωτήματα του ερωτηματολογίου φέρουν υψηλή συνοχή ή συσχετίζονται μεταξύ τους. Γι' αυτό επιτεύχθηκε ο έλεγχος αξιοπιστίας α του Cronbach.

Πίνακας 1: Δείκτης α του Cronbach για τα ερωτήματα του ερωτηματολογίου

Reliability Statistics

Cronbach's Alpha	N of Items
,865	48

Όσον αφορά την τιμή του δείκτη α του Cronbach για τα ερωτήματα του ερωτηματολογίου αντιστοιχεί στο 0,865 γεγονός που σημαίνει ότι παρουσιάζει υψηλή συνοχή και κατ' επέκταση αξιοπιστία. Αυτό δείχνει ότι τα ερωτήματα για τα ΠΣ και τις πολιτικές ασφαλείας των ΠΣ φέρουν υψηλή συνοχή μεταξύ τους και χαρακτηρίζονται ως ιδιαίτερα ικανοποιητικές μετρήσεις ως προς την μοναδικότητα τους.

4.1.2 Δημογραφικά στοιχεία

Οι παρακάτω πίνακες και τα κυκλικά διαγράμματα προσδίδουν το δημογραφικό προφίλ των συμμετεχόντων υπευθύνων των ελληνικών επιχειρήσεων, το οποίο διαμορφώνεται με την παρουσίαση των συχνοτήτων του φύλου, της ηλικίας, της οικογενειακής κατάστασης, τα έτη εμπειρίας στον τομέα των επιχειρήσεων, τη νομική μορφή, το σύνολο των εργαζομένων και τον τομέα δραστηριοποίησης.

Πίνακας 2: Φύλο

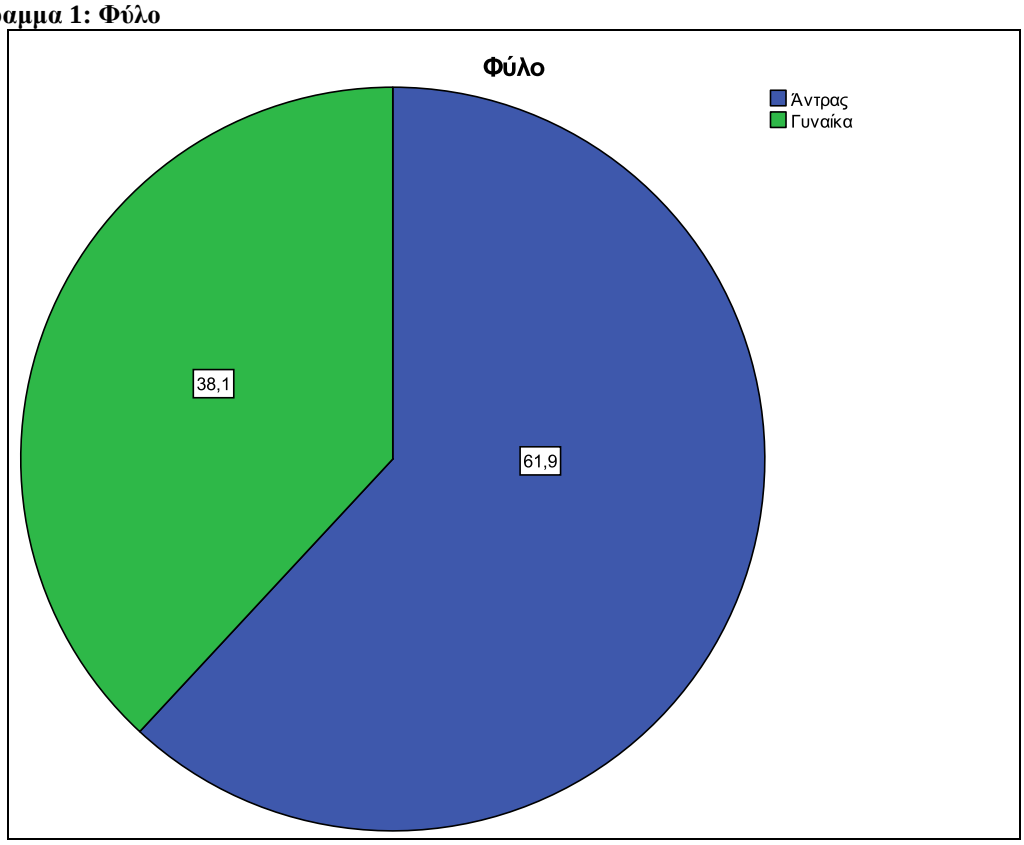
Φύλο

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Άντρας	26	61,9	61,9	61,9
	Γυναίκα	16	38,1	38,1	100,0

Φύλο

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Άντρας	26	61,9	61,9	61,9
	Γυναίκα	16	38,1	38,1	100,0
	Total	42	100,0	100,0	

Διάγραμμα 1: Φύλο



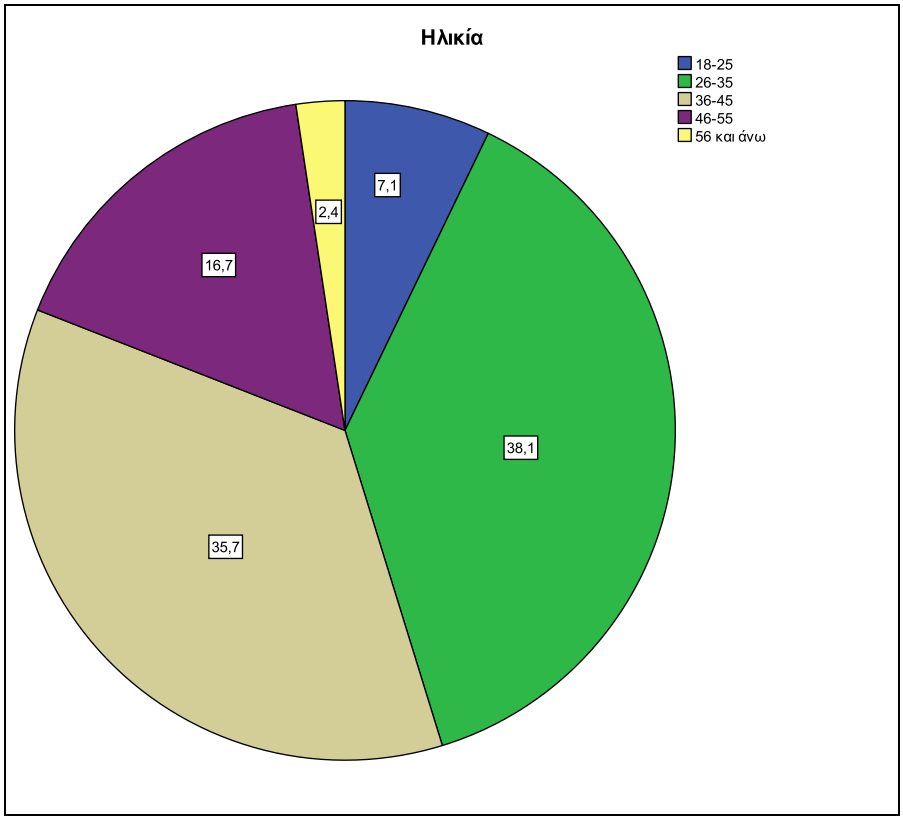
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 61,9% αφορά τους άνδρες και το 38,1% τις γυναίκες. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των υπευθύνων των ελληνικών επιχειρήσεων που συμμετείχαν στην έρευνα αυτή οι περισσότεροι είναι άνδρες.

Πίνακας 3: Ηλικία

Ηλικία

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	3	7,1	7,1	7,1
	26-35	16	38,1	38,1	45,2
	36-45	15	35,7	35,7	81,0
	46-55	7	16,7	16,7	97,6
	56 και άνω	1	2,4	2,4	100,0
	Total	42	100,0	100,0	

Διάγραμμα 2: Ηλικία



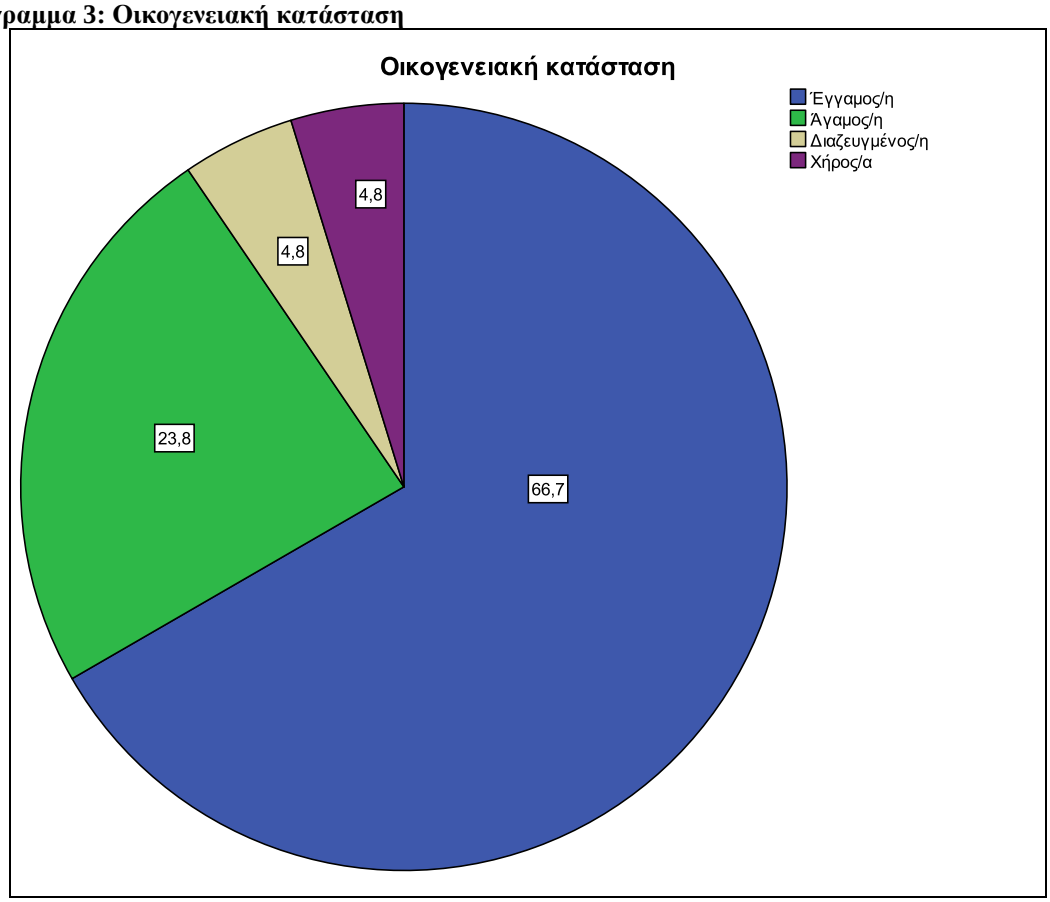
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 7,1% αφορά υπεύθυνους ελληνικών επιχειρήσεων που είναι μεταξύ 18-25 ετών, το 38,1% που είναι μεταξύ 26-35 ετών, το 35,7% που είναι μεταξύ 36-45 ετών, το 16,7% που είναι μεταξύ 46-55 ετών και το 2,4% που είναι άνω των 56 ετών. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των υπευθύνων των ελληνικών επιχειρήσεων που συμμετείχαν στην έρευνα αυτή οι περισσότεροι είναι μεταξύ 26-45 ετών.

Πίνακας 4: Οικογενειακή κατάσταση

Οικογενειακή κατάσταση

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Έγγαμος/η	28	66,7	66,7	66,7
	Άγαμος/η	10	23,8	23,8	90,5
	Διαζευγμένος/η	2	4,8	4,8	95,2
	Χήρος/α	2	4,8	4,8	100,0
	Total	42	100,0	100,0	

Διάγραμμα 3: Οικογενειακή κατάσταση



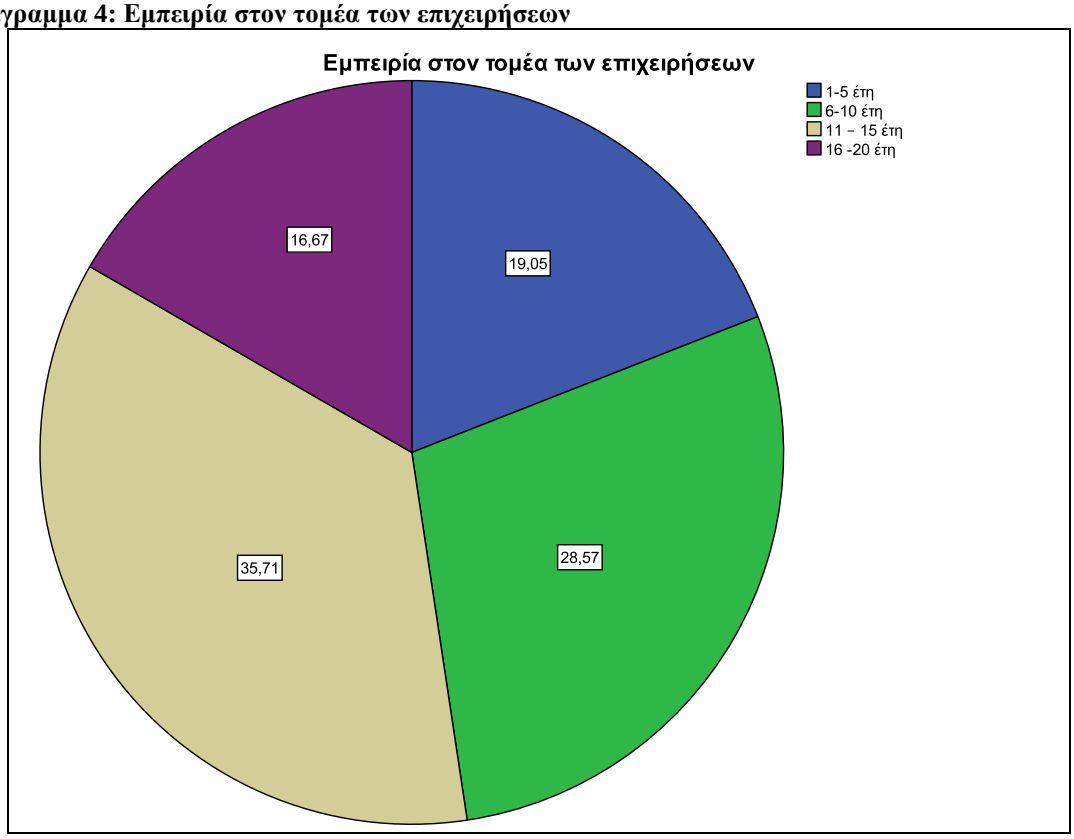
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 66,7% αφορά τους έγγαμους και το 23,8% τους άγαμους, ενώ το 4,8% τους διαζευγμένους και το 4,8% τους χήρους. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των υπευθύνων των ελληνικών επιχειρήσεων που συμμετείχαν στην έρευνα αυτή οι περισσότεροι είναι έγγαμοι.

Πίνακας 5: Εμπειρία στον τομέα των επιχειρήσεων

Εμπειρία στον τομέα των επιχειρήσεων

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5 έτη	8	19,0	19,0	19,0
	6-10 έτη	12	28,6	28,6	47,6
	11 – 15 έτη	15	35,7	35,7	83,3
	16 -20 έτη	7	16,7	16,7	100,0
	Total	42	100,0	100,0	

Διάγραμμα 4: Εμπειρία στον τομέα των επιχειρήσεων



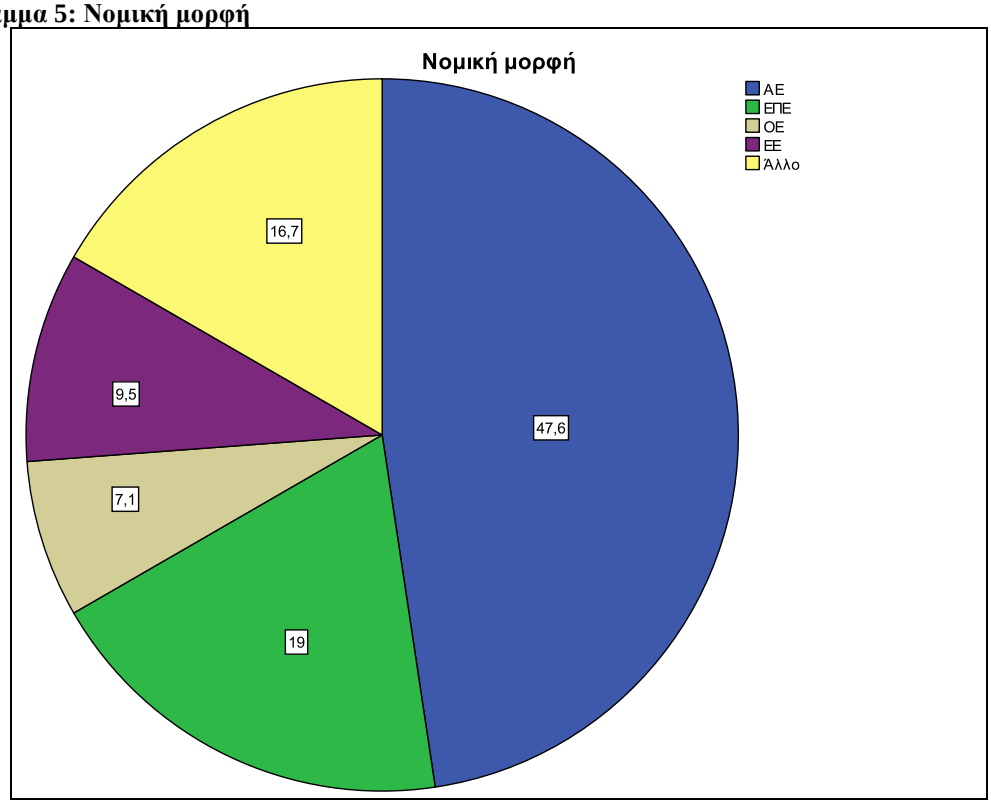
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 19,05% έχει εμπειρία από 1 έως 5 έτη, το 28,57% μεταξύ 6 έως 10 έτη, το 35,7% μεταξύ 11 έως 15 έτη και το 16,67% μεταξύ 16 έως 20 έτη. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των υπευθύνων των ελληνικών επιχειρήσεων που συμμετείχαν στην έρευνα αυτή οι περισσότεροι έχουν εμπειρία στον τομέα των επιχειρήσεων από 6 έως 15 έτη.

Πίνακας 6: Νομική μορφή

Νομική μορφή

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΑΕ	20	47,6	47,6	47,6
	ΕΠΕ	8	19,0	19,0	66,7
	ΟΕ	3	7,1	7,1	73,8
	ΕΕ	4	9,5	9,5	83,3
	Άλλο	7	16,7	16,7	100,0
	Total	42	100,0	100,0	

Διάγραμμα 5: Νομική μορφή



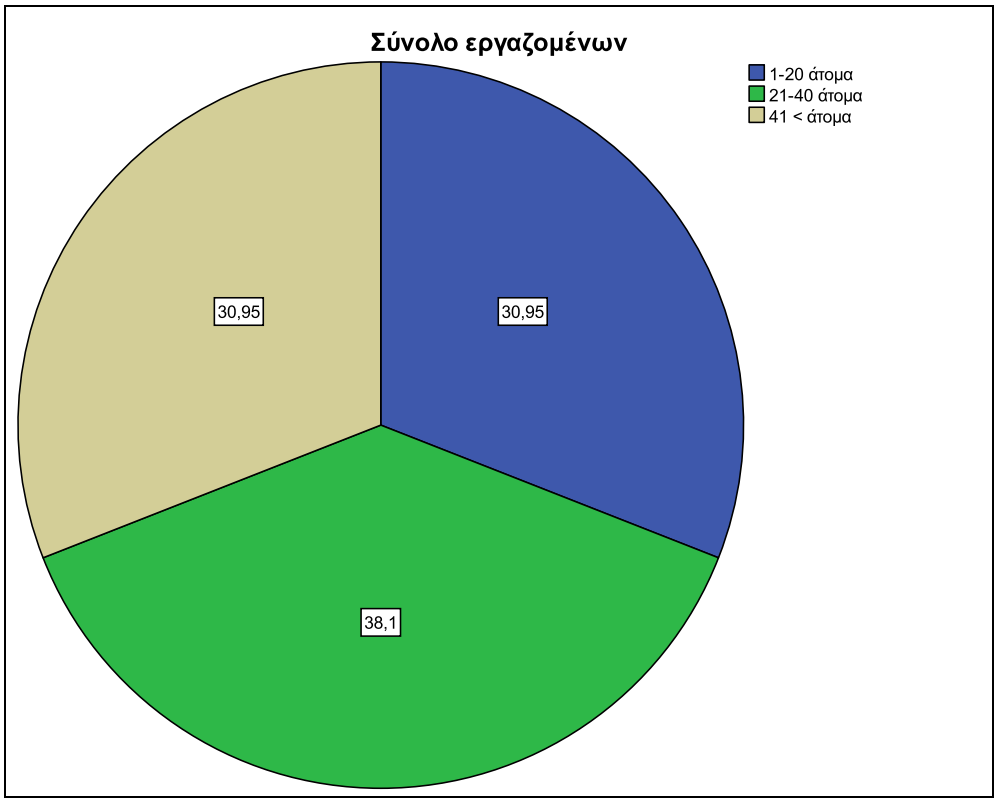
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 47,6% αφορά Ανώνυμες Επιχειρήσεις (ΑΕ), το 19% αφορά Εταιρίες Περιορισμένης Ευθύνης (ΕΠΕ), το 7,1% Ομόρρυθμες Εταιρείες (ΟΕ), το 9,5% αφορά Ετερόρρυθμες Εταιρείες και το 16,7% άλλου είδους εταιρείες. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των ελληνικών επιχειρήσεων οι περισσότερες αφορούν ΑΕ.

Πίνακας 7: Σύνολο εργαζομένων

Σύνολο εργαζομένων

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-20 άτομα	13	31,0	31,0	31,0
	21-40 άτομα	16	38,1	38,1	69,0
	41 < άτομα	13	31,0	31,0	100,0
	Total	42	100,0	100,0	

Διάγραμμα 6: Σύνολο εργαζομένων



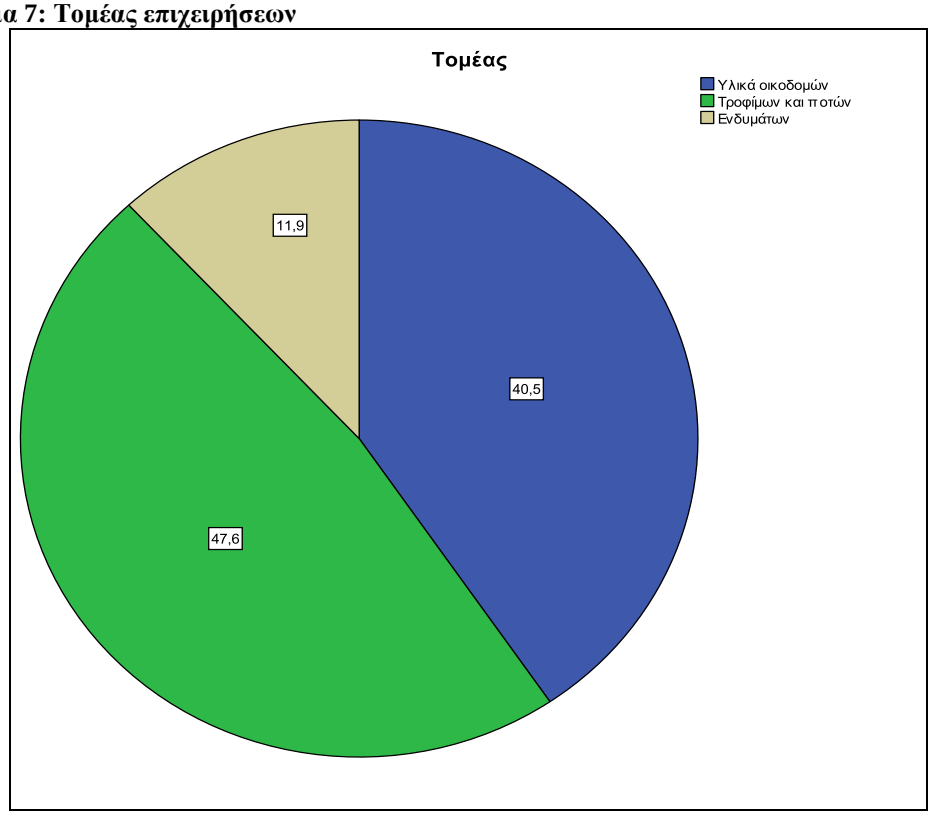
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 30,95% απασχολεί συνολικά από 1 έως 20 άτομα, το 38,1% αφορά 21 έως 40 άτομα και το 30,95% πάνω από 41 άτομα. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των ελληνικών επιχειρήσεων που συμμετείχαν στην έρευνα αυτή απασχολεί από είτε 1-20 άτομα, 21-40 και πάνω από 41 άτομα.

Πίνακας 8: Τομέας επιχειρήσεων

Τομέας

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Υλικά οικοδομών	17	40,5	40,5	40,5
	Τροφίμων και ποτών	20	47,6	47,6	88,1
	Ενδυμάτων	5	11,9	11,9	100,0
	Total	42	100,0	100,0	

Διάγραμμα 7: Τομέας επιχειρήσεων

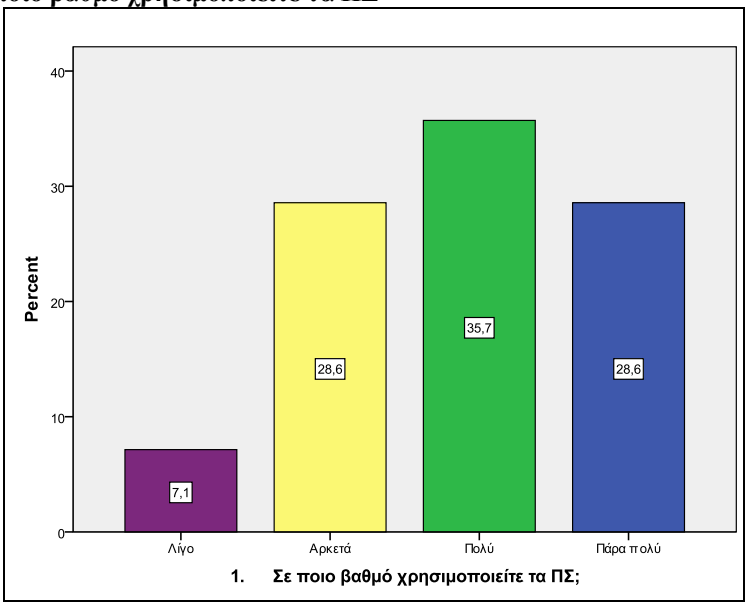


Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα το 40,5% αφορά επιχειρήσεις υλικά οικοδομών, το 47,6% αφορά επιχειρήσεις τροφίμων και ποτών και το 11,9% επιχειρήσεις ενδυμάτων. Αυτό το αποτέλεσμα υποδεικνύει ότι από το σύνολο των ελληνικών επιχειρήσεων οι περισσότερες αφορούν επιχειρήσεις τροφίμων και ποτών.

4.1.3 Βαθμός χρήσης και οφέλους των ΠΣ για τις ελληνικές επιχειρήσεις

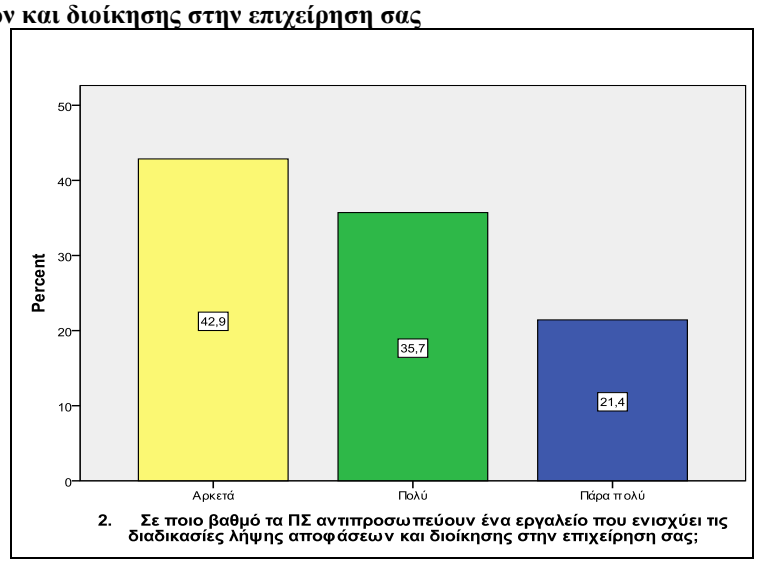
Μέσα από τα ραβδογράμματα που παρατίθενται παρακάτω προσδίδεται ο βαθμός χρήσης και οφέλους των ΠΣ για τις ελληνικές επιχειρήσεις. Τα αποτελέσματα δίνονται με ποσοστιαία κλίμακα σχετικά με το βαθμό στον οποίο χρησιμοποιούν και επωφελούνται οι ελληνικές επιχειρήσεις από τα ΠΣ.

Διάγραμμα 8: Σε ποιο βαθμό χρησιμοποιείτε τα ΠΣ



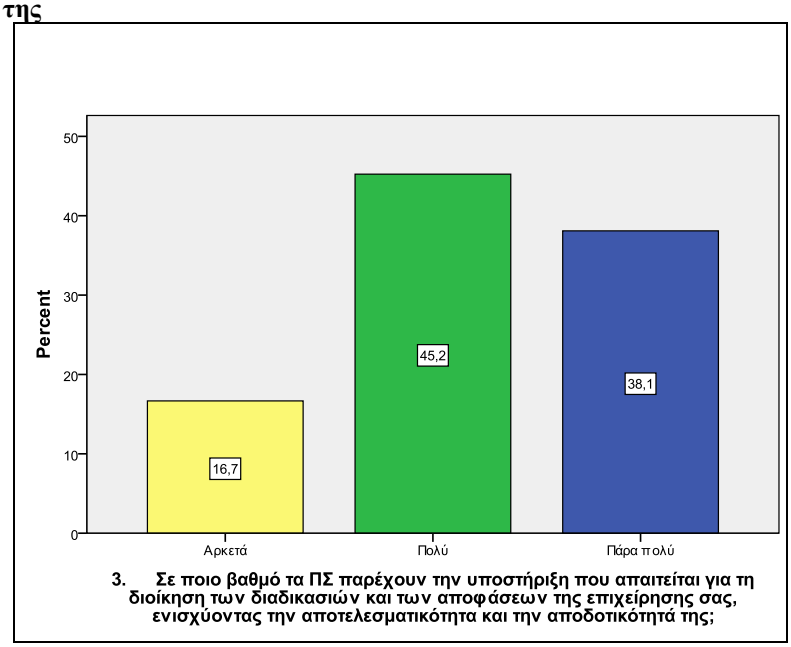
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 35,7% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων υποστηρίζει πως χρησιμοποιεί σε μεγάλο βαθμό τα ΠΣ, ενώ το 7,1% σε ελάχιστο βαθμό.

Διάγραμμα 9: Σε ποιο βαθμό τα ΠΣ αντιπροσωπεύουν ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης στην επιχείρηση σας



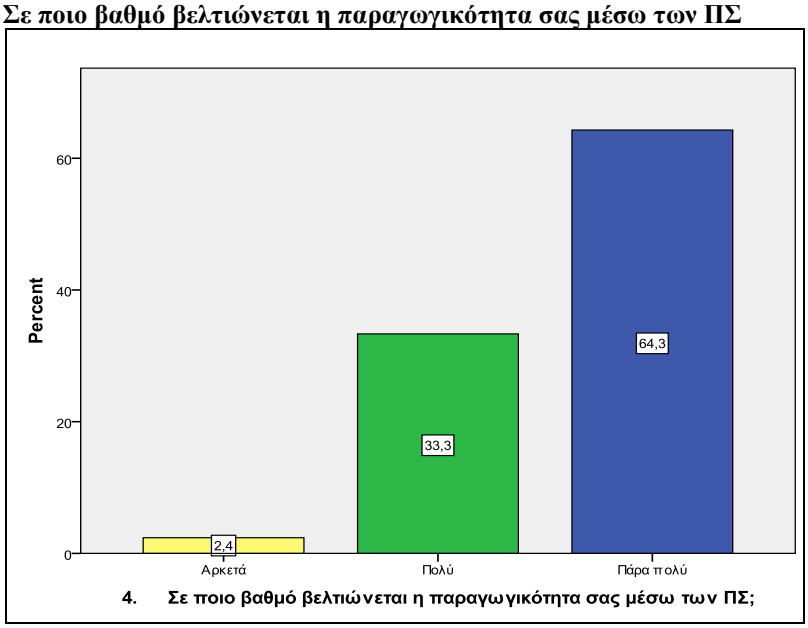
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 42,9% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως τα ΠΣ αντιπροσωπεύουν ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης στην επιχείρηση σε αρκετό βαθμό, ενώ το 21,4% σε πάρα πολύ μεγάλο βαθμό.

Διάγραμμα 10: Σε ποιο βαθμό τα ΠΣ παρέχουν την υποστήριξη που απαιτείται για τη διοίκηση των διαδικασιών και των αποφάσεων της επιχείρησης σας, ενισχύοντας την αποτελεσματικότητα και την αποδοτικότητά της



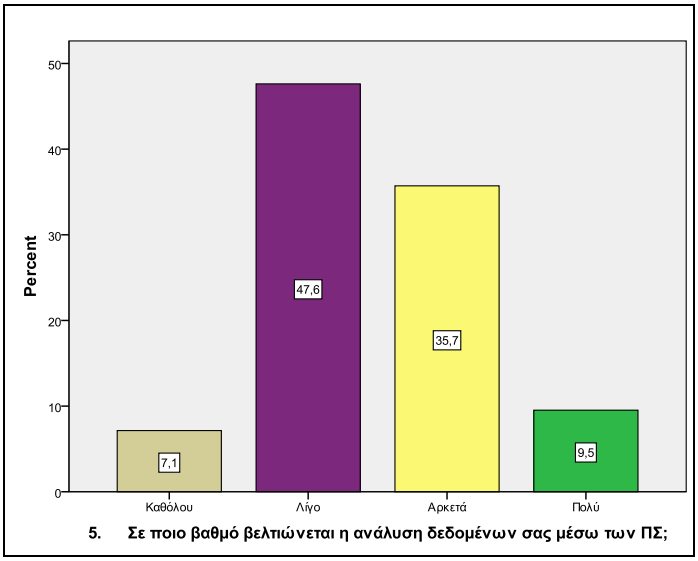
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 45,2% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως τα ΠΣ παρέχουν την υποστήριξη που απαιτείται για τη διοίκηση των διαδικασιών και των αποφάσεων της επιχείρησης τους, ενισχύοντας την αποτελεσματικότητα και την αποδοτικότητά τους σε πολύ μεγάλο βαθμό, ενώ το 16,7% σε αρκετό βαθμό.

Διάγραμμα 11: Σε ποιο βαθμό βελτιώνεται η παραγωγικότητα σας μέσω των ΠΣ



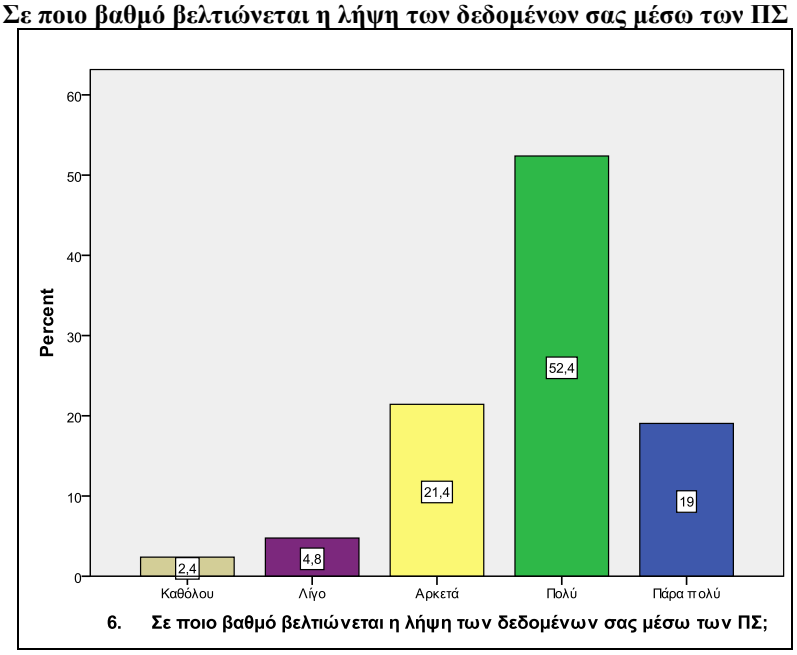
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 64,3% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η παραγωγικότητα της επιχείρησης σε πάρα πολύ μεγάλο βαθμό, ενώ το 2,4% σε αρκετό βαθμό.

Διάγραμμα 12: Σε ποιο βαθμό βελτιώνεται η ανάλυση δεδομένων σας μέσω των ΠΣ



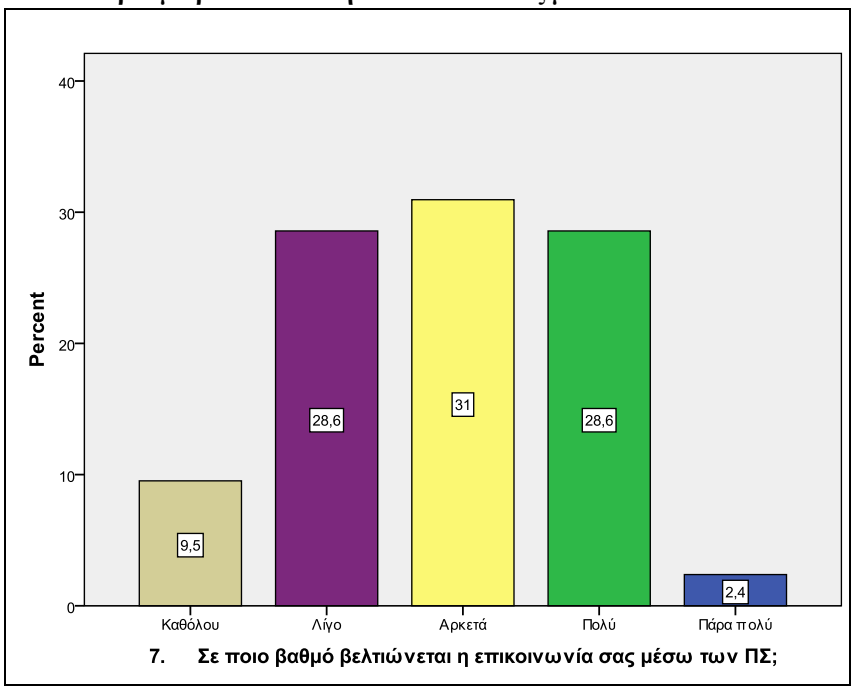
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 47,6% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η ανάλυση δεδομένων της επιχείρησης σε ελάχιστο βαθμό, ενώ το 9,5% σε πολύ μεγάλο βαθμό.

Διάγραμμα 13: Σε ποιο βαθμό βελτιώνεται η λήψη των δεδομένων σας μέσω των ΠΣ



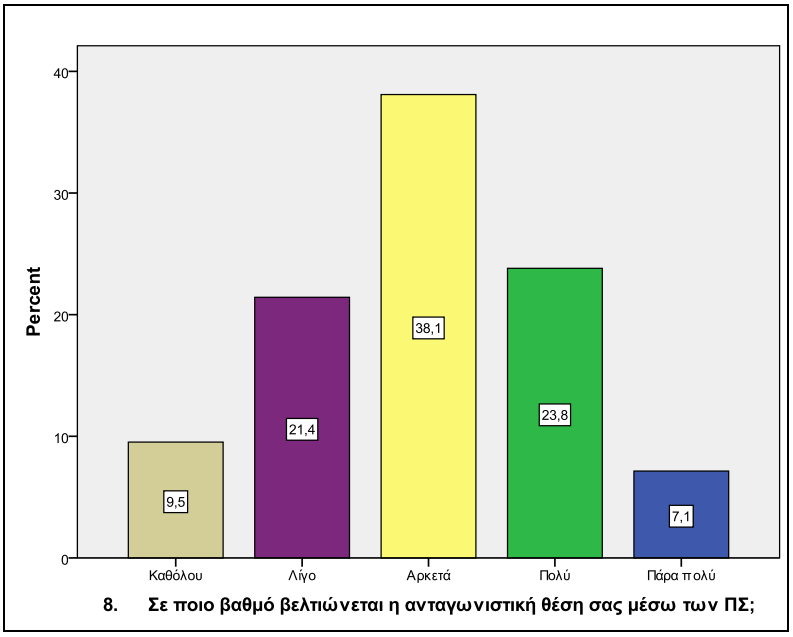
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 52,4% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η λήψη δεδομένων της επιχείρησης σε πολύ μεγάλο βαθμό, ενώ το 2,4% φέρει αντίθετη άποψη.

Διάγραμμα 14: Σε ποιο βαθμό βελτιώνεται η επικοινωνία σας μέσω των ΠΣ



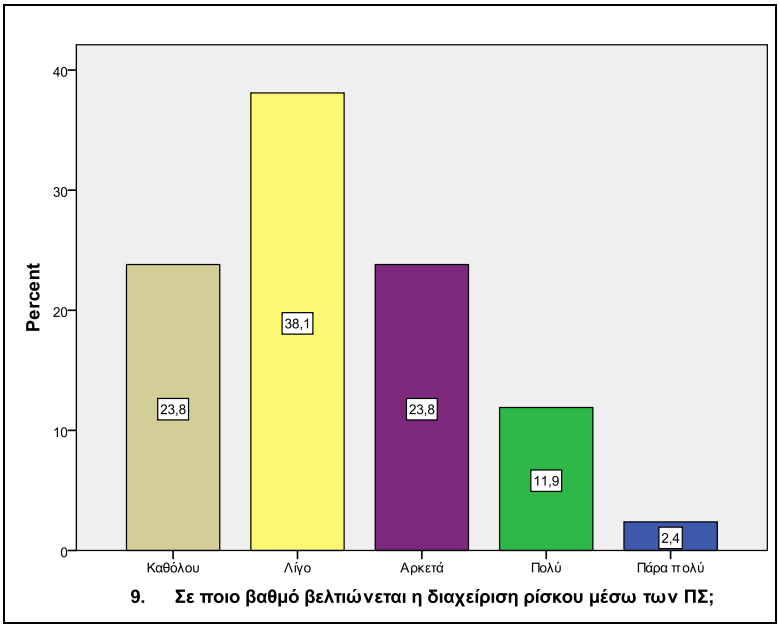
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 31% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η επικοινωνία της επιχείρησης σε αρκετό βαθμό, ενώ το 9,5% φέρει αντίθετη άποψη.

Διάγραμμα 15: Σε ποιο βαθμό βελτιώνεται η ανταγωνιστική θέση σας μέσω των ΠΣ



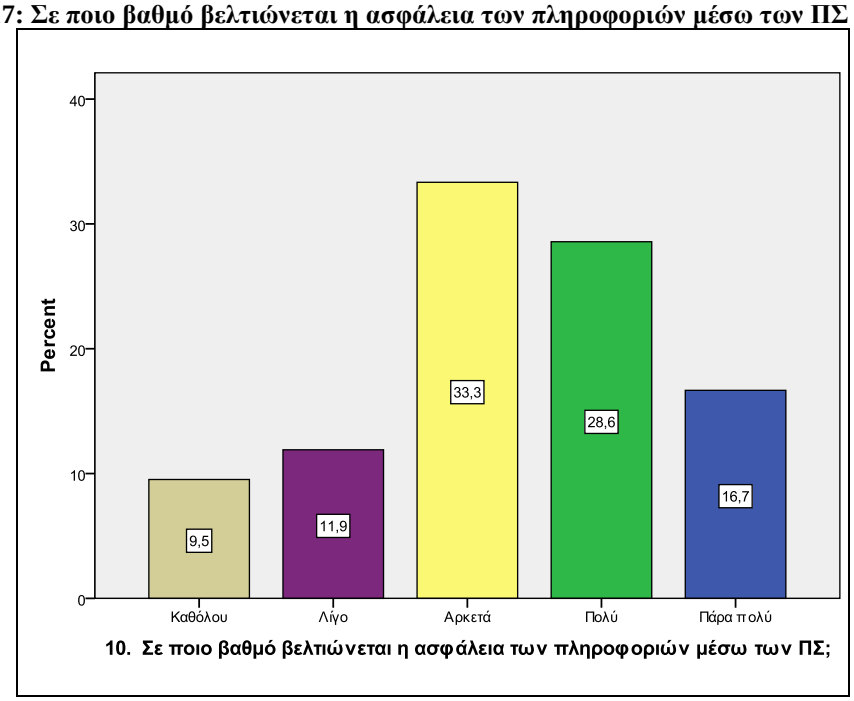
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 38,1% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η ανταγωνιστική θέση της επιχείρησης σε αρκετό βαθμό, ενώ το 9,5% φέρει αντίθετη άποψη.

Διάγραμμα 16: Σε ποιο βαθμό βελτιώνεται η διαχείριση ρίσκου μέσω των ΠΣ



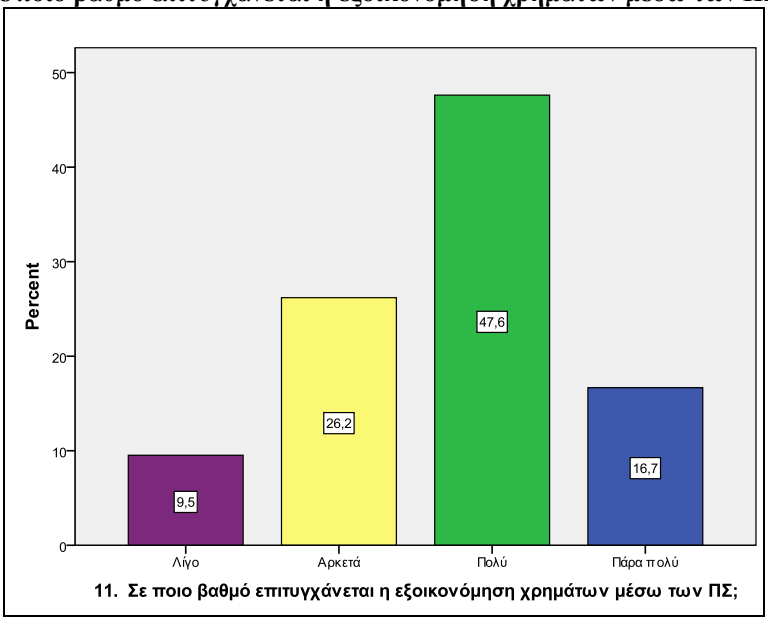
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 38,1% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η διαχείριση ρίσκου της επιχείρησης σε ελάχιστο βαθμό, ενώ το 23,8% φέρει αντίθετη άποψη.

Διάγραμμα 17: Σε ποιο βαθμό βελτιώνεται η ασφάλεια των πληροφοριών μέσω των ΠΣ



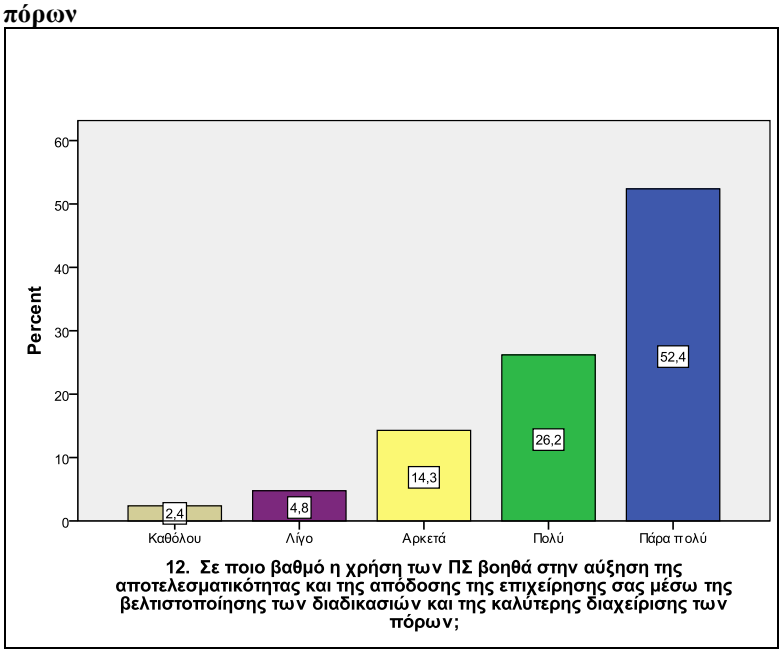
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 33,3% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως μέσω των ΠΣ βελτιώνεται η ασφάλεια των πληροφοριών της επιχείρησης σε αρκετό βαθμό, ενώ το 9,5% φέρει αντίθετη άποψη.

Διάγραμμα 18: Σε ποιο βαθμό επιτυγχάνεται η εξοικονόμηση χρημάτων μέσω των ΠΣ



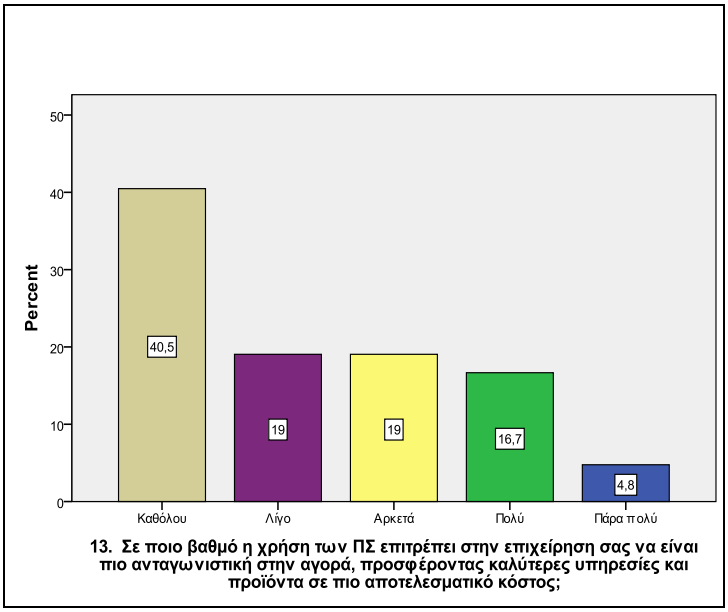
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 47,6% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως επιτυγχάνεται η εξοικονόμηση χρημάτων μέσω των ΠΣ σε πολύ μεγάλο βαθμό, ενώ το 9,5% σε ελάχιστο βαθμό.

Διάγραμμα 19: Σε ποιο βαθμό η χρήση των ΠΣ βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης της επιχείρησης σας μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων



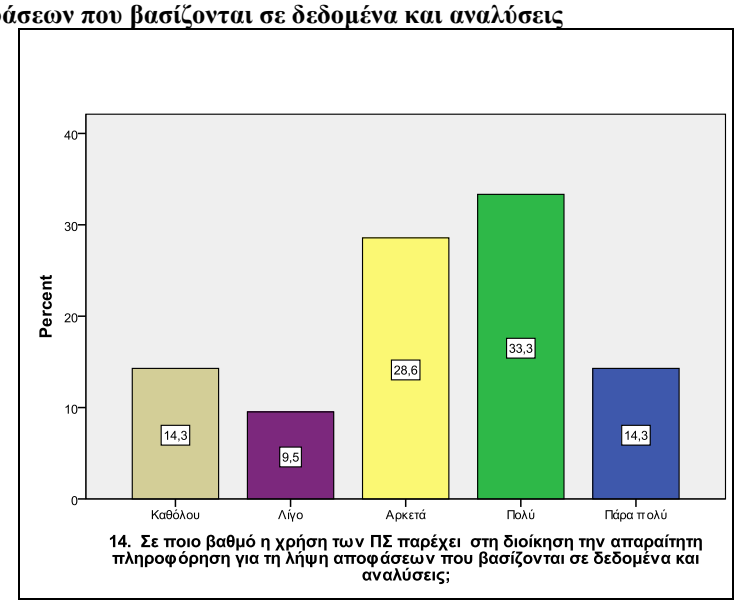
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 52,4% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης της επιχείρησης μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων σε πάρα πολύ μεγάλο βαθμό, ενώ το 2,4% έχει αντίθετη άποψη.

Διάγραμμα 20: Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει στην επιχείρηση σας να είναι πιο ανταγωνιστική στην αγορά, προσφέροντας καλύτερες υπηρεσίες και προϊόντα σε πιο αποτελεσματικό κόστος



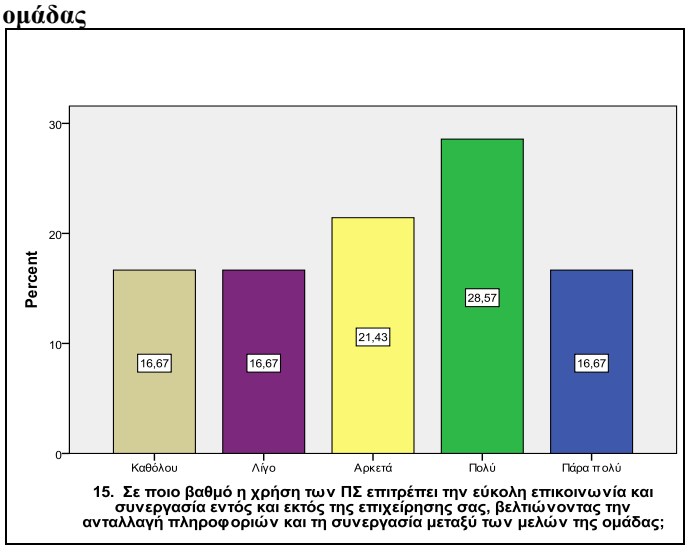
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 40,5% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ δεν επιτρέπει στην επιχείρηση να είναι πιο ανταγωνιστική στην αγορά, προσφέροντας καλύτερες υπηρεσίες και προϊόντα σε πιο αποτελεσματικό κόστος, ενώ το 4,8% έχει αντίθετη άποψη.

Διάγραμμα 21: Σε ποιο βαθμό η χρήση των ΠΣ παρέχει στη διοίκηση την απαραίτητη πληροφόρηση για τη λήψη αποφάσεων που βασίζονται σε δεδομένα και αναλύσεις



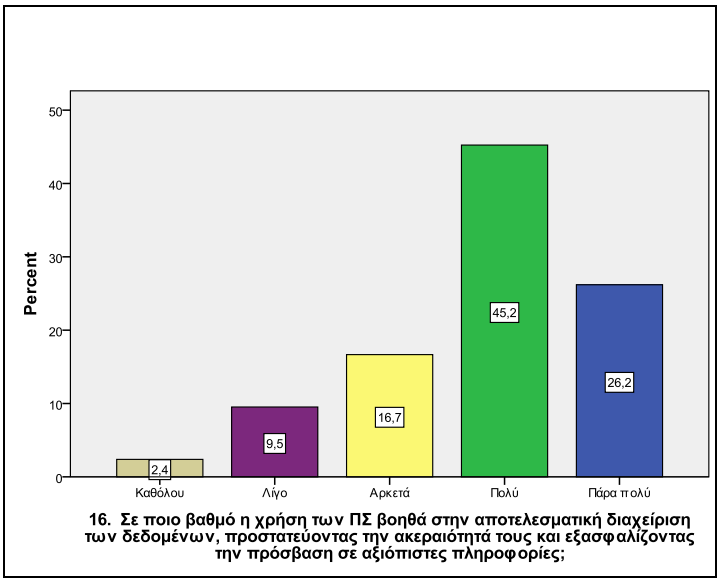
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 33,3% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ παρέχει στη διοίκηση την απαραίτητη πληροφόρηση για τη λήψη αποφάσεων που βασίζονται σε δεδομένα και αναλύσεις σε πολύ μεγάλο βαθμό, ενώ το 14,3% έχει αντίθετη άποψη.

Διάγραμμα 22: Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει την εύκολη επικοινωνία και συνεργασία εντός και εκτός της επιχείρησης σας, βελτιώνοντας την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών της ομάδας



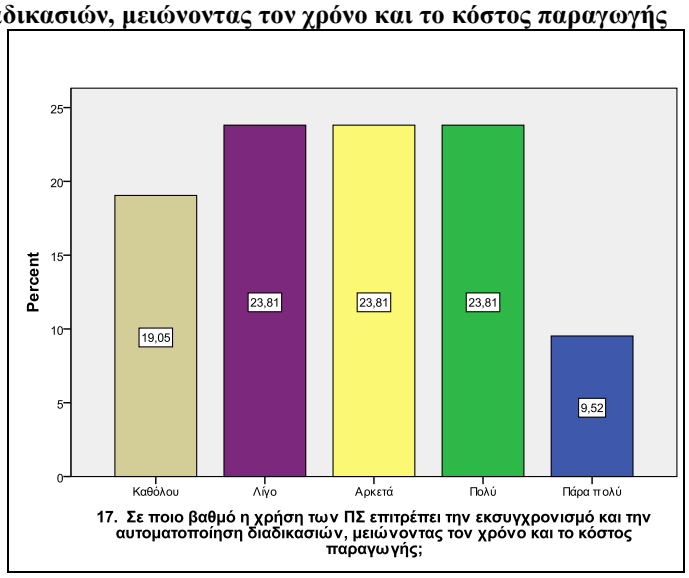
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 28,57% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ επιτρέπει την εύκολη επικοινωνία και συνεργασία εντός και εκτός της επιχείρησης, βελτιώνοντας την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών της ομάδας σε πολύ μεγάλο βαθμό, ενώ το 16,67% έχει αντίθετη άποψη.

Διάγραμμα 23: Σε ποιο βαθμό η χρήση των ΠΣ βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες



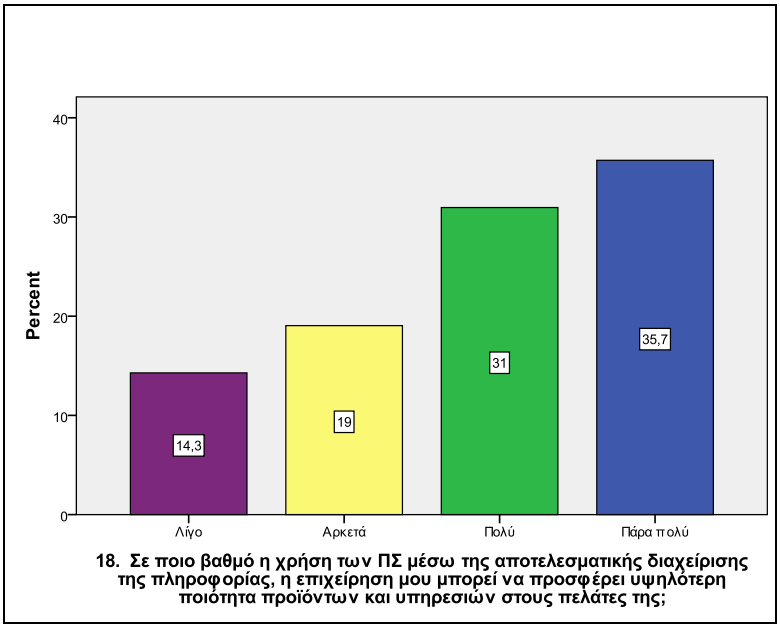
Από τα παραπάνω αποτελέσματα προκύπτει ότι το 45,2% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες σε πολύ μεγάλο βαθμό, ενώ το 2,4% έχει αντίθετη άποψη.

Διάγραμμα 24: Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών, μειώνοντας τον χρόνο και το κόστος παραγωγής



Από τα παραπάνω αποτελέσματα προκύπτει ότι το 23,81% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών, μειώνοντας τον χρόνο και το κόστος παραγωγής από ελάχιστο έως σε πολύ μεγάλο βαθμό, ενώ το 19,06% έχει αντίθετη άποψη.

Διάγραμμα 25: Σε ποιο βαθμό η χρήση των ΠΣ μέσω της αποτελεσματικής διαχείρισης της πληροφορίας, η επιχείρηση μου μπορεί να προσφέρει υψηλότερη ποιότητα προϊόντων και υπηρεσιών στους πελάτες της

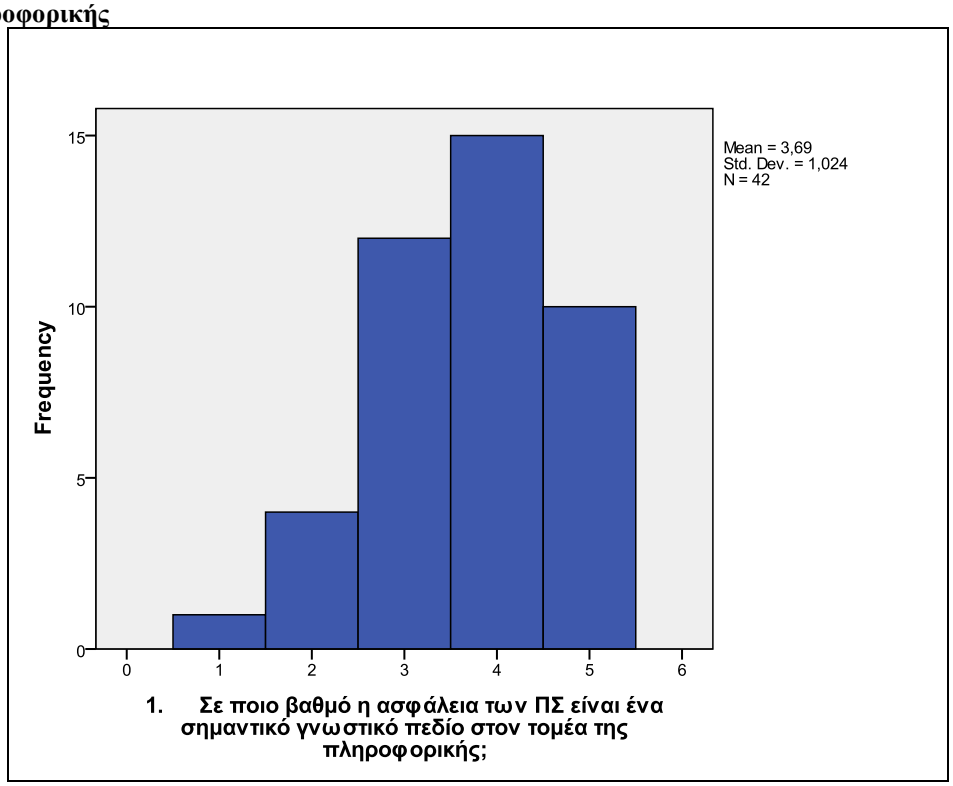


Από τα παραπάνω αποτελέσματα προκύπτει ότι το 35,7% του δείγματος των υπευθύνων των ελληνικών επιχειρήσεων εκτιμά πως η χρήση των ΠΣ μέσω της αποτελεσματικής διαχείρισης της πληροφορίας, η επιχείρηση τους μπορεί να προσφέρει υψηλότερη ποιότητα προϊόντων και υπηρεσιών στους πελάτες της σε πάρα πολύ μεγάλο βαθμό, ενώ το 14,3% σε ελάχιστο βαθμό.

4.1.4 Βαθμός συμβολής και εφαρμογής των πολιτών ασφαλείας των ΠΣ

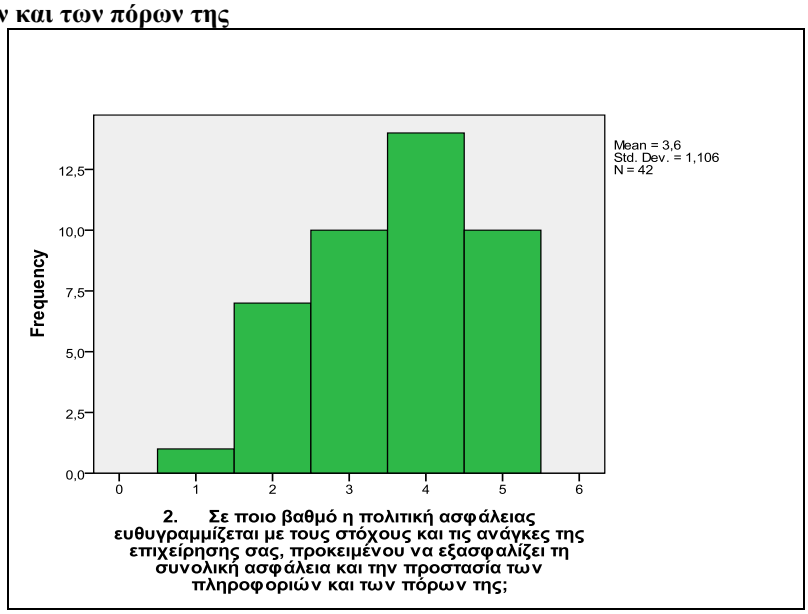
Μέσα από τα ιστογράμματα που παρατίθενται παρακάτω προσδίδεται ο μέσος βαθμός συμβολής και εφαρμογής των πολιτικών ασφαλείας των ΠΣ για τις ελληνικές επιχειρήσεις.

Διάγραμμα 26: Σε ποιο βαθμό η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής



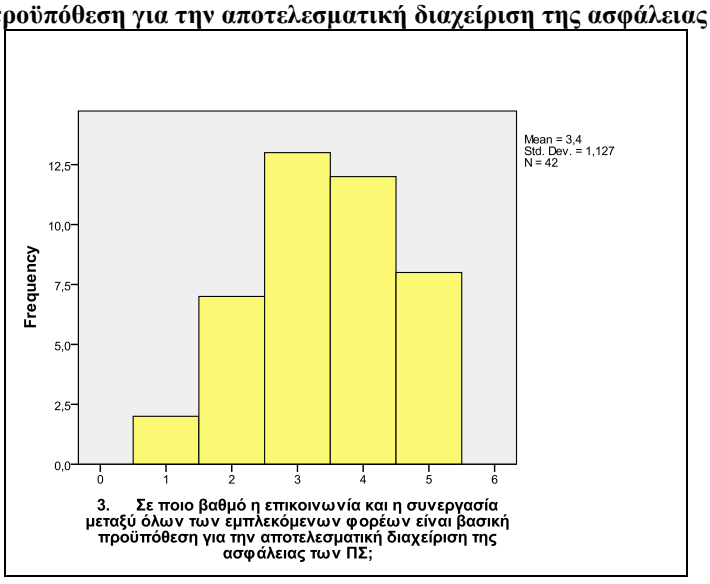
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,69).

Διάγραμμα 27: Σε ποιο βαθμό η πολιτική ασφάλειας ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης σας, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της



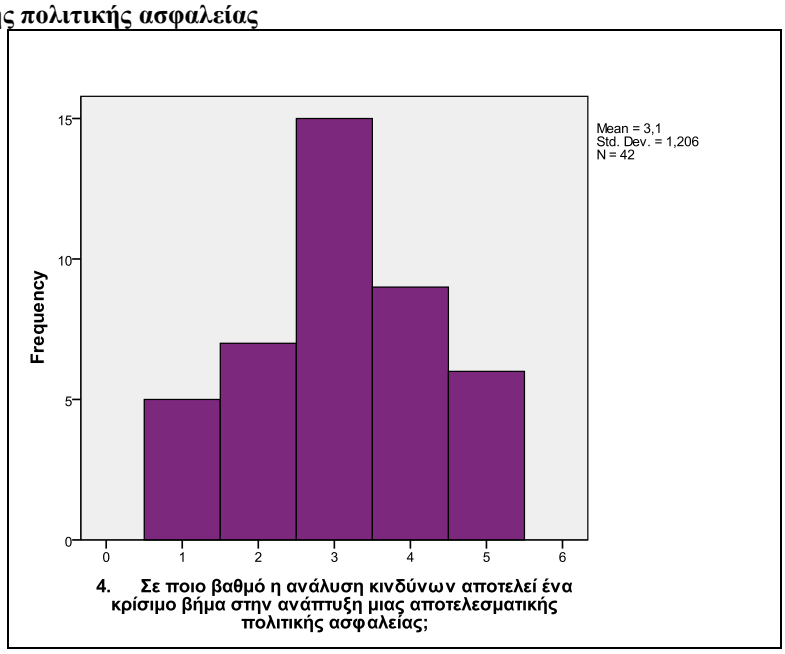
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η πολιτική ασφάλειας ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,6).

Διάγραμμα 28: Σε ποιο βαθμό η επικοινωνία και η συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ



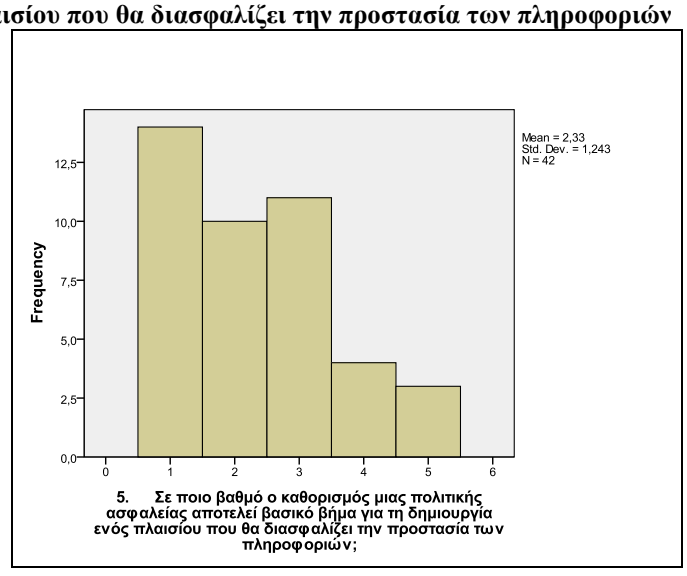
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η επικοινωνία και η συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ σε αρκετό βαθμό κατά μέσο όρο (Mean = 3,4).

Διάγραμμα 29: Σε ποιο βαθμό η ανάλυση κινδύνων αποτελεί ένα κρίσιμο βήμα στην ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας



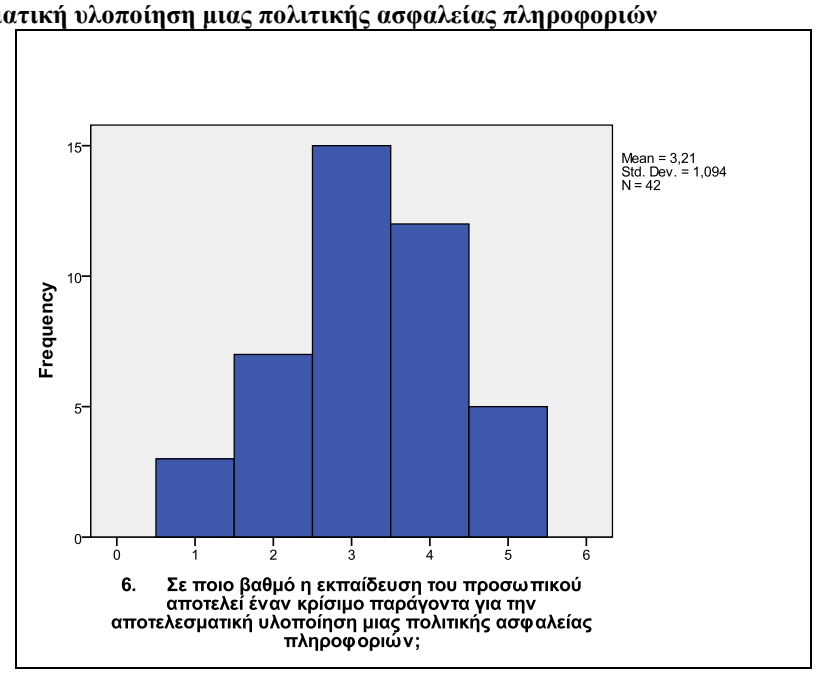
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η ανάλυση κινδύνων αποτελεί ένα κρίσιμο βήμα στην ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας σε αρκετό βαθμό κατά μέσο όρο (Mean = 3,1).

Διάγραμμα 30: Σε ποιο βαθμό ο καθορισμός μιας πολιτικής ασφαλείας αποτελεί βασικό βήμα για τη δημιουργία ενός πλαισίου που θα διασφαλίζει την προστασία των πληροφοριών



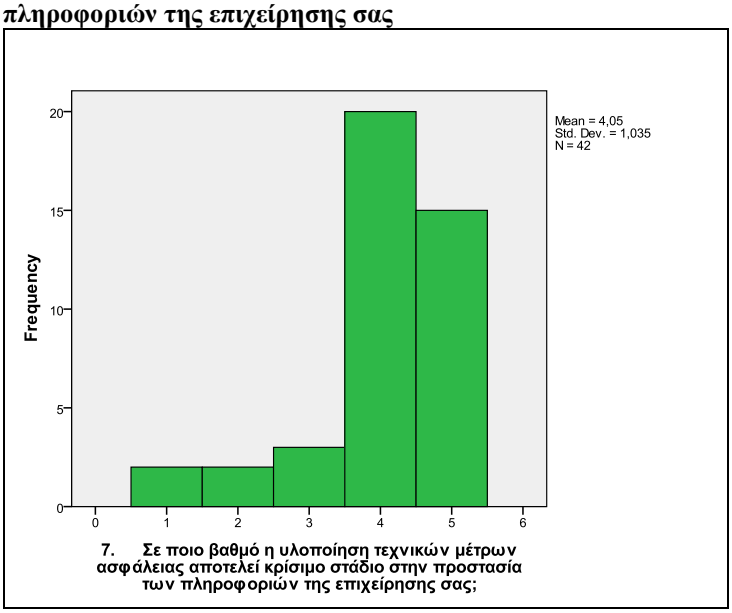
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι ο καθορισμός μιας πολιτικής ασφαλείας αποτελεί βασικό βήμα για τη δημιουργία ενός πλαισίου που θα διασφαλίζει την προστασία των πληροφοριών σε ελάχιστο βαθμό κατά μέσο όρο (Mean = 2,33).

Διάγραμμα 31: Σε ποιο βαθμό η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών



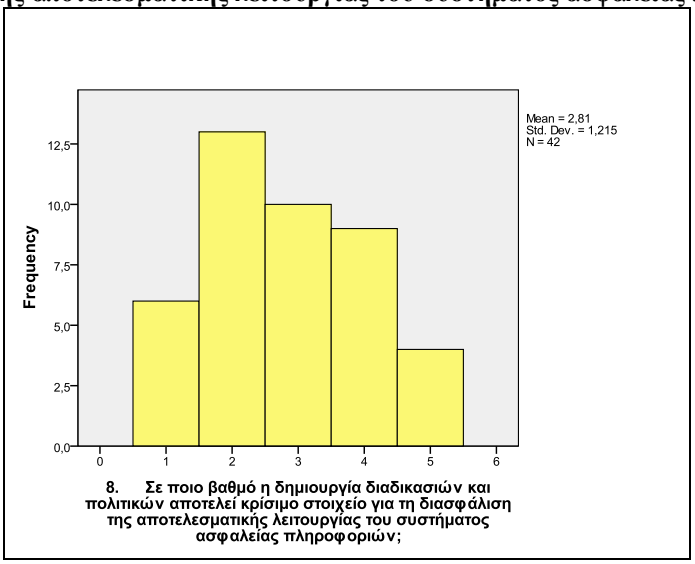
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών σε αρκετό βαθμό κατά μέσο όρο (Mean = 3,21).

Διάγραμμα 32: Σε ποιο βαθμό η υλοποίηση τεχνικών μέτρων ασφάλειας αποτελεί κρίσιμο στάδιο στην προστασία των πληροφοριών της επιχείρησης σας



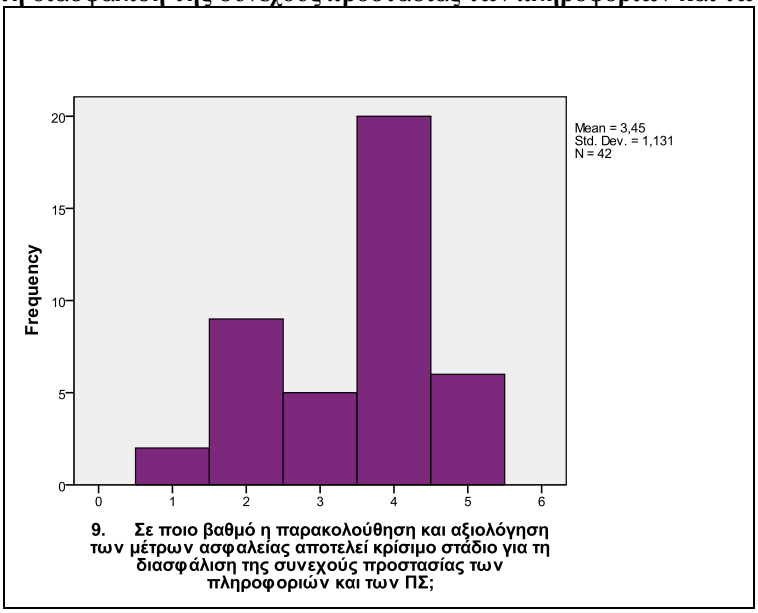
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η υλοποίηση τεχνικών μέτρων ασφάλειας αποτελεί κρίσιμο στάδιο στην προστασία των πληροφοριών της επιχείρησης τους σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,05).

Διάγραμμα 33: Σε ποιο βαθμό η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών



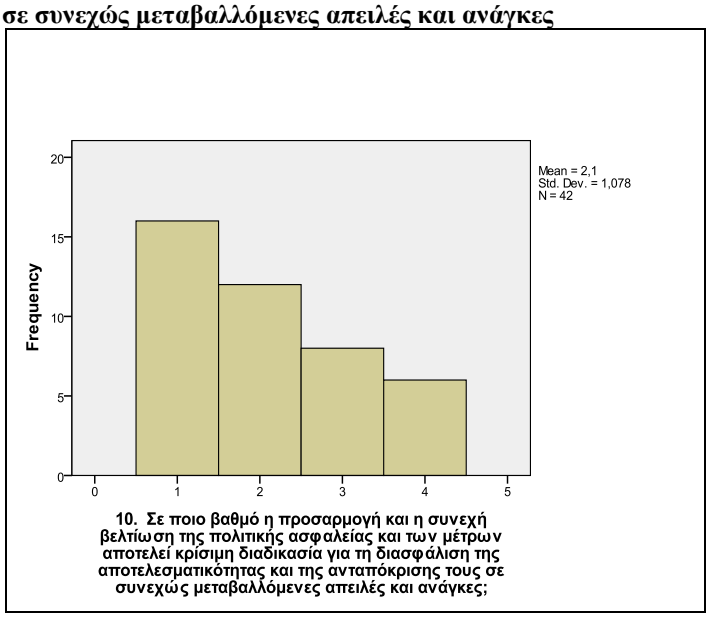
Σχετικά με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών σε αρκετό βαθμό κατά μέσο όρο (Mean = 2,81).

Διάγραμμα 34: Σε ποιο βαθμό η παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας αποτελεί κρίσιμο στάδιο για τη διασφάλιση της συνεχούς προστασίας των πληροφοριών και των ΠΣ



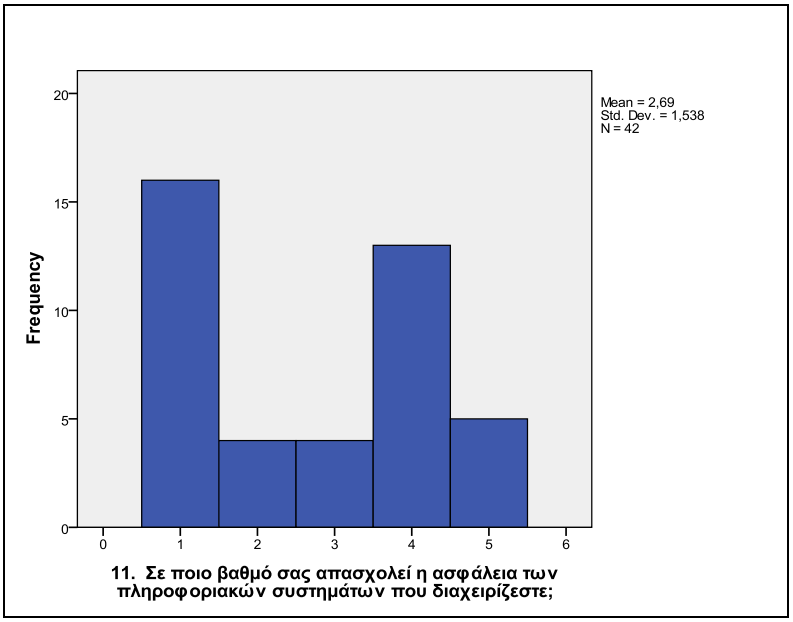
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας αποτελεί κρίσιμο στάδιο για τη διασφάλιση της συνεχούς προστασίας των πληροφοριών και των ΠΣ σε αρκετό βαθμό κατά μέσο όρο (Mean = 3,45).

Διάγραμμα 35: Σε ποιο βαθμό η προσαρμογή και η συνεχή βελτίωση της πολιτικής ασφαλείας και των μέτρων αποτελεί κρίσιμη διαδικασία για τη διασφάλιση της αποτελεσματικότητας και της ανταπόκρισης τους σε συνεχώς μεταβαλλόμενες απειλές και ανάγκες



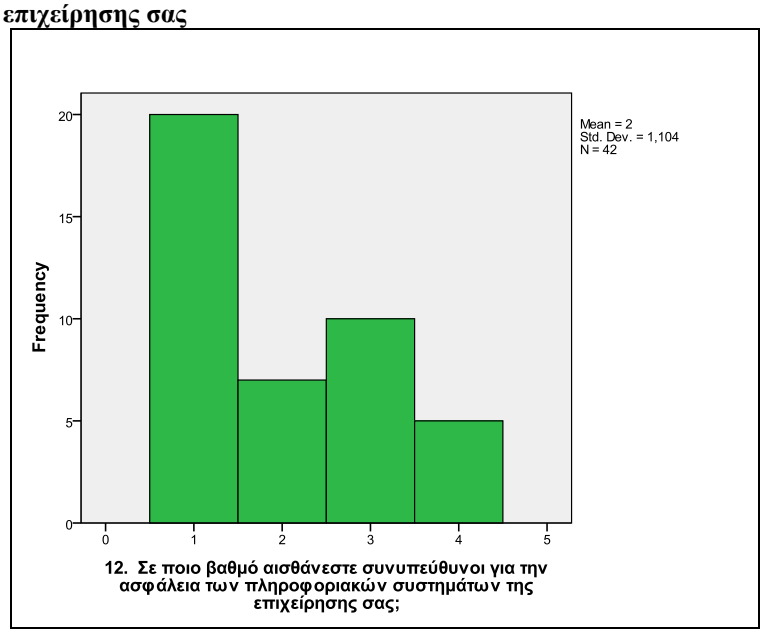
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η προσαρμογή και η συνεχή βελτίωση της πολιτικής ασφαλείας και των μέτρων αποτελεί κρίσιμη διαδικασία για τη διασφάλιση της αποτελεσματικότητας και της ανταπόκρισης τους σε συνεχώς μεταβαλλόμενες απειλές και ανάγκες σε ελάχιστο βαθμό κατά μέσο όρο (Mean = 2,1).

Διάγραμμα 36: Σε ποιο βαθμό σας απασχολεί η ασφάλεια των πληροφοριακών συστημάτων που διαχειρίζεστε



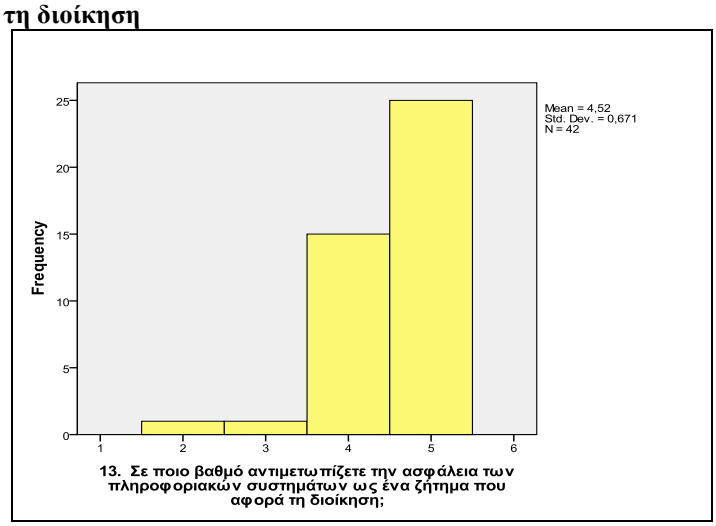
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι τους απασχολεί η ασφάλεια των πληροφοριακών συστημάτων που διαχειρίζονται σε αρκετό βαθμό κατά μέσο όρο (Mean = 2,69).

Διάγραμμα 37: Σε ποιο βαθμό αισθάνεστε συνυπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησης σας



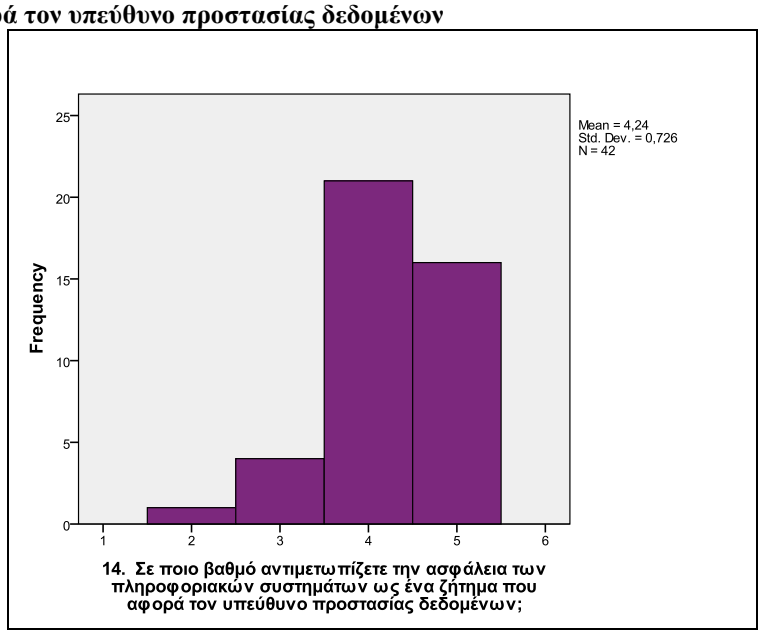
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αισθάνονται συνυπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησης τους σε ελάχιστο βαθμό κατά μέσο όρο (Mean = 2).

Διάγραμμα 38: Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τη διοίκηση



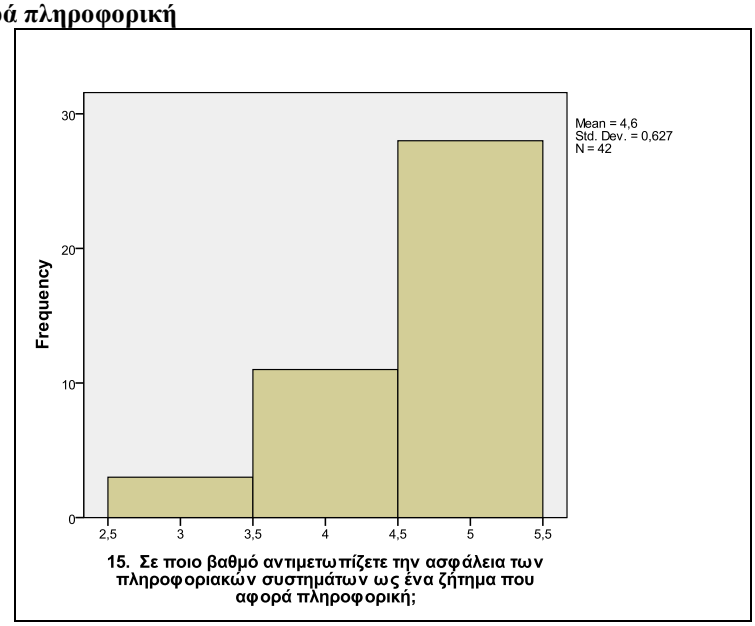
Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τη διοίκηση σε πάρα πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,52).

Διάγραμμα 39: Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τον υπεύθυνο προστασίας δεδομένων



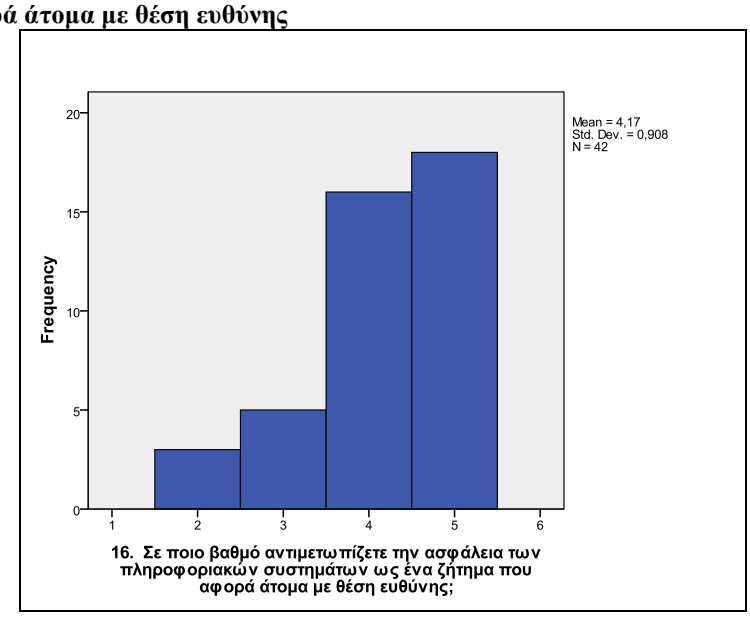
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τον υπεύθυνο προστασίας δεδομένων σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,24).

Διάγραμμα 40: Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά πληροφορική



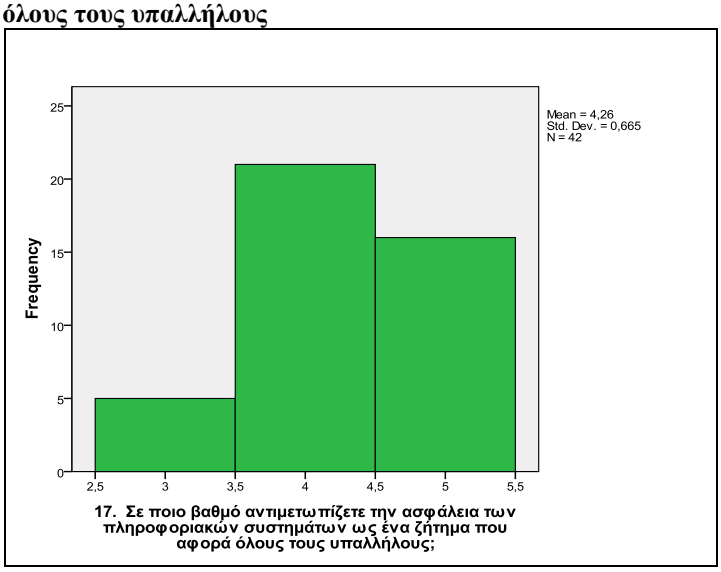
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά πληροφορική σε πάρα πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,6).

Διάγραμμα 41: Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά άτομα με θέση ευθύνης



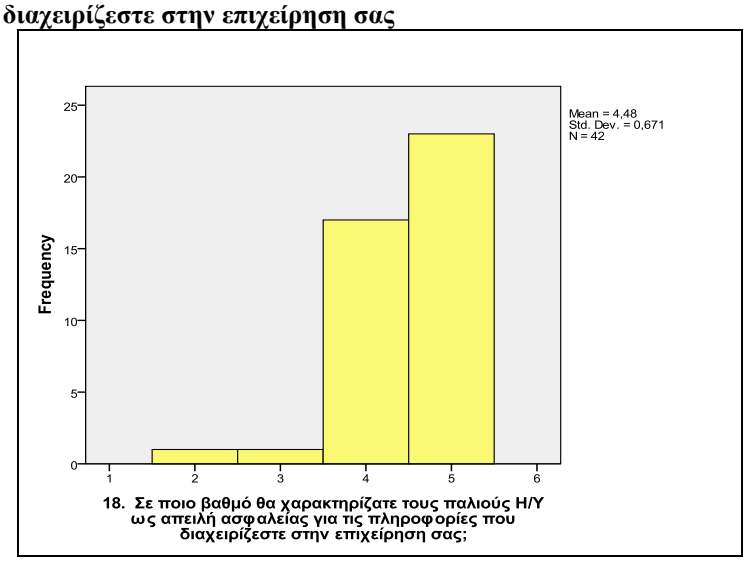
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά άτομα με θέση ευθύνης σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,17).

Διάγραμμα 42: Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά όλους τους υπαλλήλους



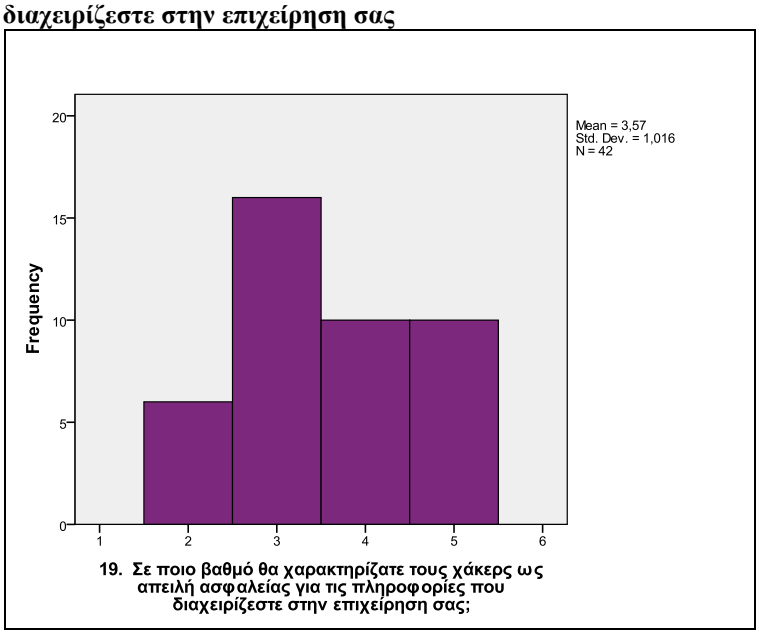
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά όλους τους υπαλλήλους σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,26).

Διάγραμμα 43: Σε ποιο βαθμό θα χαρακτηρίζατε τους παλιούς Η/Υ ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



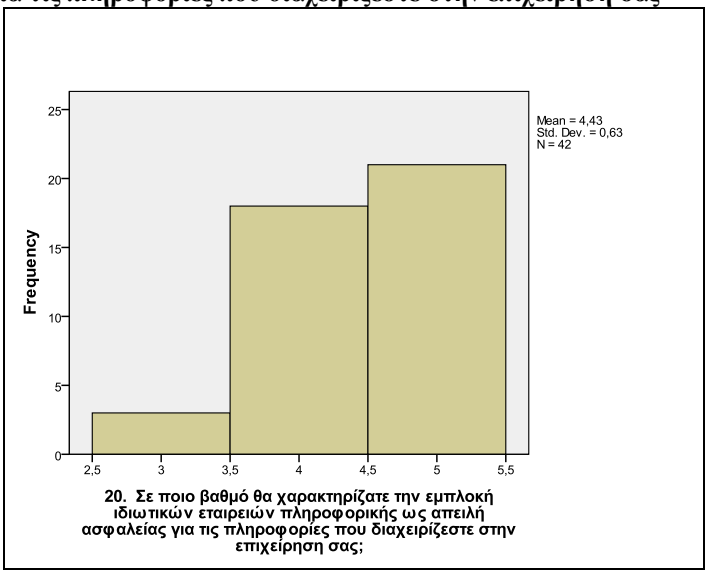
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζαν τους παλιούς Η/Υ ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πάρα πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,48).

Διάγραμμα 44: Σε ποιο βαθμό θα χαρακτηρίζατε τους χάκερς ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



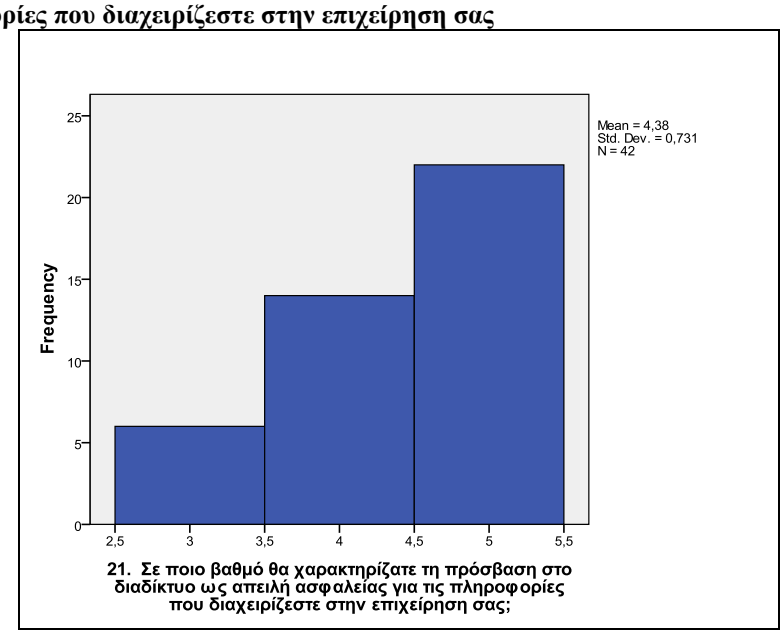
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε τους χάκερς ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,57).

Διάγραμμα 45: Σε ποιο βαθμό θα χαρακτηρίζατε την εμπλοκή ιδιωτικών εταιρειών πληροφορικής ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



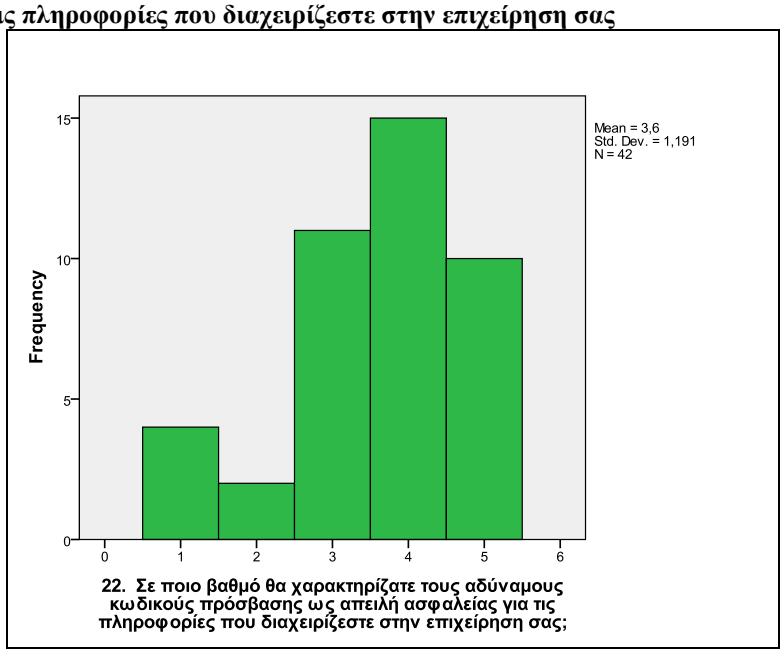
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε την εμπλοκή ιδιωτικών εταιρειών πληροφορικής ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,43).

Διάγραμμα 46: Σε ποιο βαθμό θα χαρακτηρίζατε τη πρόσβαση στο διαδίκτυο ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



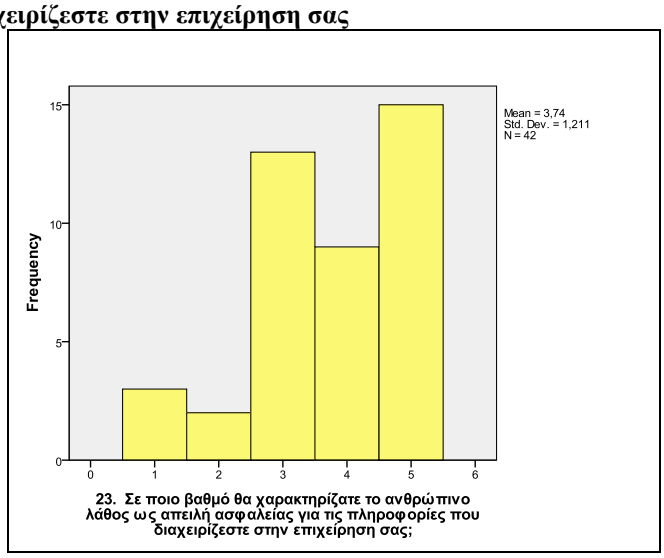
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε τη πρόσβαση στο διαδίκτυο ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 4,38).

Διάγραμμα 47: Σε ποιο βαθμό θα χαρακτηρίζατε τους αδύναμους κωδικούς πρόσβασης ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



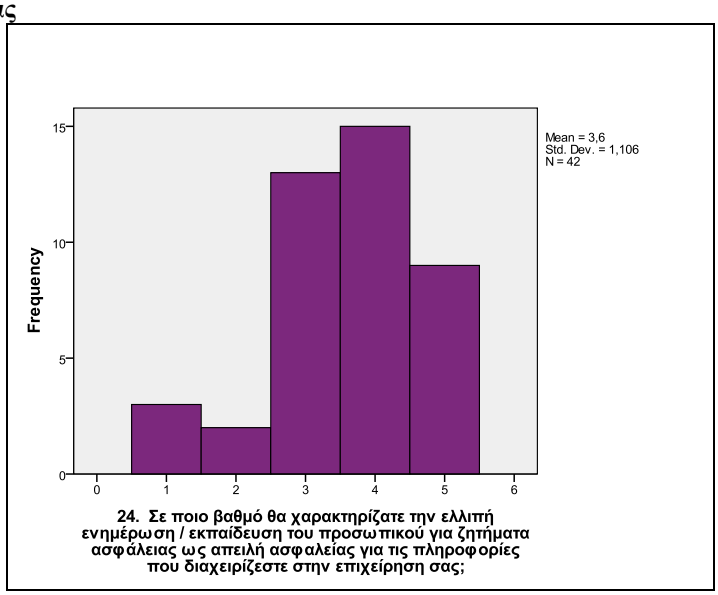
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε τους αδύναμους κωδικούς πρόσβασης ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,6).

Διάγραμμα 48: Σε ποιο βαθμό θα χαρακτηρίζατε το ανθρώπινο λάθος ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



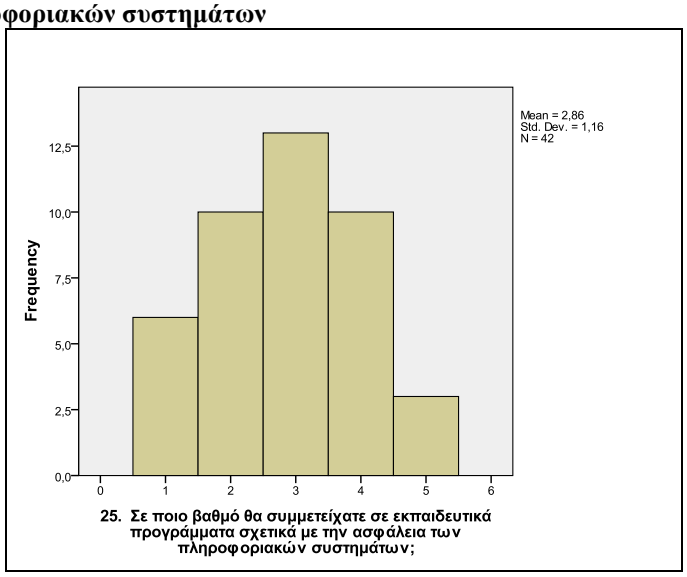
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε το ανθρώπινο λάθος ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,6).

Διάγραμμα 49: Σε ποιο βαθμό θα χαρακτηρίζατε την ελλιπή ενημέρωση / εκπαίδευση του προσωπικού για ζητήματα ασφάλειας ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας



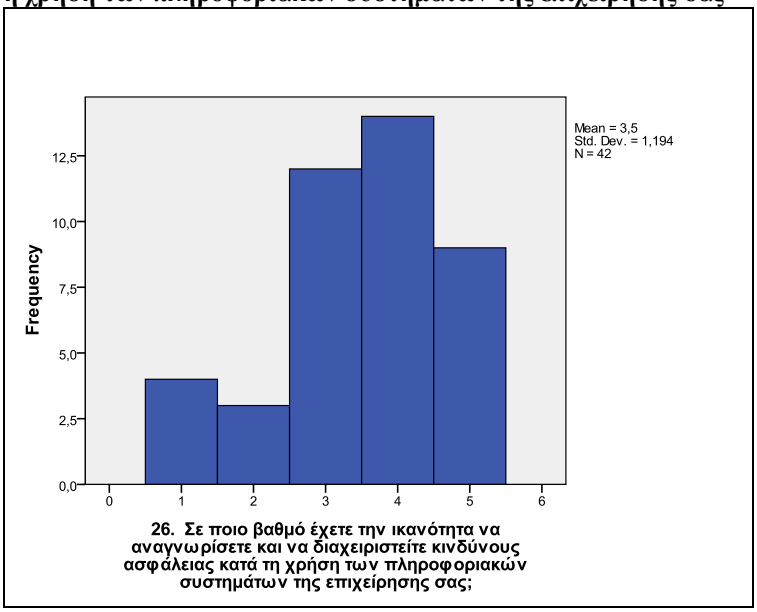
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα χαρακτήριζε την ελλιπή ενημέρωση / εκπαίδευση του προσωπικού για ζητήματα ασφάλειας ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,6).

Διάγραμμα 50: Σε ποιο βαθμό θα συμμετείχατε σε εκπαιδευτικά προγράμματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων



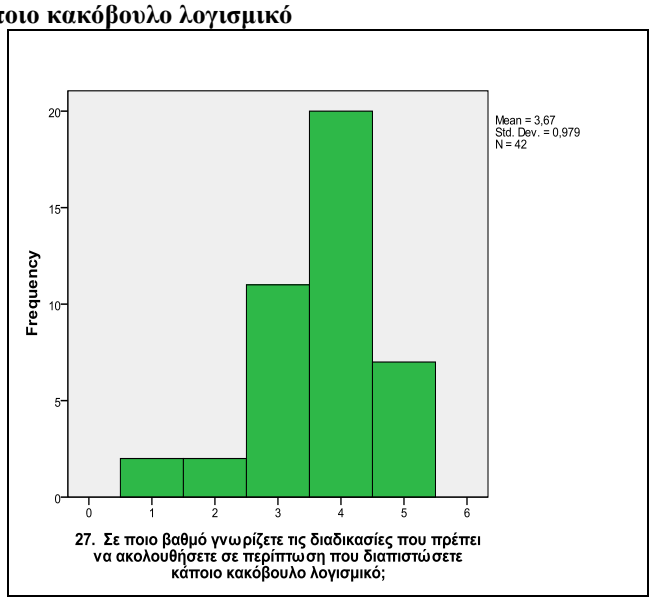
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα συμμετείχαν σε εκπαιδευτικά προγράμματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων σε πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 2,86).

Διάγραμμα 51: Σε ποιο βαθμό έχετε την ικανότητα να αναγνωρίσετε και να διαχειριστείτε κινδύνους ασφάλειας κατά τη χρήση των πληροφοριακών συστημάτων της επιχείρησης σας



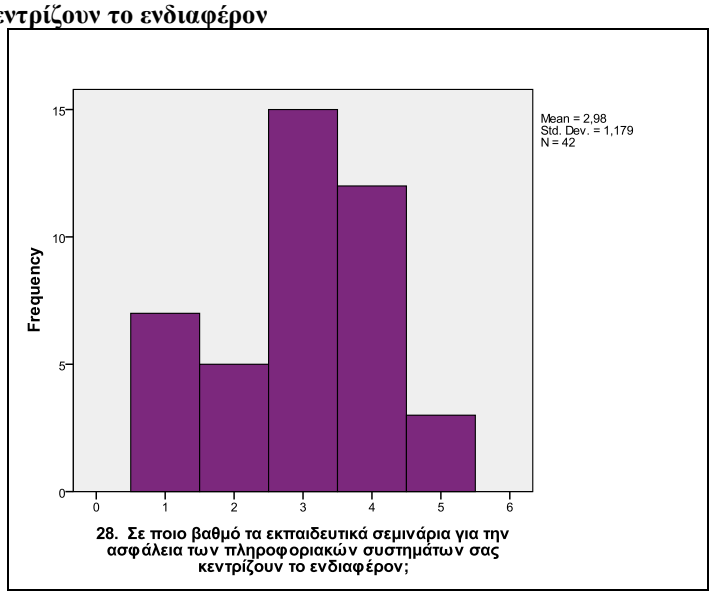
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι έχουν την ικανότητα να αναγνωρίσουν και να διαχειριστούν τους κινδύνους ασφάλειας κατά τη χρήση των πληροφοριακών συστημάτων της επιχείρησης σε πάρα πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,5).

Διάγραμμα 52: Σε ποιο βαθμό γνωρίζετε τις διαδικασίες που πρέπει να ακολουθήσετε σε περίπτωση που διαπιστώσετε κάποιο κακόβουλο λογισμικό



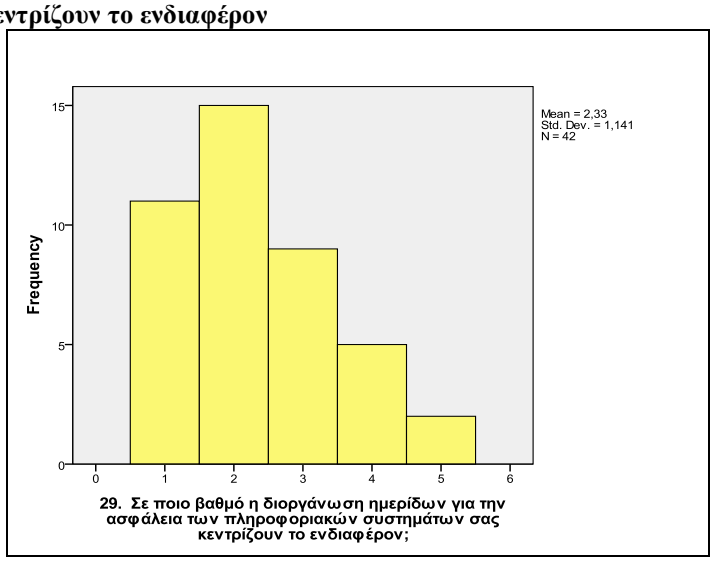
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι γνωρίζουν τις διαδικασίες που πρέπει να ακολουθήσουν σε περίπτωση που διαπιστώσουν κάποιο κακόβουλο λογισμικό σε πάρα πολύ μεγάλο βαθμό κατά μέσο όρο (Mean = 3,67).

Διάγραμμα 53: Σε ποιο βαθμό τα εκπαιδευτικά σεμινάρια για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον



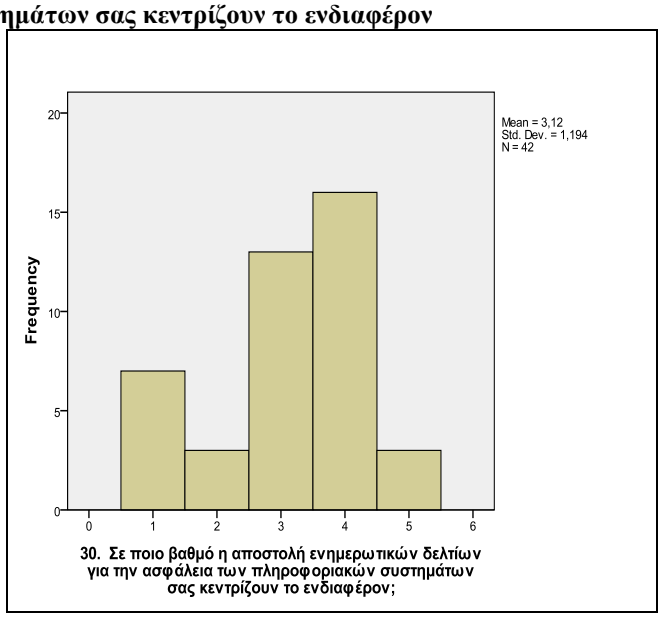
Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι τα εκπαιδευτικά σεμινάρια για την ασφάλεια των πληροφοριακών συστημάτων τους κεντρίζουν το ενδιαφέρον σε μεγάλο βαθμό κατά μέσο όρο (Mean = 2,98).

Διάγραμμα 54: Σε ποιο βαθμό η διοργάνωση ημερίδων για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον



Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η διοργάνωση ημερίδων για την ασφάλεια των πληροφοριακών συστημάτων τους κεντρίζουν το ενδιαφέρον σε ελάχιστο βαθμό κατά μέσο όρο (Mean = 2,33).

Διάγραμμα 55: Σε ποιο βαθμό η αποστολή ενημερωτικών δελτίων για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον



Με βάση τα παραπάνω αποτελέσματα προκύπτει ότι, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η αποστολή ενημερωτικών δελτίων σε αρκετό βαθμό κατά μέσο όρο (Mean = 3,12).

4.2 Συζήτηση

Σύμφωνα με τα παραπάνω αποτελέσματα προκύπτει ότι, στην πρωτογενή ποσοτική έρευνα έλαβαν μέρος κυρίως άνδρες, ηλικίας μεταξύ 26-45 ετών, έγγαμοι, που έχουν εμπειρία στον τομέα των επιχειρήσεων από 6 έως 15 έτη, πως οι περισσότερες αφορούν ΑΕ, απασχολούν από 1-20 άτομα, 21-40 και πάνω από 41 άτομα και αφορούν επιχειρήσεις τροφίμων και ποτών.

Σχετικά με τον βαθμό χρήσης και οφέλους των ΠΣ για τις ελληνικές επιχειρήσεις προέκυψε ότι η πλειοψηφία τους δείγματος εκτιμά πως χρησιμοποιεί σε μεγάλο βαθμό τα ΠΣ, πως αντιπροσωπεύουν ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης στην επιχείρηση σε αρκετό βαθμό. Εκτιμούν επίσης πως τα ΠΣ παρέχουν την υποστήριξη που απαιτείται για τη διοίκηση των διαδικασιών και των αποφάσεων της επιχείρησης τους, ενισχύοντας την αποτελεσματικότητα και την αποδοτικότητά τους, πως μέσω αυτών βελτιώνεται η παραγωγικότητα της επιχείρησης, η λήψη δεδομένων σε πολύ μεγάλο βαθμό, ενώ σε αρκετό βαθμό η ανάλυση δεδομένων, η επικοινωνία, η ανταγωνιστική θέση, η ασφάλεια των πληροφοριών και σε ελάχιστο βαθμό η διαχείριση ρίσκου.

Από την έρευνα προκύπτει ότι η χρήση των ΠΣ βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης της επιχείρησης μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων, αλλά δεν επιτρέπει στην επιχείρηση να είναι πιο ανταγωνιστική στην αγορά. Επιπλέον, εκτιμά πως η χρήση των ΠΣ παρέχει στη διοίκηση την απαραίτητη πληροφόρηση για τη λήψη αποφάσεων που βασίζονται σε δεδομένα και αναλύσεις, επιτρέπει την εύκολη επικοινωνία και συνεργασία εντός και εκτός της επιχείρησης σας, βελτιώνοντας την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών της ομάδας. Ακόμη, η χρήση των ΠΣ βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες, επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών, μειώνοντας τον χρόνο και το κόστος παραγωγής και πως η χρήση των ΠΣ μέσω της αποτελεσματικής διαχείρισης της πληροφορίας, η επιχείρηση τους μπορεί να προσφέρει υψηλότερη ποιότητα προϊόντων και υπηρεσιών στους πελάτες τους.

Προχωρώντας στον βαθμό συμβολής και εφαρμογής των πολιτικών ασφαλείας των ΠΣ για τις ελληνικές επιχειρήσεις προέκυψε ότι η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής και πως η πολιτική ασφάλειας ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της. Επιπλέον, η υλοποίηση τεχνικών μέτρων ασφάλειας αποτελεί κρίσιμο στάδιο στην προστασία των πληροφοριών της επιχείρησης τους. Σε μικρότερο βαθμό, η επικοινωνία και η συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ και η ανάλυση κινδύνων αποτελεί ένα κρίσιμο βήμα στην ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας.

Επιπρόσθετα, η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών και η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών σε αρκετό βαθμό. Παρόλα αυτά, σε ελάχιστο βαθμό ο καθορισμός μιας πολιτικής ασφαλείας αποτελεί βασικό βήμα για τη δημιουργία ενός πλαισίου που θα διασφαλίζει την προστασία των πληροφοριών και η προσαρμογή και η συνεχή βελτίωση της πολιτικής ασφαλείας και των μέτρων αποτελεί κρίσιμη διαδικασία για τη διασφάλιση της αποτελεσματικότητας και της ανταπόκρισης τους σε συνεχώς μεταβαλλόμενες απειλές και ανάγκες. Ωστόσο, η παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας αποτελεί κρίσιμο στάδιο για τη διασφάλιση της συνεχούς προστασίας των πληροφοριών και των ΠΣ σε αρκετό βαθμό.

Το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι αισθάνονται συνυπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησης τους σε ελάχιστο βαθμό, ενώ υποστηρίζει ότι αντιμετωπίζουν την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τη διοίκηση σε πάρα πολύ μεγάλο βαθμό. Εκτιμούν πως είναι ένα ζήτημα που αφορά την πληροφορική, τα άτομα με θέση ευθύνης, όλους τους υπαλλήλους. Επιπρόσθετα, θα χαρακτήριζαν τους παλιούς Η/Υ, τους χάκερς, την εμπλοκή ιδιωτικών εταιρειών πληροφορικής, τη πρόσβαση στο διαδίκτυο, τους αδύναμους κωδικούς πρόσβασης, το ανθρώπινο λάθος, την ελλιπή ενημέρωση / εκπαίδευση του προσωπικού για ζητήματα ασφάλειας ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πάρα πολύ μεγάλο βαθμό.

Επιπλέον, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα συμμετείχαν σε εκπαιδευτικά προγράμματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων κι έχουν την ικανότητα να αναγνωρίσουν και να διαχειριστούν τους κινδύνους ασφάλειας κατά τη χρήση των πληροφοριακών συστημάτων της επιχείρησης. Ακόμη, γνωρίζουν τις διαδικασίες που πρέπει να ακολουθήσουν σε περίπτωση που διαπιστώσουν κάποιο κακόβουλο λογισμικό σε πάρα πολύ μεγάλο βαθμό και πως τα εκπαιδευτικά σεμινάρια για την ασφάλεια των πληροφοριακών συστημάτων τους κεντρίζουν το ενδιαφέρον, αλλά σε ελάχιστο βαθμό η διοργάνωση ημερίδων για την ασφάλεια των πληροφοριακών συστημάτων τους κεντρίζουν το ενδιαφέρον. Τέλος, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η αποστολή ενημερωτικών δελτίων σε αρκετό βαθμό.

4.3 Περιορισμοί έρευνας

Οι ερευνητικοί περιορισμοί αναφέρονται στους περιορισμούς και τις περιοριστικές συνθήκες που μπορούν να επηρεάσουν την εκτέλεση μιας έρευνας ή την ερευνητική διαδικασία γενικότερα. Στην προκειμένη έρευνα βασικός περιορισμός θεωρείται ο δειγματοληπτικός, καθότι το δείγμα δεν ήταν ιδιαίτερα ευρύ. Επιπλέον, η έρευνα διενεργήθηκε σε συγκεκριμένα χρονικά πλαίσια, γεγονός που περιορίζει την ευχέρεια για την πραγματοποίηση μίας έρευνας χωρίς την πίεση χρόνου. Ακόμη, περιορισμός θεωρείται το γεγονός ότι η έρευνα αφορά μόνο ελληνικές επιχειρήσεις και δεν μπορεί να γίνει συσχέτιση με άλλες του εξωτερικού.

4.4 Προτάσεις για μελλοντική έρευνα

Σύμφωνα με τους ανωτέρω ερευνητικούς περιορισμούς προτείνεται να διεξαχθεί μία ερευνά στο μέλλον που να συμμετέχουν περισσότερες επιχειρήσεις και να δοθεί περισσότερο χρονικό περιθώριο για τη συλλογή των δεδομένων. Επιπρόσθετα, θα ήταν ιδιαίτερα ενδιαφέρον να διενεργηθεί στο μέλλον μία έρευνα που να συμπεριλάβει ελληνικές και ξένες επιχειρήσεις και να εξετάσει το βαθμό συμβολής των πολιτικών ασφαλείας στην διασφάλιση των ΠΣ.

Συμπεράσματα

Ένα ΠΣ αποτελείται από διαδικασίες, τεχνολογίες και ανθρώπινους πόρους που συλλέγουν, αποθηκεύουν, επεξεργάζονται και διαχειρίζονται πληροφορίες με σκοπό την υποστήριξη της διοίκησης και της λήψης αποφάσεων σε μία επιχείρηση. Όλες οι λειτουργίες εκτελούνται από το ΠΣ, προκειμένου να διασφαλιστεί ότι οι πληροφορίες που παρέχονται είναι ακριβείς, ενημερωμένες και χρήσιμες για τους χρήστες του συστήματος. Τα διαλειτουργικά και διεπιχειρησιακά ΠΣ επιτρέπουν στις επιχειρήσεις να ανταλλάσσουν πληροφορίες, να συνεργάζονται και να επιτυγχάνουν συναλλαγές με άλλους οργανισμούς με αποτελεσματικό και αποδοτικό τρόπο.

Συνολικά, η χρήση ΠΣ μπορεί να διευκολύνει τη διαδικασία της καινοτομίας και της ανάπτυξης, επιτρέποντας στις επιχειρήσεις να είναι ευέλικτες, αποτελεσματικές και προσαρμοστικές στις αλλαγές της αγοράς. Αυτοί είναι μερικοί από τους κύριους σκοπούς που εξυπηρετούν τα ΠΣ στο πλαίσιο της επιχειρηματικής δραστηριότητας. Ο ανταγωνισμός αποτελεί έναν καθοριστικό παράγοντα για τη βιωσιμότητα μιας επιχείρησης στον χώρο των επιχειρήσεων. Η κατανόηση και η αντιμετώπιση του ανταγωνισμού αποτελούν σημαντικά θέματα μελέτης για πολλούς ερευνητές και επιχειρήσεις, καθώς η αντιμετώπισή του επηρεάζει την απόδοση και την επιτυχία της επιχείρησης στην αγορά.

Η πολιτική ασφάλειας των ΠΣ ορίζει τους στόχους, τις οδηγίες, τις διαδικασίες και τους ρόλους που απαιτούνται για την προστασία των ΠΣ της επιχείρησης. Μέσα από αυτήν προσδιορίζονται οι στόχοι ασφάλειας του ΠΣ, όπως η προστασία από μη εξουσιοδοτημένη πρόσβαση, η διασφάλιση της ακεραιότητας των δεδομένων και η διαθεσιμότητα των υπηρεσιών. Οι διαδικασίες, από την άλλη πλευρά, παρέχουν συγκεκριμένες οδηγίες και βήματα που πρέπει να ακολουθηθούν για την υλοποίηση των οδηγιών και την εφαρμογή των μέτρων ασφαλείας.

Επιπλέον, η εφαρμογή μιας πολιτικής ασφάλειας των ΠΣ δεν αποτελεί μόνο μέσο προστασίας, αλλά και πηγή εμπιστοσύνης. Οι πελάτες, οι επιχειρηματικοί εταίροι και άλλοι εμπλεκόμενοι θέλουν να είναι βέβαιοι ότι τα προσωπικά τους δεδομένα είναι ασφαλή και ότι ο οργανισμός μπορεί να διαχειριστεί με ασφάλεια τις επιχειρηματικές του συναλλαγές. Μια καλά θεμελιωμένη πολιτική ασφάλειας μπορεί να δημιουργήσει ένα

περιβάλλον εμπιστοσύνης που είναι κρίσιμο για την επιτυχία και την ανάπτυξη της επιχείρησης. Μια καλά δομημένη οργανωτική δομή είναι ουσιαστική για την αποτελεσματική εφαρμογή μιας πολιτικής ασφαλείας και την προστασία των πληροφοριών της επιχείρησης

Σύμφωνα με τα αποτελέσματα της πρωτογενής ποσοτικής έρευνας η πλειοψηφία τους δείγματος εκτιμά πως χρησιμοποιεί σε μεγάλο βαθμό τα ΠΣ, πως αντιπροσωπεύουν ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης στην επιχείρηση σε αρκετό βαθμό. Εκτιμούν επίσης η χρήση των ΠΣ βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης της επιχείρησης μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων, αλλά δεν επιτρέπει στην επιχείρηση να είναι πιο ανταγωνιστική στην αγορά. Ακόμη, θεωρούν πως η χρήση των ΠΣ βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες, επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών.

Προχωρώντας στον βαθμό συμβολής και εφαρμογής των πολιτικών ασφαλείας των ΠΣ για τις ελληνικές επιχειρήσεις προέκυψε ότι η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής και πως η πολιτική ασφάλειας ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της. Επιπρόσθετα, η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών και η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών σε αρκετό βαθμό.

Επιπρόσθετα, θα χαρακτήριζαν τους παλιούς Η/Υ, τους χάκερς, την εμπλοκή ιδιωτικών εταιρειών πληροφορικής, τη πρόσβαση στο διαδίκτυο, τους αδύναμους κωδικούς πρόσβασης, το ανθρώπινο λάθος, την ελλιπή ενημέρωση / εκπαίδευση του προσωπικού για ζητήματα ασφάλειας ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζονται στην επιχείρηση σε πάρα πολύ μεγάλο βαθμό. Επιπλέον, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι θα συμμετείχαν σε εκπαιδευτικά προγράμματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων κι έχουν την ικανότητα να αναγνωρίσουν και να διαχειριστούν τους κινδύνους ασφάλειας

κατά τη χρήση των πληροφοριακών συστημάτων της επιχείρησης. Τέλος, το δείγμα των υπεύθυνων των ελληνικών επιχειρήσεων υποστηρίζει ότι η αποστολή ενημερωτικών δελτίων σε αρκετό βαθμό.

Βιβλιογραφία

Μπιλάλης, Κ., Γούναρης, Α. και Πεπελάσης, Σ. (2016). Τεχνικές ανακάλυψης ενδιαφέρουσας πληροφορίας σε βάσεις δεδομένων, Πτυχιακή μελέτη, ΤΕΙ Δυτικής Ελλάδας

Προκόπος, Γ. (2014). Ανάλυση Κινδύνων και Συστήματα Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων σε Μεγάλους Οργανισμούς. Πτυχιακή μελέτη, ΤΕΙ Πελοποννήσου

Σπηλιώτη, Γ. (2022). Η Συμβολή Των Πληροφοριακών Συστημάτων Στην Ανάπτυξη Των Μικρομεσαίων Επιχειρήσεων. Πτυχιακή μελέτη, Πανεπιστήμιο Πειραιά

Σταματινός, Μ. (2015). Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων. Πτυχιακή μελέτη, Πανεπιστήμιο Αιγαίου

Alkhazi, B., Alshaikh, M., Alkhezi, S. and Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. Digital Object Identifier, 10

Al-Mamary, Y.H., Shamsuddin, A. and Aziati, N. (2014). The Role of Different Types of Information Systems In Business Organizations: A Review. International Journal of Research (IJR), 1(7): 1279- 1286

Almazán, D., Tovar, Y.S. and Quintero, J. (2017). Influence of information systems on organizational results. Contaduría y Administración 62: 321–338

Alotaibi, M. (2022). The Role of Information Systems in Enhancing the Implementation of Administrative Decisions. International Journal of Business and Management, 17(1)

Alotaibi, M., Furnell, S. and Clarke, N. (2016). Information Security Policies: A review of Challenges and Influencing Factors.

Alshaikh, M. (2018). Information Security Management Practices in Organisations. School of Computing and Information Systems

Alshaikh, M., Maynard, S., Ahmad, A. and Chang, S. (2015). Information Security Policy: A Management Practice Perspective. Australasian Conference on Information Systems,

Altamony, H., Masa'deh, R., Alshurideh, M. and Obeidat, B.Y. (2012). Information Systems for Competitive Advantage: Implementation of an Organisational Strategic Management Process. Innovation and Sustainable Competitive Advantage: From Regional Development to World Economies, 583-592

Alter, S. (2008). Defining information systems as work systems: implications for the IS field. European Journal of Information Systems, 17: 448–469

Arici, T., Tarık Usta, A., Cigerim, E. & Sahin Gok, M. (2022). Mediating role of information systems on strategy and performance: innovation and competition perspective. Proceedings on Engineering Sciences, 4(2): 179-190

Artur, V. (2020). Security and Information.

Awamleh, F. and Ertugan, A. (2021). The Relationship Between Information Technology Capabilities, Organizational Intelligence, and Competitive Advantage. SAGE Open, 1-14

Awan, A. and Khan, F. (2016). Impact of Management Information System on the Performance of the Organization (Profitability, Innovation, and Growth). Journal of Poverty, Investment and Development, 21: 1-8

Berisha – Shaqiri, A. (2014). Management Information System and Decision-Making. Academic Journal of Interdisciplinary Studies, 3(2): 19-23

Blum, D. (2020). Rational Cybersecurity for Business. The Security Leaders' Guide to Business Alignment

Chulkov, D. (2017). On the Role of Switching Costs and Decision Reversibility in Information Technology Adoption and Investment. Journal of Information Systems and Technology Management, 14(3): 309–321

Chuma, L.L. (2020). The Role of Information Systems in Business Firms Competitiveness: Integrated Review Paper from Business Perspective. International Research Journal of Nature Science and Technology, 2(4): 29-42

Cuillier, G. W. (2022). Advantages and disadvantages of centralized versus decentralized information systems and services from a project management perspective. Electronic Theses, Projects, and Dissertations. 1487

Dusmanescu, D. and Bradic-Martinovic, A. (2011). The Role of Information Systems in Human Resource Management. 1-20

Elnagar, S. and Osei-Bryson, K.-M. (2021). The Competitive Leverage Paradox Effect on Information Systems Life Cycle. Proceedings of the 2021 Pre-ICIS SIGDSA Symposium. 2

Elvin, G. and Johansson, E. (2017). The impact of organizational culture on information security during development and management of IT systems A comparative study between Japanese and Swedish banking industry. Uppsala University

Gashi Shatri, Z. (2020). Advantages and Disadvantages of Using Information Technology in Learning Process of Students. Journal of Turkish Science Education, 17(3): 420-428

Hayati, U., Mulyani, S., Sukarsa, D.E., Winarningsih, S. (2021). Information System's Implementation and its Impact on University Organization Performance in West Java. Utopía y Praxis Latinoamericana, 26(1): 343-358

Ifinedo, P. (2012). Effects of organization insiders' self-control and relevant knowledge on participation in information systems security deviant behaviour.

Jerome, J., Sonwaney, V., Bryde, D. and Graham, G. (2023). Achieving competitive advantage through technology-driven proactive supply chain risk management: an empirical study. Annals of Operations Research

Kamariza, Y. (2017). Implementation of information security policies in public organizations: Top management as a success factor. IT Management and Innovation

Kamariotou, M. and Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics, 12(382)

Karim, A.J. (2011). The significance of management information systems for enhancing strategic and tactical planning. Journal of Information Systems and Technology Management, 8(2): 459- 470

Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability, 14, 1269

Khando, K., Gao, S., Islam, S. and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computer & Security 106, 102267

Kozhusko, O., Khaminich, S. and Alieksieieva, S. (2019). Information system protection as a factor in maintaining the leading positions in the enterprise development. Advances in Social Science, Education and Humanities Research, 318: 428-432

Limaye, R. (2013). The importance of Information Integrity, Security, Networking and Data Protection. International Journal of Innovations in Engineering and Technology, 2(3): 274-281

Lopes, I. and Oliveira, P. (2015). Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. Springer International Publishing Switzerland, 459-468

Manuscript, D. (2020). Impact of Training on Employee Actions and Information Security Awareness in Academic Institutions. Submitted to Northcentral University School of Business

Maynard, S.B. and Ruighave, A.B. (2010). Evaluating IS Security Policy Development.

Ming, T., Teng, W. and Jodaki, S. (2021). A model to investigate the effect of information technology and information systems on the ease of managers' decision-making. Kybernetes, 50(1): 100-117

Monteiro, M.H. and Pinto, R.R. (2019). The E-government adoption in higher education in Portugal the case of ISCSP at Lisbon Univeristy. Journal of Information Systems and Technology Management – Jistem USP, 16

Moussa, N. and El Arbi, R. (2020). The impact of Human Resources Information Systems on individual innovation capability in Tunisian companies: The moderating role of affective commitment. European Research on Management and Business Economics, 26(1): 18-25

Nieles, M., Dempsey, K. and Yan Pillitteri, V. (2017). An Introduction to Information Security. NIST Special Publication 800-12 Revision 1

Njenga, K. (2016). Information Systems Security Policy Violation: Systematic Literature Review on Behavior Threats by Internal Agents. CONF-IRM 2016 Proceedings, 39

Nord, J.H., Koohang, A., Floyd, K. and Paliszkiewicz, J. (2020). Impact of habits on Information Security policy compliance. Issues in Information Systems, 21(3): 217-226

Pakusadewa, P., Suryani, E., Ambarwati, R. and Bintang, M.R. (2020). Selection of Information System Strategy Recommendations in Information Technology Company. Advances in Economics, Business and Management Research, 175

Safa, S., Maple, G., Watson, T. and Furnell, S. (2017). Information security collaboration formation in organisations. IET Information Security Institution of Engineering and Technology

Santos, P. and Estender, A. (2014). The importance of the information system in the company's administrative process. Análise e Desenvolvimento de Sistemas, 4(4)

Singh K. and Kaur, B. (2012). Role of Management Information System in Business: Opportunities and Challenges. GIAN JYOTI E-JOURNAL, 1(2)

Sudirman, I., Govindaraju, R. and Pratiwi, A. (2014). Information System Quality and Its Impact on Individual Users' Benefit: Analyzing the Role of Knowledge Enablers. Jurnal Teknik Industri, 16(2): 65-74

Taherdoost, H. (2022). The Role of Different Types of Management Information System Applications in Business Development: Concepts, and Limitations. Cloud Computing and Data Science, 4(1)

Vargas, L., Leyton, E., Garcia, M. and Gonzalez, S. (2019). Information systems and their functionality in the optimization of business processes. Revista, 40(42)

Willie, M.M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. Journal of Research, Innovation and Technologies, 179-198

Zhang, Y. (2017). Management Information System. Advances in Engineering Research, 138: 280-283

Zemmouchi-Ghomari, L. (2021). Basic Concepts of information systems. Intechopen

Παράρτημα Κώδικα

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Μελέτη ασφάλειας πληροφοριακών συστημάτων σε φορείς ή επιχειρήσεις

Η ασφάλεια των Πληροφοριακών Συστημάτων (ΠΣ) είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής. Αποσκοπεί στην προστασία των υπολογιστικών συστημάτων, των δεδομένων και των δικτύων τους από απειλές και επιθέσεις που μπορούν να προκαλέσουν ζημία, δυσφήμιση, ή ακόμα και κλοπή ή καταστροφή δεδομένων. Παρακάτω καλείστε να προσδιορίσετε τον βαθμό στον οποίο είναι ασφαλή τα πληροφοριακά συστήματα που χρησιμοποιείτε στα πλαίσια των δραστηριοτήτων σας. Κάθε απάντηση σας θα χρησιμοποιηθεί για λόγους στατιστικής αξιολόγησης. Βάσει των προδιαγραφών δεοντολογίας τα προσωπικά σας στοιχεία θα είναι ανώνυμα.

Η ερευνήτρια

Παρασκευή Γέρου

<u>Μέρος Α: Δημογραφικά στοιχεία</u>

Α1. Δημογραφικά στοιχεία υπεύθυνου επιχείρησης

1. **Φύλο**
   Άντρας ☐ Γυναίκα ☐
2. **Ηλικία**
   18-25 ☐ 26-30 ☐ 31 – 35☐ 36 -45 ☐ 46 -55 ☐ 56 και άνω ☐
3. **Οικογενειακή κατάσταση:**

Άγαμος/η ☐ Έγγαμος/η ☐
Διαζευγμένος/η ☐ Χήρος/α ☐

4. **Εμπειρία στον τομέα των επιχειρήσεων**
   1-5 έτη ☐ 6-10 έτη ☐ 11 – 15 έτη ☐ 16 -20 έτη ☐ 20 έτη και άνω ☐

Α2. Δημογραφικά στοιχεία επιχείρησης

1. **Νομική μορφή**
   ΑΕ ☐ ΕΠΕ ☐ ΟΕ ☐ ΕΕ ☐ Άλλο ☐
2. **Σύνολο εργαζομένων**
   1-20 άτομα ☐ 21-40 άτομα ☐ 41 < άτομα ☐
3. **Σε ποιόν τομέα ανήκει η επιχείρησή σας**
   Υλικά οικοδομών ☐ Τροφίμων και ποτών ☐ Ενδυμάτων ☐

Μέρος Β: Ερωτήσεις για τα ΠΣ

Προσδιορίστε τον βαθμό με βάση τις επιλογές 1= Καθόλου, 2=Ελάχιστα, 3=Αρκετά, 4=Πολύ, 5=Πάρα πολύ

Ερωτήσεις	1	2	3	4	5
1. Σε ποιο βαθμό χρησιμοποιείτε τα ΠΣ;					
2. Σε ποιο βαθμό τα ΠΣ αντιπροσωπεύουν ένα εργαλείο που ενισχύει τις διαδικασίες λήψης αποφάσεων και διοίκησης στην επιχείρηση σας;					
3. Σε ποιο βαθμό τα ΠΣ παρέχουν την υποστήριξη που απαιτείται για τη διοίκηση των διαδικασιών και των αποφάσεων της επιχείρησης σας, ενισχύοντας την αποτελεσματικότητα και την αποδοτικότητά της;					
4. Σε ποιο βαθμό βελτιώνεται η παραγωγικότητα σας μέσω των ΠΣ;					
5. Σε ποιο βαθμό βελτιώνεται η ανάλυση δεδομένων σας μέσω των ΠΣ;					
6. Σε ποιο βαθμό βελτιώνεται η λήψη των δεδομένων σας μέσω των ΠΣ;					
7. Σε ποιο βαθμό βελτιώνεται η επικοινωνία σας μέσω των ΠΣ;					
8. Σε ποιο βαθμό βελτιώνεται η ανταγωνιστική θέση σας μέσω των ΠΣ;					
9. Σε ποιο βαθμό βελτιώνεται η διαχείριση ρίσκου μέσω των ΠΣ;					
10. Σε ποιο βαθμό βελτιώνεται η ασφάλεια των πληροφοριών μέσω των ΠΣ;					
11. Σε ποιο βαθμό επιτυγχάνεται η εξοικονόμηση χρημάτων μέσω των ΠΣ;					
12. Σε ποιο βαθμό η χρήση των ΠΣ βοηθά στην αύξηση της αποτελεσματικότητας και της απόδοσης της επιχείρησης σας μέσω της βελτιστοποίησης των διαδικασιών και της καλύτερης διαχείρισης των πόρων;					
13. Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει στην επιχείρηση σας να είναι πιο ανταγωνιστική στην αγορά, προσφέροντας καλύτερες υπηρεσίες και προϊόντα σε πιο αποτελεσματικό κόστος;					
14. Σε ποιο βαθμό η χρήση των ΠΣ παρέχει στη διοίκηση την απαραίτητη πληροφόρηση για τη λήψη αποφάσεων που βασίζονται σε δεδομένα και αναλύσεις;					
15. Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει την εύκολη επικοινωνία και συνεργασία εντός και εκτός της επιχείρησης σας, βελτιώνοντας την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των μελών της ομάδας;					
16. Σε ποιο βαθμό η χρήση των ΠΣ βοηθά στην αποτελεσματική διαχείριση των δεδομένων, προστατεύοντας την ακεραιότητά τους και εξασφαλίζοντας την πρόσβαση σε αξιόπιστες πληροφορίες;					
17. Σε ποιο βαθμό η χρήση των ΠΣ επιτρέπει την εκσυγχρονισμό και την αυτοματοποίηση διαδικασιών, μειώνοντας τον χρόνο και το κόστος παραγωγής;					
18. Σε ποιο βαθμό η χρήση των ΠΣ μέσω της αποτελεσματικής διαχείρισης της πληροφορίας, η επιχείρηση μου μπορεί να προσφέρει υψηλότερη ποιότητα προϊόντων και υπηρεσιών στους πελάτες της;					

Μέρος Γ: Ερωτήσεις για τις Πολιτικές Ασφάλειας των ΠΣ

Προσδιορίστε τον βαθμό με βάση τις επιλογές 1= Καθόλου, 2=Ελάχιστα, 3=Αρκετά, 4=Πολύ, 5=Πάρα πολύ

Ερωτήσεις	1	2	3	4	5
1. Σε ποιο βαθμό η ασφάλεια των ΠΣ είναι ένα σημαντικό γνωστικό πεδίο στον τομέα της πληροφορικής;					
2. Σε ποιο βαθμό η πολιτική ασφάλειας ευθυγραμμίζεται με τους στόχους και τις ανάγκες της επιχείρησης σας, προκειμένου να εξασφαλίζει τη συνολική ασφάλεια και την προστασία των πληροφοριών και των πόρων της;					
3. Σε ποιο βαθμό η επικοινωνία και η συνεργασία μεταξύ όλων των εμπλεκόμενων φορέων είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ;					
4. Σε ποιο βαθμό η ανάλυση κινδύνων αποτελεί ένα κρίσιμο βήμα στην ανάπτυξη μιας αποτελεσματικής πολιτικής ασφαλείας;					
5. Σε ποιο βαθμό ο καθορισμός μιας πολιτικής ασφαλείας αποτελεί βασικό βήμα για τη δημιουργία ενός πλαισίου που θα διασφαλίζει την προστασία των πληροφοριών;					
6. Σε ποιο βαθμό η εκπαίδευση του προσωπικού αποτελεί έναν κρίσιμο παράγοντα για την αποτελεσματική υλοποίηση μιας πολιτικής ασφαλείας πληροφοριών;					
7. Σε ποιο βαθμό η υλοποίηση τεχνικών μέτρων ασφάλειας αποτελεί κρίσιμο στάδιο στην προστασία των πληροφοριών της επιχείρησης σας;					
8. Σε ποιο βαθμό η δημιουργία διαδικασιών και πολιτικών αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της αποτελεσματικής λειτουργίας του συστήματος ασφαλείας πληροφοριών;					
9. Σε ποιο βαθμό η παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας αποτελεί κρίσιμο στάδιο για τη διασφάλιση της συνεχούς προστασίας των πληροφοριών και των ΠΣ;					
10. Σε ποιο βαθμό η προσαρμογή και η συνεχή βελτίωση της πολιτικής ασφαλείας και των μέτρων αποτελεί κρίσιμη διαδικασία για τη διασφάλιση της αποτελεσματικότητας και της ανταπόκρισης τους σε συνεχώς μεταβαλλόμενες απειλές και ανάγκες;					
11. Σε ποιο βαθμό σας απασχολεί η ασφάλεια των πληροφοριακών συστημάτων που διαχειρίζεστε;					
12. Σε ποιο βαθμό αισθάνεστε συνυπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησης σας;					
13. Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τη διοίκηση;					
14. Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά τον υπεύθυνο προστασίας δεδομένων;					
15. Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά πληροφορική;					
16. Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά άτομα με θέση ευθύνης;					
17. Σε ποιο βαθμό αντιμετωπίζετε την ασφάλεια των πληροφοριακών συστημάτων ως ένα ζήτημα που αφορά όλους τους υπαλλήλους;					
18. Σε ποιο βαθμό θα χαρακτηρίζατε τους παλιούς Η/Υ ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;					
19. Σε ποιο βαθμό θα χαρακτηρίζατε τους χάκερς ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;					

20. Σε ποιο βαθμό θα χαρακτηρίζατε την εμπλοκή ιδιωτικών εταιρειών πληροφορικής ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;
21. Σε ποιο βαθμό θα χαρακτηρίζατε τη πρόσβαση στο διαδίκτυο ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;
22. Σε ποιο βαθμό θα χαρακτηρίζατε τους αδύναμους κωδικούς πρόσβασης ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;
23. Σε ποιο βαθμό θα χαρακτηρίζατε το ανθρώπινο λάθος ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;
24. Σε ποιο βαθμό θα χαρακτηρίζατε την ελλιπή ενημέρωση / εκπαίδευση του προσωπικού για ζητήματα ασφάλειας ως απειλή ασφαλείας για τις πληροφορίες που διαχειρίζεστε στην επιχείρηση σας;
25. Σε ποιο βαθμό θα συμμετείχατε σε εκπαιδευτικά προγράμματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων;
26. Σε ποιο βαθμό έχετε την ικανότητα να αναγνωρίσετε και να διαχειριστείτε κινδύνους ασφάλειας κατά τη χρήση των πληροφοριακών συστημάτων της επιχείρησης σας;
27. Σε ποιο βαθμό γνωρίζετε τις διαδικασίες που πρέπει να ακολουθήσετε σε περίπτωση που διαπιστώσετε κάποιο κακόβουλο λογισμικό;
28. Σε ποιο βαθμό τα εκπαιδευτικά σεμινάρια για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον;
29. Σε ποιο βαθμό η διοργάνωση ημερίδων για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον;
30. Σε ποιο βαθμό η αποστολή ενημερωτικών δελτίων για την ασφάλεια των πληροφοριακών συστημάτων σας κεντρίζουν το ενδιαφέρον;

Σας ευχαριστώ πολύ!